



Utiliser StorageGRID

StorageGRID software

NetApp
December 03, 2025

Sommaire

Utiliser les locataires et les clients StorageGRID	1
Utiliser un compte locataire	1
Utiliser un compte locataire	1
Comment se connecter et se déconnecter	2
Comprendre le tableau de bord du Tenant Manager	7
API de gestion des locataires	10
Utiliser les connexions de la fédération de grille	15
Gérer les groupes et les utilisateurs	29
Gérer les clés d'accès S3	49
Gérer les buckets S3	54
Gérer les services de la plateforme S3	78
Utiliser l'API REST S3	111
Versions et mises à jour prises en charge par l'API REST S3	111
Référence rapide : requêtes API S3 prises en charge	114
Tester la configuration de l'API REST S3	133
Comment StorageGRID implémente l'API REST S3	134
Prise en charge de l'API REST Amazon S3	149
Opérations personnalisées StorageGRID	199
Politiques d'accès aux buckets et aux groupes	221
Opérations S3 suivies dans les journaux d'audit	249
Utiliser l'API REST Swift (fin de vie)	250
Utiliser l'API REST Swift	250

Utiliser les locataires et les clients StorageGRID

Utiliser un compte locataire

Utiliser un compte locataire

Un compte locataire vous permet d'utiliser l'API REST Simple Storage Service (S3) ou l'API REST Swift pour stocker et récupérer des objets dans un système StorageGRID .

Qu'est-ce qu'un compte locataire ?

Chaque compte locataire possède ses propres groupes fédérés ou locaux, utilisateurs, buckets S3 ou conteneurs Swift et objets.

Les comptes locataires peuvent être utilisés pour séparer les objets stockés par différentes entités. Par exemple, plusieurs comptes locataires peuvent être utilisés pour l'un ou l'autre de ces cas d'utilisation :

- **Cas d'utilisation d'entreprise** : si le système StorageGRID est utilisé au sein d'une entreprise, le stockage d'objets de la grille peut être séparé par les différents services de l'organisation. Par exemple, il peut y avoir des comptes locataires pour le service marketing, le service d'assistance clientèle, le service des ressources humaines, etc.



Si vous utilisez le protocole client S3, vous pouvez également utiliser des buckets S3 et des stratégies de bucket pour séparer les objets entre les services d'une entreprise. Vous n'avez pas besoin de créer des comptes locataires distincts. Voir les instructions de mise en œuvre "[Buckets S3 et politiques de buckets](#)" pour plus d'informations.

- **Cas d'utilisation du fournisseur de services** : si le système StorageGRID est utilisé par un fournisseur de services, le stockage d'objets de la grille peut être séparé par les différentes entités qui louent le stockage. Par exemple, il peut y avoir des comptes locataires pour la société A, la société B, la société C, etc.

Comment créer un compte locataire

Les comptes locataires sont créés par un "[Administrateur de grille StorageGRID utilisant Grid Manager](#)". Lors de la création d'un compte locataire, l'administrateur du réseau spécifie les éléments suivants :

- Informations de base, notamment le nom du locataire, le type de client (S3) et le quota de stockage facultatif.
- Autorisations pour le compte locataire, par exemple si le compte locataire peut utiliser les services de la plateforme S3, configurer sa propre source d'identité, utiliser S3 Select ou utiliser une connexion de fédération de grille.
- L'accès root initial pour le locataire, selon que le système StorageGRID utilise des groupes et des utilisateurs locaux, une fédération d'identité ou une authentification unique (SSO).

De plus, les administrateurs de grille peuvent activer le paramètre de verrouillage d'objet S3 pour le système StorageGRID si les comptes de locataire S3 doivent se conformer aux exigences réglementaires. Lorsque le verrouillage d'objet S3 est activé, tous les comptes de locataire S3 peuvent créer et gérer des compartiments conformes.

Configurer les locataires S3

Après un ["Le compte locataire S3 est créé"](#) , vous pouvez accéder au gestionnaire de locataires pour effectuer des tâches telles que les suivantes :

- Configurer la fédération d'identité (sauf si la source d'identité est partagée avec la grille)
- Gérer les groupes et les utilisateurs
- Utiliser la fédération de grille pour le clonage de compte et la réplication inter-grille
- Gérer les clés d'accès S3
- Créer et gérer des buckets S3
- Utiliser les services de la plateforme S3
- Utiliser S3 Select
- Surveiller l'utilisation du stockage



Bien que vous puissiez créer et gérer des buckets S3 avec Tenant Manager, vous devez utiliser un ["Client S3"](#) ou ["Console S3"](#) pour ingérer et gérer des objets.

Comment se connecter et se déconnecter

Sign in à Tenant Manager

Vous accédez au Tenant Manager en saisissant l'URL du locataire dans la barre d'adresse d'un ["navigateur Web pris en charge"](#) .

Avant de commencer

- Vous avez vos identifiants de connexion.
- Vous disposez d'une URL pour accéder au gestionnaire de locataires, fournie par votre administrateur de réseau. L'URL ressemblera à l'un de ces exemples :

```
https://FQDN_or_Admin_Node_IP/
```

```
https://FQDN_or_Admin_Node_IP:port/
```

```
https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id
```

```
https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
```

L'URL inclut toujours un nom de domaine complet (FQDN), l'adresse IP d'un nœud d'administration ou l'adresse IP virtuelle d'un groupe HA de nœuds d'administration. Il peut également inclure un numéro de port, l'ID de compte locataire à 20 chiffres ou les deux.

- Si l'URL n'inclut pas l'ID de compte à 20 chiffres du locataire, vous disposez de cet ID de compte.
- Vous utilisez un ["navigateur Web pris en charge"](#) .
- Les cookies sont activés dans votre navigateur Web.
- Vous appartenez à un groupe d'utilisateurs qui a ["autorisations d'accès spécifiques"](#) .

Étapes

1. Lancer un ["navigateur Web pris en charge"](#) .

2. Dans la barre d'adresse du navigateur, saisissez l'URL permettant d'accéder à Tenant Manager.
3. Si une alerte de sécurité s'affiche, installez le certificat à l'aide de l'assistant d'installation du navigateur.
4. Sign in au gestionnaire de locataires.

L'écran de connexion qui s'affiche dépend de l'URL que vous avez saisie et de la configuration de l'authentification unique (SSO) pour StorageGRID.

Ne pas utiliser SSO

Si StorageGRID n'utilise pas SSO, l'un des écrans suivants s'affiche :

- La page de connexion de Grid Manager. Sélectionnez le lien **Connexion du locataire**.



NetApp StorageGRID®

Grid Manager

Username

Password

[Sign in](#)

[Tenant sign in](#) | [NetApp support](#) | [NetApp.com](#)

- La page de connexion du gestionnaire de locataires. Le champ **Compte** est peut-être déjà rempli, comme indiqué ci-dessous.

The screenshot shows the NetApp StorageGRID Tenant Manager login page. At the top is the NetApp StorageGRID logo. Below it is the title 'Tenant Manager'. There are four input fields: 'Recent' (a dropdown menu showing '-- Optional --'), 'Account' (containing the ID '64600207336181242061'), 'Username' (empty), and 'Password' (empty). A blue 'Sign in' button is located below the password field. At the bottom, there is a link for 'NetApp support | NetApp.com'.

- i. Si l'ID de compte à 20 chiffres du locataire n'est pas affiché, sélectionnez le nom du compte du locataire s'il apparaît dans la liste des comptes récents ou saisissez l'ID de compte.
- ii. Entrez votre nom d'utilisateur et votre mot de passe.
- iii. Sélectionnez * Sign in*.

Le tableau de bord du gestionnaire de locataires apparaît.

- iv. Si vous avez reçu un mot de passe initial de quelqu'un d'autre, sélectionnez **username > Modifier le mot de passe** pour sécuriser votre compte.

Utilisation de SSO

Si StorageGRID utilise SSO, l'un des écrans suivants s'affiche :

- La page SSO de votre organisation. Par exemple:

Sign in with your organizational account

Sign in

Saisissez vos identifiants SSO standard et sélectionnez * Sign in*.

- La page de connexion SSO du gestionnaire de locataires.

NetApp StorageGRID®

Tenant Manager

Recent

S3 tenant ▼

Account

62984032838045582045

Sign in

[NetApp support](#) | [NetApp.com](#)

- Si l'ID de compte à 20 chiffres du locataire n'est pas affiché, sélectionnez le nom du compte du locataire s'il apparaît dans la liste des comptes récents ou saisissez l'ID de compte.
- Sélectionnez * Sign in*.
- Sign in avec vos informations d'identification SSO standard sur la page de connexion SSO de votre organisation.

Le tableau de bord du gestionnaire de locataires apparaît.

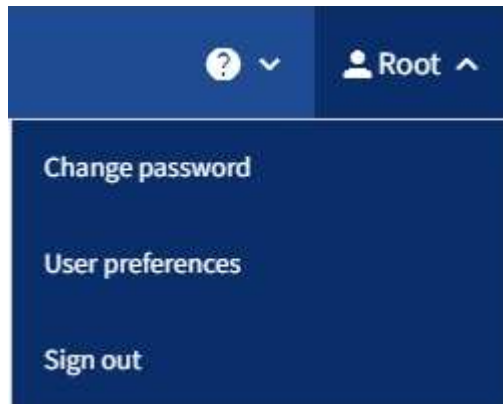
Déconnexion de Tenant Manager

Une fois que vous avez terminé de travailler avec le gestionnaire de locataires, vous

devez vous déconnecter pour garantir que les utilisateurs non autorisés ne peuvent pas accéder au système StorageGRID . La fermeture de votre navigateur peut ne pas vous déconnecter du système, en fonction des paramètres de cookies du navigateur.

Étapes

1. Localisez la liste déroulante du nom d'utilisateur dans le coin supérieur droit de l'interface utilisateur.



2. Sélectionnez le nom d'utilisateur, puis sélectionnez **Déconnexion**.

- Si SSO n'est pas utilisé :

Vous êtes déconnecté du nœud d'administration. La page de connexion du gestionnaire de locataires s'affiche.



Si vous vous êtes connecté à plusieurs nœuds d'administration, vous devez vous déconnecter de chaque nœud.

- Si SSO est activé :

Vous êtes déconnecté de tous les nœuds d'administration auxquels vous accédez. La page de Sign in StorageGRID s'affiche. Le nom du compte locataire auquel vous venez d'accéder est répertorié par défaut dans la liste déroulante **Comptes récents** et l'**ID de compte** du locataire est affiché.



Si SSO est activé et que vous êtes également connecté au Gestionnaire de grille, vous devez également vous déconnecter du Gestionnaire de grille pour vous déconnecter de SSO.

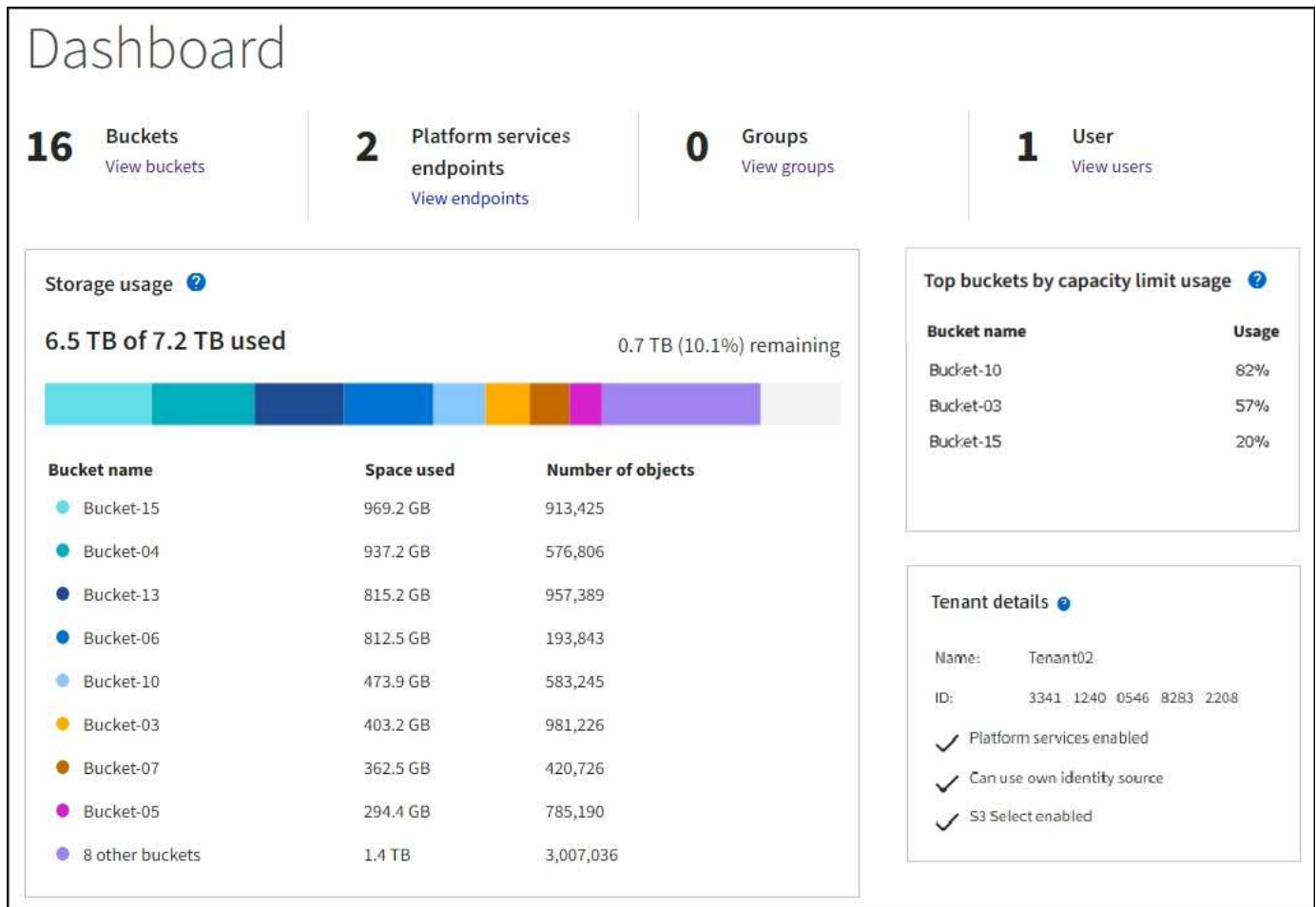
Comprendre le tableau de bord du Tenant Manager

Le tableau de bord du gestionnaire de locataires fournit un aperçu de la configuration d'un compte de locataire et de la quantité d'espace utilisée par les objets dans les compartiments (S3) ou les conteneurs (Swift) du locataire. Si le locataire dispose d'un quota, le tableau de bord indique la part du quota utilisée et la part restante. S'il y a des erreurs liées au compte locataire, les erreurs sont affichées sur le tableau de bord.



Les valeurs de l'espace utilisé sont des estimations. Ces estimations sont affectées par le moment des ingestions, la connectivité réseau et l'état du nœud.

Une fois les objets téléchargés, le tableau de bord ressemble à l'exemple suivant :



Informations sur le compte du locataire

La partie supérieure du tableau de bord affiche le nombre de buckets ou de conteneurs, de groupes et d'utilisateurs configurés. Il affiche également le nombre de points de terminaison des services de la plateforme, si des points ont été configurés. Sélectionnez les liens pour afficher les détails.

En fonction de la "[autorisations de gestion des locataires](#)" vous disposez des options que vous avez configurées, le reste du tableau de bord affiche diverses combinaisons de directives, d'utilisation du stockage, d'informations sur les objets et de détails sur les locataires.

Utilisation du stockage et des quotas

Le panneau Utilisation du stockage contient les informations suivantes :

- La quantité de données d'objet pour le locataire.

Cette valeur indique la quantité totale de données d'objet téléchargées et ne représente pas l'espace utilisé pour stocker des copies de ces objets et leurs métadonnées.

- Si un quota est défini, la quantité totale d'espace disponible pour les données de l'objet ainsi que la quantité et le pourcentage d'espace restant. Le quota limite la quantité de données d'objet pouvant être ingérées.












L'utilisation des quotas est basée sur des estimations internes et peut être dépassée dans certains cas. Par exemple, StorageGRID vérifie le quota lorsqu'un locataire commence à télécharger des objets et rejette les nouvelles acquisitions si le locataire a dépassé le quota. Cependant, StorageGRID ne prend pas en compte la taille du téléchargement actuel pour déterminer si le quota a été dépassé. Si des objets sont supprimés, un locataire peut être temporairement empêché de télécharger de nouveaux objets jusqu'à ce que l'utilisation du quota soit recalculée. Les calculs d'utilisation des quotas peuvent prendre 10 minutes ou plus.

- Un graphique à barres qui représente les tailles relatives des plus grands seaux ou conteneurs.

Vous pouvez placer votre curseur sur l'un des segments du graphique pour afficher l'espace total consommé par ce bucket ou ce conteneur.



- Pour correspondre au graphique à barres, une liste des plus grands compartiments ou conteneurs, y compris la quantité totale de données d'objet et le nombre d'objets pour chaque compartiment ou conteneur.

Bucket name	Space used	Number of objects
 Bucket-02	944.7 GB	7,575
 Bucket-09	899.6 GB	589,677
 Bucket-15	889.6 GB	623,542
 Bucket-06	846.4 GB	648,619
 Bucket-07	730.8 GB	808,655
 Bucket-04	700.8 GB	420,493
 Bucket-11	663.5 GB	993,729
 Bucket-03	656.9 GB	379,329
 9 other buckets	2.3 TB	5,171,588

Si le locataire possède plus de neuf seaux ou conteneurs, tous les autres seaux ou conteneurs sont regroupés en une seule entrée au bas de la liste.



Pour modifier les unités des valeurs de stockage affichées dans le gestionnaire de locataires, sélectionnez la liste déroulante utilisateur dans le coin supérieur droit du gestionnaire de locataires, puis sélectionnez **Préférences utilisateur**.

Alertes d'utilisation des quotas

Si les alertes d'utilisation de quota ont été activées dans le gestionnaire de grille, ces alertes apparaîtront dans le gestionnaire de locataires lorsque le quota est faible ou dépassé, comme suit :

- Si 90 % ou plus du quota d'un locataire a été utilisé, l'alerte **Utilisation élevée du quota du locataire** est déclenchée.

Pensez à demander à votre administrateur de réseau d'augmenter le quota.

- Si vous dépassez votre quota, une notification vous indique que vous ne pouvez pas télécharger de nouveaux objets.


Utilisation de la limite de capacité

Si vous avez défini une limite de capacité pour vos compartiments, le tableau de bord du gestionnaire de locataires affiche une liste des compartiments principaux par utilisation de la limite de capacité.

Si aucune limite n'est définie pour un bucket, sa capacité est illimitée. Cependant, si votre compte locataire dispose d'un quota de stockage total et que ce quota est atteint, vous ne pourrez pas ingérer davantage d'objets, quelle que soit la limite de capacité restante sur un bucket.

Erreurs de point de terminaison

Si vous avez utilisé Grid Manager pour configurer un ou plusieurs points de terminaison à utiliser avec les services de plateforme, le tableau de bord Tenant Manager affiche une alerte si des erreurs de point de terminaison se sont produites au cours des sept derniers jours.

 One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

Pour voir les détails sur "[erreurs de point de terminaison des services de plateforme](#)", sélectionnez **Points de terminaison** pour afficher la page Points de terminaison.

API de gestion des locataires

Comprendre l'API de gestion des locataires

Vous pouvez effectuer des tâches de gestion du système à l'aide de l'API REST de gestion des locataires au lieu de l'interface utilisateur du gestionnaire des locataires. Par exemple, vous souhaitez peut-être utiliser l'API pour automatiser des opérations ou créer plusieurs entités, telles que des utilisateurs, plus rapidement.

L'API de gestion des locataires :

- Utilise la plateforme API open source Swagger. Swagger fournit une interface utilisateur intuitive qui permet aux développeurs et aux non-développeurs d'interagir avec l'API. L'interface utilisateur de Swagger fournit des détails complets et une documentation pour chaque opération API.
- Utilisations "[gestion des versions pour prendre en charge les mises à niveau non perturbatrices](#)".

Pour accéder à la documentation Swagger pour l'API de gestion des locataires :

1. Sign in au gestionnaire de locataires.
2. En haut du gestionnaire de locataires, sélectionnez l'icône d'aide et sélectionnez **Documentation API**.

Opérations API

L'API de gestion des locataires organise les opérations API disponibles dans les sections suivantes :

- **compte** : opérations sur le compte locataire actuel, y compris l'obtention d'informations sur l'utilisation du stockage.
- **auth** : opérations permettant d'effectuer l'authentification de la session utilisateur.

L'API de gestion des locataires prend en charge le schéma d'authentification du jeton porteur. Pour une connexion locataire, vous fournissez un nom d'utilisateur, un mot de passe et un accountId dans le corps JSON de la demande d'authentification (c'est-à-dire, `POST /api/v3/authorize`). Si l'utilisateur est authentifié avec succès, un jeton de sécurité est renvoyé. Ce jeton doit être fourni dans l'en-tête des requêtes API ultérieures (« Autorisation : jeton porteur »).

Pour plus d'informations sur l'amélioration de la sécurité de l'authentification, consultez ["Protection contre la falsification de requêtes intersites"](#).



Si l'authentification unique (SSO) est activée pour le système StorageGRID, vous devez effectuer différentes étapes pour vous authentifier. Voir le ["instructions d'utilisation de l'API de gestion de grille"](#).

- **config** : opérations liées à la version du produit et aux versions de l'API de gestion des locataires. Vous pouvez répertorier la version du produit et les principales versions de l'API prises en charge par cette version.
- **conteneurs** : opérations sur les buckets S3 ou les conteneurs Swift.
- **fonctionnalités désactivées** : opérations permettant d'afficher les fonctionnalités qui pourraient avoir été désactivées.
- **points de terminaison** : opérations permettant de gérer un point de terminaison. Les points de terminaison permettent à un bucket S3 d'utiliser un service externe pour la réplication StorageGRID CloudMirror, les notifications ou l'intégration de la recherche.
- **grid-federation-connections** : opérations sur les connexions de fédération de grille et la réplication inter-grille.
- **groupes** : opérations de gestion des groupes de locataires locaux et de récupération des groupes de locataires fédérés à partir d'une source d'identité externe.
- **identity-source** : opérations permettant de configurer une source d'identité externe et de synchroniser manuellement les informations des groupes fédérés et des utilisateurs.
- **ilm** : opérations sur les paramètres de gestion du cycle de vie de l'information (ILM).
- **régions** : opérations permettant de déterminer quelles régions ont été configurées pour le système StorageGRID.
- **s3** : opérations de gestion des clés d'accès S3 pour les utilisateurs locataires.
- **s3-object-lock** : opérations sur les paramètres globaux de verrouillage d'objet S3, utilisées pour prendre en charge la conformité réglementaire.
- **utilisateurs** : opérations permettant d'afficher et de gérer les utilisateurs locataires.

Détails de l'opération

Lorsque vous développez chaque opération API, vous pouvez voir son action HTTP, l'URL du point de terminaison, une liste de tous les paramètres obligatoires ou facultatifs, un exemple du corps de la requête (si nécessaire) et les réponses possibles.

groups Operations on groups

GET /org/groups Lists Tenant User Groups

Parameters Try it out

Name	Description
type string (query)	filter by group type
limit integer (query)	maximum number of results
marker string (query)	marker-style pagination offset (value is Group's URN)
includeMarker boolean (query)	if set, the marker element is also returned
order string (query)	pagination order (desc requires marker)

Responses Response content type **application/json** ▼

Code	Description
200	<div><div>Example Value</div><div>Model</div><pre>{ "responseTime": "2018-02-01T16:22:31.066Z", "status": "success", "apiVersion": "2.2" }</pre></div>

Émettre des requêtes API



Toutes les opérations API que vous effectuez à l'aide de la page Web de documentation API sont des opérations en direct. Veillez à ne pas créer, mettre à jour ou supprimer des données de configuration ou d'autres données par erreur.

Étapes

1. Sélectionnez l'action HTTP pour voir les détails de la demande.

2. Déterminez si la demande nécessite des paramètres supplémentaires, tels qu'un ID de groupe ou d'utilisateur. Ensuite, obtenez ces valeurs. Vous devrez peut-être d'abord émettre une demande d'API différente pour obtenir les informations dont vous avez besoin.
3. Déterminez si vous devez modifier le corps de la demande d'exemple. Si tel est le cas, vous pouvez sélectionner **Modèle** pour connaître les exigences de chaque champ.
4. Sélectionnez **Essayer**.
5. Fournissez tous les paramètres requis ou modifiez le corps de la demande selon vos besoins.
6. Sélectionnez **Exécuter**.
7. Consultez le code de réponse pour déterminer si la demande a réussi.

Gestion des versions de l'API de gestion des locataires

L'API de gestion des locataires utilise le contrôle de version pour prendre en charge les mises à niveau sans interruption.

Par exemple, cette URL de demande spécifie la version 4 de l'API.

`https://hostname_or_ip_address/api/v4/authorize`

La version principale de l'API est mise à jour lorsque des modifications sont apportées qui ne sont pas compatibles avec les versions plus anciennes. La version mineure de l'API est mise à jour lorsque des modifications sont apportées qui sont *compatibles* avec les versions plus anciennes. Les modifications compatibles incluent l'ajout de nouveaux points de terminaison ou de nouvelles propriétés.

L'exemple suivant illustre comment la version de l'API est augmentée en fonction du type de modifications apportées.

Type de modification de l'API	Ancienne version	Nouvelle version
Compatible avec les anciennes versions	2,1	2,2
Non compatible avec les anciennes versions	2,1	3,0

Lorsque vous installez le logiciel StorageGRID pour la première fois, seule la version la plus récente de l'API est activée. Cependant, lorsque vous effectuez une mise à niveau vers une nouvelle version de fonctionnalité de StorageGRID, vous continuez à avoir accès à l'ancienne version de l'API pour au moins une version de fonctionnalité de StorageGRID .



Vous pouvez configurer les versions prises en charge. Consultez la section **config** de la documentation de l'API Swagger pour le "[API de gestion de grille](#)" pour plus d'informations. Vous devez désactiver la prise en charge de l'ancienne version après avoir mis à jour tous les clients API pour utiliser la version la plus récente.

Les demandes obsolètes sont marquées comme obsolètes des manières suivantes :

- L'en-tête de réponse est « Obsolète : vrai »
- Le corps de la réponse JSON inclut « obsolète » : vrai

- Un avertissement obsolète est ajouté à nms.log. Par exemple:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Déterminer quelles versions d'API sont prises en charge dans la version actuelle

Utilisez le GET `/versions` Requête d'API pour renvoyer une liste des versions majeures d'API prises en charge. Cette demande se trouve dans la section **config** de la documentation de l'API Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Spécifier une version d'API pour une requête

Vous pouvez spécifier la version de l'API à l'aide d'un paramètre de chemin (`/api/v4`) ou un en-tête (`Api-Version: 4`). Si vous fournissez les deux valeurs, la valeur de l'en-tête remplace la valeur du chemin.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Protection contre la falsification de requêtes intersites (CSRF)

Vous pouvez contribuer à vous protéger contre les attaques de falsification de requête intersite (CSRF) contre StorageGRID en utilisant des jetons CSRF pour améliorer l'authentification qui utilise des cookies. Le gestionnaire de grille et le gestionnaire de locataires activent automatiquement cette fonctionnalité de sécurité ; les autres clients API peuvent choisir de l'activer ou non lorsqu'ils se connectent.

Un attaquant capable de déclencher une requête vers un autre site (par exemple avec un formulaire HTTP POST) peut provoquer l'exécution de certaines requêtes à l'aide des cookies de l'utilisateur connecté.

StorageGRID aide à se protéger contre les attaques CSRF en utilisant des jetons CSRF. Lorsqu'elle est activée, le contenu d'un cookie spécifique doit correspondre au contenu d'un en-tête spécifique ou d'un paramètre de corps POST spécifique.

Pour activer la fonctionnalité, définissez le `csrfToken` paramètre à `true` lors de l'authentification. La valeur par défaut est `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept: application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Lorsque c'est vrai, un `GridCsrfToken` Le cookie est défini avec une valeur aléatoire pour les connexions au Grid Manager, et le `AccountCsrfToken` le cookie est défini avec une valeur aléatoire pour les connexions au Tenant Manager.

Si le cookie est présent, toutes les requêtes pouvant modifier l'état du système (POST, PUT, PATCH, DELETE) doivent inclure l'un des éléments suivants :

- Le `X-Csrf-Token` en-tête, avec la valeur de l'en-tête définie sur la valeur du cookie de jeton CSRF.
- Pour les points de terminaison qui acceptent un corps codé par formulaire : A `csrfToken` paramètre de corps de requête codé par formulaire.

Pour configurer la protection CSRF, utilisez le ["API de gestion de grille"](#) ou ["API de gestion des locataires"](#).



Les requêtes qui ont un cookie de jeton CSRF défini appliqueront également l'en-tête « Content-Type : application/json » pour toute requête qui attend un corps de requête JSON comme protection supplémentaire contre les attaques CSRF.

Utiliser les connexions de la fédération de grille

Cloner des groupes de locataires et des utilisateurs

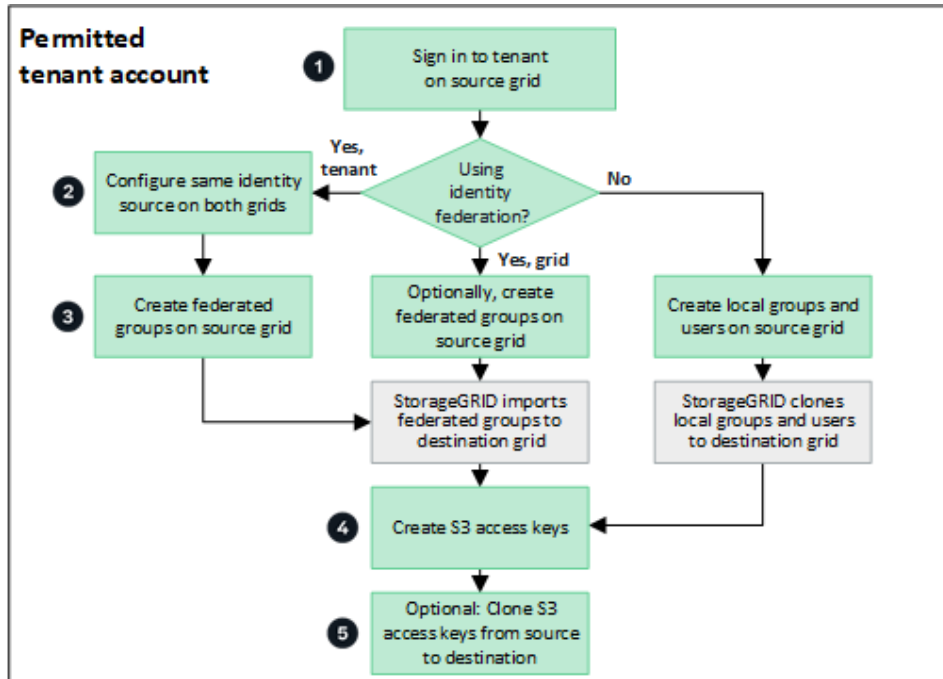
Si un locataire a été créé ou modifié pour utiliser une connexion de fédération de grille, ce locataire est répliqué d'un système StorageGRID (le locataire source) vers un autre système StorageGRID (le locataire réplique). Une fois le locataire répliqué, tous les groupes et utilisateurs ajoutés au locataire source sont clonés sur le locataire répliqué.

Le système StorageGRID dans lequel le locataire est créé à l'origine est la *grille source* du locataire. Le système StorageGRID sur lequel le locataire est répliqué est la *grille de destination* du locataire. Les deux comptes locataires ont le même ID de compte, le même nom, la même description, le même quota de stockage et les mêmes autorisations attribuées, mais le locataire de destination ne dispose pas initialement d'un mot de passe utilisateur root. Pour plus de détails, voir ["Qu'est-ce que le clonage de compte"](#) et ["Gérer les locataires autorisés"](#).

Le clonage des informations du compte locataire est requis pour ["réplication inter-réseaux"](#) d'objets de seau. Le fait d'avoir les mêmes groupes de locataires et utilisateurs sur les deux grilles garantit que vous pouvez accéder aux compartiments et objets correspondants sur l'une ou l'autre grille.

Flux de travail du locataire pour le clonage de compte

Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, consultez le diagramme de flux de travail pour voir les étapes que vous effectuerez pour cloner des groupes, des utilisateurs et des clés d'accès S3.



Voici les principales étapes du flux de travail :

1

Sign in au locataire

Sign in au compte locataire sur la grille source (la grille où le locataire a été initialement créé).

2

En option, configurer la fédération d'identité

Si votre compte locataire dispose de l'autorisation **Utiliser sa propre source d'identité** pour utiliser des groupes et des utilisateurs fédérés, configurez la même source d'identité (avec les mêmes paramètres) pour les comptes locataires source et de destination. Les groupes et utilisateurs fédérés ne peuvent pas être clonés à moins que les deux grilles n'utilisent la même source d'identité. Pour les instructions, voir ["Utiliser la fédération d'identité"](#).

3

Créer des groupes et des utilisateurs

Lors de la création de groupes et d'utilisateurs, commencez toujours par la grille source du locataire. Lorsque vous ajoutez un nouveau groupe, StorageGRID le clone automatiquement sur la grille de destination.

- Si la fédération d'identité est configurée pour l'ensemble du système StorageGRID ou pour votre compte locataire, ["créer de nouveaux groupes de locataires"](#) en important des groupes fédérés à partir de la source d'identité.
- Si vous n'utilisez pas la fédération d'identité, ["créer de nouveaux groupes locaux"](#) et puis ["créer des utilisateurs locaux"](#).

4

Créer des clés d'accès S3

Tu peux "[créer vos propres clés d'accès](#)" ou à "[créer les clés d'accès d'un autre utilisateur](#)" sur la grille source ou sur la grille de destination pour accéder aux buckets sur cette grille.

5

En option, clonez les clés d'accès S3

Si vous devez accéder à des buckets avec les mêmes clés d'accès sur les deux grilles, créez les clés d'accès sur la grille source, puis utilisez l'API Tenant Manager pour les cloner manuellement sur la grille de destination. Pour les instructions, voir "[Cloner les clés d'accès S3 à l'aide de l'API](#)".

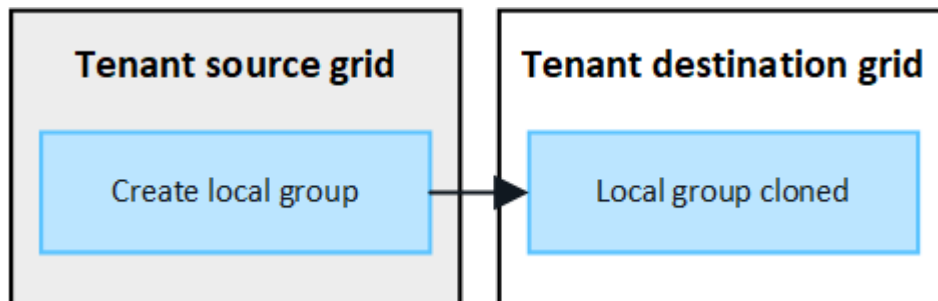
Comment les groupes, les utilisateurs et les clés d'accès S3 sont-ils clonés ?

Consultez cette section pour comprendre comment les groupes, les utilisateurs et les clés d'accès S3 sont clonés entre la grille source du locataire et la grille de destination du locataire.

Les groupes locaux créés sur la grille source sont clonés

Une fois qu'un compte de locataire est créé et répliqué sur la grille de destination, StorageGRID clone automatiquement tous les groupes locaux que vous ajoutez à la grille source du locataire vers la grille de destination du locataire.

Le groupe d'origine et son clone ont le même mode d'accès, les mêmes autorisations de groupe et la même stratégie de groupe S3. Pour les instructions, voir "[Créer des groupes pour le locataire S3](#)".

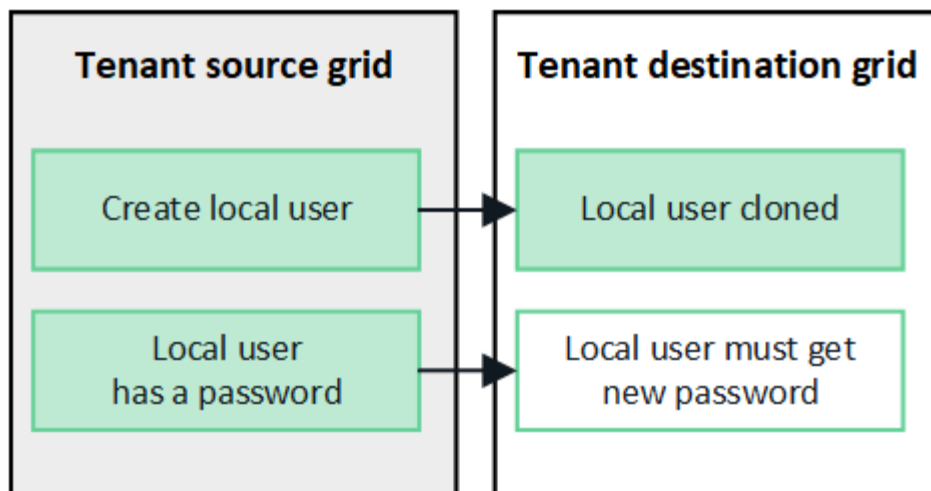


Tous les utilisateurs que vous sélectionnez lorsque vous créez un groupe local sur la grille source ne sont pas inclus lorsque le groupe est cloné sur la grille de destination. Pour cette raison, ne sélectionnez pas d'utilisateurs lorsque vous créez le groupe. Sélectionnez plutôt le groupe lorsque vous créez les utilisateurs.

Les utilisateurs locaux créés sur la grille source sont clonés

Lorsque vous créez un nouvel utilisateur local sur la grille source, StorageGRID clone automatiquement cet utilisateur sur la grille de destination. L'utilisateur d'origine et son clone ont le même nom complet, le même nom d'utilisateur et le même paramètre **Refuser l'accès**. Les deux utilisateurs appartiennent également aux mêmes groupes. Pour les instructions, voir "[Gérer les utilisateurs locaux](#)".

Pour des raisons de sécurité, les mots de passe des utilisateurs locaux ne sont pas clonés dans la grille de destination. Si un utilisateur local doit accéder à Tenant Manager sur la grille de destination, l'utilisateur root du compte locataire doit ajouter un mot de passe pour cet utilisateur sur la grille de destination. Pour les instructions, voir "[Gérer les utilisateurs locaux](#)".

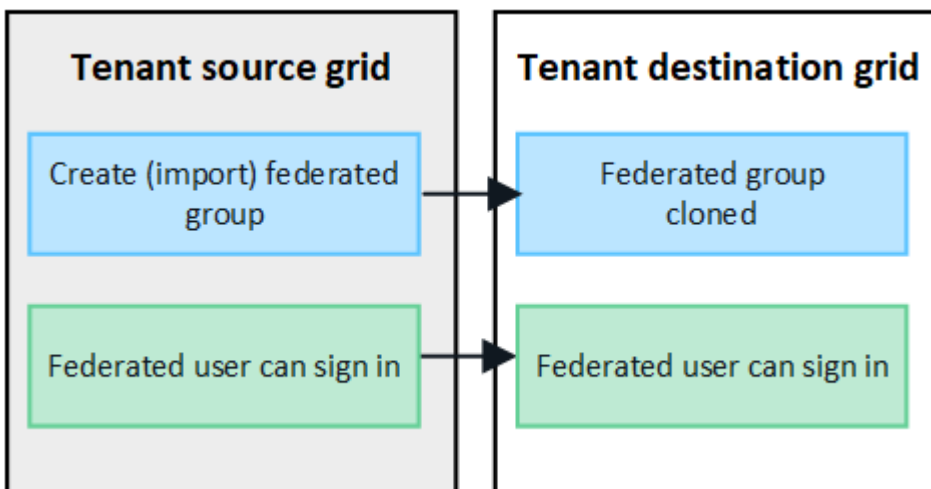


Les groupes fédérés créés sur la grille source sont clonés

En supposant que les exigences pour l'utilisation du clonage de compte avec ["authentification unique"](#) et ["fédération d'identité"](#) ont été rencontrés, les groupes fédérés que vous créez (importez) pour le locataire sur la grille source sont automatiquement clonés sur le locataire sur la grille de destination.

Les deux groupes ont le même mode d'accès, les mêmes autorisations de groupe et la même stratégie de groupe S3.

Une fois les groupes fédérés créés pour le locataire source et clonés vers le locataire de destination, les utilisateurs fédérés peuvent se connecter au locataire sur l'une ou l'autre grille.

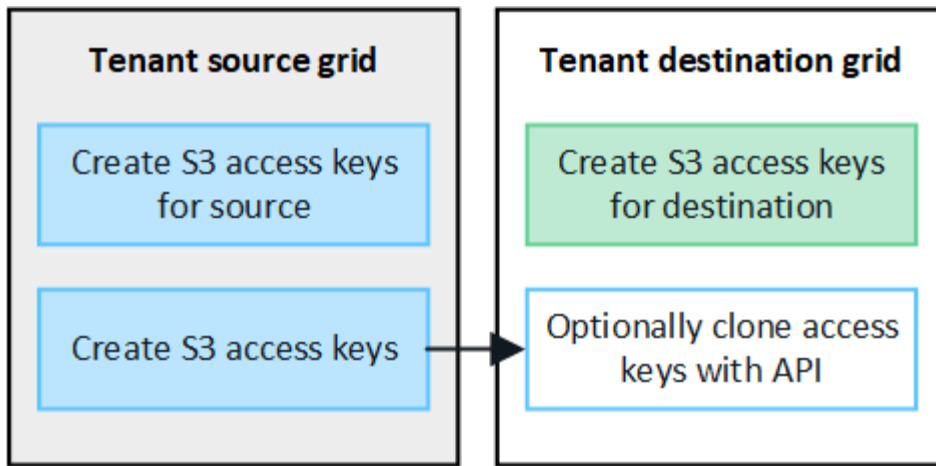


Les clés d'accès S3 peuvent être clonées manuellement

StorageGRID ne clone pas automatiquement les clés d'accès S3 car la sécurité est améliorée en ayant des clés différentes sur chaque grille.

Pour gérer les clés d'accès sur les deux grilles, vous pouvez effectuer l'une des opérations suivantes :

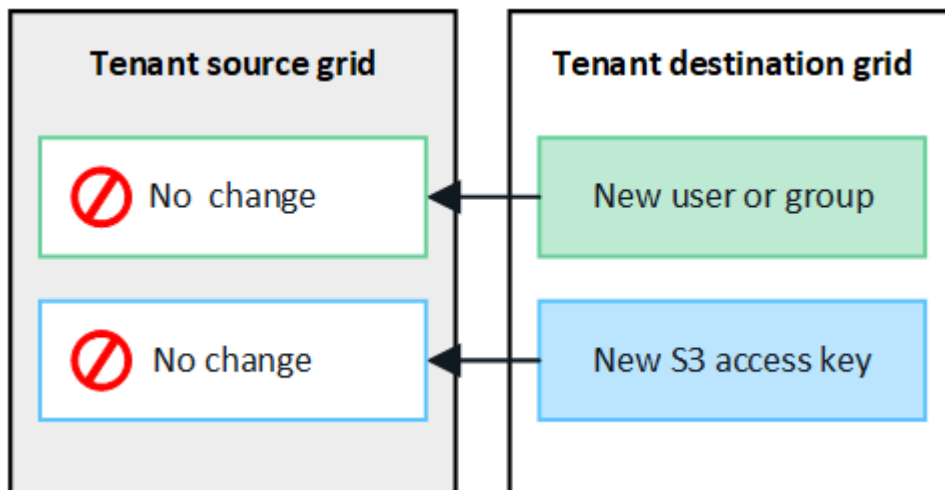
- Si vous n'avez pas besoin d'utiliser les mêmes clés pour chaque grille, vous pouvez ["créer vos propres clés d'accès"](#) ou ["créer les clés d'accès d'un autre utilisateur"](#) sur chaque grille.
- Si vous devez utiliser les mêmes clés sur les deux grilles, vous pouvez créer des clés sur la grille source, puis utiliser l'API Tenant Manager pour les utiliser manuellement. ["cloner les clés"](#) vers la grille de destination.



Lorsque vous clonez des clés d'accès S3 pour un utilisateur fédéré, l'utilisateur et les clés d'accès S3 sont clonés sur le locataire de destination.

Les groupes et les utilisateurs ajoutés à la grille de destination ne sont pas clonés

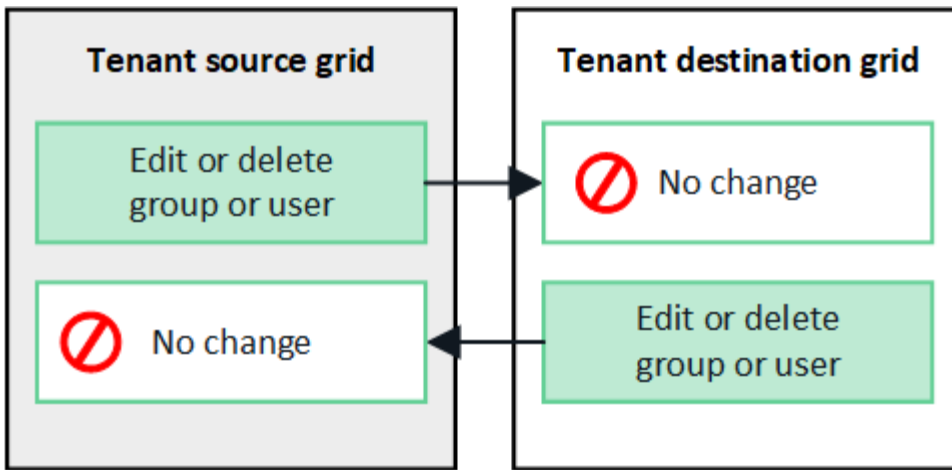
Le clonage se produit uniquement à partir de la grille source du locataire vers la grille de destination du locataire. Si vous créez ou importez des groupes et des utilisateurs sur la grille de destination du locataire, StorageGRID ne clonera pas ces éléments dans la grille source du locataire.



Les groupes, utilisateurs et clés d'accès modifiés ou supprimés ne sont pas clonés

Le clonage se produit uniquement lorsque vous créez de nouveaux groupes et utilisateurs.

Si vous modifiez ou supprimez des groupes, des utilisateurs ou des clés d'accès sur l'une ou l'autre grille, vos modifications ne seront pas clonées sur l'autre grille.



Cloner les clés d'accès S3 à l'aide de l'API

Si votre compte de locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, vous pouvez utiliser l'API de gestion des locataires pour cloner manuellement les clés d'accès S3 du locataire sur la grille source vers le locataire sur la grille de destination.

Avant de commencer

- Le compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**.
- La connexion à la fédération de grille a un **statut de connexion** de **Connecté**.
- Vous êtes connecté au gestionnaire de locataires sur la grille source du locataire à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérez vos propres informations d'identification S3 ou autorisation d'accès root"](#).
- Si vous clonez des clés d'accès pour un utilisateur local, l'utilisateur existe déjà sur les deux grilles.



Lorsque vous clonez des clés d'accès S3 pour un utilisateur fédéré, l'utilisateur et les clés d'accès S3 sont ajoutés au locataire de destination.

Clonez vos propres clés d'accès

Vous pouvez cloner vos propres clés d'accès si vous devez accéder aux mêmes compartiments sur les deux grilles.

Étapes

1. En utilisant le gestionnaire de locataires sur la grille source, ["créez vos propres clés d'accès"](#) et téléchargez le `.csv` déposer.
2. En haut du gestionnaire de locataires, sélectionnez l'icône d'aide et sélectionnez **Documentation API**.
3. Dans la section **s3**, sélectionnez le point de terminaison suivant :

```
POST /org/users/current-user/replicate-s3-access-key
```

POST

`/org/users/current-user/replicate-s3-access-key` Clone the current user's S3 key to the other grids.



4. Sélectionnez **Essayer**.
5. Dans la zone de texte **body**, remplacez les exemples d'entrées pour **accessKey** et **secretAccessKey** par les valeurs du fichier **.csv** que vous avez téléchargé.

Assurez-vous de conserver les guillemets doubles autour de chaque chaîne.



The screenshot shows a REST client interface with a field labeled 'body' marked as '* required'. Below the label, there is a tabbed interface with 'Edit Value' and 'Model' tabs. The 'Model' tab is selected, displaying a JSON object: { "accessKey": "AKIAIOSFODNN7EXAMPLE", "secretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY", "expires": "2028-09-04T00:00:00.000Z" }

6. Si la clé expire, remplacez l'exemple d'entrée pour **expires** par la date et l'heure d'expiration sous forme de chaîne au format de données-heure ISO 8601 (par exemple, 2024-02-28T22:46:33-08:00). Si la clé n'expire pas, entrez **null** comme valeur pour l'entrée **expires** (ou supprimez la ligne **Expires** et la virgule précédente).
7. Sélectionnez **Exécuter**.
8. Confirmez que le code de réponse du serveur est **204**, indiquant que la clé a été clonée avec succès sur la grille de destination.

Cloner les clés d'accès d'un autre utilisateur

Vous pouvez cloner les clés d'accès d'un autre utilisateur s'il doit accéder aux mêmes compartiments sur les deux grilles.

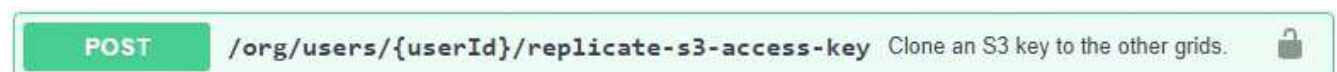
Étapes

1. En utilisant le gestionnaire de locataires sur la grille source, "[créer les clés d'accès S3 de l'autre utilisateur](#)" et téléchargez le **.csv** déposer.
2. En haut du gestionnaire de locataires, sélectionnez l'icône d'aide et sélectionnez **Documentation API**.
3. Obtenir l'ID utilisateur. Vous aurez besoin de cette valeur pour cloner les clés d'accès de l'autre utilisateur.
 - a. Dans la section **utilisateurs**, sélectionnez le point de terminaison suivant :

```
GET /org/users
```

- b. Sélectionnez **Essayer**.
 - c. Spécifiez les paramètres que vous souhaitez utiliser lors de la recherche d'utilisateurs.
 - d. Sélectionnez **Exécuter**.
 - e. Recherchez l'utilisateur dont vous souhaitez cloner les clés et copiez le numéro dans le champ **id**.
4. Dans la section **s3**, sélectionnez le point de terminaison suivant :

```
POST /org/users/{userId}/replicate-s3-access-key
```



The screenshot shows a REST client interface with a green button labeled 'POST' and a text field containing the endpoint '/org/users/{userId}/replicate-s3-access-key'. To the right of the text field, there is a description 'Clone an S3 key to the other grids.' and a lock icon.

5. Sélectionnez **Essayer**.

6. Dans la zone de texte **userid**, collez l'ID utilisateur que vous avez copié.
7. Dans la zone de texte **corps**, remplacez les exemples d'entrées pour **exemple de clé d'accès** et **clé d'accès secrète** par les valeurs du fichier **.csv** pour cet utilisateur.

Assurez-vous de conserver les guillemets doubles autour de la chaîne.

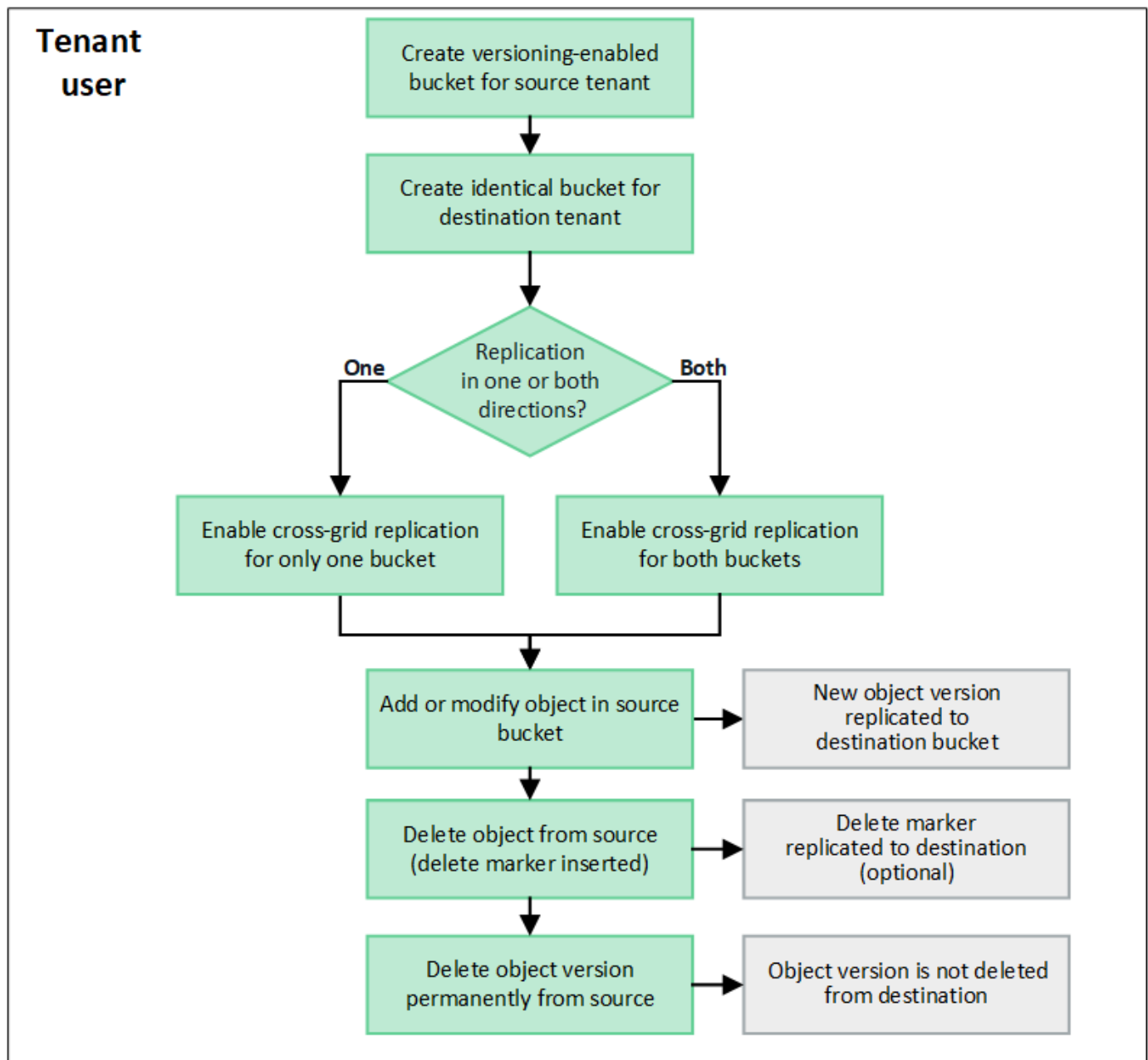
8. Si la clé expire, remplacez l'exemple d'entrée pour **expires** par la date et l'heure d'expiration sous forme de chaîne au format de données-heure ISO 8601 (par exemple, `2023-02-28T22:46:33-08:00`). Si la clé n'expire pas, entrez **null** comme valeur pour l'entrée **expires** (ou supprimez la ligne **Expires** et la virgule précédente).
9. Sélectionnez **Exécuter**.
10. Confirmez que le code de réponse du serveur est **204**, indiquant que la clé a été clonée avec succès sur la grille de destination.

Gérer la réplication inter-réseaux

Si l'autorisation **Utiliser la connexion à la fédération de grille** a été attribuée à votre compte de locataire lors de sa création, vous pouvez utiliser la réplication inter-grille pour répliquer automatiquement les objets entre les buckets de la grille source du locataire et les buckets de la grille de destination du locataire. La réplication inter-grille peut se produire dans un sens ou dans les deux sens.

Flux de travail pour la réplication inter-grille

Le diagramme de flux de travail résume les étapes que vous effectuerez pour configurer la réplication inter-grille entre les buckets sur deux grilles. Ces étapes sont décrites plus en détail ci-dessous.



Configurer la réplication inter-grille

Avant de pouvoir utiliser la réplication inter-grille, vous devez vous connecter aux comptes locataires correspondants sur chaque grille et créer des buckets identiques. Ensuite, vous pouvez activer la réplication inter-grille sur l'un ou les deux buckets.

Avant de commencer

- Vous avez examiné les exigences relatives à la réplication inter-réseaux. Voir ["Qu'est-ce que la réplication inter-réseau"](#).
- Vous utilisez un ["navigateur Web pris en charge"](#).
- Le compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et des comptes locataires identiques existent sur les deux grilles. Voir ["Gérer les locataires autorisés pour la connexion à la fédération de réseau"](#).
- L'utilisateur locataire avec lequel vous vous connecterez existe déjà sur les deux grilles et appartient à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#).

- Si vous vous connectez à la grille de destination du locataire en tant qu'utilisateur local, l'utilisateur root du compte locataire a défini un mot de passe pour votre compte utilisateur sur cette grille.

Créer deux buckets identiques

Dans un premier temps, connectez-vous aux comptes locataires correspondants sur chaque grille et créez des buckets identiques.

Étapes

1. À partir de l'une ou l'autre des grilles de la connexion à la fédération de grilles, créez un nouveau bucket :
 - a. Sign in au compte locataire à l'aide des informations d'identification d'un utilisateur locataire qui existe sur les deux grilles.



Si vous ne parvenez pas à vous connecter à la grille de destination du locataire en tant qu'utilisateur local, confirmez que l'utilisateur root du compte locataire a défini un mot de passe pour votre compte utilisateur.

- b. Suivez les instructions pour "[créer un bucket S3](#)".
 - c. Dans l'onglet **Gérer les paramètres de l'objet**, sélectionnez **Activer le contrôle de version de l'objet**.
 - d. Si le verrouillage d'objet S3 est activé pour votre système StorageGRID, n'activez pas le verrouillage d'objet S3 pour le bucket.
 - e. Sélectionnez **Créer un bucket**.
 - f. Sélectionnez **Terminer**.
2. Répétez ces étapes pour créer un bucket identique pour le même compte locataire sur l'autre grille dans la connexion de fédération de grille.



Selon les besoins, chaque bucket peut utiliser une région différente.

Activer la réplication inter-réseaux

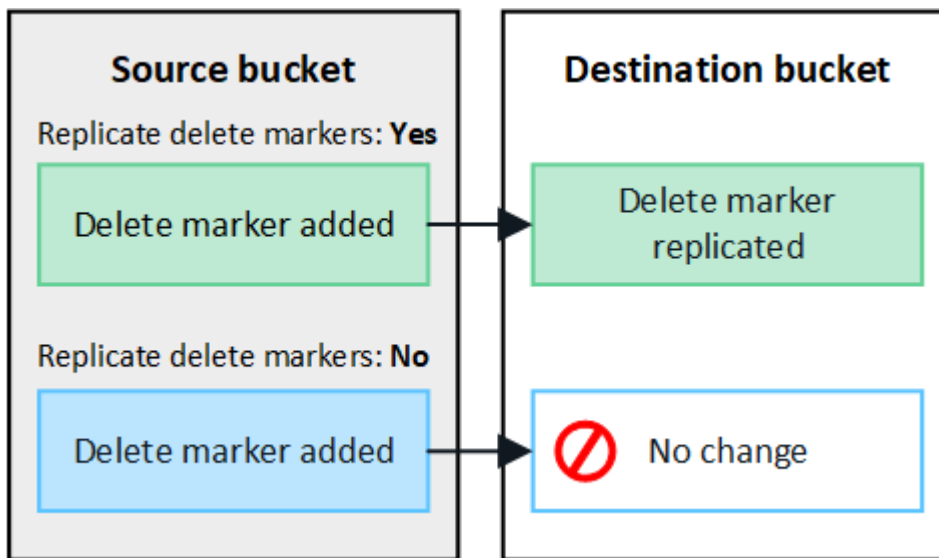
Vous devez effectuer ces étapes avant d'ajouter des objets à l'un ou l'autre des compartiments.

Étapes

1. À partir d'une grille dont vous souhaitez répliquer les objets, activez "[réplication inter-grille dans une direction](#)" :
 - a. Sign in au compte locataire du bucket.
 - b. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
 - c. Sélectionnez le nom du bucket dans le tableau pour accéder à la page des détails du bucket.
 - d. Sélectionnez l'onglet **Réplication inter-grille**.
 - e. Sélectionnez **Activer** et examinez la liste des exigences.
 - f. Si toutes les exigences sont remplies, sélectionnez la connexion à la fédération de réseau que vous souhaitez utiliser.
 - g. Vous pouvez également modifier le paramètre **Répliquer les marqueurs de suppression** pour déterminer ce qui se passe sur la grille de destination si un client S3 émet une demande de

suppression vers la grille source qui n'inclut pas d'ID de version :

- **Oui** (par défaut) : un marqueur de suppression est ajouté au bucket source et répliqué vers le bucket de destination.
- **Non** : un marqueur de suppression est ajouté au bucket source mais n'est pas répliqué dans le bucket de destination.



Si la demande de suppression inclut un ID de version, cette version d'objet est définitivement supprimée du bucket source. StorageGRID ne réplique pas les demandes de suppression qui incluent un ID de version, donc la même version d'objet n'est pas supprimée de la destination.

Voir ["Qu'est-ce que la réplication inter-réseau"](#) pour plus de détails.

- a. Vous pouvez également modifier le paramètre de la catégorie d'audit **Réplication inter-grille** pour gérer le volume des messages d'audit :
 - **Erreur** (par défaut) : seules les demandes de réplication inter-grille ayant échoué sont incluses dans la sortie d'audit.
 - **Normal** : toutes les demandes de réplication inter-grille sont incluses, ce qui augmente considérablement le volume de sortie d'audit.
- b. Revoyez vos sélections. Vous ne pouvez pas modifier ces paramètres à moins que les deux compartiments soient vides.
- c. Sélectionnez **Activer et tester**.

Après quelques instants, un message de réussite apparaît. Les objets ajoutés à ce bucket seront désormais automatiquement répliqués sur l'autre grille. La **réplication inter-grille** est affichée comme une fonctionnalité activée sur la page des détails du bucket.

2. En option, accédez au bucket correspondant sur l'autre grille et ["activer la réplication inter-réseau dans les deux sens"](#).

Réplication des tests entre les grilles

Si la réplication inter-grille est activée pour un bucket, vous devrez peut-être vérifier que la connexion et la réplication inter-grille fonctionnent correctement et que les buckets source et de destination répondent toujours

à toutes les exigences (par exemple, le contrôle de version est toujours activé).

Avant de commencer

- Vous utilisez un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#) .

Étapes

1. Sign in au compte locataire du bucket.
2. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
3. Sélectionnez le nom du bucket dans le tableau pour accéder à la page des détails du bucket.
4. Sélectionnez l'onglet **Réplication inter-grille**.
5. Sélectionnez **Tester la connexion**.

Si la connexion est saine, une bannière de réussite apparaît. Sinon, un message d'erreur s'affiche, que vous et l'administrateur du réseau pouvez utiliser pour résoudre le problème. Pour plus de détails, consultez la section ["Résoudre les erreurs de fédération de grille"](#) .

6. Si la réplication inter-grille est configurée pour se produire dans les deux sens, accédez au bucket correspondant sur l'autre grille et sélectionnez **Tester la connexion** pour vérifier que la réplication inter-grille fonctionne dans l'autre sens.

Désactiver la réplication inter-grille

Vous pouvez arrêter définitivement la réplication inter-grille si vous ne souhaitez plus copier d'objets vers l'autre grille.

Avant de désactiver la réplication inter-grille, notez les points suivants :

- La désactivation de la réplication inter-grille ne supprime aucun objet qui a déjà été copié entre les grilles. Par exemple, les objets dans `my-bucket` sur la grille 1 qui ont été copiés sur `my-bucket` sur la grille 2 ne sont pas supprimés si vous désactivez la réplication inter-grille pour ce bucket. Si vous souhaitez supprimer ces objets, vous devez les supprimer manuellement.
- Si la réplication inter-grille a été activée pour chacun des buckets (c'est-à-dire si la réplication se produit dans les deux sens), vous pouvez désactiver la réplication inter-grille pour l'un ou les deux buckets. Par exemple, vous souhaitez peut-être désactiver la réplication d'objets à partir de `my-bucket` sur la grille 1 à `my-bucket` sur la grille 2, tout en continuant à répliquer les objets de `my-bucket` sur la grille 2 à `my-bucket` sur la grille 1.
- Vous devez désactiver la réplication inter-grille avant de pouvoir supprimer l'autorisation d'un locataire d'utiliser la connexion de fédération de grille. Voir ["Gérer les locataires autorisés"](#) .
- Si vous désactivez la réplication inter-grille pour un bucket contenant des objets, vous ne pourrez pas réactiver la réplication inter-grille, sauf si vous supprimez tous les objets des buckets source et de destination.



Vous ne pouvez pas réactiver la réplication à moins que les deux buckets ne soient vides.

Avant de commencer

- Vous utilisez un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#) .

Étapes

1. En partant de la grille dont vous ne souhaitez plus répliquer les objets, arrêtez la réplication inter-grille pour le bucket :
 - a. Sign in au compte locataire du bucket.
 - b. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
 - c. Sélectionnez le nom du bucket dans le tableau pour accéder à la page des détails du bucket.
 - d. Sélectionnez l'onglet **Réplication inter-grille**.
 - e. Sélectionnez **Désactiver la réplication**.
 - f. Si vous êtes sûr de vouloir désactiver la réplication inter-grille pour ce bucket, saisissez **Oui** dans la zone de texte et sélectionnez **Désactiver**.

Après quelques instants, un message de réussite apparaît. Les nouveaux objets ajoutés à ce bucket ne peuvent plus être automatiquement répliqués sur l'autre grille. La **réplication inter-grille** n'est plus affichée comme une fonctionnalité activée sur la page Buckets.

2. Si la réplication inter-grille a été configurée pour se produire dans les deux sens, accédez au bucket correspondant sur l'autre grille et arrêtez la réplication inter-grille dans l'autre sens.

Afficher les connexions de la fédération de grille

Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, vous pouvez afficher les connexions autorisées.

Avant de commencer

- Le compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**.
- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#).

Étapes

1. Sélectionnez **STOCKAGE (S3) > Connexions de fédération de grille**.

La page de connexion à la fédération Grid apparaît et inclut un tableau qui résume les informations suivantes :

Colonne	Description
Nom de la connexion	Les connexions de la fédération de grille que ce locataire est autorisé à utiliser.
Buckets avec réplication inter-grille	Pour chaque connexion de fédération de grille, les buckets de locataire pour lesquels la réplication inter-grille est activée. Les objets ajoutés à ces buckets seront répliqués sur l'autre grille de la connexion.
Dernière erreur	Pour chaque connexion de fédération de grille, l'erreur la plus récente survenue, le cas échéant, lors de la réplication des données sur l'autre grille. Voir Effacer la dernière erreur .

2. Vous pouvez également sélectionner un nom de bucket pour "[afficher les détails du godet](#)".

Effacer la dernière erreur

Une erreur peut apparaître dans la colonne **Dernière erreur** pour l'une des raisons suivantes :

- La version de l'objet source n'a pas été trouvée.
- Le bucket source n'a pas été trouvé.
- Le bucket de destination a été supprimé.
- Le bucket de destination a été recréé par un compte différent.
- Le contrôle de version du bucket de destination est suspendu.
- Le bucket de destination a été recréé par le même compte mais n'est désormais plus versionné.



Cette colonne affiche uniquement la dernière erreur de réplication inter-grille survenue ; les erreurs précédentes qui auraient pu se produire ne seront pas affichées.

Étapes

1. Si un message apparaît dans la colonne **Dernière erreur**, affichez le texte du message.

Par exemple, cette erreur indique que le bucket de destination pour la réplication inter-grille était dans un état non valide, probablement parce que le contrôle de version a été suspendu ou que le verrouillage d'objet S3 a été activé.

Grid federation connections

Clear error

Displaying one result

Connection name	Buckets with cross-grid replication	Last error
<input type="radio"/> Grid 1-Grid 2	my-cgr-bucket	<div>2022-12-07 16:02:20 MST</div> <div>Cross-grid replication has encountered an error. Failed to send cross-grid replication request from source bucket 'my-cgr-bucket' to destination bucket 'my-cgr-bucket'. Error code: DestinationRequestError. Detail: InvalidBucketState. Confirm that the source and destination buckets have object versioning enabled and S3 Object Lock disabled. (logID 4791585492825418592)</div>

2. Effectuez toutes les actions recommandées. Par exemple, si le contrôle de version a été suspendu sur le bucket de destination pour la réplication inter-grille, réactivez le contrôle de version pour ce bucket.
3. Sélectionnez la connexion dans le tableau.
4. Sélectionnez **Effacer l'erreur**.
5. Sélectionnez **Oui** pour effacer le message et mettre à jour l'état du système.
6. Attendez 5 à 6 minutes, puis ingérez un nouvel objet dans le seau. Vérifiez que le message d'erreur ne réapparaît pas.



Pour vous assurer que le message d'erreur est effacé, attendez au moins 5 minutes après l'horodatage du message avant d'ingérer un nouvel objet.

7. Pour déterminer si des objets n'ont pas pu être répliqués en raison de l'erreur de compartiment, consultez "[Identifier et réessayer les opérations de réplication ayant échoué](#)".

Gérer les groupes et les utilisateurs

Utiliser la fédération d'identité

L'utilisation de la fédération d'identité accélère la configuration des groupes de locataires et des utilisateurs et permet aux utilisateurs locataires de se connecter au compte locataire à l'aide d'informations d'identification familières.

Configurer la fédération d'identité pour Tenant Manager

Vous pouvez configurer la fédération d'identité pour Tenant Manager si vous souhaitez que les groupes de locataires et les utilisateurs soient gérés dans un autre système tel qu'Active Directory, Azure Active Directory (Azure AD), OpenLDAP ou Oracle Directory Server.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#) .
- Vous utilisez Active Directory, Azure AD, OpenLDAP ou Oracle Directory Server comme fournisseur d'identité.



Si vous souhaitez utiliser un service LDAP v3 qui n'est pas répertorié, contactez le support technique.

- Si vous prévoyez d'utiliser OpenLDAP, vous devez configurer le serveur OpenLDAP. Voir [Directives pour la configuration du serveur OpenLDAP](#) .
- Si vous prévoyez d'utiliser Transport Layer Security (TLS) pour les communications avec le serveur LDAP, le fournisseur d'identité doit utiliser TLS 1.2 ou 1.3. Voir ["Chiffres pris en charge pour les connexions TLS sortantes"](#) .

À propos de cette tâche

La possibilité de configurer un service de fédération d'identité pour votre locataire dépend de la façon dont votre compte de locataire a été configuré. Votre locataire peut partager le service de fédération d'identité qui a été configuré pour Grid Manager. Si vous voyez ce message lorsque vous accédez à la page Fédération d'identité, vous ne pouvez pas configurer une source d'identité fédérée distincte pour ce locataire.



This tenant account uses the LDAP server that is configured for the Grid Manager.
Contact the grid administrator for information or to change this setting.

Entrer la configuration

Lorsque vous configurez l'identification de la fédération, vous fournissez les valeurs dont StorageGRID a besoin pour se connecter à un service LDAP.

Étapes

1. Sélectionnez **GESTION DES ACCÈS > Fédération d'identité**.
2. Sélectionnez **Activer la fédération d'identité**.
3. Dans la section Type de service LDAP, sélectionnez le type de service LDAP que vous souhaitez configurer.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Azure	OpenLDAP	Other
------------------	-------	----------	-------

Sélectionnez **Autre** pour configurer les valeurs d'un serveur LDAP qui utilise Oracle Directory Server.

4. Si vous avez sélectionné **Autre**, remplissez les champs de la section Attributs LDAP. , passez à l'étape suivante.
 - **Nom unique de l'utilisateur** : le nom de l'attribut qui contient l'identifiant unique d'un utilisateur LDAP. Cet attribut est équivalent à `sAMAccountName` pour Active Directory et `uid` pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `uid` .
 - **UUID utilisateur** : le nom de l'attribut qui contient l'identifiant unique permanent d'un utilisateur LDAP. Cet attribut est équivalent à `objectGUID` pour Active Directory et `entryUUID` pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `nsuniqueid` . La valeur de chaque utilisateur pour l'attribut spécifié doit être un nombre hexadécimal à 32 chiffres au format 16 octets ou chaîne, où les tirets sont ignorés.
 - **Nom unique du groupe** : le nom de l'attribut qui contient l'identifiant unique d'un groupe LDAP. Cet attribut est équivalent à `sAMAccountName` pour Active Directory et `cn` pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `cn` .
 - **UUID de groupe** : le nom de l'attribut qui contient l'identifiant unique permanent d'un groupe LDAP. Cet attribut est équivalent à `objectGUID` pour Active Directory et `entryUUID` pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `nsuniqueid` . La valeur de chaque groupe pour l'attribut spécifié doit être un nombre hexadécimal à 32 chiffres au format 16 octets ou chaîne, où les tirets sont ignorés.
5. Pour tous les types de services LDAP, saisissez les informations de serveur LDAP et de connexion réseau requises dans la section Configurer le serveur LDAP.
 - **Nom d'hôte** : le nom de domaine complet (FQDN) ou l'adresse IP du serveur LDAP.
 - **Port** : Le port utilisé pour se connecter au serveur LDAP.



Le port par défaut pour STARTTLS est 389 et le port par défaut pour LDAPS est 636. Cependant, vous pouvez utiliser n'importe quel port à condition que votre pare-feu soit correctement configuré.

- **Nom d'utilisateur** : le chemin complet du nom distinctif (DN) de l'utilisateur qui se connectera au serveur LDAP.

Pour Active Directory, vous pouvez également spécifier le nom de connexion de niveau inférieur ou le nom d'utilisateur principal.

L'utilisateur spécifié doit avoir l'autorisation de répertorier les groupes et les utilisateurs et d'accéder aux attributs suivants :

- `sAMAccountName` ou `uid`

- objectGUID, entryUUID, ou nsuniqueid
 - cn
 - memberOf`ou `isMemberOf
 - **Active Directory:** objectSid, primaryGroupID, userAccountControl, et userPrincipalName
 - **Azuré:** accountEnabled et userPrincipalName
- **Mot de passe :** Le mot de passe associé au nom d'utilisateur.



Si vous modifiez le mot de passe à l'avenir, vous devez le mettre à jour sur cette page.

- **DN de base du groupe :** le chemin complet du nom distinctif (DN) d'une sous-arborescence LDAP dans laquelle vous souhaitez rechercher des groupes. Dans l'exemple Active Directory (ci-dessous), tous les groupes dont le nom unique est relatif au DN de base (DC=storagegrid,DC=example,DC=com) peuvent être utilisés comme groupes fédérés.



Les valeurs **Nom unique du groupe** doivent être uniques dans le **DN de base du groupe** auquel elles appartiennent.

- **DN de base utilisateur :** le chemin complet du nom distinctif (DN) d'une sous-arborescence LDAP dans laquelle vous souhaitez rechercher des utilisateurs.



Les valeurs **Nom unique de l'utilisateur** doivent être uniques dans le **DN de base de l'utilisateur** auquel elles appartiennent.

- * **Format de nom d'utilisateur de liaison *** (facultatif) : le modèle de nom d'utilisateur par défaut que StorageGRID doit utiliser si le modèle ne peut pas être déterminé automatiquement.

Il est recommandé de fournir le **format de nom d'utilisateur de liaison** car il peut permettre aux utilisateurs de se connecter si StorageGRID ne parvient pas à se lier au compte de service.

Saisissez l'un de ces modèles :

- **Modèle UserPrincipalName (Active Directory et Azure):** [USERNAME]@example.com
- **Modèle de nom de connexion de niveau inférieur (Active Directory et Azure):**
example\[USERNAME]
- **Modèle de nom distinctif:** CN=[USERNAME],CN=Users,DC=example,DC=com

Incluez [USERNAME] exactement comme écrit.

6. Dans la section Sécurité de la couche de transport (TLS), sélectionnez un paramètre de sécurité.

- **Utiliser STARTTLS :** Utilisez STARTTLS pour sécuriser les communications avec le serveur LDAP. Il s'agit de l'option recommandée pour Active Directory, OpenLDAP ou Autre, mais cette option n'est pas prise en charge pour Azure.
- **Utiliser LDAPS :** L'option LDAPS (LDAP sur SSL) utilise TLS pour établir une connexion au serveur LDAP. Vous devez sélectionner cette option pour Azure.
- **N'utilisez pas TLS :** le trafic réseau entre le système StorageGRID et le serveur LDAP ne sera pas sécurisé. Cette option n'est pas prise en charge pour Azure.



L'utilisation de l'option **Ne pas utiliser TLS** n'est pas prise en charge si votre serveur Active Directory applique la signature LDAP. Vous devez utiliser STARTTLS ou LDAPS.

7. Si vous avez sélectionné STARTTLS ou LDAPS, choisissez le certificat utilisé pour sécuriser la connexion.
 - **Utiliser le certificat CA du système d'exploitation** : utilisez le certificat CA Grid par défaut installé sur le système d'exploitation pour sécuriser les connexions.
 - **Utiliser un certificat CA personnalisé** : utilisez un certificat de sécurité personnalisé.

Si vous sélectionnez ce paramètre, copiez et collez le certificat de sécurité personnalisé dans la zone de texte Certificat CA.

Tester la connexion et enregistrer la configuration

Après avoir saisi toutes les valeurs, vous devez tester la connexion avant de pouvoir enregistrer la configuration. StorageGRID vérifie les paramètres de connexion pour le serveur LDAP et le format du nom d'utilisateur de liaison, si vous en avez fourni un.

Étapes

1. Sélectionnez **Tester la connexion**.
2. Si vous n'avez pas fourni de format de nom d'utilisateur de liaison :
 - Un message « Test de connexion réussi » s'affiche si les paramètres de connexion sont valides. Sélectionnez **Enregistrer** pour enregistrer la configuration.
 - Un message « La connexion de test n'a pas pu être établie » s'affiche si les paramètres de connexion ne sont pas valides. Sélectionnez **Fermer**. Ensuite, résolvez tous les problèmes et testez à nouveau la connexion.
3. Si vous avez fourni un format de nom d'utilisateur de liaison, saisissez le nom d'utilisateur et le mot de passe d'un utilisateur fédéré valide.

Par exemple, entrez votre propre nom d'utilisateur et votre mot de passe. N'incluez aucun caractère spécial dans le nom d'utilisateur, tel que @ ou /.

Test Connection

To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.

Test username

The username of a federated user.

Test password

[Cancel](#) [Test Connection](#)

- Un message « Test de connexion réussi » s'affiche si les paramètres de connexion sont valides. Sélectionnez **Enregistrer** pour enregistrer la configuration.

- Un message d'erreur s'affiche si les paramètres de connexion, le format du nom d'utilisateur de liaison ou le nom d'utilisateur et le mot de passe de test ne sont pas valides. Résolvez tous les problèmes et testez à nouveau la connexion.

Forcer la synchronisation avec la source d'identité

Le système StorageGRID synchronise périodiquement les groupes fédérés et les utilisateurs à partir de la source d'identité. Vous pouvez forcer le démarrage de la synchronisation si vous souhaitez activer ou restreindre les autorisations des utilisateurs le plus rapidement possible.

Étapes

1. Accédez à la page Fédération d'identité.
2. Sélectionnez **Serveur de synchronisation** en haut de la page.

Le processus de synchronisation peut prendre un certain temps en fonction de votre environnement.



L'alerte **Échec de la synchronisation de la fédération d'identité** est déclenchée s'il y a un problème de synchronisation des groupes fédérés et des utilisateurs à partir de la source d'identité.

Désactiver la fédération d'identité

Vous pouvez désactiver temporairement ou définitivement la fédération d'identité pour les groupes et les utilisateurs. Lorsque la fédération d'identité est désactivée, il n'y a aucune communication entre StorageGRID et la source d'identité. Cependant, tous les paramètres que vous avez configurés sont conservés, ce qui vous permet de réactiver facilement la fédération d'identité à l'avenir.

À propos de cette tâche

Avant de désactiver la fédération d'identité, vous devez tenir compte des points suivants :

- Les utilisateurs fédérés ne pourront pas se connecter.
- Les utilisateurs fédérés actuellement connectés conserveront l'accès au système StorageGRID jusqu'à l'expiration de leur session, mais ils ne pourront pas se connecter après l'expiration de leur session.
- La synchronisation entre le système StorageGRID et la source d'identité n'aura pas lieu et les alertes ne seront pas générées pour les comptes qui n'ont pas été synchronisés.
- La case à cocher **Activer la fédération d'identité** est désactivée si l'authentification unique (SSO) est définie sur **Activé** ou **Mode Sandbox**. Le statut SSO sur la page d'authentification unique doit être **Désactivé** avant de pouvoir désactiver la fédération d'identité. Voir "[Désactiver l'authentification unique](#)".

Étapes

1. Accédez à la page Fédération d'identité.
2. Décochez la case **Activer la fédération d'identité**.

Directives pour la configuration du serveur OpenLDAP

Si vous souhaitez utiliser un serveur OpenLDAP pour la fédération d'identité, vous devez configurer des paramètres spécifiques sur le serveur OpenLDAP.



Pour les sources d'identité qui ne sont pas ActiveDirectory ou Azure, StorageGRID ne bloquera pas automatiquement l'accès S3 aux utilisateurs désactivés en externe. Pour bloquer l'accès S3, supprimez toutes les clés S3 de l'utilisateur ou supprimez l'utilisateur de tous les groupes.

Superpositions Memberof et refint

Les superpositions memberof et refint doivent être activées. Pour plus d'informations, consultez les instructions relatives à la maintenance de l'appartenance à un groupe inversé dans <http://www.openldap.org/doc/admin24/index.html> ["Documentation OpenLDAP : Guide de l'administrateur version 2.4"] .

Indexage

Vous devez configurer les attributs OpenLDAP suivants avec les mots-clés d'index spécifiés :

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

De plus, assurez-vous que les champs mentionnés dans l'aide pour le nom d'utilisateur sont indexés pour des performances optimales.

Consultez les informations sur la maintenance de l'appartenance à un groupe inversé dans <http://www.openldap.org/doc/admin24/index.html> ["Documentation OpenLDAP : Guide de l'administrateur version 2.4"] .

Gérer les groupes de locataires

Créer des groupes pour un locataire S3

Vous pouvez gérer les autorisations des groupes d'utilisateurs S3 en important des groupes fédérés ou en créant des groupes locaux.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#) .
- Si vous envisagez d'importer un groupe fédéré, vous devez ["fédération d'identité configurée"](#) , et le groupe fédéré existe déjà dans la source d'identité configurée.
- Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, vous avez examiné le flux de travail et les considérations pour ["clonage de groupes de locataires et d'utilisateurs"](#) , et vous êtes connecté à la grille source du locataire.

Accéder à l'assistant de création de groupe

Dans un premier temps, accédez à l'assistant de création de groupe.

Étapes

1. Sélectionnez **GESTION DES ACCÈS > Groupes**.

2. Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, confirmez qu'une bannière bleue apparaît, indiquant que les nouveaux groupes créés sur cette grille seront clonés sur le même locataire sur l'autre grille de la connexion. Si cette bannière n'apparaît pas, vous êtes peut-être connecté à la grille de destination du locataire.

3. Sélectionnez **Créer un groupe**.

Choisissez un type de groupe

Vous pouvez créer un groupe local ou importer un groupe fédéré.

Étapes

1. Sélectionnez l'onglet **Groupe local** pour créer un groupe local ou sélectionnez l'onglet **Groupe fédéré** pour importer un groupe à partir de la source d'identité précédemment configurée.

Si l'authentification unique (SSO) est activée pour votre système StorageGRID, les utilisateurs appartenant à des groupes locaux ne pourront pas se connecter au gestionnaire de locataires, bien qu'ils puissent utiliser des applications clientes pour gérer les ressources du locataire, en fonction des autorisations de groupe.

2. Entrez le nom du groupe.

- **Groupe local** : saisissez un nom d'affichage et un nom unique. Vous pouvez modifier le nom d'affichage ultérieurement.



Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, une erreur de clonage se produira si le même **Nom unique** existe déjà pour le locataire sur la grille de destination.

- **Groupe fédéré** : Saisissez le nom unique. Pour Active Directory, le nom unique est le nom associé au sAMAccountName attribut. Pour OpenLDAP, le nom unique est le nom associé au uid attribut.

3. Sélectionnez **Continuer**.

Gérer les autorisations de groupe

Les autorisations de groupe contrôlent les tâches que les utilisateurs peuvent effectuer dans Tenant Manager et l'API Tenant Management.

Étapes

1. Pour le **Mode d'accès**, sélectionnez l'une des options suivantes :

- **Lecture-écriture** (par défaut) : les utilisateurs peuvent se connecter à Tenant Manager et gérer la configuration du locataire.
- **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent apporter aucune modification ni effectuer aucune opération dans l'API Tenant Manager ou Tenant Management. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.



Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur Lecture seule, l'utilisateur aura un accès en lecture seule à tous les paramètres et fonctionnalités sélectionnés.

2. Sélectionnez une ou plusieurs autorisations pour ce groupe.

Voir "[Autorisations de gestion des locataires](#)".

3. Sélectionnez **Continuer**.

Définir la stratégie de groupe S3

La stratégie de groupe détermine les autorisations d'accès S3 dont disposeront les utilisateurs.

Étapes

1. Sélectionnez la politique que vous souhaitez utiliser pour ce groupe.

Politique de groupe	Description
Pas d'accès S3	Défaut. Les utilisateurs de ce groupe n'ont pas accès aux ressources S3, sauf si l'accès est accordé avec une stratégie de compartiment. Si vous sélectionnez cette option, seul l'utilisateur root aura accès aux ressources S3 par défaut.
Accès en lecture seule	Les utilisateurs de ce groupe ont un accès en lecture seule aux ressources S3. Par exemple, les utilisateurs de ce groupe peuvent répertorier les objets et lire les données d'objet, les métadonnées et les balises. Lorsque vous sélectionnez cette option, la chaîne JSON d'une stratégie de groupe en lecture seule apparaît dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
Accès complet	Les utilisateurs de ce groupe ont un accès complet aux ressources S3, y compris les buckets. Lorsque vous sélectionnez cette option, la chaîne JSON d'une stratégie de groupe à accès complet apparaît dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.

Politique de groupe	Description
Atténuation des ransomwares	<p>Cet exemple de politique s'applique à tous les compartiments de ce locataire. Les utilisateurs de ce groupe peuvent effectuer des actions courantes, mais ne peuvent pas supprimer définitivement les objets des buckets pour lesquels le contrôle de version des objets est activé.</p> <p>Les utilisateurs de Tenant Manager qui disposent de l'autorisation Gérer tous les compartiments peuvent remplacer cette stratégie de groupe. Limitez l'autorisation Gérer tous les compartiments aux utilisateurs de confiance et utilisez l'authentification multifacteur (MFA) lorsqu'elle est disponible.</p>
Coutume	Les utilisateurs du groupe bénéficient des autorisations que vous spécifiez dans la zone de texte.

2. Si vous avez sélectionné **Personnalisé**, saisissez la stratégie de groupe. Chaque stratégie de groupe a une limite de taille de 5 120 octets. Vous devez saisir une chaîne formatée JSON valide.

Pour des informations détaillées sur les stratégies de groupe, y compris la syntaxe du langage et des exemples, voir ["Exemples de stratégies de groupe"](#).

3. Si vous créez un groupe local, sélectionnez **Continuer**. Si vous créez un groupe fédéré, sélectionnez **Créer un groupe** et **Terminer**.

Ajouter des utilisateurs (groupes locaux uniquement)

Vous pouvez enregistrer le groupe sans ajouter d'utilisateurs, ou vous pouvez éventuellement ajouter des utilisateurs locaux déjà existants.



Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, tous les utilisateurs que vous sélectionnez lorsque vous créez un groupe local sur la grille source ne sont pas inclus lorsque le groupe est cloné sur la grille de destination. Pour cette raison, ne sélectionnez pas d'utilisateurs lorsque vous créez le groupe. Sélectionnez plutôt le groupe lorsque vous créez les utilisateurs.

Étapes

1. Vous pouvez également sélectionner un ou plusieurs utilisateurs locaux pour ce groupe.
2. Sélectionnez **Créer un groupe** et **Terminer**.

Le groupe que vous avez créé apparaît dans la liste des groupes.

Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous êtes sur la grille source du locataire, le nouveau groupe est cloné sur la grille de destination du locataire. **Succès** apparaît comme **Statut de clonage** dans la section Présentation de la page de détails du groupe.

Créer des groupes pour un locataire Swift

Vous pouvez gérer les autorisations d'accès pour un compte locataire Swift en important des groupes fédérés ou en créant des groupes locaux. Au moins un groupe doit disposer

de l'autorisation Administrateur Swift, qui est requise pour gérer les conteneurs et les objets d'un compte locataire Swift.



La prise en charge des applications clientes Swift est obsolète et sera supprimée dans une prochaine version.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#) .
- Si vous envisagez d'importer un groupe fédéré, vous devez ["fédération d'identité configurée"](#) , et le groupe fédéré existe déjà dans la source d'identité configurée.

Accéder à l'assistant de création de groupe

Étapes

Dans un premier temps, accédez à l'assistant de création de groupe.

1. Sélectionnez **GESTION DES ACCÈS > Groupes**.
2. Sélectionnez **Créer un groupe**.

Choisissez un type de groupe

Vous pouvez créer un groupe local ou importer un groupe fédéré.

Étapes

1. Sélectionnez l'onglet **Groupe local** pour créer un groupe local ou sélectionnez l'onglet **Groupe fédéré** pour importer un groupe à partir de la source d'identité précédemment configurée.

Si l'authentification unique (SSO) est activée pour votre système StorageGRID , les utilisateurs appartenant à des groupes locaux ne pourront pas se connecter au gestionnaire de locataires, bien qu'ils puissent utiliser des applications clientes pour gérer les ressources du locataire, en fonction des autorisations de groupe.

2. Entrez le nom du groupe.
 - **Groupe local** : saisissez un nom d'affichage et un nom unique. Vous pouvez modifier le nom d'affichage ultérieurement.
 - **Groupe fédéré** : Saisissez le nom unique. Pour Active Directory, le nom unique est le nom associé au sAMAccountName attribut. Pour OpenLDAP, le nom unique est le nom associé au uid attribut.
3. Sélectionnez **Continuer**.

Gérer les autorisations de groupe

Les autorisations de groupe contrôlent les tâches que les utilisateurs peuvent effectuer dans Tenant Manager et l'API Tenant Management.

Étapes

1. Pour le **Mode d'accès**, sélectionnez l'une des options suivantes :
 - **Lecture-écriture** (par défaut) : les utilisateurs peuvent se connecter à Tenant Manager et gérer la configuration du locataire.

- **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent apporter aucune modification ni effectuer aucune opération dans l'API Tenant Manager ou Tenant Management. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.



Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur Lecture seule, l'utilisateur aura un accès en lecture seule à tous les paramètres et fonctionnalités sélectionnés.

2. Cochez la case **Accès root** si les utilisateurs du groupe doivent se connecter au gestionnaire de locataires ou à l'API de gestion des locataires.
3. Sélectionnez **Continuer**.

Définir la politique de groupe Swift

Les utilisateurs de Swift ont besoin d'une autorisation d'administrateur pour s'authentifier dans l'API REST Swift afin de créer des conteneurs et d'ingérer des objets.

1. Cochez la case **Administrateur Swift** si les utilisateurs du groupe doivent utiliser l'API REST Swift pour gérer les conteneurs et les objets.
2. Si vous créez un groupe local, sélectionnez **Continuer**. Si vous créez un groupe fédéré, sélectionnez **Créer un groupe** et **Terminer**.

Ajouter des utilisateurs (groupes locaux uniquement)

Vous pouvez enregistrer le groupe sans ajouter d'utilisateurs, ou vous pouvez éventuellement ajouter des utilisateurs locaux déjà existants.

Étapes

1. Vous pouvez également sélectionner un ou plusieurs utilisateurs locaux pour ce groupe.

Si vous n'avez pas encore créé d'utilisateurs locaux, vous pouvez ajouter ce groupe à l'utilisateur sur la page Utilisateurs. Voir "[Gérer les utilisateurs locaux](#)".

2. Sélectionnez **Créer un groupe** et **Terminer**.

Le groupe que vous avez créé apparaît dans la liste des groupes.

Autorisations de gestion des locataires

Avant de créer un groupe de locataires, réfléchissez aux autorisations que vous souhaitez attribuer à ce groupe. Les autorisations de gestion des locataires déterminent les tâches que les utilisateurs peuvent effectuer à l'aide du gestionnaire de locataires ou de l'API de gestion des locataires. Un utilisateur peut appartenir à un ou plusieurs groupes. Les autorisations sont cumulatives si un utilisateur appartient à plusieurs groupes.

Pour se connecter au gestionnaire de locataires ou utiliser l'API de gestion des locataires, les utilisateurs doivent appartenir à un groupe disposant d'au moins une autorisation. Tous les utilisateurs qui peuvent se connecter peuvent effectuer les tâches suivantes :

- Afficher le tableau de bord
- Changer leur propre mot de passe (pour les utilisateurs locaux)

Pour toutes les autorisations, le paramètre Mode d'accès du groupe détermine si les utilisateurs peuvent modifier les paramètres et effectuer des opérations ou s'ils peuvent uniquement afficher les paramètres et fonctionnalités associés.



Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur Lecture seule, l'utilisateur aura un accès en lecture seule à tous les paramètres et fonctionnalités sélectionnés.

Vous pouvez attribuer les autorisations suivantes à un groupe. Notez que les locataires S3 et les locataires Swift ont des autorisations de groupe différentes.

Autorisation	Description	Détails
Accès root	Fournit un accès complet au gestionnaire de locataires et à l'API de gestion des locataires.	Les utilisateurs Swift doivent disposer de l'autorisation d'accès root pour se connecter au compte locataire.
Administrateur	Locataires rapides seulement. Fournit un accès complet aux conteneurs et objets Swift pour ce compte locataire	Les utilisateurs Swift doivent disposer de l'autorisation d'administrateur Swift pour effectuer des opérations avec l'API REST Swift.
Gérez vos propres identifiants S3	Permet aux utilisateurs de créer et de supprimer leurs propres clés d'accès S3.	Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu STOCKAGE (S3) > Mes clés d'accès S3 .
Voir tous les seaux	<ul style="list-style-type: none"> • Locataires S3 * : permet aux utilisateurs d'afficher tous les buckets et configurations de buckets. • Locataires Swift * : permet aux utilisateurs Swift d'afficher tous les conteneurs et configurations de conteneurs à l'aide de l'API de gestion des locataires. 	<p>Les utilisateurs qui ne disposent pas de l'autorisation Afficher tous les buckets ou Gérer tous les buckets ne voient pas l'option de menu Buckets.</p> <p>Cette autorisation est remplacée par l'autorisation Gérer tous les buckets. Cela n'affecte pas les stratégies de groupe ou de compartiment S3 utilisées par les clients S3 ou la console S3.</p> <p>Vous ne pouvez attribuer cette autorisation qu'aux groupes Swift à partir de l'API de gestion des locataires. Vous ne pouvez pas attribuer cette autorisation aux groupes Swift à l'aide du gestionnaire de locataires.</p>

Autorisation	Description	Détails
Gérer tous les compartiments	<ul style="list-style-type: none"> Locataires S3 * : permet aux utilisateurs d'utiliser le gestionnaire de locataires et l'API de gestion des locataires pour créer et supprimer des compartiments S3 et pour gérer les paramètres de tous les compartiments S3 du compte de locataire, quels que soient les compartiments S3 ou les stratégies de groupe. Locataires Swift * : permet aux utilisateurs Swift de contrôler la cohérence des conteneurs Swift à l'aide de l'API de gestion des locataires. 	<p>Les utilisateurs qui ne disposent pas de l'autorisation Afficher tous les buckets ou Gérer tous les buckets ne voient pas l'option de menu Buckets.</p> <p>Cette autorisation remplace l'autorisation Afficher tous les buckets. Cela n'affecte pas les stratégies de groupe ou de compartiment S3 utilisées par les clients S3 ou la console S3.</p> <p>Vous ne pouvez attribuer cette autorisation qu'aux groupes Swift à partir de l'API de gestion des locataires. Vous ne pouvez pas attribuer cette autorisation aux groupes Swift à l'aide du gestionnaire de locataires.</p>
Gérer les points de terminaison	Permet aux utilisateurs d'utiliser Tenant Manager ou l'API Tenant Management pour créer ou modifier des points de terminaison de service de plateforme, qui sont utilisés comme destination pour les services de plateforme StorageGRID .	Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu Points de terminaison des services de plateforme .
Utiliser l'onglet Console S3	Associée à l'autorisation Afficher tous les buckets ou Gérer tous les buckets, cette option permet aux utilisateurs d'afficher et de gérer les objets à partir de l'onglet Console S3 sur la page de détails d'un bucket.	

Gérer les groupes

Gérez vos groupes de locataires selon vos besoins pour afficher, modifier ou dupliquer un groupe, et bien plus encore.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#) .

Afficher ou modifier le groupe


Vous pouvez afficher et modifier les informations de base et les détails de chaque groupe.

Étapes

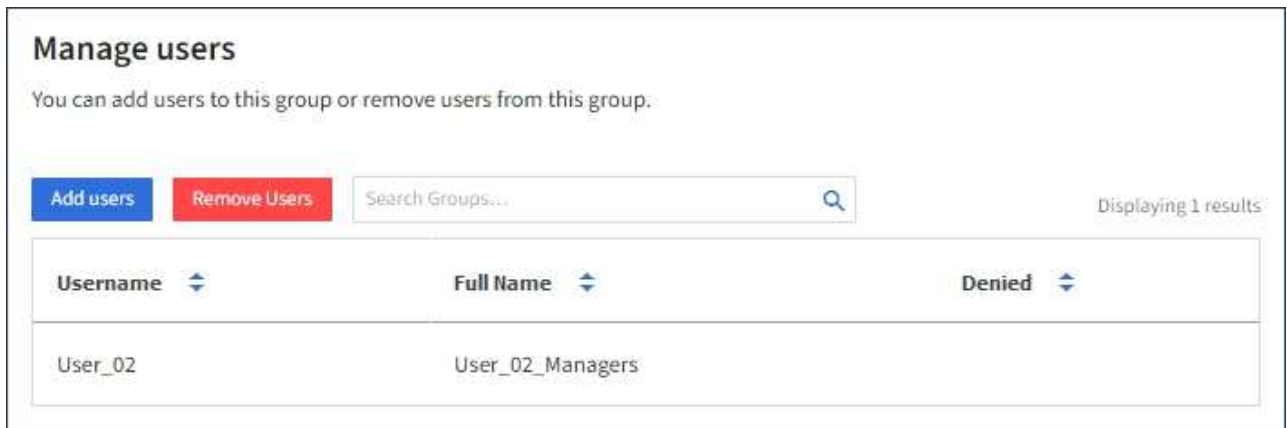
- Sélectionnez **GESTION DES ACCÈS > Groupes**.
- Consultez les informations fournies sur la page Groupes, qui répertorie les informations de base pour tous les groupes locaux et fédérés pour ce compte locataire.

Si le compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous

visualisez les groupes sur la grille source du locataire :

- Un message de bannière indique que si vous modifiez ou supprimez un groupe, vos modifications ne seront pas synchronisées avec l'autre grille.
 - Si nécessaire, un message de bannière indique si les groupes n'ont pas été clonés sur le locataire sur la grille de destination. Tu peux [réessayer un clonage de groupe](#) ça a échoué.
3. Si vous souhaitez modifier le nom du groupe :
- a. Cochez la case correspondant au groupe.
 - b. Sélectionnez **Actions > Modifier le nom du groupe**.
 - c. Entrez le nouveau nom.
 - d. Sélectionnez **Enregistrer les modifications**.
4. Si vous souhaitez afficher plus de détails ou apporter des modifications supplémentaires, effectuez l'une des opérations suivantes :
- Sélectionnez le nom du groupe.
 - Cochez la case correspondant au groupe, puis sélectionnez **Actions > Afficher les détails du groupe**.
5. Consultez la section Présentation, qui affiche les informations suivantes pour chaque groupe :
- Nom d'affichage
 - Nom unique
 - Type
 - Mode d'accès
 - Autorisations
 - Politique S3
 - Nombre d'utilisateurs dans ce groupe
 - Champs supplémentaires si le compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous visualisez le groupe sur la grille source du locataire :
 - Statut du clonage, soit **Succès** soit **Échec**
 - Une bannière bleue indiquant que si vous modifiez ou supprimez ce groupe, vos modifications ne seront pas synchronisées avec l'autre grille.
6. Modifiez les paramètres du groupe selon vos besoins. Voir "[Créer des groupes pour un locataire S3](#)" et "[Créer des groupes pour un locataire Swift](#)" pour plus de détails sur ce qu'il faut saisir.
- a. Dans la section Aperçu, modifiez le nom d'affichage en sélectionnant le nom ou l'icône de modification  .
 - b. Dans l'onglet **Autorisations de groupe**, mettez à jour les autorisations et sélectionnez **Enregistrer les modifications**.
 - c. Dans l'onglet **Stratégie de groupe**, apportez les modifications nécessaires et sélectionnez **Enregistrer les modifications**.
 - Si vous modifiez un groupe S3, sélectionnez éventuellement une autre stratégie de groupe S3 ou saisissez la chaîne JSON d'une stratégie personnalisée, selon vos besoins.
 - Si vous modifiez un groupe Swift, cochez ou décochez éventuellement la case **Administrateur Swift**.
7. Pour ajouter un ou plusieurs utilisateurs locaux existants au groupe :

- a. Sélectionnez l'onglet Utilisateurs.



Username	Full Name	Denied
User_02	User_02_Managers	

- b. Sélectionnez **Ajouter des utilisateurs**.

- c. Sélectionnez les utilisateurs existants que vous souhaitez ajouter, puis sélectionnez **Ajouter des utilisateurs**.

Un message de réussite apparaît dans le coin supérieur droit.

8. Pour supprimer les utilisateurs locaux du groupe :

- a. Sélectionnez l'onglet Utilisateurs.

- b. Sélectionnez **Supprimer les utilisateurs**.

- c. Sélectionnez les utilisateurs que vous souhaitez supprimer, puis sélectionnez **Supprimer les utilisateurs**.

Un message de réussite apparaît dans le coin supérieur droit.

9. Confirmez que vous avez sélectionné **Enregistrer les modifications** pour chaque section que vous avez modifiée.

Groupe en double

Vous pouvez dupliquer un groupe existant pour créer de nouveaux groupes plus rapidement.



Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous dupliquez un groupe à partir de la grille source du locataire, le groupe dupliqué sera cloné sur la grille de destination du locataire.

Étapes

1. Sélectionnez **GESTION DES ACCÈS > Groupes**.
2. Cochez la case correspondant au groupe que vous souhaitez dupliquer.
3. Sélectionnez **Actions > Dupliquer le groupe**.
4. Voir "[Créer des groupes pour un locataire S3](#)" ou "[Créer des groupes pour un locataire Swift](#)" pour plus de détails sur ce qu'il faut saisir.
5. Sélectionnez **Créer un groupe**.

Réessayer le clonage du groupe

Pour réessayer un clonage qui a échoué :

1. Sélectionnez chaque groupe qui indique (*Échec du clonage*) sous le nom du groupe.
2. Sélectionnez **Actions** > **Cloner les groupes**.
3. Affichez l'état de l'opération de clonage à partir de la page de détails de chaque groupe que vous clonez.

Pour plus d'informations, voir "[Cloner des groupes de locataires et des utilisateurs](#)".

Supprimer un ou plusieurs groupes

Vous pouvez supprimer un ou plusieurs groupes. Tous les utilisateurs appartenant uniquement à un groupe supprimé ne pourront plus se connecter au gestionnaire de locataires ni utiliser le compte de locataire.



Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous supprimez un groupe, StorageGRID ne supprimera pas le groupe correspondant sur l'autre grille. Si vous devez conserver ces informations synchronisées, vous devez supprimer le même groupe des deux grilles.

Étapes

1. Sélectionnez **GESTION DES ACCÈS** > **Groupes**.
2. Cochez la case correspondant à chaque groupe que vous souhaitez supprimer.
3. Sélectionnez **Actions** > **Supprimer le groupe** ou **Actions** > **Supprimer les groupes**.

Une boîte de dialogue de confirmation apparaît.

4. Sélectionnez **Supprimer le groupe** ou **Supprimer les groupes**.

Gérer les utilisateurs locaux

Vous pouvez créer des utilisateurs locaux et les affecter à des groupes locaux pour déterminer les fonctionnalités auxquelles ces utilisateurs peuvent accéder. Le gestionnaire de locataires comprend un utilisateur local prédéfini, nommé « root ». Bien que vous puissiez ajouter et supprimer des utilisateurs locaux, vous ne pouvez pas supprimer l'utilisateur root.



Si l'authentification unique (SSO) est activée pour votre système StorageGRID, les utilisateurs locaux ne pourront pas se connecter au gestionnaire de locataires ou à l'API de gestion des locataires, bien qu'ils puissent utiliser des applications clientes pour accéder aux ressources du locataire, en fonction des autorisations de groupe.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Autorisation d'accès root](#)".
- Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, vous avez examiné le flux de travail et les considérations pour "[clonage de groupes de locataires et d'utilisateurs](#)", et vous êtes connecté à la grille source du locataire.

Créer un utilisateur local

Vous pouvez créer un utilisateur local et l'affecter à un ou plusieurs groupes locaux pour contrôler ses autorisations d'accès.

Les utilisateurs S3 qui n'appartiennent à aucun groupe ne disposent pas d'autorisations de gestion ni de stratégies de groupe S3 qui leur sont appliquées. Ces utilisateurs peuvent bénéficier d'un accès au compartiment S3 accordé via une politique de compartiment.

Les utilisateurs Swift qui n'appartiennent à aucun groupe ne disposent pas d'autorisations de gestion ni d'accès au conteneur Swift.

Accéder à l'assistant de création d'utilisateur

Étapes

1. Sélectionnez **GESTION DES ACCÈS > Utilisateurs**.

Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, une bannière bleue indique qu'il s'agit de la grille source du locataire. Tous les utilisateurs locaux que vous créez sur cette grille seront clonés sur l'autre grille de la connexion.

2. Sélectionnez **Créer un utilisateur**.

Entrez les informations d'identification

Étapes

1. Pour l'étape **Saisir les informations d'identification de l'utilisateur**, remplissez les champs suivants.

Champ	Description
Nom et prénom	Le nom complet de cet utilisateur, par exemple, le prénom et le nom d'une personne ou le nom d'une application.

Champ	Description
Nom d'utilisateur	<p>Le nom que cet utilisateur utilisera pour se connecter. Les noms d'utilisateur doivent être uniques et ne peuvent pas être modifiés.</p> <p>Remarque : si votre compte de locataire dispose de l'autorisation Utiliser la connexion à la fédération de grille, une erreur de clonage se produira si le même Nom d'utilisateur existe déjà pour le locataire sur la grille de destination.</p>
Mot de passe et confirmation du mot de passe	Le mot de passe que l'utilisateur utilisera initialement lors de la connexion.
Refuser l'accès	<p>Sélectionnez Oui pour empêcher cet utilisateur de se connecter au compte locataire, même s'il appartient toujours à un ou plusieurs groupes.</p> <p>Par exemple, sélectionnez Oui pour suspendre temporairement la possibilité pour un utilisateur de se connecter.</p>

2. Sélectionnez **Continuer**.

Affecter à des groupes

Étapes

1. Affectez l'utilisateur à un ou plusieurs groupes locaux pour déterminer les tâches qu'il peut effectuer.

L'affectation d'un utilisateur à des groupes est facultative. Si vous préférez, vous pouvez sélectionner des utilisateurs lorsque vous créez ou modifiez des groupes.

Les utilisateurs qui n'appartiennent à aucun groupe n'auront aucune autorisation de gestion. Les autorisations sont cumulatives. Les utilisateurs disposeront de toutes les autorisations pour tous les groupes auxquels ils appartiennent. Voir "[Autorisations de gestion des locataires](#)".

2. Sélectionnez **Créer un utilisateur**.

Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous êtes sur la grille source du locataire, le nouvel utilisateur local est cloné sur la grille de destination du locataire. **Succès** apparaît comme **Statut de clonage** dans la section Présentation de la page de détails de l'utilisateur.


3. Sélectionnez **Terminer** pour revenir à la page Utilisateurs.

Afficher ou modifier l'utilisateur local

Étapes

1. Sélectionnez **GESTION DES ACCÈS > Utilisateurs**.
2. Consultez les informations fournies sur la page Utilisateurs, qui répertorie les informations de base pour tous les utilisateurs locaux et fédérés de ce compte locataire.

Si le compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous visualisez l'utilisateur sur la grille source du locataire :

- Un message de bannière indique que si vous modifiez ou supprimez un utilisateur, vos modifications ne seront pas synchronisées avec l'autre grille.
 - Si nécessaire, un message de bannière indique si les utilisateurs n'ont pas été clonés sur le locataire sur la grille de destination. Vous pouvez [réessayer un clone d'utilisateur qui a échoué](#) .
3. Si vous souhaitez modifier le nom complet de l'utilisateur :
 - a. Cochez la case correspondant à l'utilisateur.
 - b. Sélectionnez **Actions > Modifier le nom complet**.
 - c. Entrez le nouveau nom.
 - d. Sélectionnez **Enregistrer les modifications**.
 4. Si vous souhaitez afficher plus de détails ou apporter des modifications supplémentaires, effectuez l'une des opérations suivantes :
 - Sélectionnez le nom d'utilisateur.
 - Cochez la case correspondant à l'utilisateur, puis sélectionnez **Actions > Afficher les détails de l'utilisateur**.
 5. Consultez la section Présentation, qui affiche les informations suivantes pour chaque utilisateur :
 - Nom et prénom
 - Nom d'utilisateur
 - Type d'utilisateur
 - Accès refusé
 - Mode d'accès
 - Adhésion au groupe
 - Champs supplémentaires si le compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous visualisez l'utilisateur sur la grille source du locataire :
 - Statut du clonage, soit **Succès** soit **Échec**
 - Une bannière bleue indiquant que si vous modifiez cet utilisateur, vos modifications ne seront pas synchronisées avec l'autre grille.
 6. Modifiez les paramètres utilisateur selon vos besoins. Voir [Créer un utilisateur local](#) pour plus de détails sur ce qu'il faut saisir.
 - a. Dans la section Aperçu, modifiez le nom complet en sélectionnant le nom ou l'icône de modification  .

Vous ne pouvez pas changer le nom d'utilisateur.
 - b. Dans l'onglet **Mot de passe**, modifiez le mot de passe de l'utilisateur et sélectionnez **Enregistrer les modifications**.
 - c. Dans l'onglet **Accès**, sélectionnez **Non** pour autoriser l'utilisateur à se connecter ou sélectionnez **Oui** pour empêcher l'utilisateur de se connecter. Ensuite, sélectionnez **Enregistrer les modifications**.
 - d. Dans l'onglet **Clés d'accès**, sélectionnez **Créer une clé** et suivez les instructions pour "[créer les clés d'accès S3 d'un autre utilisateur](#)" .
 - e. Dans l'onglet **Groupe**s, sélectionnez **Modifier les groupes** pour ajouter l'utilisateur à des groupes ou supprimer l'utilisateur des groupes. Ensuite, sélectionnez **Enregistrer les modifications**.
 7. Confirmez que vous avez sélectionné **Enregistrer les modifications** pour chaque section que vous avez modifiée.

Utilisateur local en double

Vous pouvez dupliquer un utilisateur local pour créer un nouvel utilisateur plus rapidement.



Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous dupliquez un utilisateur à partir de la grille source du locataire, l'utilisateur dupliqué sera cloné sur la grille de destination du locataire.

Étapes

1. Sélectionnez **GESTION DES ACCÈS > Utilisateurs**.
2. Cochez la case correspondant à l'utilisateur que vous souhaitez dupliquer.
3. Sélectionnez **Actions > Dupliquer l'utilisateur**.
4. Voir [Créer un utilisateur local](#) pour plus de détails sur ce qu'il faut saisir.
5. Sélectionnez **Créer un utilisateur**.

Réessayer le clonage de l'utilisateur

Pour réessayer un clonage qui a échoué :

1. Sélectionnez chaque utilisateur qui indique (*Échec du clonage*) sous le nom d'utilisateur.
2. Sélectionnez **Actions > Cloner les utilisateurs**.
3. Affichez l'état de l'opération de clonage à partir de la page de détails de chaque utilisateur que vous clonez.

Pour plus d'informations, voir "[Cloner des groupes de locataires et des utilisateurs](#)".

Supprimer un ou plusieurs utilisateurs locaux

Vous pouvez supprimer définitivement un ou plusieurs utilisateurs locaux qui n'ont plus besoin d'accéder au compte locataire StorageGRID .



Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous supprimez un utilisateur local, StorageGRID ne supprimera pas l'utilisateur correspondant sur l'autre grille. Si vous devez conserver ces informations synchronisées, vous devez supprimer le même utilisateur des deux grilles.



Vous devez utiliser la source d'identité fédérée pour supprimer les utilisateurs fédérés.

Étapes

1. Sélectionnez **GESTION DES ACCÈS > Utilisateurs**.
2. Cochez la case correspondant à chaque utilisateur que vous souhaitez supprimer.
3. Sélectionnez **Actions > Supprimer l'utilisateur** ou **Actions > Supprimer les utilisateurs**.

Une boîte de dialogue de confirmation apparaît.

4. Sélectionnez **Supprimer l'utilisateur** ou **Supprimer les utilisateurs**.

Gérer les clés d'accès S3

Gérer les clés d'accès S3

Chaque utilisateur d'un compte locataire S3 doit disposer d'une clé d'accès pour stocker et récupérer des objets dans le système StorageGRID . Une clé d'accès se compose d'un ID de clé d'accès et d'une clé d'accès secrète.

Les clés d'accès S3 peuvent être gérées comme suit :

- Les utilisateurs disposant de l'autorisation **Gérer vos propres informations d'identification S3** peuvent créer ou supprimer leurs propres clés d'accès S3.
- Les utilisateurs disposant de l'autorisation **Accès root** peuvent gérer les clés d'accès pour le compte root S3 et tous les autres utilisateurs. Les clés d'accès racine fournissent un accès complet à tous les compartiments et objets du locataire, sauf si elles sont explicitement désactivées par une stratégie de compartiment.

StorageGRID prend en charge l'authentification Signature Version 2 et Signature Version 4. L'accès entre comptes n'est pas autorisé, sauf s'il est explicitement activé par une politique de compartiment.

Créez vos propres clés d'accès S3

Si vous utilisez un locataire S3 et que vous disposez de l'autorisation appropriée, vous pouvez créer vos propres clés d'accès S3. Vous devez disposer d'une clé d'accès pour accéder à vos buckets et objets.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérez vos propres informations d'identification S3 ou autorisation d'accès root"](#) .

À propos de cette tâche

Vous pouvez créer une ou plusieurs clés d'accès S3 qui vous permettent de créer et de gérer des buckets pour votre compte locataire. Après avoir créé une nouvelle clé d'accès, mettez à jour l'application avec votre nouvel ID de clé d'accès et votre clé d'accès secrète. Pour des raisons de sécurité, ne créez pas plus de clés que nécessaire et supprimez les clés que vous n'utilisez pas. Si vous n'avez qu'une seule clé et qu'elle est sur le point d'expirer, créez une nouvelle clé avant l'expiration de l'ancienne, puis supprimez l'ancienne.

Chaque clé peut avoir une date d'expiration spécifique ou aucune date d'expiration. Suivez ces directives concernant le délai d'expiration :

- Définissez une heure d'expiration pour vos clés afin de limiter votre accès à une certaine période. La définition d'un délai d'expiration court peut vous aider à réduire vos risques si votre ID de clé d'accès et votre clé d'accès secrète sont accidentellement exposés. Les clés expirées sont supprimées automatiquement.
- Si le risque de sécurité dans votre environnement est faible et que vous n'avez pas besoin de créer périodiquement de nouvelles clés, vous n'avez pas besoin de définir un délai d'expiration pour vos clés. Si vous décidez ultérieurement de créer de nouvelles clés, supprimez les anciennes clés manuellement.



Les compartiments et objets S3 appartenant à votre compte sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichées pour votre compte dans le gestionnaire de locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites tourner régulièrement les clés d'accès, supprimez toutes les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **STOCKAGE (S3) > Mes clés d'accès**.

La page Mes clés d'accès apparaît et répertorie toutes les clés d'accès existantes.

2. Sélectionnez **Créer une clé**.

3. Effectuez l'une des opérations suivantes :

- Sélectionnez **Ne pas définir de délai d'expiration** pour créer une clé qui n'expirera pas. (Défaut)
- Sélectionnez **Définir une heure d'expiration** et définissez la date et l'heure d'expiration.



La date d'expiration peut être au maximum de cinq ans à compter de la date actuelle. Le délai d'expiration peut être d'au moins une minute à partir de l'heure actuelle.

4. Sélectionnez **Créer une clé d'accès**.

La boîte de dialogue Télécharger la clé d'accès s'affiche, répertoriant votre ID de clé d'accès et votre clé d'accès secrète.

5. Copiez l'ID de clé d'accès et la clé d'accès secrète dans un emplacement sûr ou sélectionnez **Télécharger .csv** pour enregistrer un fichier de feuille de calcul contenant l'ID de clé d'accès et la clé d'accès secrète.



Ne fermez pas cette boîte de dialogue tant que vous n'avez pas copié ou téléchargé ces informations. Vous ne pouvez pas copier ou télécharger des clés une fois la boîte de dialogue fermée.

6. Sélectionnez **Terminer**.

La nouvelle clé est répertoriée sur la page Mes clés d'accès.

7. Si votre compte de locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, utilisez éventuellement l'API de gestion des locataires pour cloner manuellement les clés d'accès S3 du locataire sur la grille source vers le locataire sur la grille de destination. Voir "[Cloner les clés d'accès S3 à l'aide de l'API](#)".

Afficher vos clés d'accès S3

Si vous utilisez un locataire S3 et que vous avez le "[autorisation appropriée](#)", vous pouvez afficher une liste de vos clés d'accès S3. Vous pouvez trier la liste par heure d'expiration, afin de déterminer quelles clés expireront bientôt. Au besoin, vous pouvez "[créer de nouvelles clés](#)" ou "[touches de suppression](#)" que vous n'utilisez plus.



Les compartiments et objets S3 appartenant à votre compte sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichées pour votre compte dans le gestionnaire de locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites tourner régulièrement les clés d'accès, supprimez toutes les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs disposant de l'autorisation Gérer vos propres informations d'identification S3 ["autorisation"](#).

Étapes

1. Sélectionnez **STOCKAGE (S3) > Mes clés d'accès**.
2. Depuis la page Mes clés d'accès, triez toutes les clés d'accès existantes par **Délai d'expiration** ou **ID de clé d'accès**.
3. Selon vos besoins, créez de nouvelles clés ou supprimez celles que vous n'utilisez plus.

Si vous créez de nouvelles clés avant l'expiration des clés existantes, vous pouvez commencer à utiliser les nouvelles clés sans perdre temporairement l'accès aux objets du compte.

Les clés expirées sont supprimées automatiquement.

Supprimez vos propres clés d'accès S3

Si vous utilisez un locataire S3 et que vous disposez de l'autorisation appropriée, vous pouvez supprimer vos propres clés d'accès S3. Une fois qu'une clé d'accès est supprimée, elle ne peut plus être utilisée pour accéder aux objets et aux buckets du compte locataire.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Gérez vos propres autorisations d'informations d'identification S3"](#).



Les compartiments et objets S3 appartenant à votre compte sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichées pour votre compte dans le gestionnaire de locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites tourner régulièrement les clés d'accès, supprimez toutes les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **STOCKAGE (S3) > Mes clés d'accès**.
2. Sur la page Mes clés d'accès, cochez la case correspondant à chaque clé d'accès que vous souhaitez supprimer.
3. Sélectionnez **Touche Suppr.**
4. Dans la boîte de dialogue de confirmation, sélectionnez **Touche Supprimer**.

Un message de confirmation apparaît dans le coin supérieur droit de la page.

Créer les clés d'accès S3 d'un autre utilisateur

Si vous utilisez un locataire S3 et que vous disposez de l'autorisation appropriée, vous pouvez créer des clés d'accès S3 pour d'autres utilisateurs, tels que les applications qui ont besoin d'accéder aux buckets et aux objets.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#) .

À propos de cette tâche

Vous pouvez créer une ou plusieurs clés d'accès S3 pour d'autres utilisateurs afin qu'ils puissent créer et gérer des buckets pour leur compte locataire. Après avoir créé une nouvelle clé d'accès, mettez à jour l'application avec le nouvel ID de clé d'accès et la clé d'accès secrète. Pour des raisons de sécurité, ne créez pas plus de clés que nécessaire pour l'utilisateur et supprimez les clés qui ne sont pas utilisées. Si vous n'avez qu'une seule clé et qu'elle est sur le point d'expirer, créez une nouvelle clé avant l'expiration de l'ancienne, puis supprimez l'ancienne.

Chaque clé peut avoir une date d'expiration spécifique ou aucune date d'expiration. Suivez ces directives concernant le délai d'expiration :

- Définissez un délai d'expiration pour les clés afin de limiter l'accès de l'utilisateur à une certaine période. La définition d'un délai d'expiration court peut aider à réduire les risques si l'ID de clé d'accès et la clé d'accès secrète sont accidentellement exposés. Les clés expirées sont supprimées automatiquement.
- Si le risque de sécurité dans votre environnement est faible et que vous n'avez pas besoin de créer périodiquement de nouvelles clés, vous n'avez pas besoin de définir un délai d'expiration pour les clés. Si vous décidez ultérieurement de créer de nouvelles clés, supprimez les anciennes clés manuellement.



Les compartiments et objets S3 appartenant à un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichées pour cet utilisateur dans le gestionnaire de locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites tourner régulièrement les clés d'accès, supprimez toutes les clés inutilisées du compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **GESTION DES ACCÈS > Utilisateurs**.
2. Sélectionnez l'utilisateur dont vous souhaitez gérer les clés d'accès S3.

La page de détails de l'utilisateur apparaît.

3. Sélectionnez **Clés d'accès**, puis sélectionnez **Créer une clé**.
4. Effectuez l'une des opérations suivantes :
 - Sélectionnez **Ne pas définir de délai d'expiration** pour créer une clé qui n'expire pas. (Défaut)
 - Sélectionnez **Définir une heure d'expiration** et définissez la date et l'heure d'expiration.



La date d'expiration peut être au maximum de cinq ans à compter de la date actuelle. Le délai d'expiration peut être d'au moins une minute à partir de l'heure actuelle.

5. Sélectionnez **Créer une clé d'accès**.

La boîte de dialogue Télécharger la clé d'accès s'affiche, répertoriant l'ID de la clé d'accès et la clé d'accès secrète.

6. Copiez l'ID de clé d'accès et la clé d'accès secrète dans un emplacement sûr ou sélectionnez **Télécharger .csv** pour enregistrer un fichier de feuille de calcul contenant l'ID de clé d'accès et la clé d'accès secrète.



Ne fermez pas cette boîte de dialogue tant que vous n'avez pas copié ou téléchargé ces informations. Vous ne pouvez pas copier ou télécharger des clés une fois la boîte de dialogue fermée.

7. Sélectionnez **Terminer**.

La nouvelle clé est répertoriée dans l'onglet Clés d'accès de la page des détails de l'utilisateur.

8. Si votre compte de locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, utilisez éventuellement l'API de gestion des locataires pour cloner manuellement les clés d'accès S3 du locataire sur la grille source vers le locataire sur la grille de destination. Voir "[Cloner les clés d'accès S3 à l'aide de l'API](#)".

Afficher les clés d'accès S3 d'un autre utilisateur

Si vous utilisez un locataire S3 et que vous disposez des autorisations appropriées, vous pouvez afficher les clés d'accès S3 d'un autre utilisateur. Vous pouvez trier la liste par heure d'expiration afin de déterminer quelles clés expireront bientôt. Selon vos besoins, vous pouvez créer de nouvelles clés et supprimer des clés qui ne sont plus utilisées.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous avez le "[Autorisation d'accès root](#)".



Les compartiments et objets S3 appartenant à un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichées pour cet utilisateur dans le gestionnaire de locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites tourner régulièrement les clés d'accès, supprimez toutes les clés inutilisées du compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **GESTION DES ACCÈS > Utilisateurs**.
2. Depuis la page Utilisateurs, sélectionnez l'utilisateur dont vous souhaitez afficher les clés d'accès S3.
3. Depuis la page Détails de l'utilisateur, sélectionnez **Clés d'accès**.
4. Trier les clés par **Délai d'expiration** ou **ID de clé d'accès**.
5. Selon les besoins, créez de nouvelles clés et supprimez manuellement les clés qui ne sont plus utilisées.

Si vous créez de nouvelles clés avant l'expiration des clés existantes, l'utilisateur peut commencer à utiliser les nouvelles clés sans perdre temporairement l'accès aux objets du compte.

Les clés expirées sont supprimées automatiquement.

Informations connexes

- ["Créer les clés d'accès S3 d'un autre utilisateur"](#)
- ["Supprimer les clés d'accès S3 d'un autre utilisateur"](#)

Supprimer les clés d'accès S3 d'un autre utilisateur

Si vous utilisez un locataire S3 et que vous disposez des autorisations appropriées, vous pouvez supprimer les clés d'accès S3 d'un autre utilisateur. Une fois qu'une clé d'accès est supprimée, elle ne peut plus être utilisée pour accéder aux objets et aux buckets du compte locataire.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès root"](#).



Les compartiments et objets S3 appartenant à un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichées pour cet utilisateur dans le gestionnaire de locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites tourner régulièrement les clés d'accès, supprimez toutes les clés inutilisées du compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **GESTION DES ACCÈS > Utilisateurs**.
2. Depuis la page Utilisateurs, sélectionnez l'utilisateur dont vous souhaitez gérer les clés d'accès S3.
3. Sur la page Détails de l'utilisateur, sélectionnez **Clés d'accès**, puis cochez la case correspondant à chaque clé d'accès que vous souhaitez supprimer.
4. Sélectionnez **Actions > Supprimer la clé sélectionnée**.
5. Dans la boîte de dialogue de confirmation, sélectionnez **Touche Supprimer**.

Un message de confirmation apparaît dans le coin supérieur droit de la page.

Gérer les buckets S3

Créer un bucket S3

Vous pouvez utiliser Tenant Manager pour créer des compartiments S3 pour les données d'objet.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs disposant de l'accès Root ou Gérer tous les buckets ["autorisation"](#). Ces autorisations remplacent les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.



Les autorisations permettant de définir ou de modifier les propriétés de verrouillage d'objet S3 des compartiments ou des objets peuvent être accordées par ["politique de compartiment"](#) ou ["politique de groupe"](#).

- Si vous prévoyez d'activer le verrouillage d'objet S3 pour un bucket, un administrateur de grille a activé le paramètre global de verrouillage d'objet S3 pour le système StorageGRID et vous avez examiné les exigences pour les buckets et objets de verrouillage d'objet S3.
- Si chaque locataire dispose de 5 000 buckets, chaque nœud de stockage de la grille dispose d'un minimum de 64 Go de RAM.



Chaque grille peut contenir un maximum de 100 000 buckets.

Accéder à l'assistant

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
2. Sélectionnez **Créer un bucket**.

Entrez les détails

Étapes

1. Saisissez les détails du bucket.

Champ	Description
Nom du bucket	<p>Un nom pour le bucket qui respecte ces règles :</p> <ul style="list-style-type: none"> • Doit être unique sur chaque système StorageGRID (pas seulement unique au sein du compte locataire). • Doit être conforme au DNS. • Doit contenir au moins 3 et pas plus de 63 caractères. • Chaque étiquette doit commencer et se terminer par une lettre minuscule ou un chiffre et ne peut utiliser que des lettres minuscules, des chiffres et des traits d'union. • Ne doit pas contenir de points dans les demandes de style hébergé virtuellement. Les points entraîneront des problèmes avec la vérification du certificat générique du serveur. <p>Pour plus d'informations, consultez le "Documentation d'Amazon Web Services (AWS) sur les règles de dénomination des buckets".</p> <p>Remarque : vous ne pouvez pas modifier le nom du bucket après l'avoir créé.</p>
Région	<p>La région du seau.</p> <p>Votre administrateur StorageGRID gère les régions disponibles. La région d'un bucket peut affecter la politique de protection des données appliquée aux objets. Par défaut, tous les buckets sont créés dans le us-east-1 région.</p> <p>Remarque : vous ne pouvez pas modifier la région après avoir créé le bucket.</p>

2. Sélectionnez **Continuer**.

Étapes

1. Vous pouvez également activer le contrôle de version des objets pour le bucket.

Activez le contrôle de version des objets si vous souhaitez stocker chaque version de chaque objet dans ce bucket. Vous pouvez ensuite récupérer les versions précédentes d'un objet selon vos besoins. Vous devez activer le contrôle de version des objets si le bucket doit être utilisé pour la réplication inter-grille.

2. Si le paramètre global de verrouillage d'objet S3 est activé, activez éventuellement le verrouillage d'objet S3 pour que le bucket stocke les objets à l'aide d'un modèle WORM (écriture unique, lecture multiple).

Activez le verrouillage d'objet S3 pour un bucket uniquement si vous devez conserver des objets pendant une durée déterminée, par exemple pour répondre à certaines exigences réglementaires. S3 Object Lock est un paramètre permanent qui vous aide à empêcher la suppression ou l'écrasement d'objets pendant une durée déterminée ou indéfiniment.



Une fois le paramètre de verrouillage d'objet S3 activé pour un bucket, il ne peut pas être désactivé. Toute personne disposant des autorisations appropriées peut ajouter des objets à ce bucket qui ne peuvent pas être modifiés. Vous ne pourrez peut-être pas supprimer ces objets ni le bucket lui-même.

Si vous activez le verrouillage d'objet S3 pour un bucket, le contrôle de version du bucket est activé automatiquement.

3. Si vous avez sélectionné **Activer le verrouillage d'objet S3**, activez éventuellement la **Rétention par défaut** pour ce bucket.



Votre administrateur de réseau doit vous donner la permission de "[utiliser les fonctionnalités spécifiques de S3 Object Lock](#)".

Lorsque la **rétention par défaut** est activée, les nouveaux objets ajoutés au bucket seront automatiquement protégés contre la suppression ou l'écrasement. Le paramètre **Conservation par défaut** ne s'applique pas aux objets qui ont leurs propres périodes de conservation.

- a. Si la **Rétention par défaut** est activée, spécifiez un **Mode de rétention par défaut** pour le bucket.

Mode de rétention par défaut	Description
Gouvernance	<ul style="list-style-type: none">• Les utilisateurs avec le <code>s3:BypassGovernanceRetention</code> l'autorisation peut utiliser le <code>x-amz-bypass-governance-retention: true</code> en-tête de demande pour contourner les paramètres de conservation.• Ces utilisateurs peuvent supprimer une version d'objet avant que sa date de conservation ne soit atteinte.• Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

Mode de rétention par défaut	Description
Conformité	<ul style="list-style-type: none"> • L'objet ne peut pas être supprimé tant que sa date de conservation n'est pas atteinte. • La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être diminuée. • La date de conservation de l'objet ne peut pas être supprimée tant que cette date n'est pas atteinte. <p>Remarque : votre administrateur de réseau doit vous autoriser à utiliser le mode de conformité.</p>

- b. Si la **Conservation par défaut** est activée, spécifiez la **Période de conservation par défaut** pour le bucket.

La **Période de conservation par défaut** indique la durée pendant laquelle les nouveaux objets ajoutés à ce bucket doivent être conservés, à compter du moment où ils sont ingérés. Spécifiez une valeur inférieure ou égale à la période de conservation maximale du locataire, telle que définie par l'administrateur de la grille.

Une période de conservation *maximale*, qui peut être une valeur comprise entre 1 jour et 100 ans, est définie lorsque l'administrateur de la grille crée le locataire. Lorsque vous définissez une période de conservation par défaut, elle ne peut pas dépasser la valeur définie pour la période de conservation maximale. Si nécessaire, demandez à votre administrateur de réseau d'augmenter ou de diminuer la période de conservation maximale.

4. Vous pouvez également sélectionner **Activer la limite de capacité**.

La limite de capacité est la capacité maximale disponible pour les objets de ce bucket. Cette valeur représente une quantité logique (taille de l'objet), et non une quantité physique (taille sur le disque).

Si aucune limite n'est définie, la capacité de ce bucket est illimitée. Consultez ["Utilisation de la limite de capacité"](#) pour plus d'informations.

5. Sélectionnez **Créer un bucket**.

Le bucket est créé et ajouté au tableau sur la page Buckets.

6. En option, sélectionnez **Accéder à la page des détails du bucket** pour ["afficher les détails du godet"](#) et effectuer une configuration supplémentaire.

Afficher les détails du godet

Vous pouvez afficher les buckets dans votre compte locataire.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Accès root, autorisation Gérer tous les buckets ou Afficher tous les buckets"](#). Ces autorisations remplacent les paramètres d'autorisation dans les stratégies de groupe ou de compartiment.

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.

La page Buckets apparaît.

2. Consultez le tableau récapitulatif pour chaque compartiment.

Selon vos besoins, vous pouvez trier les informations par colonne ou parcourir la liste en avant et en arrière.



Les valeurs de nombre d'objets, d'espace utilisé et d'utilisation affichées sont des estimations. Ces estimations sont affectées par le moment des ingestions, la connectivité réseau et l'état du nœud. Si le contrôle de version est activé pour les buckets, les versions d'objet supprimées sont incluses dans le nombre d'objets.

Nom

Le nom unique du bucket, qui ne peut pas être modifié.

Fonctionnalités activées

La liste des fonctionnalités activées pour le bucket.

Verrouillage d'objet S3

Si le verrouillage d'objet S3 est activé pour le bucket.

Cette colonne apparaît uniquement si le verrouillage d'objet S3 est activé pour la grille. Cette colonne affiche également des informations sur tous les buckets conformes hérités.

Région

La région du bucket, qui ne peut pas être modifiée. Cette colonne est masquée par défaut.

Nombre d'objets

Le nombre d'objets dans ce bucket. Si le contrôle de version est activé pour les buckets, les versions d'objet non actuelles sont incluses dans cette valeur.

Lorsque des objets sont ajoutés ou supprimés, cette valeur peut ne pas être mise à jour immédiatement.

Espace utilisé

La taille logique de tous les objets dans le bucket. La taille logique n'inclut pas l'espace réel requis pour les copies répliquées ou codées par effacement ou pour les métadonnées de l'objet.

La mise à jour de cette valeur peut prendre jusqu'à 10 minutes.

Usage

Le pourcentage utilisé de la limite de capacité du bucket, si elle a été définie.

La valeur d'utilisation est basée sur des estimations internes et peut être dépassée dans certains cas. Par exemple, StorageGRID vérifie la limite de capacité (si définie) lorsqu'un locataire commence à télécharger des objets et rejette les nouvelles ingestions dans ce bucket si le locataire a dépassé la limite de capacité. Cependant, StorageGRID ne prend pas en compte la taille du téléchargement actuel pour déterminer si la limite de capacité a été dépassée. Si des objets sont supprimés, un locataire peut être temporairement empêché de télécharger de nouveaux objets dans ce bucket jusqu'à ce que l'utilisation de la limite de capacité soit recalculée. Les calculs peuvent prendre 10 minutes ou plus.

Cette valeur indique la taille logique, et non la taille physique nécessaire pour stocker les objets et leurs métadonnées.

Capacité

Si défini, la limite de capacité du bucket.

Date de création

La date et l'heure de création du bucket. Cette colonne est masquée par défaut.

3. Pour afficher les détails d'un bucket spécifique, sélectionnez le nom du bucket dans le tableau.
 - a. Consultez les informations récapitulatives en haut de la page Web pour confirmer les détails du bucket, tels que la région et le nombre d'objets.
 - b. Afficher la barre d'utilisation de la limite de capacité. Si l'utilisation est de 100 % ou proche de 100 %, envisagez d'augmenter la limite ou de supprimer certains objets.
 - c. Si nécessaire, sélectionnez **Supprimer les objets dans le bucket** et **Supprimer le bucket**.



Portez une attention particulière aux avertissements qui s'affichent lorsque vous sélectionnez chacune de ces options. Pour plus d'informations, reportez-vous à :

- ["Supprimer tous les objets d'un bucket"](#)
- ["Supprimer un bucket"](#)(le seau doit être vide)

- d. Affichez ou modifiez les paramètres du bucket dans chacun des onglets selon vos besoins.
 - **Console S3** : Afficher les objets du bucket. Pour plus d'informations, reportez-vous à ["Utiliser la console S3"](#) .
 - **Options du bucket** : afficher ou modifier les paramètres des options. Certains paramètres, tels que le verrouillage d'objet S3, ne peuvent pas être modifiés une fois le bucket créé.
 - ["Gérer la cohérence des buckets"](#)
 - ["Mises à jour de l'heure du dernier accès"](#)
 - ["Limite de capacité"](#)
 - ["Versionnage d'objet"](#)
 - ["Verrouillage d'objet S3"](#)
 - ["Rétention du bucket par défaut"](#)
 - ["Gérer la réplication inter-réseaux"](#)(si autorisé pour le locataire)
 - **Services de la plateforme**:["Gérer les services de la plateforme"](#) (si autorisé pour le locataire)
 - **Accès au bucket** : afficher ou modifier les paramètres des options. Vous devez disposer d'autorisations d'accès spécifiques.
 - Configurez ["Partage des ressources inter-origines \(CORS\)"](#) ainsi, le bucket et les objets qu'il contient seront accessibles aux applications Web dans d'autres domaines.
 - ["Contrôler l'accès des utilisateurs"](#) pour un bucket S3 et les objets dans ce bucket.

Appliquer une balise de stratégie ILM à un bucket

Choisissez une balise de stratégie ILM à appliquer à un bucket en fonction de vos besoins de stockage d'objets.

La politique ILM contrôle où les données de l'objet sont stockées et si elles sont supprimées après une certaine période. Votre administrateur de réseau crée des stratégies ILM et les attribue à des balises de stratégie ILM lors de l'utilisation de plusieurs stratégies actives.



Évitez de réaffecter fréquemment la balise de stratégie d'un bucket. Dans le cas contraire, des problèmes de performances pourraient survenir.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Accès root, autorisation Gérer tous les buckets ou Afficher tous les buckets"](#) . Ces autorisations remplacent les paramètres d'autorisation dans les stratégies de groupe ou de compartiment.

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.

La page Buckets apparaît. Selon vos besoins, vous pouvez trier les informations par colonne ou parcourir la liste en avant et en arrière.

2. Sélectionnez le nom du bucket auquel vous souhaitez attribuer une balise de stratégie ILM.

Vous pouvez également modifier l'attribution de balise de stratégie ILM pour un bucket auquel une balise est déjà attribuée.



Les valeurs affichées pour le nombre d'objets et l'espace utilisé sont des estimations. Ces estimations sont affectées par le moment des ingestions, la connectivité réseau et l'état du nœud. Si le contrôle de version est activé pour les buckets, les versions d'objet supprimées sont incluses dans le nombre d'objets.

3. Dans l'onglet Options du compartiment, développez l'accordéon de balise de stratégie ILM. Cet accordéon n'apparaît que si votre administrateur de grille a activé l'utilisation de balises de stratégie personnalisées.
4. Lisez la description de chaque balise de stratégie pour déterminer quelle balise doit être appliquée au bucket.



La modification de la balise de politique ILM pour un bucket déclenchera la réévaluation ILM de tous les objets du bucket. Si la nouvelle politique conserve les objets pendant une durée limitée, les objets plus anciens seront supprimés.

5. Sélectionnez le bouton radio correspondant à la balise que vous souhaitez attribuer au bucket.
6. Sélectionnez **Enregistrer les modifications**. Une nouvelle balise de compartiment S3 sera définie sur le compartiment avec la clé `NTAP-SG-ILM-BUCKET-TAG` et la valeur du nom de la balise de politique ILM.



Assurez-vous que vos applications S3 ne remplacent pas ou ne suppriment pas accidentellement la nouvelle balise de compartiment. Si cette balise est omise lors de l'application d'un nouveau TagSet au bucket, les objets du bucket seront à nouveau évalués par rapport à la stratégie ILM par défaut.



Définissez et modifiez les balises de stratégie ILM à l'aide uniquement de Tenant Manager ou de l'API Tenant Manager où la balise de stratégie ILM est validée. Ne pas modifier le NTAP-SG-ILM-BUCKET-TAG Balise de stratégie ILM utilisant l'API S3 PutBucketTagging ou l'API S3 DeleteBucketTagging.



La modification de la balise de stratégie attribuée à un bucket a un impact temporaire sur les performances pendant que les objets sont réévalués à l'aide de la nouvelle stratégie ILM.

Gérer la politique de compartiment

Vous pouvez contrôler l'accès des utilisateurs à un compartiment S3 et aux objets de ce compartiment.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#) . Les autorisations Afficher tous les compartiments et Gérer tous les compartiments permettent uniquement l'affichage.
- Vous avez vérifié que le nombre requis de nœuds de stockage et de sites est disponible. Si deux ou plusieurs nœuds de stockage ne sont pas disponibles sur un site, ou si un site n'est pas disponible, les modifications apportées à ces paramètres peuvent ne pas être disponibles.

Étapes

1. Sélectionnez **Buckets**, puis sélectionnez le bucket que vous souhaitez gérer.
2. Sur la page des détails du bucket, sélectionnez **Accès au bucket > Politique du bucket**.
3. Effectuez l'une des opérations suivantes :
 - Saisissez une politique de compartiment en cochant la case **Activer la politique**. Saisissez ensuite une chaîne formatée JSON valide.

Chaque politique de compartiment a une limite de taille de 20 480 octets.
 - Modifier une politique existante en modifiant la chaîne.
 - Désactivez une politique en désélectionnant **Activer la politique**.

Pour des informations détaillées sur les politiques de bucket, y compris la syntaxe du langage et des exemples, voir ["Exemples de politiques de compartiment"](#) .

Gérer la cohérence des buckets

Les valeurs de cohérence peuvent être utilisées pour spécifier la disponibilité des modifications des paramètres de bucket ainsi que pour fournir un équilibre entre la disponibilité des objets dans un bucket et la cohérence de ces objets sur différents nœuds de stockage et sites. Vous pouvez modifier les valeurs de cohérence pour qu'elles soient différentes des valeurs par défaut afin que les applications clientes puissent répondre à leurs besoins opérationnels.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .

- Vous appartenez à un groupe d'utilisateurs qui possède le "[Gérer tous les buckets ou l'autorisation d'accès root](#)". Ces autorisations remplacent les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.

Directives relatives à la cohérence des seaux

La cohérence du bucket est utilisée pour déterminer la cohérence des applications clientes affectant les objets dans ce bucket S3. En général, vous devez utiliser la cohérence **Lecture après nouvelle écriture** pour vos buckets.

Modifier la cohérence du bucket

Si la cohérence **Lecture après nouvelle écriture** ne répond pas aux exigences de l'application cliente, vous pouvez modifier la cohérence en définissant la cohérence du compartiment ou en utilisant le Consistency-Control en-tête. Le Consistency-Control l'en-tête remplace la cohérence du bucket.



Lorsque vous modifiez la cohérence d'un bucket, seuls les objets ingérés après la modification sont assurés de respecter le paramètre révisé.

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
2. Sélectionnez le nom du bucket dans le tableau.

La page des détails du bucket apparaît.

3. Dans l'onglet **Options du bucket**, sélectionnez l'accordéon **.
4. Sélectionnez une cohérence pour les opérations effectuées sur les objets de ce bucket.
 - **Tous** : Offre le plus haut niveau de cohérence. Tous les nœuds reçoivent les données immédiatement, sinon la demande échouera.
 - **Strong-global** : garantit la cohérence de lecture après écriture pour toutes les demandes client sur tous les sites.
 - **Strong-site** : garantit la cohérence de lecture après écriture pour toutes les requêtes client au sein d'un site.
 - **Lecture après nouvelle écriture** (par défaut) : assure la cohérence de lecture après écriture pour les nouveaux objets et la cohérence éventuelle pour les mises à jour d'objets. Offre des garanties de haute disponibilité et de protection des données. Recommandé dans la plupart des cas.
 - **Disponible** : Fournit une cohérence éventuelle pour les nouveaux objets et les mises à jour d'objets. Pour les buckets S3, utilisez-les uniquement si nécessaire (par exemple, pour un bucket contenant des valeurs de journal rarement lues ou pour des opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les buckets S3 FabricPool .
5. Sélectionnez **Enregistrer les modifications**.

Que se passe-t-il lorsque vous modifiez les paramètres du bucket

Les buckets ont plusieurs paramètres qui affectent le comportement des buckets et des objets qu'ils contiennent.

Les paramètres de bucket suivants utilisent une cohérence **forte** par défaut. Si deux ou plusieurs nœuds de stockage ne sont pas disponibles sur un site, ou si un site n'est pas disponible, les modifications apportées à ces paramètres peuvent ne pas être disponibles.

- ["Suppression du bucket vide en arrière-plan"](#)
- ["Heure du dernier accès"](#)
- ["Cycle de vie du bucket"](#)
- ["Politique de compartiment"](#)
- ["Étiquetage des buckets"](#)
- ["Gestion des versions de buckets"](#)
- ["Verrouillage d'objet S3"](#)
- ["Chiffrement du bucket"](#)



La valeur de cohérence pour le contrôle de version du bucket, le verrouillage d'objet S3 et le chiffrement du bucket ne peut pas être définie sur une valeur qui n'est pas fortement cohérente.

Les paramètres de compartiment suivants n'utilisent pas de cohérence forte et ont une plus grande disponibilité pour les modifications. Les modifications apportées à ces paramètres peuvent prendre un certain temps avant d'avoir un effet.

- ["Configuration des services de la plateforme : intégration des notifications, de la réplication ou de la recherche"](#)
- ["Configuration CORS"](#)
- [Modifier la cohérence du bucket](#)



Si la cohérence par défaut utilisée lors de la modification des paramètres de compartiment ne répond pas aux exigences de l'application cliente, vous pouvez modifier la cohérence à l'aide de l' `Consistency-Control` en-tête pour le ["API REST S3"](#) ou en utilisant le `reducedConsistency` ou `force` options dans le ["API de gestion des locataires"](#) .

Activer ou désactiver les mises à jour de l'heure du dernier accès

Lorsque les administrateurs de grille créent les règles de gestion du cycle de vie des informations (ILM) pour un système StorageGRID , ils peuvent éventuellement spécifier que l'heure du dernier accès d'un objet soit utilisée pour déterminer s'il faut déplacer cet objet vers un autre emplacement de stockage. Si vous utilisez un locataire S3, vous pouvez tirer parti de ces règles en activant les mises à jour de l'heure du dernier accès pour les objets d'un compartiment S3.

Ces instructions s'appliquent uniquement aux systèmes StorageGRID qui incluent au moins une règle ILM qui utilise l'option **Dernière heure d'accès** comme filtre avancé ou comme heure de référence. Vous pouvez ignorer ces instructions si votre système StorageGRID n'inclut pas une telle règle. Voir ["Utiliser l'heure du dernier accès dans les règles ILM"](#) pour plus de détails.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer tous les buckets ou l'autorisation d'accès root"](#) . Ces autorisations remplacent les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.

À propos de cette tâche

L'heure du dernier accès est l'une des options disponibles pour l'instruction de placement **Heure de référence** pour une règle ILM. La définition de l'heure de référence d'une règle sur l'heure du dernier accès permet aux administrateurs de grille de spécifier que les objets doivent être placés dans certains emplacements de stockage en fonction du moment où ces objets ont été récupérés pour la dernière fois (lus ou visualisés).

Par exemple, pour garantir que les objets récemment consultés restent sur un stockage plus rapide, un administrateur de grille peut créer une règle ILM spécifiant les éléments suivants :

- Les objets récupérés au cours du mois dernier doivent rester sur les nœuds de stockage locaux.
- Les objets qui n'ont pas été récupérés au cours du mois dernier doivent être déplacés vers un emplacement hors site.

Par défaut, les mises à jour de l'heure du dernier accès sont désactivées. Si votre système StorageGRID inclut une règle ILM qui utilise l'option **Dernière heure d'accès** et que vous souhaitez que cette option s'applique aux objets de ce compartiment, vous devez activer les mises à jour de la dernière heure d'accès pour les compartiments S3 spécifiés dans cette règle.



La mise à jour de l'heure du dernier accès lors de la récupération d'un objet peut réduire les performances de StorageGRID , en particulier pour les petits objets.

Un impact sur les performances se produit avec les mises à jour de l'heure du dernier accès, car StorageGRID doit effectuer ces étapes supplémentaires à chaque fois que des objets sont récupérés :

- Mettre à jour les objets avec de nouveaux horodatages
- Ajoutez les objets à la file d'attente ILM afin qu'ils puissent être réévalués par rapport aux règles et politiques ILM actuelles

Le tableau résume le comportement appliqué à tous les objets du compartiment lorsque l'heure du dernier accès est désactivée ou activée.

Type de demande	Comportement si l'heure du dernier accès est désactivée (par défaut)		Comportement si l'heure du dernier accès est activée	
	Dernière heure d'accès mise à jour ?	Objet ajouté à la file d'attente d'évaluation ILM ?	Dernière heure d'accès mise à jour ?	Objet ajouté à la file d'attente d'évaluation ILM ?
Demande de récupération d'un objet, de sa liste de contrôle d'accès ou de ses métadonnées	Non	Non	Oui	Oui
Demande de mise à jour des métadonnées d'un objet	Oui	Oui	Oui	Oui

Demande de liste d'objets ou de versions d'objets	Non	Non	Non	Non
Demande de copie d'un objet d'un bucket à un autre	<ul style="list-style-type: none"> • Non, pour la copie source • Oui, pour la copie de destination 	<ul style="list-style-type: none"> • Non, pour la copie source • Oui, pour la copie de destination 	<ul style="list-style-type: none"> • Oui, pour la copie source • Oui, pour la copie de destination 	<ul style="list-style-type: none"> • Oui, pour la copie source • Oui, pour la copie de destination
Demande de finalisation d'un téléchargement en plusieurs parties	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
2. Sélectionnez le nom du bucket dans le tableau.

La page des détails du bucket apparaît.

3. Dans l'onglet **Options du bucket**, sélectionnez l'accordéon **Dernières mises à jour de l'heure d'accès**.
4. Activer ou désactiver les mises à jour de l'heure du dernier accès.
5. Sélectionnez **Enregistrer les modifications**.

Modifier la version d'objet pour un bucket

Si vous utilisez un locataire S3, vous pouvez modifier l'état de contrôle de version des buckets S3.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer tous les buckets ou l'autorisation d'accès root"](#). Ces autorisations remplacent les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.
- Vous avez vérifié que le nombre requis de nœuds de stockage et de sites est disponible. Si deux ou plusieurs nœuds de stockage ne sont pas disponibles sur un site, ou si un site n'est pas disponible, les modifications apportées à ces paramètres peuvent ne pas être disponibles.

À propos de cette tâche

Vous pouvez activer ou suspendre le contrôle de version d'objet pour un bucket. Une fois que vous avez activé le contrôle de version pour un bucket, celui-ci ne peut pas revenir à un état non versionné. Cependant, vous pouvez suspendre le contrôle de version du bucket.

- Désactivé : le contrôle de version n'a jamais été activé
- Activé : le contrôle de version est activé
- Suspendu : le contrôle de version était précédemment activé et est suspendu

Pour plus d'informations, consultez les éléments suivants :

- ["Versionnage d'objet"](#)
- ["Règles et politiques ILM pour les objets versionnés S3 \(exemple 4\)"](#)
- ["Comment les objets sont supprimés"](#)

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
2. Sélectionnez le nom du bucket dans le tableau.

La page des détails du bucket apparaît.

3. Dans l'onglet **Options du bucket**, sélectionnez l'accordéon **Versionnement d'objet**.
4. Sélectionnez un état de version pour les objets de ce bucket.

Le contrôle de version des objets doit rester activé pour un bucket utilisé pour la réplication inter-grille. Si le verrouillage d'objet S3 ou la conformité héritée est activé, les options **Versionnage d'objet** sont désactivées.

Option	Description
Activer le contrôle de version	Activez le contrôle de version des objets si vous souhaitez stocker chaque version de chaque objet dans ce bucket. Vous pouvez ensuite récupérer les versions précédentes d'un objet selon vos besoins. Les objets qui étaient déjà dans le bucket seront versionnés lorsqu'ils seront modifiés par un utilisateur.
Suspendre le contrôle de version	Suspendez le contrôle de version des objets si vous ne souhaitez plus que de nouvelles versions d'objets soient créées. Vous pouvez toujours récupérer toutes les versions d'objet existantes.

5. Sélectionnez **Enregistrer les modifications**.

Utilisez S3 Object Lock pour conserver les objets

Vous pouvez utiliser S3 Object Lock si les buckets et les objets doivent être conformes aux exigences réglementaires en matière de conservation.



Votre administrateur de grille doit vous donner l'autorisation d'utiliser des fonctionnalités spécifiques de S3 Object Lock.

Qu'est-ce que S3 Object Lock ?

La fonctionnalité StorageGRID S3 Object Lock est une solution de protection d'objets équivalente à S3 Object Lock dans Amazon Simple Storage Service (Amazon S3).

Lorsque le paramètre global de verrouillage d'objet S3 est activé pour un système StorageGRID , un compte de locataire S3 peut créer des buckets avec ou sans verrouillage d'objet S3 activé. Si le verrouillage d'objet S3 est activé pour un bucket, le contrôle de version du bucket est requis et est activé automatiquement.

Un bucket sans verrouillage d'objet S3 ne peut contenir que des objets sans paramètres de conservation spécifiés. Aucun objet ingéré n'aura de paramètres de rétention.

Un bucket avec verrouillage d'objet S3 peut contenir des objets avec et sans paramètres de rétention spécifiés par les applications clientes S3. Certains objets ingérés auront des paramètres de rétention.

Un bucket avec verrouillage d'objet S3 et rétention par défaut configuré peut contenir des objets téléchargés avec des paramètres de rétention spécifiés et de nouveaux objets sans paramètres de rétention. Les nouveaux objets utilisent le paramètre par défaut, car le paramètre de rétention n'a pas été configuré au niveau de l'objet.

En effet, tous les objets nouvellement ingérés ont des paramètres de rétention lorsque la rétention par défaut est configurée. Les objets existants sans paramètres de conservation d'objets restent inchangés.

Modes de rétention

La fonctionnalité de verrouillage d'objet StorageGRID S3 prend en charge deux modes de conservation pour appliquer différents niveaux de protection aux objets. Ces modes sont équivalents aux modes de rétention d'Amazon S3.

- En mode conformité :
 - L'objet ne peut pas être supprimé tant que sa date de conservation n'est pas atteinte.
 - La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être diminuée.
 - La date de conservation de l'objet ne peut pas être supprimée tant que cette date n'est pas atteinte.
- En mode gouvernance :
 - Les utilisateurs disposant d'une autorisation spéciale peuvent utiliser un en-tête de contournement dans les demandes pour modifier certains paramètres de conservation.
 - Ces utilisateurs peuvent supprimer une version d'objet avant que sa date de conservation ne soit atteinte.
 - Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

Paramètres de conservation pour les versions d'objet

Si un compartiment est créé avec le verrouillage d'objet S3 activé, les utilisateurs peuvent utiliser l'application cliente S3 pour spécifier éventuellement les paramètres de conservation suivants pour chaque objet ajouté au compartiment :

- **Mode de conservation** : Soit la conformité, soit la gouvernance.
- **Date de conservation jusqu'à** : si la date de conservation jusqu'à d'une version d'objet est dans le futur, l'objet peut être récupéré, mais il ne peut pas être supprimé.
- **Conservation légale** : L'application d'une conservation légale à une version d'objet verrouille immédiatement cet objet. Par exemple, vous pourriez avoir besoin de suspendre légalement un objet lié à une enquête ou à un litige juridique. Une conservation légale n'a pas de date d'expiration, mais reste en place jusqu'à ce qu'elle soit explicitement supprimée. Les conservations légales sont indépendantes de la date de conservation.



Si un objet est sous conservation légale, personne ne peut supprimer l'objet, quel que soit son mode de conservation.

Pour plus de détails sur les paramètres de l'objet, voir ["Utiliser l'API REST S3 pour configurer le"](#)

Paramètre de rétention par défaut pour les buckets

Si un bucket est créé avec le verrouillage d'objet S3 activé, les utilisateurs peuvent éventuellement spécifier les paramètres par défaut suivants pour le bucket :

- **Mode de conservation par défaut** : Conformité ou gouvernance.
- **Période de conservation par défaut** : durée pendant laquelle les nouvelles versions d'objet ajoutées à ce bucket doivent être conservées, à compter du jour de leur ajout.

Les paramètres de compartiment par défaut s'appliquent uniquement aux nouveaux objets qui ne disposent pas de leurs propres paramètres de conservation. Les objets de compartiment existants ne sont pas affectés lorsque vous ajoutez ou modifiez ces paramètres par défaut.

Voir "[Créer un bucket S3](#)" et "[Mettre à jour la conservation par défaut du verrouillage des objets S3](#)".

Tâches de verrouillage d'objet S3

Les listes suivantes destinées aux administrateurs de grille et aux utilisateurs locataires contiennent les tâches de haut niveau pour l'utilisation de la fonctionnalité de verrouillage d'objet S3.

Administrateur de réseau

- Activez le paramètre de verrouillage d'objet S3 global pour l'ensemble du système StorageGRID .
- Assurez-vous que les politiques de gestion du cycle de vie de l'information (ILM) sont *conformes* ; c'est-à-dire qu'elles répondent aux "[exigences des buckets avec S3 Object Lock activé](#)".
- Si nécessaire, autorisez un locataire à utiliser la conformité comme mode de conservation. Sinon, seul le mode Gouvernance est autorisé.
- Si nécessaire, définissez une période de conservation maximale pour un locataire.

Utilisateur locataire

- Passez en revue les considérations relatives aux buckets et aux objets avec S3 Object Lock.
- Si nécessaire, contactez l'administrateur de la grille pour activer le paramètre de verrouillage d'objet S3 global et définir les autorisations.
- Créez des buckets avec le verrouillage d'objet S3 activé.
- Vous pouvez également configurer les paramètres de conservation par défaut pour un bucket :
 - Mode de conservation par défaut : Gouvernance ou Conformité, si autorisé par l'administrateur du réseau.
 - Période de conservation par défaut : doit être inférieure ou égale à la période de conservation maximale définie par l'administrateur du réseau.
- Utilisez l'application client S3 pour ajouter des objets et éventuellement définir une conservation spécifique à l'objet :
 - Mode de rétention. Gouvernance ou conformité, si autorisée par l'administrateur du réseau.
 - Date de conservation : doit être inférieure ou égale à ce qui est autorisé par la période de conservation maximale définie par l'administrateur de la grille.

Exigences pour les buckets avec S3 Object Lock activé

- Si le paramètre global de verrouillage d'objet S3 est activé pour le système StorageGRID , vous pouvez utiliser le gestionnaire de locataires, l'API de gestion des locataires ou l'API REST S3 pour créer des buckets avec le verrouillage d'objets S3 activé.
- Si vous prévoyez d'utiliser S3 Object Lock, vous devez activer S3 Object Lock lorsque vous créez le bucket. Vous ne pouvez pas activer le verrouillage d'objet S3 pour un bucket existant.
- Lorsque le verrouillage d'objet S3 est activé pour un bucket, StorageGRID active automatiquement le contrôle de version pour ce bucket. Vous ne pouvez pas désactiver le verrouillage d'objet S3 ou suspendre le contrôle de version du bucket.
- Vous pouvez également spécifier un mode de conservation par défaut et une période de conservation pour chaque compartiment à l'aide du gestionnaire de locataires, de l'API de gestion des locataires ou de l'API REST S3. Les paramètres de conservation par défaut du bucket s'appliquent uniquement aux nouveaux objets ajoutés au bucket qui ne disposent pas de leurs propres paramètres de conservation. Vous pouvez remplacer ces paramètres par défaut en spécifiant un mode de conservation et une date de conservation pour chaque version d'objet lors de son téléchargement.
- La configuration du cycle de vie du bucket est prise en charge pour les buckets avec S3 Object Lock activé.
- La réplication CloudMirror n'est pas prise en charge pour les buckets avec S3 Object Lock activé.

Exigences relatives aux objets dans les compartiments avec le verrouillage d'objet S3 activé

- Pour protéger une version d'objet, vous pouvez spécifier des paramètres de rétention par défaut pour le compartiment ou spécifier des paramètres de rétention pour chaque version d'objet. Les paramètres de conservation au niveau de l'objet peuvent être spécifiés à l'aide de l'application cliente S3 ou de l'API REST S3.
- Les paramètres de conservation s'appliquent aux versions d'objet individuelles. Une version d'objet peut avoir à la fois une date de conservation et un paramètre de conservation légale, l'un mais pas l'autre, ou aucun des deux. La spécification d'une date de conservation ou d'un paramètre de conservation légale pour un objet protège uniquement la version spécifiée dans la demande. Vous pouvez créer de nouvelles versions de l'objet, tandis que la version précédente de l'objet reste verrouillée.

Cycle de vie des objets dans les buckets avec S3 Object Lock activé

Chaque objet enregistré dans un bucket avec S3 Object Lock activé passe par ces étapes :

1. Objet ingéré

Lorsqu'une version d'objet est ajoutée à un bucket sur lequel le verrouillage d'objet S3 est activé, les paramètres de rétention sont appliqués comme suit :

- Si des paramètres de conservation sont spécifiés pour l'objet, les paramètres au niveau de l'objet sont appliqués. Tous les paramètres de bucket par défaut sont ignorés.
- Si aucun paramètre de conservation n'est spécifié pour l'objet, les paramètres de compartiment par défaut sont appliqués, s'ils existent.
- Si aucun paramètre de conservation n'est spécifié pour l'objet ou le compartiment, l'objet n'est pas protégé par S3 Object Lock.

Si les paramètres de conservation sont appliqués, l'objet et toutes les métadonnées définies par l'utilisateur S3 sont protégés.

2. Conservation et suppression d'objets

Plusieurs copies de chaque objet protégé sont stockées par StorageGRID pendant la période de conservation spécifiée. Le nombre et le type exacts de copies d'objets ainsi que les emplacements de stockage sont déterminés par les règles de conformité des politiques ILM actives. La possibilité de supprimer un objet protégé avant que sa date de conservation ne soit atteinte dépend de son mode de conservation.

- Si un objet est sous conservation légale, personne ne peut supprimer l'objet, quel que soit son mode de conservation.

Puis-je toujours gérer les buckets conformes hérités ?

La fonctionnalité de verrouillage d'objet S3 remplace la fonctionnalité de conformité qui était disponible dans les versions précédentes de StorageGRID. Si vous avez créé des buckets conformes à l'aide d'une version précédente de StorageGRID, vous pouvez continuer à gérer les paramètres de ces buckets ; toutefois, vous ne pouvez plus créer de nouveaux buckets conformes. Pour les instructions, voir https://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_manage_legacy_Compliant_buckets_in_StorageGRID_11.5 [Base de connaissances NetApp : Gestion des buckets compatibles hérités dans StorageGRID 11.5].

Mettre à jour la conservation par défaut du verrouillage des objets S3

Si vous avez activé le verrouillage d'objet S3 lors de la création du bucket, vous pouvez modifier le bucket pour modifier les paramètres de rétention par défaut. Vous pouvez activer (ou désactiver) la conservation par défaut et définir un mode de conservation par défaut et une période de conservation.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer tous les buckets ou l'autorisation d'accès root"](#). Ces autorisations remplacent les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.
- Le verrouillage des objets S3 est activé globalement pour votre système StorageGRID et vous avez activé le verrouillage des objets S3 lorsque vous avez créé le bucket. Voir ["Utilisez S3 Object Lock pour conserver les objets"](#).

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
2. Sélectionnez le nom du bucket dans le tableau.

La page des détails du bucket apparaît.

3. Dans l'onglet **Options du bucket**, sélectionnez l'accordéon **Verrouillage d'objet S3**.
4. En option, activez ou désactivez la **Rétention par défaut** pour ce bucket.

Les modifications apportées à ce paramètre ne s'appliquent pas aux objets déjà présents dans le bucket ni aux objets susceptibles d'avoir leurs propres périodes de conservation.

5. Si la **Rétention par défaut** est activée, spécifiez un **Mode de rétention par défaut** pour le bucket.

Mode de rétention par défaut	Description
Gouvernance	<ul style="list-style-type: none"> • Les utilisateurs avec le <code>s3:BypassGovernanceRetention</code> l'autorisation peut utiliser le <code>x-amz-bypass-governance-retention: true</code> en-tête de demande pour contourner les paramètres de conservation. • Ces utilisateurs peuvent supprimer une version d'objet avant que sa date de conservation ne soit atteinte. • Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.
Conformité	<ul style="list-style-type: none"> • L'objet ne peut pas être supprimé tant que sa date de conservation n'est pas atteinte. • La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être diminuée. • La date de conservation de l'objet ne peut pas être supprimée tant que cette date n'est pas atteinte. <p>Remarque : votre administrateur de réseau doit vous autoriser à utiliser le mode de conformité.</p>

6. Si la **Conservation par défaut** est activée, spécifiez la **Période de conservation par défaut** pour le bucket.

La **Période de conservation par défaut** indique la durée pendant laquelle les nouveaux objets ajoutés à ce bucket doivent être conservés, à compter du moment où ils sont ingérés. Spécifiez une valeur inférieure ou égale à la période de conservation maximale du locataire, telle que définie par l'administrateur de la grille.

Une période de conservation *maximale*, qui peut être une valeur comprise entre 1 jour et 100 ans, est définie lorsque l'administrateur de la grille crée le locataire. Lorsque vous définissez une période de conservation par défaut, elle ne peut pas dépasser la valeur définie pour la période de conservation maximale. Si nécessaire, demandez à votre administrateur de réseau d'augmenter ou de diminuer la période de conservation maximale.

7. Sélectionnez **Enregistrer les modifications**.

Configurer le partage de ressources inter-origines (CORS)

Vous pouvez configurer le partage de ressources inter-origines (CORS) pour un bucket S3 si vous souhaitez que ce bucket et les objets qu'il contient soient accessibles aux applications Web d'autres domaines.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Pour les demandes de configuration GET CORS, vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation de gérer tous les compartiments ou d'afficher tous les compartiments"](#). Ces autorisations remplacent les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.
- Pour les demandes de configuration PUT CORS, vous appartenez à un groupe d'utilisateurs qui possède

le ["Gérer toutes les autorisations des buckets"](#) . Cette autorisation remplace les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.

- Le ["Autorisation d'accès root"](#) donne accès à toutes les demandes de configuration CORS.

À propos de cette tâche

Le partage de ressources inter-origines (CORS) est un mécanisme de sécurité qui permet aux applications Web clientes d'un domaine d'accéder aux ressources d'un domaine différent. Par exemple, supposons que vous utilisiez un bucket S3 nommé `Images` pour stocker des graphiques. En configurant CORS pour le `Images` bucket, vous pouvez autoriser l'affichage des images de ce bucket sur le site Web `http://www.example.com`.

Activer CORS pour un bucket

Étapes

1. Utilisez un éditeur de texte pour créer le XML requis. Cet exemple montre le XML utilisé pour activer CORS pour un bucket S3. Spécifiquement:
 - Permet à n'importe quel domaine d'envoyer des requêtes GET au bucket
 - Autorise uniquement le `http://www.example.com` domaine pour envoyer des requêtes GET, POST et DELETE
 - Tous les en-têtes de requête sont autorisés

```
<CORSConfiguration
  xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
  <CORSRule>
    <AllowedOrigin>*</AllowedOrigin>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedHeader>*</AllowedHeader>
  </CORSRule>
  <CORSRule>
    <AllowedOrigin>http://www.example.com</AllowedOrigin>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedMethod>POST</AllowedMethod>
    <AllowedMethod>DELETE</AllowedMethod>
    <AllowedHeader>*</AllowedHeader>
  </CORSRule>
</CORSConfiguration>
```

Pour plus d'informations sur le XML de configuration CORS, voir ["Documentation Amazon Web Services \(AWS\) : Guide de l'utilisateur d'Amazon Simple Storage Service"](#) .

2. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
3. Sélectionnez le nom du bucket dans le tableau.

La page des détails du bucket apparaît.

4. Dans l'onglet **Accès au bucket**, sélectionnez l'accordéon **Partage de ressources inter-origines (CORS)**.
5. Cochez la case **Activer CORS**.

6. Collez le XML de configuration CORS dans la zone de texte.
7. Sélectionnez **Enregistrer les modifications**.

Modifier le paramètre CORS

Étapes

1. Mettez à jour le XML de configuration CORS dans la zone de texte ou sélectionnez **Effacer** pour recommencer.
2. Sélectionnez **Enregistrer les modifications**.

Désactiver le paramètre CORS

Étapes

1. Décochez la case **Activer CORS**.
2. Sélectionnez **Enregistrer les modifications**.

Supprimer les objets dans le bucket

Vous pouvez utiliser le gestionnaire de locataires pour supprimer les objets dans un ou plusieurs compartiments.

Considérations et exigences

Avant d'effectuer ces étapes, notez les points suivants :

- Lorsque vous supprimez les objets d'un bucket, StorageGRID supprime définitivement tous les objets et toutes les versions d'objets de chaque bucket sélectionné de tous les nœuds et sites de votre système StorageGRID . StorageGRID supprime également toutes les métadonnées d'objet associées. Vous ne pourrez pas récupérer ces informations.
- La suppression de tous les objets d'un bucket peut prendre des minutes, des jours, voire des semaines, en fonction du nombre d'objets, de copies d'objets et d'opérations simultanées.
- Si un seau a "**Verrouillage d'objet S3 activé**", il pourrait rester dans l'état **Suppression d'objets : lecture seule** pendant *années*.



Un bucket qui utilise S3 Object Lock restera dans l'état **Suppression d'objets : lecture seule** jusqu'à ce que la date de conservation soit atteinte pour tous les objets et que toutes les conservations légales soient supprimées.

- Pendant la suppression des objets, l'état du bucket est **Suppression d'objets : lecture seule**. Dans cet état, vous ne pouvez pas ajouter de nouveaux objets au bucket.
- Lorsque tous les objets ont été supprimés, le bucket reste en état de lecture seule. Vous pouvez effectuer l'une des opérations suivantes :
 - Remettre le bucket en mode écriture et le réutiliser pour de nouveaux objets
 - Supprimer le bucket
 - Gardez le bucket en mode lecture seule pour réserver son nom pour une utilisation ultérieure
- Si le contrôle de version d'objet est activé pour un bucket, les marqueurs de suppression créés dans StorageGRID 11.8 ou version ultérieure peuvent être supprimés à l'aide des opérations Supprimer des objets dans le bucket.
- Si le contrôle de version d'objet est activé pour un bucket, l'opération de suppression d'objets ne

supprimera pas les marqueurs de suppression créés dans StorageGRID 11.7 ou une version antérieure. Consultez les informations sur la suppression d'objets dans un bucket dans "[Comment les objets versionnés S3 sont supprimés](#)".

- Si vous utilisez "[réplication inter-réseaux](#)", notez ce qui suit :
 - L'utilisation de cette option ne supprime aucun objet du bucket sur l'autre grille.
 - Si vous sélectionnez cette option pour le bucket source, l'alerte **Échec de la réplication inter-grille** sera déclenchée si vous ajoutez des objets au bucket de destination sur l'autre grille. Si vous ne pouvez pas garantir que personne n'ajoutera d'objets au seau sur l'autre grille, "[désactiver la réplication inter-grille](#)" pour ce bucket avant de supprimer tous les objets du bucket.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Autorisation d'accès root](#)". Cette autorisation remplace les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.

La page Buckets apparaît et affiche tous les buckets S3 existants.

2. Utilisez le menu **Actions** ou la page de détails pour un bucket spécifique.

Menu Actions

- a. Cochez la case correspondant à chaque compartiment dont vous souhaitez supprimer des objets.
- b. Sélectionnez **Actions > Supprimer les objets dans le bucket**.

Page de détails

- a. Sélectionnez un nom de bucket pour afficher ses détails.
- b. Sélectionnez **Supprimer les objets dans le bucket**.

3. Lorsque la boîte de dialogue de confirmation s'affiche, vérifiez les détails, entrez **Oui** et sélectionnez **OK**.
4. Attendez que l'opération de suppression commence.

Après quelques minutes :

- Une bannière d'état jaune apparaît sur la page des détails du bucket. La barre de progression représente le pourcentage d'objets supprimés.
- **(lecture seule)** apparaît après le nom du bucket sur la page des détails du bucket.
- **(Suppression d'objets : lecture seule)** apparaît à côté du nom du bucket sur la page Buckets.

Buckets > my-bucket

my-bucket (read-only)


Region: us-east-1

Date created: 2022-12-14 10:09:50 MST

Object count: 3

View bucket contents in Experimental S3 Console [↗](#)

Delete bucket

 **All bucket objects are being deleted**

StorageGRID is deleting all copies of the objects in this bucket, which might take days or weeks. While objects are being deleted, the bucket is read only. To stop the operation, select **Stop deleting objects**. You cannot restore objects that have already been deleted.

0% (0 of 3 objects deleted)

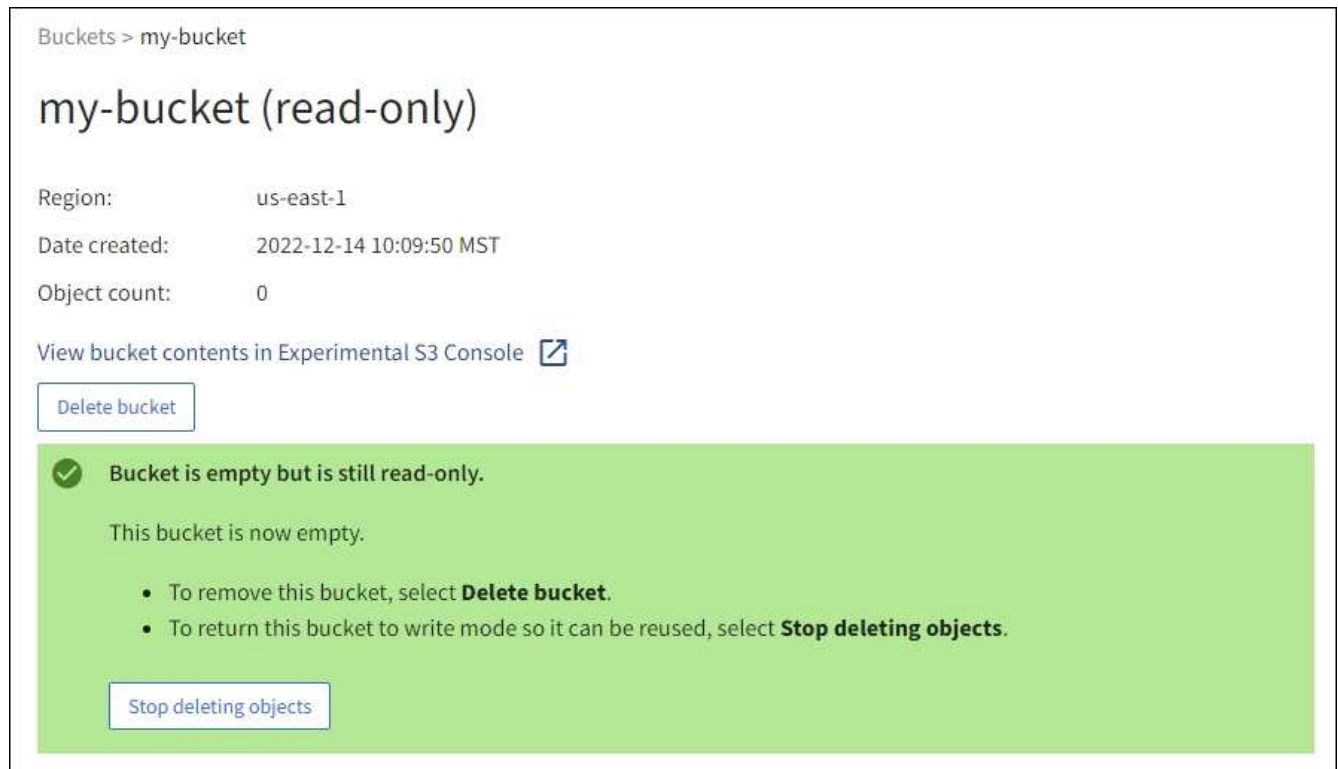
Stop deleting objects

5. Si nécessaire, pendant que l'opération est en cours, sélectionnez **Arrêter la suppression des objets** pour arrêter le processus. Ensuite, si vous le souhaitez, sélectionnez **Supprimer les objets dans le bucket** pour reprendre le processus.

Lorsque vous sélectionnez **Arrêter la suppression des objets**, le bucket revient en mode écriture ; cependant, vous ne pouvez pas accéder ni restaurer les objets qui ont été supprimés.

6. Attendez que l'opération soit terminée.

Lorsque le bucket est vide, la bannière d'état est mise à jour, mais le bucket reste en lecture seule.



7. Effectuez l'une des opérations suivantes :

- Quittez la page pour conserver le bucket en mode lecture seule. Par exemple, vous pouvez conserver un bucket vide en mode lecture seule pour réserver le nom du bucket pour une utilisation ultérieure.
- Supprimer le bucket. Vous pouvez sélectionner **Supprimer le bucket** pour supprimer un seul bucket ou revenir à la page Buckets et sélectionner **Actions > Supprimer** les buckets pour supprimer plusieurs buckets.



Si vous ne parvenez pas à supprimer un bucket versionné après la suppression de tous les objets, des marqueurs de suppression peuvent rester. Pour supprimer le bucket, vous devez supprimer tous les marqueurs de suppression restants.

- Remettez le bucket en mode écriture et réutilisez-le éventuellement pour de nouveaux objets. Vous pouvez sélectionner **Arrêter la suppression des objets** pour un seul bucket ou revenir à la page Buckets et sélectionner **Action > Arrêter la suppression des objets** pour plusieurs buckets.

Supprimer le compartiment S3

Vous pouvez utiliser le gestionnaire de locataires pour supprimer un ou plusieurs compartiments S3 vides.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer tous les buckets ou l'autorisation d'accès root"](#) . Ces autorisations remplacent les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.
- Les buckets que vous souhaitez supprimer sont vides. Si les buckets que vous souhaitez supprimer ne sont pas vides, ["supprimer des objets du bucket"](#) .

À propos de cette tâche

Ces instructions décrivent comment supprimer un compartiment S3 à l'aide du gestionnaire de locataires. Vous pouvez également supprimer des compartiments S3 à l'aide de la ["API de gestion des locataires"](#) ou le ["API REST S3"](#).

Vous ne pouvez pas supprimer un compartiment S3 s'il contient des objets, des versions d'objet non actuelles ou des marqueurs de suppression. Pour plus d'informations sur la manière dont les objets versionnés S3 sont supprimés, consultez ["Comment les objets sont supprimés"](#).

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.

La page Buckets apparaît et affiche tous les buckets S3 existants.

2. Utilisez le menu **Actions** ou la page de détails pour un bucket spécifique.

Menu Actions

- a. Cochez la case correspondant à chaque compartiment que vous souhaitez supprimer.
- b. Sélectionnez **Actions > Supprimer les buckets**.

Page de détails

- a. Sélectionnez un nom de bucket pour afficher ses détails.
- b. Sélectionnez **Supprimer le bucket**.

3. Lorsque la boîte de dialogue de confirmation apparaît, sélectionnez **Oui**.

StorageGRID confirme que chaque bucket est vide, puis supprime chaque bucket. Cette opération peut prendre quelques minutes.

Si un bucket n'est pas vide, un message d'erreur s'affiche. Vous devez ["supprimer tous les objets et tous les marqueurs de suppression dans le bucket"](#) avant de pouvoir supprimer le bucket.

Utiliser la console S3

Vous pouvez utiliser la console S3 pour afficher et gérer les objets dans un bucket S3.

La console S3 vous permet de :

- Télécharger, renommer, copier, déplacer et supprimer des objets
- Afficher, rétablir, télécharger et supprimer les versions d'objets
- Rechercher des objets par préfixe
- Gérer les balises d'objet
- Afficher les métadonnées de l'objet
- Afficher, créer, renommer, copier, déplacer et supprimer des dossiers

La console S3 offre une expérience utilisateur améliorée pour les cas les plus courants. Il n'est pas conçu pour remplacer les opérations CLI ou API dans toutes les situations.



Si l'utilisation de la console S3 entraîne des opérations qui prennent trop de temps (par exemple, des minutes ou des heures), tenez compte des éléments suivants :

- Réduire le nombre d'objets sélectionnés
- Utiliser des méthodes non graphiques (API ou CLI) pour accéder à vos données

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Si vous souhaitez gérer des objets, vous appartenez à un groupe d'utilisateurs disposant de l'autorisation d'accès Root. Vous pouvez également appartenir à un groupe d'utilisateurs disposant de l'autorisation Utiliser l'onglet Console S3 et de l'autorisation Afficher tous les buckets ou Gérer tous les buckets. Voir ["Autorisations de gestion des locataires"](#) .
- Une stratégie de groupe ou de compartiment S3 a été configurée pour l'utilisateur. Voir ["Utiliser des politiques d'accès aux buckets et aux groupes"](#) .
- Vous connaissez l'ID de la clé d'accès et la clé d'accès secrète de l'utilisateur. En option, vous disposez d'un .csv fichier contenant ces informations. Voir le ["instructions pour créer des clés d'accès"](#) .

Étapes

1. Sélectionnez **STOCKAGE > Compartiments > nom du compartiment**.
2. Sélectionnez l'onglet Console S3.
3. Collez l'ID de la clé d'accès et la clé d'accès secrète dans les champs. Sinon, sélectionnez **Télécharger les clés d'accès** et sélectionnez votre .csv déposer.
4. Sélectionnez * Sign in*.
5. Le tableau des objets du bucket apparaît. Vous pouvez gérer les objets selon vos besoins.

Informations Complémentaires

- **Recherche par préfixe** : La fonction de recherche par préfixe recherche uniquement les objets commençant par un mot spécifique relatif au dossier actuel. La recherche n'inclut pas les objets qui contiennent le mot ailleurs. Cette règle s'applique également aux objets contenus dans les dossiers. Par exemple, une recherche de folder1/folder2/somefile- renverrait les objets qui sont dans le folder1/folder2/ dossier et commencer par le mot somefile- .
- **Glisser-déposer** : vous pouvez glisser-déposer des fichiers du gestionnaire de fichiers de votre ordinateur vers la console S3. Cependant, vous ne pouvez pas télécharger de dossiers.
- **Opérations sur les dossiers** : Lorsque vous déplacez, copiez ou renommez un dossier, tous les objets du dossier sont mis à jour un par un, ce qui peut prendre du temps.
- **Suppression permanente lorsque le contrôle de version du bucket est désactivé** : lorsque vous écrasez ou supprimez un objet dans un bucket avec le contrôle de version désactivé, l'opération est permanente. Voir ["Modifier la version d'objet pour un bucket"](#) .

Gérer les services de la plateforme S3

Services de la plateforme S3

Présentation et considérations relatives aux services de la plateforme

Avant d'implémenter les services de plateforme, consultez la présentation et les considérations relatives à l'utilisation de ces services.

Pour plus d'informations sur S3, voir ["Utiliser l'API REST S3"](#) .

Aperçu des services de la plateforme

Les services de la plateforme StorageGRID peuvent vous aider à mettre en œuvre une stratégie de cloud hybride en vous permettant d'envoyer des notifications d'événements et des copies d'objets S3 et de métadonnées d'objets vers des destinations externes.

Étant donné que l'emplacement cible des services de plateforme est généralement externe à votre déploiement StorageGRID , les services de plateforme vous offrent la puissance et la flexibilité qui découlent de l'utilisation de ressources de stockage externes, de services de notification et de services de recherche ou d'analyse pour vos données.

N'importe quelle combinaison de services de plateforme peut être configurée pour un seul compartiment S3. Par exemple, vous pouvez configurer à la fois le ["Service CloudMirror"](#) et ["notifications"](#) sur un bucket StorageGRID S3 afin que vous puissiez mettre en miroir des objets spécifiques sur Amazon Simple Storage Service (S3), tout en envoyant une notification sur chacun de ces objets à une application de surveillance tierce pour vous aider à suivre vos dépenses AWS.



L'utilisation des services de plateforme doit être activée pour chaque compte de locataire par un administrateur StorageGRID à l'aide de Grid Manager ou de l'API Grid Management.

Comment les services de la plateforme sont configurés

Les services de plateforme communiquent avec des points de terminaison externes que vous configurez à l'aide de l'["Gestionnaire de locataires"](#) ou le ["API de gestion des locataires"](#) . Chaque point de terminaison représente une destination externe, telle qu'un bucket StorageGRID S3, un bucket Amazon Web Services, une rubrique Amazon SNS ou un cluster Elasticsearch hébergé localement, sur AWS ou ailleurs.

Après avoir créé un point de terminaison externe, vous pouvez activer un service de plateforme pour un bucket en ajoutant une configuration XML au bucket. La configuration XML identifie les objets sur lesquels le bucket doit agir, l'action que le bucket doit entreprendre et le point de terminaison que le bucket doit utiliser pour le service.

Vous devez ajouter des configurations XML distinctes pour chaque service de plateforme que vous souhaitez configurer. Par exemple:

- Si vous voulez tous les objets dont les clés commencent par `/images` pour être répliqué vers un compartiment Amazon S3, vous devez ajouter une configuration de réplication au compartiment source.
- Si vous souhaitez également envoyer des notifications lorsque ces objets sont stockés dans le bucket, vous devez ajouter une configuration de notifications.
- Si vous souhaitez indexer les métadonnées de ces objets, vous devez ajouter la configuration de notification de métadonnées utilisée pour implémenter l'intégration de la recherche.

Le format du XML de configuration est régi par les API REST S3 utilisées pour implémenter les services de la plateforme StorageGRID :

Service de plateforme	API REST S3	Se référer à
Réplication CloudMirror	<ul style="list-style-type: none"> • Réplication GetBucket • Réplication de PutBucket 	<ul style="list-style-type: none"> • "Réplication CloudMirror" • "Opérations sur les godets"
Notifications	<ul style="list-style-type: none"> • Configuration de GetBucketNotification • Configuration de PutBucketNotification 	<ul style="list-style-type: none"> • "Notifications" • "Opérations sur les godets"
Intégration de la recherche	<ul style="list-style-type: none"> • Configuration de la notification des métadonnées du bucket GET • Configuration des notifications de métadonnées du compartiment PUT 	<ul style="list-style-type: none"> • "Intégration de la recherche" • "Opérations personnalisées StorageGRID"

Considérations relatives à l'utilisation des services de plateforme

Considération	Détails
Surveillance du point de terminaison de destination	<p>Vous devez surveiller la disponibilité de chaque point de terminaison de destination. Si la connectivité au point de terminaison de destination est perdue pendant une période prolongée et qu'un important arriéré de demandes existe, les demandes client supplémentaires (telles que les demandes PUT) adressées à StorageGRID échoueront. Vous devez réessayer ces demandes ayant échoué lorsque le point de terminaison redevient accessible.</p>
Limitation du point de terminaison de destination	<p>Le logiciel StorageGRID peut limiter les requêtes S3 entrantes pour un bucket si la vitesse à laquelle les requêtes sont envoyées dépasse la vitesse à laquelle le point de terminaison de destination peut recevoir les requêtes. La limitation se produit uniquement lorsqu'il existe un arriéré de requêtes en attente d'être envoyées au point de terminaison de destination.</p> <p>Le seul effet visible est que les requêtes S3 entrantes prendront plus de temps à s'exécuter. Si vous commencez à détecter des performances nettement plus lentes, vous devez réduire le taux d'ingestion ou utiliser un point de terminaison avec une capacité supérieure. Si l'arriéré des demandes continue de croître, les opérations S3 du client (telles que les demandes PUT) finiront par échouer.</p> <p>Les requêtes CloudMirror sont plus susceptibles d'être affectées par les performances du point de terminaison de destination, car ces requêtes impliquent généralement plus de transfert de données que les requêtes d'intégration de recherche ou de notification d'événements.</p>

Considération	Détails
Garanties de commande	<p>StorageGRID garantit l'ordre des opérations sur un objet au sein d'un site. Tant que toutes les opérations sur un objet se déroulent sur le même site, l'état final de l'objet (pour la réplication) sera toujours égal à l'état dans StorageGRID.</p> <p>StorageGRID fait de son mieux pour ordonner les demandes lorsque des opérations sont effectuées sur les sites StorageGRID . Par exemple, si vous écrivez initialement un objet sur le site A, puis écrasez ultérieurement le même objet sur le site B, il n'est pas garanti que l'objet final répliqué par CloudMirror vers le bucket de destination soit l'objet le plus récent.</p>
Suppressions d'objets pilotées par ILM	<p>Pour correspondre au comportement de suppression d'AWS CRR et d'Amazon Simple Notification Service, les demandes de notification d'événements et CloudMirror ne sont pas envoyées lorsqu'un objet dans le compartiment source est supprimé en raison des règles StorageGRID ILM. Par exemple, aucune demande de notification CloudMirror ou d'événement n'est envoyée si une règle ILM supprime un objet après 14 jours.</p> <p>En revanche, les demandes d'intégration de recherche sont envoyées lorsque des objets sont supprimés en raison de l'ILM.</p>
Utilisation des points de terminaison Kafka	<p>Pour les points de terminaison Kafka, le protocole TLS mutuel n'est pas pris en charge. Par conséquent, si vous avez <code>ssl.client.auth</code> réglé sur <code>required</code> dans la configuration de votre courtier Kafka, cela peut entraîner des problèmes de configuration du point de terminaison Kafka.</p> <p>L'authentification des points de terminaison Kafka utilise les types d'authentification suivants. Ces types sont différents de ceux utilisés pour l'authentification d'autres points de terminaison, tels qu'Amazon SNS, et nécessitent des informations d'identification de nom d'utilisateur et de mot de passe.</p> <ul style="list-style-type: none"> • SASL/PLAIN • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 <p>Remarque : les paramètres de proxy de stockage configurés ne s'appliquent pas aux points de terminaison des services de la plateforme Kafka.</p>

Considérations relatives à l'utilisation du service de réplication CloudMirror

Considération	Détails
État de réplication	StorageGRID ne prend pas en charge le <code>x-amz-replication-status</code> en-tête.

Considération	Détails
Taille de l'objet	<p>La taille maximale des objets pouvant être répliqués vers un bucket de destination par le service de réplication CloudMirror est de 5 Tio, ce qui correspond à la taille maximale de l'objet <i>pris en charge</i>.</p> <p>Remarque : la taille maximale <i>recommandée</i> pour une seule opération PutObject est de 5 Gio (5 368 709 120 octets). Si vous avez des objets dont la taille est supérieure à 5 Gio, utilisez plutôt le téléchargement en plusieurs parties.</p>
Gestion des versions de bucket et identifiants de version	<p>Si le contrôle de version est activé pour le bucket S3 source dans StorageGRID , vous devez également activer le contrôle de version pour le bucket de destination.</p> <p>Lorsque vous utilisez le contrôle de version, notez que l'ordre des versions d'objet dans le compartiment de destination est le meilleur effort et n'est pas garanti par le service CloudMirror, en raison des limitations du protocole S3.</p> <p>Remarque : les ID de version du bucket source dans StorageGRID ne sont pas liés aux ID de version du bucket de destination.</p>
Balisateur des versions d'objet	<p>Le service CloudMirror ne réplique aucune requête PutObjectTagging ou DeleteObjectTagging qui fournit un ID de version, en raison des limitations du protocole S3. Étant donné que les ID de version de la source et de la destination ne sont pas liés, il n'existe aucun moyen de garantir qu'une mise à jour de balise vers un ID de version spécifique sera répliquée.</p> <p>En revanche, le service CloudMirror réplique les requêtes PutObjectTagging ou DeleteObjectTagging qui ne spécifient pas d'ID de version. Ces requêtes mettent à jour les balises de la dernière clé (ou de la dernière version si le bucket est versionné). Les ingestions normales avec des balises (pas de mises à jour de balisage) sont également répliquées.</p>
Téléchargements en plusieurs parties et ETag valeurs	<p>Lors de la mise en miroir d'objets téléchargés à l'aide d'un téléchargement en plusieurs parties, le service CloudMirror ne conserve pas les parties. En conséquence, le ETag la valeur de l'objet en miroir sera différente de la ETag valeur de l'objet d'origine.</p>
Objets chiffrés avec SSE-C (chiffrement côté serveur avec clés fournies par le client)	<p>Le service CloudMirror ne prend pas en charge les objets chiffrés avec SSE-C. Si vous tentez d'ingérer un objet dans le bucket source pour la réplication CloudMirror et que la requête inclut les en-têtes de requête SSE-C, l'opération échoue.</p>
Bucket avec verrouillage d'objet S3 activé	<p>La réplication n'est pas prise en charge pour les buckets source ou de destination avec le verrouillage d'objet S3 activé.</p>

Comprendre le service de réplication CloudMirror

Vous pouvez activer la réplication CloudMirror pour un bucket S3 si vous souhaitez que StorageGRID réplique les objets spécifiés ajoutés au bucket vers un ou plusieurs buckets de destination externes.

Par exemple, vous pouvez utiliser la réplication CloudMirror pour mettre en miroir des enregistrements clients spécifiques dans Amazon S3, puis exploiter les services AWS pour effectuer des analyses sur vos données.



La réplication CloudMirror n'est pas prise en charge si le verrouillage d'objet S3 est activé pour le compartiment source.

CloudMirror et ILM

La réplication CloudMirror fonctionne indépendamment des politiques ILM actives de la grille. Le service CloudMirror réplique les objets au fur et à mesure qu'ils sont stockés dans le bucket source et les livre au bucket de destination dès que possible. La livraison des objets répliqués est déclenchée lorsque l'ingestion de l'objet réussit.

CloudMirror et réplication inter-grille

La réplication CloudMirror présente des similitudes et des différences importantes avec la fonctionnalité de réplication inter-grille. "[Comparer la réplication inter-grille et la réplication CloudMirror](#)".

CloudMirror et buckets S3

La réplication CloudMirror est généralement configurée pour utiliser un bucket S3 externe comme destination. Cependant, vous pouvez également configurer la réplication pour utiliser un autre déploiement StorageGRID ou tout service compatible S3.

Buckets existants

Lorsque vous activez la réplication CloudMirror pour un bucket existant, seuls les nouveaux objets ajoutés à ce bucket sont répliqués. Tous les objets existants dans le bucket ne sont pas répliqués. Pour forcer la réplication d'objets existants, vous pouvez mettre à jour les métadonnées de l'objet existant en effectuant une copie d'objet.



Si vous utilisez la réplication CloudMirror pour copier des objets vers une destination Amazon S3, sachez qu'Amazon S3 limite la taille des métadonnées définies par l'utilisateur dans chaque en-tête de requête PUT à 2 Ko. Si un objet possède des métadonnées définies par l'utilisateur supérieures à 2 Ko, cet objet ne sera pas répliqué.

Plusieurs buckets de destination

Pour répliquer des objets d'un seul bucket vers plusieurs buckets de destination, spécifiez la destination de chaque règle dans le XML de configuration de réplication. Vous ne pouvez pas répliquer un objet dans plusieurs buckets en même temps.

Buckets versionnés ou non versionnés

Vous pouvez configurer la réplication CloudMirror sur des buckets versionnés ou non versionnés. Les buckets de destination peuvent être versionnés ou non. Vous pouvez utiliser n'importe quelle combinaison de buckets versionnés et non versionnés. Par exemple, vous pouvez spécifier un bucket versionné comme destination pour un bucket source non versionné, ou vice versa. Vous pouvez également effectuer une réplication entre des buckets non versionnés.

Suppression, boucles de réplication et événements

Comportement de suppression

Il s'agit du même comportement de suppression que le service Amazon S3, la réplication interrégionale (CRR). La suppression d'un objet dans un bucket source ne supprime jamais un objet répliqué dans la

destination. Si les buckets source et de destination sont tous deux versionnés, le marqueur de suppression est répliqué. Si le bucket de destination n'est pas versionné, la suppression d'un objet dans le bucket source ne réplique pas le marqueur de suppression dans le bucket de destination ni ne supprime l'objet de destination.

Protection contre les boucles de réplication

Lorsque les objets sont répliqués vers le bucket de destination, StorageGRID les marque comme « répliqués ». Un bucket StorageGRID de destination ne répliquera plus les objets marqués comme répliqués, vous protégeant ainsi des boucles de réplication accidentelles. Ce marquage de réplication est interne à StorageGRID et ne vous empêche pas d'exploiter AWS CRR lorsque vous utilisez un compartiment Amazon S3 comme destination.



L'en-tête personnalisé utilisé pour marquer une réplique est `x-ntap-sg-replica`. Ce marquage empêche un miroir en cascade. StorageGRID prend en charge un CloudMirror bidirectionnel entre deux grilles.

Événements dans le bucket de destination

L'unicité et l'ordre des événements dans le bucket de destination ne sont pas garantis. Plusieurs copies identiques d'un objet source peuvent être livrées à la destination à la suite d'opérations effectuées pour garantir la réussite de la livraison. Dans de rares cas, lorsque le même objet est mis à jour simultanément à partir de deux ou plusieurs sites StorageGRID différents, l'ordre des opérations sur le bucket de destination peut ne pas correspondre à l'ordre des événements sur le bucket source.

Comprendre les notifications pour les buckets

Vous pouvez activer la notification d'événement pour un compartiment S3 si vous souhaitez que StorageGRID envoie des notifications sur des événements spécifiés à un cluster Kafka de destination ou à Amazon Simple Notification Service.

Par exemple, vous pouvez configurer des alertes à envoyer aux administrateurs pour chaque objet ajouté à un bucket, où les objets représentent des fichiers journaux associés à un événement système critique.

Les notifications d'événements sont créées dans le bucket source comme spécifié dans la configuration de notification et sont livrées à la destination. Si un événement associé à un objet réussit, une notification concernant cet événement est créée et mise en file d'attente pour livraison.

L'unicité et l'ordre des notifications ne sont pas garantis. Plusieurs notifications d'un événement peuvent être délivrées à la destination à la suite d'opérations effectuées pour garantir le succès de la livraison. Et comme la livraison est asynchrone, il n'est pas garanti que l'ordre temporel des notifications à la destination corresponde à l'ordre des événements sur le bucket source, en particulier pour les opérations provenant de différents sites StorageGRID. Vous pouvez utiliser le `sequencer` saisissez le message d'événement pour déterminer l'ordre des événements pour un objet particulier, comme décrit dans la documentation Amazon S3.

Les notifications d'événements StorageGRID suivent l'API Amazon S3 avec certaines limitations.

- Les types d'événements suivants sont pris en charge :
 - s3 : Objet créé :
 - s3:ObjetCréé:Mettre
 - s3 : Objet créé : Publication
 - s3:ObjetCréé:Copier
 - s3 : Objet créé : Téléchargement multi-parties complet

- s3 : Objet supprimé :
- s3:ObjectRemoved:Supprimer
- s3 : Objet supprimé : Supprimer le marqueur créé
- s3 : Restauration d'objet : Publication
- Les notifications d'événements envoyées depuis StorageGRID utilisent le format JSON standard mais n'incluent pas certaines clés et utilisent des valeurs spécifiques pour d'autres, comme indiqué dans le tableau :

Nom de la clé	Valeur StorageGRID
Source de l'événement	sgws:s3
Région AWS	<i>non inclus</i>
x-amz-id-2	<i>non inclus</i>
arn	urn:sgws:s3:::bucket_name

Comprendre le service d'intégration de recherche

Vous pouvez activer l'intégration de la recherche pour un compartiment S3 si vous souhaitez utiliser un service de recherche et d'analyse de données externe pour les métadonnées de votre objet.

Le service d'intégration de recherche est un service StorageGRID personnalisé qui envoie automatiquement et de manière asynchrone les métadonnées d'objet S3 à un point de terminaison de destination chaque fois qu'un objet est créé ou supprimé, ou que ses métadonnées ou balises sont mises à jour. Vous pouvez ensuite utiliser des outils sophistiqués de recherche, d'analyse de données, de visualisation ou d'apprentissage automatique fournis par le service de destination pour rechercher, analyser et obtenir des informations à partir des données de vos objets.

Par exemple, vous pouvez configurer vos buckets pour envoyer des métadonnées d'objet S3 à un service Elasticsearch distant. Vous pouvez ensuite utiliser Elasticsearch pour effectuer des recherches dans plusieurs compartiments et effectuer des analyses sophistiquées des modèles présents dans les métadonnées de votre objet.

Bien que l'intégration Elasticsearch puisse être configurée sur un bucket avec S3 Object Lock activé, les métadonnées S3 Object Lock (y compris la date de conservation et le statut de conservation légale) des objets ne seront pas incluses dans les métadonnées envoyées à Elasticsearch.



Étant donné que le service d'intégration de recherche provoque l'envoi des métadonnées d'objet vers une destination, sa configuration XML est appelée « XML de configuration de notification *metadata* ». Ce XML de configuration est différent du « XML de configuration de notification » utilisé pour activer les notifications d'événements.

Intégration de la recherche et buckets S3

Vous pouvez activer le service d'intégration de recherche pour n'importe quel bucket versionné ou non versionné. L'intégration de la recherche est configurée en associant la configuration XML de notification de

métadonnées au bucket qui spécifie les objets sur lesquels agir et la destination des métadonnées de l'objet.

Les notifications de métadonnées sont générées sous la forme d'un document JSON nommé avec le nom du bucket, le nom de l'objet et l'ID de version, le cas échéant. Chaque notification de métadonnées contient un ensemble standard de métadonnées système pour l'objet en plus de toutes les balises de l'objet et des métadonnées utilisateur.



Pour les balises et les métadonnées utilisateur, StorageGRID transmet des dates et des nombres à Elasticsearch sous forme de chaînes ou de notifications d'événements S3. Pour configurer Elasticsearch afin d'interpréter ces chaînes comme des dates ou des nombres, suivez les instructions Elasticsearch pour le mappage de champs dynamiques et pour le mappage des formats de date. Vous devez activer les mappages de champs dynamiques sur l'index avant de configurer le service d'intégration de recherche. Une fois qu'un document est indexé, vous ne pouvez pas modifier les types de champs du document dans l'index.

Notifications de recherche

Les notifications de métadonnées sont générées et mises en file d'attente pour être envoyées chaque fois que :

- Un objet est créé.
- Un objet est supprimé, y compris lorsque des objets sont supprimés suite au fonctionnement de la politique ILM de la grille.
- Les métadonnées ou balises d'objet sont ajoutées, mises à jour ou supprimées. L'ensemble complet des métadonnées et des balises est toujours envoyé lors de la mise à jour, pas seulement les valeurs modifiées.

Une fois que vous avez ajouté une configuration XML de notification de métadonnées à un bucket, des notifications sont envoyées pour tous les nouveaux objets que vous créez et pour tous les objets que vous modifiez en mettant à jour ses données, ses métadonnées utilisateur ou ses balises. Cependant, les notifications ne sont pas envoyées pour les objets qui se trouvaient déjà dans le bucket. Pour garantir que les métadonnées d'objet pour tous les objets du bucket sont envoyées à la destination, vous devez effectuer l'une des opérations suivantes :

- Configurez le service d'intégration de recherche immédiatement après la création du bucket et avant d'ajouter des objets.
- Exécutez une action sur tous les objets déjà présents dans le bucket qui déclenchera l'envoi d'un message de notification de métadonnées à la destination.

Service d'intégration de recherche et Elasticsearch

Le service d'intégration de recherche StorageGRID prend en charge un cluster Elasticsearch comme destination. Comme pour les autres services de plateforme, la destination est spécifiée dans le point de terminaison dont l'URN est utilisée dans le XML de configuration du service. Utilisez le "[Outil de matrice d'interopérabilité NetApp](#)" pour déterminer les versions prises en charge d'Elasticsearch.

Gérer les points de terminaison des services de la plateforme

Configurer les points de terminaison des services de la plateforme

Avant de pouvoir configurer un service de plateforme pour un bucket, vous devez configurer au moins un point de terminaison comme destination du service de plateforme.

L'accès aux services de la plateforme est activé pour chaque locataire par un administrateur StorageGRID . Pour créer ou utiliser un point de terminaison de services de plateforme, vous devez être un utilisateur locataire avec l'autorisation d'accès Gérer les points de terminaison ou Racine, dans une grille dont la mise en réseau a été configurée pour permettre aux nœuds de stockage d'accéder aux ressources de point de terminaison externes. Pour un seul locataire, vous pouvez configurer un maximum de 500 points de terminaison de services de plateforme. Contactez votre administrateur StorageGRID pour plus d'informations.

Qu'est-ce qu'un point de terminaison de services de plateforme ?

Un point de terminaison de services de plateforme spécifie les informations dont StorageGRID a besoin pour accéder à la destination externe.

Par exemple, si vous souhaitez répliquer des objets d'un compartiment StorageGRID vers un compartiment Amazon S3, vous créez un point de terminaison de services de plateforme qui inclut les informations et les informations d'identification dont StorageGRID a besoin pour accéder au compartiment de destination sur Amazon.

Chaque type de service de plateforme nécessite son propre point de terminaison. Vous devez donc configurer au moins un point de terminaison pour chaque service de plateforme que vous prévoyez d'utiliser. Après avoir défini un point de terminaison de services de plateforme, vous utilisez l'URN du point de terminaison comme destination dans le XML de configuration utilisé pour activer le service.

Vous pouvez utiliser le même point de terminaison comme destination pour plusieurs buckets sources. Par exemple, vous pouvez configurer plusieurs buckets sources pour envoyer des métadonnées d'objet au même point de terminaison d'intégration de recherche afin de pouvoir effectuer des recherches dans plusieurs buckets. Vous pouvez également configurer un bucket source pour utiliser plusieurs points de terminaison comme cible, ce qui vous permet d'effectuer des opérations telles que l'envoi de notifications sur la création d'objets à une rubrique Amazon Simple Notification Service (Amazon SNS) et de notifications sur la suppression d'objets à une deuxième rubrique Amazon SNS.

Points de terminaison pour la réplication CloudMirror

StorageGRID prend en charge les points de terminaison de réplication qui représentent des buckets S3. Ces buckets peuvent être hébergés sur Amazon Web Services, le même déploiement StorageGRID ou un déploiement distant, ou un autre service.

Points de terminaison pour les notifications

StorageGRID prend en charge les points de terminaison Amazon SNS et Kafka. Les points de terminaison Simple Queue Service (SQS) ou AWS Lambda ne sont pas pris en charge.

Pour les points de terminaison Kafka, le protocole TLS mutuel n'est pas pris en charge. Par conséquent, si vous avez `ssl.client.auth` réglé sur `required` dans la configuration de votre courtier Kafka, cela peut entraîner des problèmes de configuration du point de terminaison Kafka.

Points de terminaison pour le service d'intégration de recherche

StorageGRID prend en charge les points de terminaison d'intégration de recherche qui représentent les clusters Elasticsearch. Ces clusters Elasticsearch peuvent être situés dans un centre de données local ou hébergés dans un cloud AWS ou ailleurs.

Le point de terminaison d'intégration de recherche fait référence à un index et un type Elasticsearch spécifiques. Vous devez créer l'index dans Elasticsearch avant de créer le point de terminaison dans StorageGRID, sinon la création du point de terminaison échouera. Vous n'avez pas besoin de créer le type avant de créer le point de terminaison. StorageGRID créera le type si nécessaire lorsqu'il envoie les

métadonnées de l'objet au point de terminaison.

Informations connexes

["Administrer StorageGRID"](#)

Spécifier l'URN pour le point de terminaison des services de la plateforme

Lorsque vous créez un point de terminaison de services de plateforme, vous devez spécifier un nom de ressource unique (URN). Vous utiliserez l'URN pour référencer le point de terminaison lorsque vous créerez un XML de configuration pour le service de plateforme. L'URN de chaque point de terminaison doit être unique.

StorageGRID valide les points de terminaison des services de la plateforme au fur et à mesure que vous les créez. Avant de créer un point de terminaison de services de plateforme, confirmez que la ressource spécifiée dans le point de terminaison existe et qu'elle est accessible.

éléments URN

L'URN d'un point de terminaison de services de plateforme doit commencer par `arn:aws` ou `urn:mysite`, comme suit :

- Si le service est hébergé sur Amazon Web Services (AWS), utilisez `arn:aws`
- Si le service est hébergé sur Google Cloud Platform (GCP), utilisez `arn:aws`
- Si le service est hébergé localement, utilisez `urn:mysite`

Par exemple, si vous spécifiez l'URN d'un point de terminaison CloudMirror hébergé sur StorageGRID, l'URN peut commencer par `urn:sgws`.

L'élément suivant de l'URN spécifie le type de service de plateforme, comme suit :

Service	Type
Réplication CloudMirror	s3
Notifications	sns`ou `kafka
Intégration de la recherche	es

Par exemple, pour continuer à spécifier l'URN d'un point de terminaison CloudMirror hébergé sur StorageGRID, vous devez ajouter `s3` obtenir `urn:sgws:s3`.

L'élément final de l'URN identifie la ressource cible spécifique à l'URI de destination.

Service	Ressource spécifique
Réplication CloudMirror	bucket-name
Notifications	sns-topic-name`ou `kafka-topic-name

Service	Ressource spécifique
Intégration de la recherche	domain-name/index-name/type-name Remarque : si le cluster Elasticsearch n'est pas configuré pour créer des index automatiquement, vous devez créer l'index manuellement avant de créer le point de terminaison.

URN pour les services hébergés sur AWS et GCP

Pour les entités AWS et GCP, l'URN complet est un ARN AWS valide. Par exemple:

- Réplication CloudMirror :

```
arn:aws:s3:::bucket-name
```

- Notifications:

```
arn:aws:sns:region:account-id:topic-name
```

- Intégration de la recherche :

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```



Pour un point de terminaison d'intégration de recherche AWS, le domain-name doit inclure la chaîne littérale domain/ , comme indiqué ici.

URN pour les services hébergés localement

Lorsque vous utilisez des services hébergés localement au lieu de services cloud, vous pouvez spécifier l'URN de toute manière qui crée un URN valide et unique, à condition que l'URN inclue les éléments requis dans les troisième et dernière positions. Vous pouvez laisser les éléments indiqués par facultatif vides, ou vous pouvez les spécifier de toute manière qui vous aide à identifier la ressource et à rendre l'URN unique. Par exemple:

- Réplication CloudMirror :

```
urn:mysite:s3:optional:optional:bucket-name
```

Pour un point de terminaison CloudMirror hébergé sur StorageGRID, vous pouvez spécifier un URN valide qui commence par urn:sgws :

```
urn:sgws:s3:optional:optional:bucket-name
```

- Notifications:

Spécifiez un point de terminaison Amazon Simple Notification Service :

```
urn:mysite:sns:optional:optional:sns-topic-name
```

Spécifiez un point de terminaison Kafka :

```
urn:mysite:kafka:optional:optional:kafka-topic-name
```

- Intégration de la recherche :

```
urn:mysite:es:optional:optional:domain-name/index-name/type-name
```



Pour les points de terminaison d'intégration de recherche hébergés localement, le domain-name l'élément peut être n'importe quelle chaîne à condition que l'URN du point de terminaison soit unique.

Créer un point de terminaison des services de plateforme

Vous devez créer au moins un point de terminaison du type correct avant de pouvoir activer un service de plateforme.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Les services de plateforme ont été activés pour votre compte locataire par un administrateur StorageGRID .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer les points de terminaison ou l'autorisation d'accès root"](#) .
- La ressource référencée par le point de terminaison des services de la plateforme a été créée :
 - Réplication CloudMirror : compartiment S3
 - Notification d'événement : Amazon Simple Notification Service (Amazon SNS) ou rubrique Kafka
 - Notification de recherche : index Elasticsearch, si le cluster de destination n'est pas configuré pour créer automatiquement des index.
- Vous avez les informations sur la ressource de destination :
 - Hôte et port pour l'identifiant de ressource uniforme (URI)



Si vous prévoyez d'utiliser un bucket hébergé sur un système StorageGRID comme point de terminaison pour la réplication CloudMirror, contactez l'administrateur de la grille pour déterminer les valeurs à saisir.

- Nom de ressource unique (URN)

"Spécifier l'URN pour le point de terminaison des services de la plateforme"

- Informations d'authentification (si nécessaire) :

Points de terminaison d'intégration de recherche

Pour les points de terminaison d'intégration de recherche, vous pouvez utiliser les informations d'identification suivantes :

- Clé d'accès : ID de clé d'accès et clé d'accès secrète
- HTTP de base : nom d'utilisateur et mot de passe

Points de terminaison de réplication CloudMirror

Pour les points de terminaison de réplication CloudMirror, vous pouvez utiliser les informations d'identification suivantes :

- Clé d'accès : ID de clé d'accès et clé d'accès secrète
- CAP (portail d'accès C2S) : URL d'informations d'identification temporaires, certificats serveur et client, clés client et une phrase secrète de clé privée client facultative.

Points de terminaison Amazon SNS

Pour les points de terminaison Amazon SNS, vous pouvez utiliser les informations d'identification suivantes :

- Clé d'accès : ID de clé d'accès et clé d'accès secrète

Points de terminaison Kafka

Pour les points de terminaison Kafka, vous pouvez utiliser les informations d'identification suivantes :

- SASL/PLAIN : Nom d'utilisateur et mot de passe
- SASL/SCRAM-SHA-256 : Nom d'utilisateur et mot de passe
- SASL/SCRAM-SHA-512 : Nom d'utilisateur et mot de passe

- Certificat de sécurité (si vous utilisez un certificat CA personnalisé)

- Si les fonctionnalités de sécurité Elasticsearch sont activées, vous disposez du privilège de surveillance du cluster pour les tests de connectivité, ainsi que du privilège d'écriture d'index ou des privilèges d'index et de suppression d'index pour les mises à jour de documents.

Étapes

1. Sélectionnez **STOCKAGE (S3) > Points de terminaison des services de plateforme**. La page Points de terminaison des services de la plateforme s'affiche.
2. Sélectionnez **Créer un point de terminaison**.
3. Saisissez un nom d'affichage pour décrire brièvement le point de terminaison et son objectif.

Le type de service de plateforme pris en charge par le point de terminaison est affiché à côté du nom du point de terminaison lorsqu'il est répertorié sur la page Points de terminaison. Vous n'avez donc pas besoin d'inclure ces informations dans le nom.

4. Dans le champ **URI**, spécifiez l'identifiant de ressource unique (URI) du point de terminaison.

Utilisez l'un des formats suivants :

```
https://host:port  
http://host:port
```

Si vous ne spécifiez pas de port, les ports par défaut suivants sont utilisés :

- Port 443 pour les URI HTTPS et port 80 pour les URI HTTP (la plupart des points de terminaison)
- Port 9092 pour les URI HTTPS et HTTP (points de terminaison Kafka uniquement)

Par exemple, l'URI d'un bucket hébergé sur StorageGRID pourrait être :

```
https://s3.example.com:10443
```

Dans cet exemple, `s3.example.com` représente l'entrée DNS pour l'IP virtuelle (VIP) du groupe haute disponibilité (HA) StorageGRID , et `10443` représente le port défini dans le point de terminaison de l'équilibreur de charge.



Dans la mesure du possible, vous devez vous connecter à un groupe HA de nœuds d'équilibrage de charge pour éviter un point de défaillance unique.

De même, l'URI d'un bucket hébergé sur AWS pourrait être :

```
https://s3-aws-region.amazonaws.com
```



Si le point de terminaison est utilisé pour le service de réplication CloudMirror, n'incluez pas le nom du bucket dans l'URI. Vous incluez le nom du bucket dans le champ **URN**.

5. Saisissez le nom de ressource unique (URN) pour le point de terminaison.



Vous ne pouvez pas modifier l'URN d'un point de terminaison une fois le point de terminaison créé.

6. Sélectionnez **Continuer**.

7. Sélectionnez une valeur pour **Type d'authentification**.

Points de terminaison d'intégration de recherche

Saisissez ou téléchargez les informations d'identification d'un point de terminaison d'intégration de recherche.

Les informations d'identification que vous fournissez doivent disposer d'autorisations d'écriture pour la ressource de destination.

Type d'authentification	Description	Informations d'identification
Anonyme	Fournit un accès anonyme à la destination. Fonctionne uniquement pour les points de terminaison dont la sécurité est désactivée.	Aucune authentification.
Clé d'accès	Utilise les informations d'identification de style AWS pour authentifier les connexions avec la destination.	<ul style="list-style-type: none">• ID de la clé d'accès• Clé d'accès secrète
HTTP de base	Utilise un nom d'utilisateur et un mot de passe pour authentifier les connexions à la destination.	<ul style="list-style-type: none">• Nom d'utilisateur• Mot de passe

Points de terminaison de réplication CloudMirror

Saisissez ou téléchargez les informations d'identification d'un point de terminaison de réplication CloudMirror.

Les informations d'identification que vous fournissez doivent disposer d'autorisations d'écriture pour la ressource de destination.

Type d'authentification	Description	Informations d'identification
Anonyme	Fournit un accès anonyme à la destination. Fonctionne uniquement pour les points de terminaison dont la sécurité est désactivée.	Aucune authentification.
Clé d'accès	Utilise les informations d'identification de style AWS pour authentifier les connexions avec la destination.	<ul style="list-style-type: none">• ID de la clé d'accès• Clé d'accès secrète

Type d'authentification	Description	Informations d'identification
CAP (Portail d'accès C2S)	Utilise des certificats et des clés pour authentifier les connexions à la destination.	<ul style="list-style-type: none"> • URL des informations d'identification temporaires • Certificat d'autorité de certification du serveur (téléchargement de fichier PEM) • Certificat client (téléchargement de fichier PEM) • Clé privée du client (téléchargement de fichier PEM, format crypté OpenSSL ou format de clé privée non cryptée) • Mot de passe de la clé privée du client (facultatif)

Points de terminaison Amazon SNS

Saisissez ou téléchargez les informations d'identification d'un point de terminaison Amazon SNS.

Les informations d'identification que vous fournissez doivent disposer d'autorisations d'écriture pour la ressource de destination.

Type d'authentification	Description	Informations d'identification
Anonyme	Fournit un accès anonyme à la destination. Fonctionne uniquement pour les points de terminaison dont la sécurité est désactivée.	Aucune authentification.
Clé d'accès	Utilise les informations d'identification de style AWS pour authentifier les connexions avec la destination.	<ul style="list-style-type: none"> • ID de la clé d'accès • Clé d'accès secrète

Points de terminaison Kafka

Saisissez ou téléchargez les informations d'identification d'un point de terminaison Kafka.

Les informations d'identification que vous fournissez doivent disposer d'autorisations d'écriture pour la ressource de destination.

Type d'authentification	Description	Informations d'identification
Anonyme	Fournit un accès anonyme à la destination. Fonctionne uniquement pour les points de terminaison dont la sécurité est désactivée.	Aucune authentification.

Type d'authentification	Description	Informations d'identification
SASL/PLAIN	Utilise un nom d'utilisateur et un mot de passe en texte brut pour authentifier les connexions à la destination.	<ul style="list-style-type: none"> Nom d'utilisateur Mot de passe
SASL/SCRAM-SHA-256	Utilise un nom d'utilisateur et un mot de passe à l'aide d'un protocole de défi-réponse et d'un hachage SHA-256 pour authentifier les connexions à la destination.	<ul style="list-style-type: none"> Nom d'utilisateur Mot de passe
SASL/SCRAM-SHA-512	Utilise un nom d'utilisateur et un mot de passe à l'aide d'un protocole de défi-réponse et d'un hachage SHA-512 pour authentifier les connexions à la destination.	<ul style="list-style-type: none"> Nom d'utilisateur Mot de passe

Sélectionnez **Utiliser l'authentification par délégation** si le nom d'utilisateur et le mot de passe sont dérivés d'un jeton de délégation obtenu à partir d'un cluster Kafka.

8. Sélectionnez **Continuer**.

9. Sélectionnez un bouton radio pour **Vérifier le serveur** pour choisir comment la connexion TLS au point de terminaison est vérifiée.

Type de vérification du certificat	Description
Utiliser un certificat CA personnalisé	Utilisez un certificat de sécurité personnalisé. Si vous sélectionnez ce paramètre, copiez et collez le certificat de sécurité personnalisé dans la zone de texte Certificat CA .
Utiliser le certificat CA du système d'exploitation	Utilisez le certificat Grid CA par défaut installé sur le système d'exploitation pour sécuriser les connexions.
Ne pas vérifier le certificat	Le certificat utilisé pour la connexion TLS n'est pas vérifié. Cette option n'est pas sécurisée.

10. Sélectionnez **Tester et créer un point de terminaison**.

- Un message de réussite s'affiche si le point de terminaison peut être atteint à l'aide des informations d'identification spécifiées. La connexion au point de terminaison est validée à partir d'un nœud sur chaque site.
- Un message d'erreur s'affiche si la validation du point de terminaison échoue. Si vous devez modifier le point de terminaison pour corriger l'erreur, sélectionnez **Retour aux détails du point de terminaison** et mettez à jour les informations. Ensuite, sélectionnez **Tester et créer un point de terminaison**.



La création du point de terminaison échoue si les services de plateforme ne sont pas activés pour votre compte locataire. Contactez votre administrateur StorageGRID .

Après avoir configuré un point de terminaison, vous pouvez utiliser son URN pour configurer un service de plateforme.

Informations connexes

- ["Spécifier l'URN pour le point de terminaison des services de la plateforme"](#)
- ["Configurer la réplication CloudMirror"](#)
- ["Configurer les notifications d'événements"](#)
- ["Configurer le service d'intégration de recherche"](#)

Tester la connexion pour le point de terminaison des services de la plateforme

Si la connexion à un service de plateforme a changé, vous pouvez tester la connexion pour le point de terminaison afin de valider que la ressource de destination existe et qu'elle est accessible à l'aide des informations d'identification que vous avez spécifiées.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer les points de terminaison ou l'autorisation d'accès root"](#) .

À propos de cette tâche

StorageGRID ne valide pas que les informations d'identification disposent des autorisations correctes.

Étapes

1. Sélectionnez **STOCKAGE (S3) > Points de terminaison des services de plateforme**.

La page Points de terminaison des services de plateforme s'affiche et affiche la liste des points de terminaison des services de plateforme qui ont déjà été configurés.

2. Sélectionnez le point de terminaison dont vous souhaitez tester la connexion.

La page des détails du point de terminaison s'affiche.

3. Sélectionnez **Tester la connexion**.

- Un message de réussite s'affiche si le point de terminaison peut être atteint à l'aide des informations d'identification spécifiées. La connexion au point de terminaison est validée à partir d'un nœud sur chaque site.
- Un message d'erreur s'affiche si la validation du point de terminaison échoue. Si vous devez modifier le point de terminaison pour corriger l'erreur, sélectionnez **Configuration** et mettez à jour les informations. Ensuite, sélectionnez **Tester et enregistrer les modifications**.

Modifier le point de terminaison des services de la plateforme

Vous pouvez modifier la configuration d'un point de terminaison de services de plateforme pour modifier son nom, son URI ou d'autres détails. Par exemple, vous devrez peut-être mettre à jour des informations d'identification expirées ou modifier l'URI pour

pointer vers un index Elasticsearch de sauvegarde pour le basculement. Vous ne pouvez pas modifier l'URN d'un point de terminaison de services de plateforme.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer les points de terminaison ou l'autorisation d'accès root"](#) .

Étapes

1. Sélectionnez **STOCKAGE (S3) > Points de terminaison des services de plateforme**.

La page Points de terminaison des services de plateforme s'affiche et affiche la liste des points de terminaison des services de plateforme qui ont déjà été configurés.


2. Sélectionnez le point de terminaison que vous souhaitez modifier.

La page des détails du point de terminaison s'affiche.

3. Sélectionnez **Configuration**.
4. Selon les besoins, modifiez la configuration du point de terminaison.



Vous ne pouvez pas modifier l'URN d'un point de terminaison une fois le point de terminaison créé.

- a. Pour modifier le nom d'affichage du point de terminaison, sélectionnez l'icône de modification  .
- b. Si nécessaire, modifiez l'URL.
- c. Si nécessaire, modifiez le type d'authentification.
 - Pour l'authentification par clé d'accès, modifiez la clé si nécessaire en sélectionnant **Modifier la clé S3** et en collant un nouvel ID de clé d'accès et une clé d'accès secrète. Si vous devez annuler vos modifications, sélectionnez **Annuler la modification de la clé S3**.
 - Pour l'authentification CAP (portail d'accès C2S), modifiez l'URL des informations d'identification temporaires ou la phrase secrète de la clé privée facultative du client et téléchargez de nouveaux fichiers de certificat et de clé selon les besoins.



La clé privée du client doit être au format crypté OpenSSL ou au format de clé privée non cryptée.

- d. Si nécessaire, modifiez la méthode de vérification du serveur.
5. Sélectionnez **Tester et enregistrer les modifications**.
 - Un message de réussite s'affiche si le point de terminaison peut être atteint à l'aide des informations d'identification spécifiées. La connexion au point de terminaison est vérifiée à partir d'un nœud sur chaque site.
 - Un message d'erreur s'affiche si la validation du point de terminaison échoue. Modifiez le point de terminaison pour corriger l'erreur, puis sélectionnez **Tester et enregistrer les modifications**.

Supprimer le point de terminaison des services de la plateforme

Vous pouvez supprimer un point de terminaison si vous ne souhaitez plus utiliser le service de plateforme associé.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer les points de terminaison ou l'autorisation d'accès root"](#) .

Étapes

1. Sélectionnez **STOCKAGE (S3) > Points de terminaison des services de plateforme**.

La page Points de terminaison des services de plateforme s'affiche et affiche la liste des points de terminaison des services de plateforme qui ont déjà été configurés.

2. Cochez la case correspondant à chaque point de terminaison que vous souhaitez supprimer.



Si vous supprimez un point de terminaison de services de plateforme en cours d'utilisation, le service de plateforme associé sera désactivé pour tous les buckets qui utilisent le point de terminaison. Toutes les demandes qui n'ont pas encore été traitées seront abandonnées. Toutes les nouvelles demandes continueront d'être générées jusqu'à ce que vous modifiez la configuration de votre bucket pour ne plus référencer l'URN supprimée. StorageGRID signalera ces demandes comme des erreurs irrécupérables.

3. Sélectionnez **Actions > Supprimer le point de terminaison**.

Un message de confirmation apparaît.

4. Sélectionnez **Supprimer le point de terminaison**.

Résoudre les erreurs de point de terminaison des services de plateforme

Si une erreur se produit lorsque StorageGRID tente de communiquer avec un point de terminaison de services de plateforme, un message s'affiche sur le tableau de bord. Sur la page Points de terminaison des services de la plateforme, la colonne Dernière erreur indique depuis combien de temps l'erreur s'est produite. Aucune erreur ne s'affiche si les autorisations associées aux informations d'identification d'un point de terminaison sont incorrectes.

Déterminer si une erreur s'est produite

Si des erreurs de point de terminaison des services de plateforme se sont produites au cours des 7 derniers jours, le tableau de bord du gestionnaire de locataires affiche un message d'alerte. Vous pouvez accéder à la page Points de terminaison des services de la plateforme pour voir plus de détails sur l'erreur.




One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

La même erreur qui apparaît sur le tableau de bord apparaît également en haut de la page Points de terminaison des services de la plateforme. Pour afficher un message d'erreur plus détaillé :

Étapes

1. Dans la liste des points de terminaison, sélectionnez le point de terminaison qui présente l'erreur.
2. Sur la page des détails du point de terminaison, sélectionnez **Connexion**. Cet onglet affiche uniquement

l'erreur la plus récente pour un point de terminaison et indique depuis combien de temps l'erreur s'est produite. Erreurs qui incluent l'icône X rouge  survenu au cours des 7 derniers jours.

Vérifiez si l'erreur est toujours d'actualité

Certaines erreurs peuvent continuer à s'afficher dans la colonne **Dernière erreur** même après avoir été résolues. Pour voir si une erreur est actuelle ou pour forcer la suppression d'une erreur résolue du tableau :

Étapes

1. Sélectionnez le point de terminaison.

La page des détails du point de terminaison s'affiche.

2. Sélectionnez **Connexion > Tester la connexion**.

La sélection de **Tester la connexion** amène StorageGRID à valider que le point de terminaison des services de la plateforme existe et qu'il est accessible avec les informations d'identification actuelles. La connexion au point de terminaison est validée à partir d'un nœud sur chaque site.

Résoudre les erreurs de point de terminaison

Vous pouvez utiliser le message **Dernière erreur** sur la page des détails du point de terminaison pour vous aider à déterminer la cause de l'erreur. Certaines erreurs peuvent nécessiter de modifier le point de terminaison pour résoudre le problème. Par exemple, une erreur CloudMirroring peut se produire si StorageGRID ne peut pas accéder au bucket S3 de destination car il ne dispose pas des autorisations d'accès appropriées ou si la clé d'accès a expiré. Le message est « Les informations d'identification du point de terminaison ou l'accès à la destination doivent être mis à jour » et les détails sont « AccessDenied » ou « InvalidAccessKeyId ».

Si vous devez modifier le point de terminaison pour résoudre une erreur, la sélection de **Tester et enregistrer les modifications** amène StorageGRID à valider le point de terminaison mis à jour et à confirmer qu'il est accessible avec les informations d'identification actuelles. La connexion au point de terminaison est validée à partir d'un nœud sur chaque site.

Étapes

1. Sélectionnez le point de terminaison.
2. Sur la page des détails du point de terminaison, sélectionnez **Configuration**.
3. Modifiez la configuration du point de terminaison selon vos besoins.
4. Sélectionnez **Connexion > Tester la connexion**.

Informations d'identification du point de terminaison avec des autorisations insuffisantes

Lorsque StorageGRID valide un point de terminaison de services de plateforme, il confirme que les informations d'identification du point de terminaison peuvent être utilisées pour contacter la ressource de destination et effectue une vérification des autorisations de base. Cependant, StorageGRID ne valide pas toutes les autorisations requises pour certaines opérations de services de plateforme. Pour cette raison, si vous recevez une erreur lorsque vous tentez d'utiliser un service de plateforme (par exemple « 403 Forbidden »), vérifiez les autorisations associées aux informations d'identification du point de terminaison.

Informations connexes

- [Administrer StorageGRID > Résoudre les problèmes des services de la plateforme](#)

- ["Créer un point de terminaison des services de plateforme"](#)
- ["Tester la connexion pour le point de terminaison des services de la plateforme"](#)
- ["Modifier le point de terminaison des services de la plateforme"](#)

Configurer la réplication CloudMirror

Pour activer la réplication CloudMirror pour un bucket, vous créez et appliquez un XML de configuration de réplication de bucket valide.

Avant de commencer

- Les services de plateforme ont été activés pour votre compte locataire par un administrateur StorageGRID.
- Vous avez déjà créé un bucket pour servir de source de réplication.
- Le point de terminaison que vous souhaitez utiliser comme destination pour la réplication CloudMirror existe déjà et vous disposez de son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer tous les buckets ou l'autorisation d'accès root"](#). Ces autorisations remplacent les paramètres d'autorisation dans les stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du gestionnaire de locataires.

À propos de cette tâche

La réplication CloudMirror copie les objets d'un bucket source vers un bucket de destination spécifié dans un point de terminaison.

Pour obtenir des informations générales sur la réplication de bucket et comment la configurer, consultez ["Documentation Amazon Simple Storage Service \(S3\) : Réplication d'objets"](#). Pour plus d'informations sur la manière dont StorageGRID implémente GetBucketReplication, DeleteBucketReplication et PutBucketReplication, consultez le ["Opérations sur les godets"](#).



La réplication CloudMirror présente des similitudes et des différences importantes avec la fonctionnalité de réplication inter-grille. Pour en savoir plus, voir ["Comparer la réplication inter-grille et la réplication CloudMirror"](#).

Notez les exigences et caractéristiques suivantes lors de la configuration de la réplication CloudMirror :

- Lorsque vous créez et appliquez un XML de configuration de réplication de compartiment valide, il doit utiliser l'URN d'un point de terminaison de compartiment S3 pour chaque destination.
- La réplication n'est pas prise en charge pour les buckets source ou de destination avec le verrouillage d'objet S3 activé.
- Si vous activez la réplication CloudMirror sur un bucket contenant des objets, les nouveaux objets ajoutés au bucket sont répliqués, mais les objets existants dans le bucket ne sont pas répliqués. Vous devez mettre à jour les objets existants pour déclencher la réplication.
- Si vous spécifiez une classe de stockage dans le XML de configuration de réplication, StorageGRID utilise cette classe lors de l'exécution d'opérations sur le point de terminaison S3 de destination. Le point de terminaison de destination doit également prendre en charge la classe de stockage spécifiée. Assurez-vous de suivre toutes les recommandations fournies par le fournisseur du système de destination.

Étapes

1. Activer la réplication pour votre bucket source :
 - Utilisez un éditeur de texte pour créer le XML de configuration de réplication requis pour activer la

réplication, comme spécifié dans l'API de réplication S3.

◦ Lors de la configuration du XML :

- Notez que StorageGRID ne prend en charge que la version V1 de la configuration de réplication. Cela signifie que StorageGRID ne prend pas en charge l'utilisation du `Filter` élément pour les règles et suit les conventions V1 pour la suppression des versions d'objet. Consultez la documentation Amazon sur la configuration de la réplication pour plus de détails.
- Utilisez l'URN d'un point de terminaison de compartiment S3 comme destination.
- Ajoutez éventuellement le `<StorageClass>` élément et spécifiez l'un des éléments suivants :
 - `STANDARD`: La classe de stockage par défaut. Si vous ne spécifiez pas de classe de stockage lorsque vous téléchargez un objet, le `STANDARD` la classe de stockage est utilisée.
 - `STANDARD_IA`: (Standard - accès peu fréquent.) Utilisez cette classe de stockage pour les données auxquelles on accède moins fréquemment, mais qui nécessitent néanmoins un accès rapide en cas de besoin.
 - `REDUCED_REDUNDANCY`: Utilisez cette classe de stockage pour les données non critiques et reproductibles qui peuvent être stockées avec moins de redondance que les `STANDARD` classe de stockage.
- Si vous spécifiez un `Role` dans la configuration XML, il sera ignoré. Cette valeur n'est pas utilisée par StorageGRID.

```
<ReplicationConfiguration>
  <Role></Role>
  <Rule>
    <Status>Enabled</Status>
    <Prefix>2020</Prefix>
    <Destination>
      <Bucket>urn:sgws:s3:::2017-records</Bucket>
      <StorageClass>STANDARD</StorageClass>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

2. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
3. Sélectionnez le nom du bucket source.

La page des détails du bucket apparaît.

4. Sélectionnez **Services de plateforme > Réplication**.
5. Cochez la case **Activer la réplication**.
6. Collez le XML de configuration de réplication dans la zone de texte et sélectionnez **Enregistrer les modifications**.



Les services de plateforme doivent être activés pour chaque compte de locataire par un administrateur StorageGRID à l'aide de Grid Manager ou de l'API Grid Management. Contactez votre administrateur StorageGRID si une erreur se produit lorsque vous enregistrez le XML de configuration.

7. Vérifiez que la réplication est correctement configurée :

- a. Ajoutez un objet au bucket source qui répond aux exigences de réplication telles que spécifiées dans la configuration de réplication.

Dans l'exemple présenté précédemment, les objets correspondant au préfixe « 2020 » sont répliqués.

- b. Confirmez que l'objet a été répliqué dans le bucket de destination.

Pour les petits objets, la réplication se produit rapidement.

Informations connexes

["Créer un point de terminaison des services de plateforme"](#)

Configurer les notifications d'événements

Vous activez les notifications pour un bucket en créant un XML de configuration de notification et en utilisant le gestionnaire de locataires pour appliquer le XML à un bucket.

Avant de commencer

- Les services de plateforme ont été activés pour votre compte locataire par un administrateur StorageGRID .
- Vous avez déjà créé un bucket pour servir de source de notifications.
- Le point de terminaison que vous souhaitez utiliser comme destination pour les notifications d'événements existe déjà et vous disposez de son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer tous les buckets ou l'autorisation d'accès root"](#) . Ces autorisations remplacent les paramètres d'autorisation dans les stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du gestionnaire de locataires.

À propos de cette tâche

Vous configurez les notifications d'événements en associant le XML de configuration de notification à un bucket source. Le XML de configuration de notification suit les conventions S3 pour la configuration des notifications de compartiment, avec la rubrique de destination Kafka ou Amazon SNS spécifiée comme URN d'un point de terminaison.

Pour obtenir des informations générales sur les notifications d'événements et comment les configurer, reportez-vous à la ["Documentation Amazon"](#) . Pour plus d'informations sur la manière dont StorageGRID implémente l'API de configuration des notifications de compartiment S3, reportez-vous à la ["instructions pour la mise en œuvre des applications clientes S3"](#) .

Notez les exigences et caractéristiques suivantes lors de la configuration des notifications d'événements pour un bucket :

- Lorsque vous créez et appliquez un XML de configuration de notification valide, il doit utiliser l'URN d'un point de terminaison de notifications d'événements pour chaque destination.
- Bien que la notification d'événement puisse être configurée sur un bucket avec le verrouillage d'objet S3 activé, les métadonnées du verrouillage d'objet S3 (y compris la date de conservation et le statut de conservation légale) des objets ne seront pas incluses dans les messages de notification.
- Une fois que vous avez configuré les notifications d'événements, chaque fois qu'un événement spécifié se produit pour un objet dans le compartiment source, une notification est générée et envoyée à la rubrique Amazon SNS ou Kafka utilisée comme point de terminaison de destination.

- Si vous activez les notifications d'événements pour un compartiment contenant des objets, les notifications sont envoyées uniquement pour les actions effectuées après l'enregistrement de la configuration de notification.

Étapes

1. Activer les notifications pour votre bucket source :

- Utilisez un éditeur de texte pour créer le XML de configuration de notification requis pour activer les notifications d'événements, comme spécifié dans l'API de notification S3.
- Lors de la configuration du XML, utilisez l'URN d'un point de terminaison de notifications d'événements comme rubrique de destination.

```
<NotificationConfiguration>
  <TopicConfiguration>
    <Id>Image-created</Id>
    <Filter>
      <S3Key>
        <FilterRule>
          <Name>prefix</Name>
          <Value>images/</Value>
        </FilterRule>
      </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
  </TopicConfiguration>
</NotificationConfiguration>
```

2. Dans le gestionnaire de locataires, sélectionnez **STOCKAGE (S3) > Buckets**.

3. Sélectionnez le nom du bucket source.

La page des détails du bucket apparaît.

4. Sélectionnez **Services de plateforme > Notifications d'événements**.

5. Cochez la case **Activer les notifications d'événements**.

6. Collez le XML de configuration de notification dans la zone de texte et sélectionnez **Enregistrer les modifications**.



Les services de plateforme doivent être activés pour chaque compte de locataire par un administrateur StorageGRID à l'aide de Grid Manager ou de l'API Grid Management. Contactez votre administrateur StorageGRID si une erreur se produit lorsque vous enregistrez le XML de configuration.

7. Vérifiez que les notifications d'événements sont correctement configurées :

- a. Exécutez une action sur un objet dans le bucket source qui répond aux exigences de déclenchement d'une notification telle que configurée dans le XML de configuration.

Dans l'exemple, une notification d'événement est envoyée chaque fois qu'un objet est créé avec le `images/` préfixe.

- b. Confirmez qu'une notification a été envoyée à la rubrique Amazon SNS ou Kafka de destination.

Par exemple, si votre rubrique de destination est hébergée sur Amazon SNS, vous pouvez configurer le service pour qu'il vous envoie un e-mail lorsque la notification est envoyée.

```
{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "sgws:s3",
      "eventTime": "2017-08-08T23:52:38Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "11111111111111111111"
      },
      "requestParameters": {
        "sourceIPAddress": "193.51.100.20"
      },
      "responseElements": {
        "x-amz-request-id": "122047343"
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "Image-created",
        "bucket": {
          "name": "test1",
          "ownerIdentity": {
            "principalId": "11111111111111111111"
          },
          "arn": "arn:sgws:s3:::test1"
        },
        "object": {
          "key": "images/cat.jpg",
          "size": 0,
          "eTag": "d41d8cd98f00b204e9800998ecf8427e",
          "sequencer": "14D90402421461C7"
        }
      }
    }
  ]
}
```

+

Si la notification est reçue sur la rubrique de destination, vous avez correctement configuré votre bucket

source pour les notifications StorageGRID .

Informations connexes

["Comprendre les notifications pour les buckets"](#)

["Utiliser l'API REST S3"](#)

["Créer un point de terminaison des services de plateforme"](#)

Configurer le service d'intégration de recherche

Vous activez l'intégration de recherche pour un bucket en créant un XML d'intégration de recherche et en utilisant le gestionnaire de locataires pour appliquer le XML au bucket.

Avant de commencer

- Les services de plateforme ont été activés pour votre compte locataire par un administrateur StorageGRID .
- Vous avez déjà créé un bucket S3 dont vous souhaitez indexer le contenu.
- Le point de terminaison que vous souhaitez utiliser comme destination pour le service d'intégration de recherche existe déjà et vous disposez de son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer tous les buckets ou l'autorisation d'accès root"](#) . Ces autorisations remplacent les paramètres d'autorisation dans les stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du gestionnaire de locataires.

À propos de cette tâche

Une fois que vous avez configuré le service d'intégration de recherche pour un bucket source, la création d'un objet ou la mise à jour des métadonnées ou des balises d'un objet déclenche l'envoi des métadonnées de l'objet au point de terminaison de destination.

Si vous activez le service d'intégration de recherche pour un bucket qui contient déjà des objets, les notifications de métadonnées ne sont pas automatiquement envoyées pour les objets existants. Mettez à jour ces objets existants pour garantir que leurs métadonnées sont ajoutées à l'index de recherche de destination.

Étapes

1. Activer l'intégration de la recherche pour un bucket :

- Utilisez un éditeur de texte pour créer le XML de notification de métadonnées requis pour activer l'intégration de la recherche.
- Lors de la configuration du XML, utilisez l'URN d'un point de terminaison d'intégration de recherche comme destination.

Les objets peuvent être filtrés sur le préfixe du nom de l'objet. Par exemple, vous pouvez envoyer des métadonnées pour des objets avec le préfixe `images` vers une destination et des métadonnées pour les objets avec le préfixe `videos` à un autre. Les configurations dont les préfixes se chevauchent ne sont pas valides et sont rejetées lorsqu'elles sont soumises. Par exemple, une configuration qui inclut une règle pour les objets avec le préfixe `test` et une deuxième règle pour les objets avec le préfixe `test2` n'est pas autorisé.

Au besoin, reportez-vous à [laexemples pour la configuration des métadonnées XML](#) .

```

<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>/Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Éléments dans le XML de configuration des notifications de métadonnées :

Nom	Description	Obligatoire
Configuration des notifications de métadonnées	<p>Balise de conteneur pour les règles utilisées pour spécifier les objets et la destination des notifications de métadonnées.</p> <p>Contient un ou plusieurs éléments de règle.</p>	Oui
Règle	<p>Balise de conteneur pour une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié.</p> <p>Les règles avec des préfixes qui se chevauchent sont rejetées.</p> <p>Inclus dans l'élément MetadataNotificationConfiguration.</p>	Oui
ID	<p>Identifiant unique de la règle.</p> <p>Inclus dans l'élément Règle.</p>	Non
Statut	<p>Le statut peut être « Activé » ou « Désactivé ». Aucune action n'est entreprise pour les règles désactivées.</p> <p>Inclus dans l'élément Règle.</p>	Oui
Préfixe	<p>Les objets qui correspondent au préfixe sont affectés par la règle et leurs métadonnées sont envoyées à la destination spécifiée.</p> <p>Pour faire correspondre tous les objets, spécifiez un préfixe vide.</p> <p>Inclus dans l'élément Règle.</p>	Oui
Destination	<p>Balise de conteneur pour la destination d'une règle.</p> <p>Inclus dans l'élément Règle.</p>	Oui

Nom	Description	Obligatoire
Urne	<p>URN de la destination où les métadonnées de l'objet sont envoyées. Doit être l'URN d'un point de terminaison StorageGRID avec les propriétés suivantes :</p> <ul style="list-style-type: none"> • `es` doit être le troisième élément. • L'URN doit se terminer par l'index et le type où les métadonnées sont stockées, sous la forme <code>domain-name/myindex/mytype</code>. <p>Les points de terminaison sont configurés à l'aide de l'API Tenant Manager ou Tenant Management. Ils prennent la forme suivante :</p> <ul style="list-style-type: none"> • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> <p>Le point de terminaison doit être configuré avant que le XML de configuration ne soit soumis, sinon la configuration échouera avec une erreur 404.</p> <p>L'URN est incluse dans l'élément Destination.</p>	Oui

2. Dans le gestionnaire de locataires, sélectionnez **STOCKAGE (S3) > Compartiments**.

3. Sélectionnez le nom du bucket source.

La page des détails du bucket apparaît.

4. Sélectionnez **Services de plateforme > Intégration de recherche**

5. Cochez la case **Activer l'intégration de la recherche**.

6. Collez la configuration de notification des métadonnées dans la zone de texte et sélectionnez **Enregistrer les modifications**.



Les services de plateforme doivent être activés pour chaque compte de locataire par un administrateur StorageGRID à l'aide de Grid Manager ou de l'API de gestion. Contactez votre administrateur StorageGRID si une erreur se produit lorsque vous enregistrez le XML de configuration.

7. Vérifiez que le service d'intégration de recherche est correctement configuré :

- Ajoutez un objet au bucket source qui répond aux exigences de déclenchement d'une notification de métadonnées comme spécifié dans le XML de configuration.

Dans l'exemple présenté précédemment, tous les objets ajoutés au bucket déclenchent une notification de métadonnées.

- Confirmez qu'un document JSON contenant les métadonnées et les balises de l'objet a été ajouté à l'index de recherche spécifié dans le point de terminaison.

Après avoir terminé

Si nécessaire, vous pouvez désactiver l'intégration de la recherche pour un bucket en utilisant l'une des méthodes suivantes :

- Sélectionnez **STOCKAGE (S3) > Compartiments** et décochez la case **Activer l'intégration de la recherche**.
- Si vous utilisez directement l'API S3, utilisez une demande de notification de métadonnées DELETE Bucket. Consultez les instructions pour implémenter les applications clientes S3.

Exemple : Configuration de notification de métadonnées qui s'applique à tous les objets

Dans cet exemple, les métadonnées d'objet pour tous les objets sont envoyées vers la même destination.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Exemple : Configuration de notification de métadonnées avec deux règles

Dans cet exemple, les métadonnées d'objet pour les objets qui correspondent au préfixe `/images` est envoyé à une destination, tandis que les métadonnées d'objet pour les objets qui correspondent au préfixe `/videos` est envoyé vers une deuxième destination.

```

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:2222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Format de notification des métadonnées

Lorsque vous activez le service d'intégration de recherche pour un bucket, un document JSON est généré et envoyé au point de terminaison de destination chaque fois que des métadonnées ou des balises d'objet sont ajoutées, mises à jour ou supprimées.

Cet exemple montre un exemple de JSON qui pourrait être généré lorsqu'un objet avec la clé `SGWS/Tagging.txt` est créé dans un bucket nommé `test`. Le `test` le bucket n'est pas versionné, donc le `versionId` la balise est vide.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region": "us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Champs inclus dans le document JSON

Le nom du document inclut le nom du bucket, le nom de l'objet et l'ID de version s'il est présent.

Informations sur le bucket et l'objet

bucket: Nom du bucket

key: Nom de la clé de l'objet

versionID: Version de l'objet, pour les objets dans les buckets versionnés

region: Région de bucket, par exemple us-east-1

Métadonnées du système

size: Taille de l'objet (en octets) telle que visible par un client HTTP

md5: Hachage d'objet

Métadonnées de l'utilisateur

metadata: Toutes les métadonnées utilisateur pour l'objet, sous forme de paires clé-valeur

key: valeur

Mots-clés

tags: Toutes les balises d'objet définies pour l'objet, sous forme de paires clé-valeur

key: valeur

Comment afficher les résultats dans Elasticsearch

Pour les balises et les métadonnées utilisateur, StorageGRID transmet des dates et des nombres à Elasticsearch sous forme de chaînes ou de notifications d'événements S3. Pour configurer Elasticsearch afin

d'interpréter ces chaînes comme des dates ou des nombres, suivez les instructions Elasticsearch pour le mappage de champs dynamiques et pour le mappage des formats de date. Activez les mappages de champs dynamiques sur l'index avant de configurer le service d'intégration de recherche. Une fois qu'un document est indexé, vous ne pouvez pas modifier les types de champs du document dans l'index.

Utiliser l'API REST S3

Versions et mises à jour prises en charge par l'API REST S3

StorageGRID prend en charge l'API Simple Storage Service (S3), qui est implémentée sous la forme d'un ensemble de services Web Representational State Transfer (REST).

La prise en charge de l'API REST S3 vous permet de connecter des applications orientées services développées pour les services Web S3 avec un stockage d'objets sur site qui utilise le système StorageGRID . Des modifications minimales sont requises dans l'utilisation actuelle des appels d'API REST S3 par une application cliente.

Versions prises en charge

StorageGRID prend en charge les versions spécifiques suivantes de S3 et HTTP.

Article	Version
Spécification de l'API S3	"Documentation Amazon Web Services (AWS) : Référence de l'API Amazon Simple Storage Service"
HTTP	<p>1,1</p> <p>Pour plus d'informations sur HTTP, consultez HTTP/1.1 (RFC 7230-35).</p> <p>"IETF RFC 2616 : Protocole de transfert hypertexte (HTTP/1.1)"</p> <p>Remarque : StorageGRID ne prend pas en charge le pipeline HTTP/1.1.</p>

Mises à jour de la prise en charge de l'API REST S3

Libérer	Commentaires
11,9	<ul style="list-style-type: none"> • Ajout de la prise en charge des valeurs de somme de contrôle SHA-256 précalculées pour les requêtes suivantes et les en-têtes pris en charge. Vous pouvez utiliser cette fonctionnalité pour vérifier l'intégrité des objets téléchargés : <ul style="list-style-type: none"> ◦ Téléchargement complet en plusieurs parties : <code>x-amz-checksum-sha256</code> ◦ Créer un téléchargement multi-parties : <code>x-amz-checksum-algorithm</code> ◦ Obtenir l'objet : <code>x-amz-checksum-mode</code> ◦ HeadObject : <code>x-amz-checksum-mode</code> ◦ Liste des pièces ◦ PutObject : <code>x-amz-checksum-sha256</code> ◦ TéléchargerPartie : <code>x-amz-checksum-sha256</code> • Ajout de la possibilité pour l'administrateur de la grille de contrôler les paramètres de conservation et de conformité au niveau du locataire. Ces paramètres affectent les paramètres de verrouillage d'objet S3. <ul style="list-style-type: none"> ◦ Mode de conservation par défaut du bucket et mode de conservation des objets : Gouvernance ou Conformité, si autorisé par l'administrateur de la grille. ◦ Période de conservation par défaut du bucket et date de conservation de l'objet : doit être inférieure ou égale à ce qui est autorisé par la période de conservation maximale définie par l'administrateur de la grille. • Prise en charge améliorée pour <code>aws-chunked</code> encodage et streaming de contenu <code>x-amz-content-sha256</code> valeurs. Limites: <ul style="list-style-type: none"> ◦ Si présent, <code>chunk-signature</code> est facultatif et non validé ◦ Si présent, <code>x-amz-trailer</code> le contenu est ignoré
11,8	Mise à jour des noms des opérations S3 pour correspondre aux noms utilisés dans le "Documentation Amazon Web Services (AWS) : Référence de l'API Amazon Simple Storage Service" .
11,7	<ul style="list-style-type: none"> • Ajouté "Référence rapide : requêtes API S3 prises en charge" . • Ajout de la prise en charge de l'utilisation du mode GOUVERNANCE avec S3 Object Lock. • Ajout de la prise en charge spécifique à StorageGRID <code>x-ntap-sg-cgr-replication-status</code> en-tête de réponse pour les requêtes GET Object et HEAD Object. Cet en-tête fournit l'état de réplification d'un objet pour la réplification inter-grille. • Les requêtes SelectObjectContent prennent désormais en charge les objets Parquet.

Libérer	Commentaires
11,6	<ul style="list-style-type: none"> • Ajout de la prise en charge de l'utilisation du <code>partNumber</code> paramètre de requête dans les requêtes d'objet GET et d'objet HEAD. • Ajout de la prise en charge d'un mode de conservation par défaut et d'une période de conservation par défaut au niveau du bucket pour S3 Object Lock. • Ajout du support pour le <code>s3:object-lock-remaining-retention-days</code> clé de condition de politique pour définir la plage de périodes de conservation autorisées pour vos objets. • La taille maximale <i>recommandée</i> pour une seule opération d'objet PUT a été modifiée à 5 Gio (5 368 709 120 octets). Si vous avez des objets dont la taille est supérieure à 5 Gio, utilisez plutôt le téléchargement en plusieurs parties.
11,5	<ul style="list-style-type: none"> • Prise en charge ajoutée pour la gestion du chiffrement du bucket. • Ajout de la prise en charge du verrouillage d'objet S3 et des demandes de conformité héritées obsolètes. • Ajout de la prise en charge de l'utilisation de DELETE Multiple Objects sur des buckets versionnés. • Le <code>Content-MD5</code> l'en-tête de requête est désormais correctement pris en charge.
11,4	<ul style="list-style-type: none"> • Prise en charge ajoutée pour le balisage des buckets DELETE, GET et PUT. Les balises d'allocation des coûts ne sont pas prises en charge. • Pour les buckets créés dans StorageGRID 11.4, la restriction des noms de clés d'objet pour respecter les meilleures pratiques en matière de performances n'est plus nécessaire. • Ajout de la prise en charge des notifications de bucket sur le <code>s3:ObjectRestore:Post</code> type d'événement. • Les limites de taille AWS pour les pièces en plusieurs parties sont désormais appliquées. Chaque partie d'un téléchargement en plusieurs parties doit être comprise entre 5 Mio et 5 Gio. La dernière partie peut être inférieure à 5 Mio. • Ajout de la prise en charge de TLS 1.3
11,3	<ul style="list-style-type: none"> • Ajout de la prise en charge du chiffrement côté serveur des données d'objet avec des clés fournies par le client (SSE-C). • Prise en charge ajoutée pour les opérations de cycle de vie du bucket DELETE, GET et PUT (action d'expiration uniquement) et pour le <code>x-amz-expiration</code> en-tête de réponse. • Objet PUT mis à jour, Objet PUT - Copie et Téléchargement en plusieurs parties pour décrire l'impact des règles ILM qui utilisent le placement synchrone lors de l'ingestion. • Les chiffrements TLS 1.1 ne sont plus pris en charge.

Libérer	Commentaires
11,2	<p>Prise en charge ajoutée pour la restauration d'objets POST à utiliser avec les pools de stockage cloud. Ajout de la prise en charge de l'utilisation de la syntaxe AWS pour l'ARN, les clés de condition de stratégie et les variables de stratégie dans les stratégies de groupe et de compartiment. Les stratégies de groupe et de compartiment existantes qui utilisent la syntaxe StorageGRID continueront d'être prises en charge.</p> <p>Remarque : les utilisations d'ARN/URN dans d'autres configurations JSON/XML, y compris celles utilisées dans les fonctionnalités StorageGRID personnalisées, n'ont pas changé.</p>
11,1	Ajout de la prise en charge du partage de ressources inter-origines (CORS), du HTTP pour les connexions client S3 aux nœuds de grille et des paramètres de conformité sur les buckets.
11,0	Prise en charge ajoutée pour la configuration des services de plateforme (réplication CloudMirror, notifications et intégration de recherche Elasticsearch) pour les buckets. La prise en charge des contraintes d'emplacement de balisage d'objets pour les buckets et la cohérence disponible ont également été ajoutées.
10,4	Ajout de la prise en charge des modifications d'analyse ILM apportées au contrôle de version, aux mises à jour de la page Noms de domaine de point de terminaison, aux conditions et variables dans les politiques, aux exemples de politiques et à l'autorisation PutOverwriteObject.
10,3	Prise en charge ajoutée pour le contrôle de version.
10,2	Ajout de la prise en charge des stratégies d'accès aux groupes et aux buckets, ainsi que de la copie en plusieurs parties (Télécharger une partie - Copier).
10,1	Prise en charge ajoutée pour le téléchargement en plusieurs parties, les demandes de type hébergé virtuellement et l'authentification v4.
10,0	Prise en charge initiale de l'API REST S3 par le système StorageGRID . La version actuellement prise en charge de la <i>Référence API du service de stockage simple</i> est le 01/03/2006.

Référence rapide : requêtes API S3 prises en charge

Cette page résume la manière dont StorageGRID prend en charge les API Amazon Simple Storage Service (S3).

Cette page inclut uniquement les opérations S3 prises en charge par StorageGRID.



Pour voir la documentation AWS pour chaque opération, sélectionnez le lien dans l'en-tête.

Paramètres de requête URI courants et en-têtes de requête

Sauf indication contraire, les paramètres de requête URI courants suivants sont pris en charge :

- `versionId`(comme requis pour les opérations sur les objets)

Sauf indication contraire, les en-têtes de requête courants suivants sont pris en charge :

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

Informations connexes

- ["Détails d'implémentation de l'API REST S3"](#)
- ["Référence de l'API Amazon Simple Storage Service : en-têtes de requête courants"](#)

"Abandonner le téléchargement en plusieurs parties"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus ce paramètre de requête URI supplémentaire :

- `uploadId`

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations pour les téléchargements en plusieurs parties"](#)

"Téléchargement complet en plusieurs parties"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus ce paramètre de requête URI supplémentaire :

- `uploadId`
- `x-amz-checksum-sha256`

Balises XML du corps de la requête

StorageGRID prend en charge ces balises XML de corps de requête :

- ChecksumSHA256
- CompleteMultipartUpload
- ETag
- Part
- PartNumber

Documentation de StorageGRID

["Téléchargement complet en plusieurs parties"](#)

"Copier l'objet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande, plus ces en-têtes supplémentaires :

- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-modified-since
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-metadata-directive
- x-amz-object-lock-legal-hold
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-storage-class
- x-amz-tagging
- x-amz-tagging-directive
- x-amz-meta-`<metadata-name>`

Corps de la requête

Aucune

Documentation de StorageGRID

["Copier l'objet"](#)

"Créer un bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande, plus ces en-têtes supplémentaires :

- x-amz-bucket-object-lock-enabled

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Créer un téléchargement multi-parties"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande, plus ces en-têtes supplémentaires :

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-algorithm
- x-amz-server-side-encryption
- x-amz-storage-class
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-tagging
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold
- x-amz-meta-`<metadata-name>`

Corps de la requête

Aucune

Documentation de StorageGRID

["Créer un téléchargement multi-parties"](#)

"Supprimer le bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Documentation de StorageGRID

["Opérations sur les godets"](#)

"SupprimerBucketCors"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Supprimer le chiffrement du bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Supprimer le cycle de vie du bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

- ["Opérations sur les godets"](#)
- ["Créer une configuration du cycle de vie S3"](#)

"Supprimer la politique de bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"SupprimerBucketReplication"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Supprimer le balisage du bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Supprimer l'objet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus cet en-tête de requête supplémentaire :

- `x-amz-bypass-governance-retention`

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les objets"](#)

"Supprimer les objets"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus cet en-tête de requête supplémentaire :

- `x-amz-bypass-governance-retention`

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

["Opérations sur les objets"](#)

"Supprimer l'étiquetage des objets"

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les objets"](#)

"ObtenirBucketAcl"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"ObtenirBucketCors"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Obtenir le chiffrement du bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"GetBucketLifecycleConfiguration"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

- ["Opérations sur les godets"](#)
- ["Créer une configuration du cycle de vie S3"](#)

"Obtenir l'emplacement du bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Configuration de GetBucketNotification"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Obtenir la politique de Bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Réplication GetBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Obtenir le balisage du bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Obtenir la gestion des versions du bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Obtenir l'objet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus ces paramètres de requête URI supplémentaires :

- `x-amz-checksum-mode`
- `partNumber`
- `response-cache-control`
- `response-content-disposition`
- `response-content-encoding`
- `response-content-language`
- `response-content-type`
- `response-expires`

Et ces en-têtes de requête supplémentaires :

- `Range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`

- If-None-Match
- If-Unmodified-Since

Corps de la requête

Aucune

Documentation de StorageGRID

["Obtenir l'objet"](#)

"ObtenirObjectAcl"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les objets"](#)

"Obtenir la conservation légale de l'objet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#)

"Obtenir la configuration du verrouillage de l'objet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#)

"Obtenir la rétention d'objet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

"Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"

"Obtenir l'étiquetage des objets"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les objets"](#)

"Tête de godet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"HeadObject"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande, plus ces en-têtes supplémentaires :

- x-amz-checksum-mode
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since
- Range

Corps de la requête

Aucune

Documentation de StorageGRID

["HeadObject"](#)

"Listes de seaux"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

[Opérations sur le service](#) › [ListBuckets](#)

"ListeMultipartUploads"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus ces paramètres supplémentaires :

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`

Corps de la requête

Aucune

Documentation de StorageGRID

["ListeMultipartUploads"](#)

"Liste d'objets"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus ces paramètres supplémentaires :

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`
- `prefix`

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"ListObjectsV2"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus ces paramètres supplémentaires :

- continuation-token
- delimiter
- encoding-type
- fetch-owner
- max-keys
- prefix
- start-after

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"ListObjectVersions"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus ces paramètres supplémentaires :

- delimiter
- encoding-type
- key-marker
- max-keys
- prefix
- version-id-marker

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Liste des pièces"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus ces paramètres supplémentaires :

- max-parts

- part-number-marker
- uploadId

Corps de la requête

Aucune

Documentation de StorageGRID

["ListeMultipartUploads"](#)

"PutBucketCors"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Cryptage PutBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Balises XML du corps de la requête

StorageGRID prend en charge ces balises XML de corps de requête :

- ApplyServerSideEncryptionByDefault
- Rule
- ServerSideEncryptionConfiguration
- SSEAlgorithm

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Configuration du cycle de vie de PutBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Balises XML du corps de la requête

StorageGRID prend en charge ces balises XML de corps de requête :

- And
- Days
- Expiration

- ExpiredObjectDeleteMarker
- Filter
- ID
- Key
- LifecycleConfiguration
- NewerNoncurrentVersions
- NoncurrentDays
- NoncurrentVersionExpiration
- Prefix
- Rule
- Status
- Tag
- Value

Documentation de StorageGRID

- ["Opérations sur les godets"](#)
- ["Créer une configuration du cycle de vie S3"](#)

"Configuration de PutBucketNotification"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Balises XML du corps de la requête

StorageGRID prend en charge ces balises XML de corps de requête :

- Event
- Filter
- FilterRule
- Id
- Name
- NotificationConfiguration
- Prefix
- S3Key
- Suffix
- Topic
- TopicConfiguration
- Value

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Politique de PutBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Pour plus de détails sur les champs de corps JSON pris en charge, voir ["Utiliser des politiques d'accès aux buckets et aux groupes"](#).

"Réplication de PutBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Balises XML du corps de la requête

- Bucket
- Destination
- Prefix
- ReplicationConfiguration
- Rule
- Status
- StorageClass

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Balisage de PutBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Gestion des versions de PutBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Paramètres du corps de la requête

StorageGRID prend en charge ces paramètres de corps de requête :

- VersioningConfiguration
- Status

Documentation de StorageGRID

"Opérations sur les godets"

"Mettre l'objet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande, plus ces en-têtes supplémentaires :

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-sha256
- x-amz-server-side-encryption
- x-amz-storage-class
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-tagging
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold
- x-amz-meta-`<metadata-name>`

Corps de la requête

- Données binaires de l'objet

Documentation de StorageGRID

"Mettre l'objet"

"MettreObjetLegalHold"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#)

"Configuration de PutObjectLock"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#)

"PutObjectRetention"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande, plus cet en-tête supplémentaire :

- x-amz-bypass-governance-retention

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#)

"Balisage d'objets"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

["Opérations sur les objets"](#)

"Restaurer l'objet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Pour plus de détails sur les champs de corps pris en charge, voir ["Restaurer l'objet"](#) .

"Sélectionner le contenu de l'objet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Pour plus de détails sur les champs de corps pris en charge, consultez les éléments suivants :

- ["Utiliser S3 Select"](#)
- ["Sélectionner le contenu de l'objet"](#)

"Télécharger une partie"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus ces paramètres de requête URI supplémentaires :

- `partNumber`
- `uploadId`

Et ces en-têtes de requête supplémentaires :

- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

Corps de la requête

- Données binaires de la pièce

Documentation de StorageGRID

["Télécharger une partie"](#)

"TéléchargerPartCopy"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus ces paramètres de requête URI supplémentaires :

- `partNumber`
- `uploadId`

Et ces en-têtes de requête supplémentaires :

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`

- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-range
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5

Corps de la requête

Aucune

Documentation de StorageGRID

["TéléchargerPartCopy"](#)

Tester la configuration de l'API REST S3

Vous pouvez utiliser l'interface de ligne de commande Amazon Web Services (AWS CLI) pour tester votre connexion au système et vérifier que vous pouvez lire et écrire des objets.

Avant de commencer

- Vous avez téléchargé et installé l'AWS CLI depuis ["aws.amazon.com/cli"](https://aws.amazon.com/cli) .
- En option, vous avez ["créé un point de terminaison d'équilibrage de charge"](#) . Sinon, vous connaissez l'adresse IP du nœud de stockage auquel vous souhaitez vous connecter et le numéro de port à utiliser. Voir ["Adresses IP et ports pour les connexions client"](#) .
- Tu as ["créé un compte locataire S3"](#) .
- Vous vous êtes connecté au locataire et ["créé une clé d'accès"](#) .

Pour plus de détails sur ces étapes, voir ["Configurer les connexions client"](#) .

Étapes

1. Configurez les paramètres AWS CLI pour utiliser le compte que vous avez créé dans le système StorageGRID :
 - a. Entrer en mode configuration : `aws configure`
 - b. Saisissez l'ID de clé d'accès pour le compte que vous avez créé.
 - c. Saisissez la clé d'accès secrète du compte que vous avez créé.
 - d. Entrez la région par défaut à utiliser. Par exemple : `us-east-1` .
 - e. Saisissez le format de sortie par défaut à utiliser ou appuyez sur **Entrée** pour sélectionner JSON.
2. Créer un bucket.

Cet exemple suppose que vous avez configuré un point de terminaison d'équilibrage de charge pour utiliser l'adresse IP 10.96.101.17 et le port 10443.

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

Si le bucket est créé avec succès, l'emplacement du bucket est renvoyé, comme indiqué dans l'exemple suivant :

```
"Location": "/testbucket"
```

3. Télécharger un objet.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
put-object --bucket testbucket --key s3.pdf --body C:\s3-
test\upload\s3.pdf
```

Si l'objet est téléchargé avec succès, un Etag est renvoyé, qui est un hachage des données de l'objet.

4. Répertoirez le contenu du bucket pour vérifier que l'objet a été téléchargé.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

5. Supprimer l'objet.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

6. Supprimer le bucket.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

Comment StorageGRID implémente l'API REST S3

Demandes clients conflictuelles

Les demandes client conflictuelles, telles que deux clients écrivant sur la même clé, sont résolues sur la base des « derniers gagnants ».

Le moment de l'évaluation des « dernières victoires » est basé sur le moment où le système StorageGRID termine une demande donnée, et non sur le moment où les clients S3 commencent une opération.

Valeurs de cohérence

La cohérence fournit un équilibre entre la disponibilité des objets et la cohérence de ces objets sur différents nœuds de stockage et sites. Vous pouvez modifier la cohérence selon les besoins de votre application.

Par défaut, StorageGRID garantit la cohérence de lecture après écriture pour les objets nouvellement créés. Tout GET suivant un PUT terminé avec succès pourra lire les données nouvellement écrites. Les écrasements d'objets existants, les mises à jour de métadonnées et les suppressions sont finalement cohérents. Les écrasements prennent généralement quelques secondes ou minutes pour se propager, mais peuvent prendre jusqu'à 15 jours.

Si vous souhaitez effectuer des opérations sur les objets avec une cohérence différente, vous pouvez :

- Spécifier une consistance pour [chaque seau](#) .
- Spécifier une consistance pour [chaque opération API](#) .
- Modifiez la cohérence par défaut de l'ensemble de la grille en effectuant l'une des tâches suivantes :
 - Dans le gestionnaire de grille, accédez à **CONFIGURATION > Système > Paramètres de stockage > Cohérence par défaut**.
 - .



Une modification de la cohérence à l'échelle de la grille s'applique uniquement aux compartiments créés après la modification du paramètre. Pour déterminer les détails d'une modification, consultez le journal d'audit situé à l'adresse `/var/local/log` (rechercher **consistencyLevel**).

Valeurs de cohérence

La cohérence affecte la manière dont les métadonnées utilisées par StorageGRID pour suivre les objets sont distribuées entre les nœuds et, par conséquent, la disponibilité des objets pour les demandes des clients.

Vous pouvez définir la cohérence d'un bucket ou d'une opération API sur l'une des valeurs suivantes :

- **Tous** : Tous les nœuds reçoivent les données immédiatement, sinon la demande échouera.
- **Strong-global** : garantit la cohérence de lecture après écriture pour toutes les demandes client sur tous les sites.
- **Strong-site** : garantit la cohérence de lecture après écriture pour toutes les requêtes client au sein d'un site.
- **Lecture après nouvelle écriture** : (par défaut) Fournit une cohérence de lecture après écriture pour les nouveaux objets et une cohérence éventuelle pour les mises à jour d'objets. Offre des garanties de haute disponibilité et de protection des données. Recommandé dans la plupart des cas.
- **Disponible** : Fournit une cohérence éventuelle pour les nouveaux objets et les mises à jour d'objets. Pour les buckets S3, utilisez-les uniquement si nécessaire (par exemple, pour un bucket contenant des valeurs de journal rarement lues ou pour des opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les buckets S3 FabricPool .

Utiliser la cohérence « Lecture après nouvelle écriture » et « Disponible »

Lorsqu'une opération HEAD ou GET utilise la cohérence « Lecture après nouvelle écriture », StorageGRID effectue la recherche en plusieurs étapes, comme suit :

- Il recherche d'abord l'objet en utilisant une faible cohérence.
- Si cette recherche échoue, elle répète la recherche à la valeur de cohérence suivante jusqu'à ce qu'elle atteigne une cohérence équivalente au comportement de strong-global.

Si une opération HEAD ou GET utilise la cohérence « Lecture après nouvelle écriture » mais que l'objet n'existe pas, la recherche d'objet atteindra toujours une cohérence équivalente au comportement de strong-global. Étant donné que cette cohérence nécessite que plusieurs copies des métadonnées de l'objet soient disponibles sur chaque site, vous pouvez recevoir un nombre élevé d'erreurs de serveur interne 500 si deux ou plusieurs nœuds de stockage sur le même site ne sont pas disponibles.

À moins que vous n'ayez besoin de garanties de cohérence similaires à celles d'Amazon S3, vous pouvez éviter ces erreurs pour les opérations HEAD et GET en définissant la cohérence sur « Disponible ».

Lorsqu'une opération HEAD ou GET utilise la cohérence « Disponible », StorageGRID fournit uniquement la cohérence éventuelle. Il ne réessaye pas une opération ayant échoué en augmentant la cohérence, il ne nécessite donc pas que plusieurs copies des métadonnées de l'objet soient disponibles.

Spécifier la cohérence pour le fonctionnement de l'API

Pour définir la cohérence d'une opération API individuelle, les valeurs de cohérence doivent être prises en charge pour l'opération et vous devez spécifier la cohérence dans l'en-tête de la demande. Cet exemple définit la cohérence sur « Strong-site » pour une opération GetObject.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```



Vous devez utiliser la même cohérence pour les opérations PutObject et GetObject.

Spécifier la cohérence du bucket

Pour définir la cohérence du bucket, vous pouvez utiliser le StorageGRID ["Cohérence du seau PUT"](#) demande. Ou vous pouvez ["changer la consistance d'un seau"](#) du gestionnaire locataire.

Lorsque vous définissez la cohérence d'un bucket, tenez compte des éléments suivants :

- La définition de la cohérence d'un bucket détermine la cohérence utilisée pour les opérations S3 effectuées sur les objets du bucket ou sur la configuration du bucket. Cela n'affecte pas les opérations sur le bucket lui-même.
- La cohérence d'une opération API individuelle remplace la cohérence du bucket.
- En général, les buckets doivent utiliser la cohérence par défaut, « Lecture après nouvelle écriture ». Si les requêtes ne fonctionnent pas correctement, modifiez le comportement du client de l'application si possible. Ou configurez le client pour spécifier la cohérence de chaque demande d'API. Définissez la consistance au niveau du seau uniquement en dernier recours.

Comment les règles de cohérence et de gestion des informations interagissent pour affecter la protection des données

Votre choix de cohérence et votre règle ILM affectent la manière dont les objets sont protégés. Ces paramètres peuvent interagir.

Par exemple, la cohérence utilisée lors du stockage d'un objet affecte le placement initial des métadonnées de l'objet, tandis que le comportement d'ingestion sélectionné pour la règle ILM affecte le placement initial des copies de l'objet. Étant donné que StorageGRID nécessite l'accès aux métadonnées d'un objet et à ses données pour répondre aux demandes des clients, la sélection de niveaux de protection correspondants pour la cohérence et le comportement d'ingestion peut fournir une meilleure protection initiale des données et des réponses système plus prévisibles.

Ce qui suit "options d'ingestion" sont disponibles pour les règles ILM :

Double engagement

StorageGRID effectue immédiatement des copies intermédiaires de l'objet et renvoie le succès au client. Les copies spécifiées dans la règle ILM sont réalisées lorsque cela est possible.

Strict

Toutes les copies spécifiées dans la règle ILM doivent être effectuées avant que le succès ne soit renvoyé au client.

Équilibré

StorageGRID tente de réaliser toutes les copies spécifiées dans la règle ILM lors de l'ingestion ; si cela n'est pas possible, des copies intermédiaires sont réalisées et le succès est renvoyé au client. Les copies spécifiées dans la règle ILM sont réalisées lorsque cela est possible.

Exemple de la manière dont la règle de cohérence et la règle ILM peuvent interagir

Supposons que vous ayez une grille à deux sites avec la règle ILM suivante et la cohérence suivante :

- **Règle ILM** : Créez deux copies d'objet, une sur le site local et une sur un site distant. Adoptez un comportement d'ingestion strict.
- **cohérence** : Global fort (les métadonnées de l'objet sont immédiatement distribuées à tous les sites).

Lorsqu'un client stocke un objet dans la grille, StorageGRID effectue les deux copies de l'objet et distribue les métadonnées aux deux sites avant de renvoyer le succès au client.

L'objet est entièrement protégé contre la perte au moment de l'ingestion réussie du message. Par exemple, si le site local est perdu peu de temps après l'ingestion, des copies des données d'objet et des métadonnées d'objet existent toujours sur le site distant. L'objet est entièrement récupérable.

Si vous avez utilisé la même règle ILM et la cohérence de site forte, le client peut recevoir un message de réussite après la répllication des données d'objet sur le site distant, mais avant que les métadonnées d'objet y soient distribuées. Dans ce cas, le niveau de protection des métadonnées de l'objet ne correspond pas au niveau de protection des données de l'objet. Si le site local est perdu peu de temps après l'ingestion, les métadonnées de l'objet sont perdues. L'objet ne peut pas être récupéré.

L'interrelation entre la cohérence et les règles ILM peut être complexe. Contactez NetApp si vous avez besoin d'aide.

Versionnage d'objet

Vous pouvez définir l'état de version d'un bucket si vous souhaitez conserver plusieurs versions de chaque objet. L'activation du contrôle de version pour un bucket peut aider à protéger contre la suppression accidentelle d'objets et vous permet de récupérer et de restaurer des versions antérieures d'un objet.

Le système StorageGRID implémente le contrôle de version avec prise en charge de la plupart des fonctionnalités et avec certaines limitations. StorageGRID prend en charge jusqu'à 10 000 versions de chaque objet.

Le contrôle de version des objets peut être combiné avec la gestion du cycle de vie des informations StorageGRID (ILM) ou avec la configuration du cycle de vie du bucket S3. Vous devez activer explicitement le contrôle de version pour chaque bucket. Lorsque le contrôle de version est activé pour un bucket, chaque objet ajouté au bucket se voit attribuer un ID de version, généré par le système StorageGRID .

L'utilisation de l'authentification multifacteur (MFA) n'est pas prise en charge.



Le contrôle de version ne peut être activé que sur les buckets créés avec StorageGRID version 10.3 ou ultérieure.

ILM et gestion des versions

Les politiques ILM sont appliquées à chaque version d'un objet. Un processus d'analyse ILM analyse en continu tous les objets et les réévalue par rapport à la politique ILM actuelle. Toutes les modifications que vous apportez aux stratégies ILM sont appliquées à tous les objets précédemment ingérés. Cela inclut les versions précédemment ingérées si le contrôle de version est activé. L'analyse ILM applique de nouvelles modifications ILM aux objets précédemment ingérés.

Pour les objets S3 dans les compartiments activés pour le contrôle de version, la prise en charge du contrôle de version vous permet de créer des règles ILM qui utilisent « Heure non actuelle » comme heure de référence (sélectionnez **Oui** pour la question « Appliquer cette règle uniquement aux anciennes versions d'objet ? » dans "[Étape 1 de l'assistant Créer une règle ILM](#)"). Lorsqu'un objet est mis à jour, ses versions précédentes deviennent obsolètes. L'utilisation d'un filtre « Heure non actuelle » vous permet de créer des politiques qui réduisent l'impact sur le stockage des versions précédentes des objets.



Lorsque vous téléchargez une nouvelle version d'un objet à l'aide d'une opération de téléchargement en plusieurs parties, l'heure non actuelle de la version d'origine de l'objet reflète le moment où le téléchargement en plusieurs parties a été créé pour la nouvelle version, et non le moment où le téléchargement en plusieurs parties a été terminé. Dans des cas limités, l'heure non actuelle de la version originale peut être antérieure de plusieurs heures ou jours à l'heure de la version actuelle.

Informations connexes

- "[Comment les objets versionnés S3 sont supprimés](#)"
- "[Règles et politiques ILM pour les objets versionnés S3 \(exemple 4\)](#)".

Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3

Si le paramètre global de verrouillage d'objet S3 est activé pour votre système StorageGRID , vous pouvez créer des buckets avec le verrouillage d'objet S3 activé. Vous pouvez spécifier la rétention par défaut pour chaque compartiment ou les paramètres de rétention pour chaque version d'objet.

Comment activer le verrouillage d'objet S3 pour un bucket

Si le paramètre global de verrouillage d'objet S3 est activé pour votre système StorageGRID , vous pouvez éventuellement activer le verrouillage d'objet S3 lorsque vous créez chaque bucket.

Le verrouillage d'objet S3 est un paramètre permanent qui ne peut être activé que lorsque vous créez un bucket. Vous ne pouvez pas ajouter ou désactiver le verrouillage d'objet S3 après la création d'un bucket.

Pour activer le verrouillage d'objet S3 pour un bucket, utilisez l'une de ces méthodes :

- Créez le bucket à l'aide du gestionnaire de locataires. Voir ["Créer un bucket S3"](#) .
- Créez le bucket à l'aide d'une requête CreateBucket avec le `x-amz-bucket-object-lock-enabled` en-tête de requête. Voir ["Opérations sur les godets"](#) .

S3 Object Lock nécessite le contrôle de version du bucket, qui est activé automatiquement lors de la création du bucket. Vous ne pouvez pas suspendre le contrôle de version du bucket. Voir ["Versionnage d'objet"](#) .

Paramètres de conservation par défaut pour un bucket

Lorsque le verrouillage d'objet S3 est activé pour un compartiment, vous pouvez éventuellement activer la rétention par défaut pour le compartiment et spécifier un mode de rétention par défaut et une période de rétention par défaut.

Mode de rétention par défaut

- En mode CONFORMITÉ :
 - L'objet ne peut pas être supprimé tant que sa date de conservation n'est pas atteinte.
 - La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être diminuée.
 - La date de conservation de l'objet ne peut pas être supprimée tant que cette date n'est pas atteinte.
- En mode GOUVERNANCE :
 - Les utilisateurs avec le `s3:BypassGovernanceRetention` l'autorisation peut utiliser le `x-amz-bypass-governance-retention: true` en-tête de demande pour contourner les paramètres de conservation.
 - Ces utilisateurs peuvent supprimer une version d'objet avant que sa date de conservation ne soit atteinte.
 - Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

Période de conservation par défaut

Chaque bucket peut avoir une période de conservation par défaut spécifiée en années ou en jours.

Comment définir la rétention par défaut pour un bucket

Pour définir la rétention par défaut d'un bucket, utilisez l'une de ces méthodes :

- Gérez les paramètres du bucket à partir du gestionnaire de locataires. Voir ["Créer un bucket S3"](#) et ["Mettre à jour la conservation par défaut du verrouillage des objets S3"](#) .
- Émettez une demande PutObjectLockConfiguration pour le bucket afin de spécifier le mode par défaut et le nombre de jours ou d'années par défaut.

Configuration de PutObjectLock

La demande PutObjectLockConfiguration vous permet de définir et de modifier le mode de conservation par défaut et la période de conservation par défaut pour un bucket sur lequel le verrouillage d'objet S3 est activé. Vous pouvez également supprimer les paramètres de conservation par défaut précédemment configurés.

Lorsque de nouvelles versions d'objet sont ingérées dans le bucket, le mode de rétention par défaut est appliqué si `x-amz-object-lock-mode` et `x-amz-object-lock-retain-until-date` ne sont pas spécifiés. La période de conservation par défaut est utilisée pour calculer la date de conservation si `x-amz-object-lock-retain-until-date` n'est pas spécifié.

Si la période de conservation par défaut est modifiée après l'ingestion d'une version d'objet, la date de conservation de la version d'objet reste la même et n'est pas recalculée à l'aide de la nouvelle période de conservation par défaut.

Vous devez avoir le `s3:PutBucketObjectLockConfiguration` autorisation, ou être un compte root, pour terminer cette opération.

Le `Content-MD5` l'en-tête de la requête doit être spécifié dans la requête PUT.

Exemple de demande

Cet exemple active le verrouillage d'objet S3 pour un bucket et définit le mode de conservation par défaut sur CONFORMITÉ et la période de conservation par défaut sur 6 ans.

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>
```

Comment déterminer la rétention par défaut d'un bucket

Pour déterminer si le verrouillage d'objet S3 est activé pour un bucket et pour voir le mode de conservation par défaut et la période de conservation, utilisez l'une de ces méthodes :

- Afficher le bucket dans le gestionnaire de locataires. Voir ["Afficher les buckets S3"](#) .
- Émettez une demande `GetObjectLockConfiguration`.

Obtenir la configuration du verrouillage de l'objet

La demande `GetObjectLockConfiguration` vous permet de déterminer si le verrouillage d'objet S3 est activé pour un compartiment et, s'il est activé, de voir s'il existe un mode de conservation par défaut et une période de conservation configurés pour le compartiment.

Lorsque de nouvelles versions d'objet sont ingérées dans le bucket, le mode de rétention par défaut est appliqué si `x-amz-object-lock-mode` n'est pas spécifié. La période de conservation par défaut est utilisée pour calculer la date de conservation si `x-amz-object-lock-retain-until-date` n'est pas spécifié.

Vous devez avoir le `s3:GetBucketObjectLockConfiguration` autorisation, ou être un compte root, pour terminer cette opération.

Exemple de demande

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

Exemple de réponse

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>
```

Comment spécifier les paramètres de conservation d'un objet

Un bucket avec S3 Object Lock activé peut contenir une combinaison d'objets avec et sans paramètres de conservation S3 Object Lock.

Les paramètres de conservation au niveau de l'objet sont spécifiés à l'aide de l'API REST S3. Les paramètres de rétention d'un objet remplacent tous les paramètres de rétention par défaut du compartiment.

Vous pouvez spécifier les paramètres suivants pour chaque objet :

- **Mode de conservation** : Soit CONFORMITÉ, soit GOUVERNANCE.
- **Retain-until-date** : une date spécifiant la durée pendant laquelle la version de l'objet doit être conservée par StorageGRID.
 - En mode CONFORMITÉ, si la date de conservation est dans le futur, l'objet peut être récupéré, mais il ne peut pas être modifié ou supprimé. La date de conservation peut être augmentée, mais cette date ne peut pas être diminuée ou supprimée.
 - En mode GOUVERNANCE, les utilisateurs disposant d'une autorisation spéciale peuvent contourner le paramètre de conservation jusqu'à la date. Ils peuvent supprimer une version d'objet avant l'expiration de sa période de conservation. Ils peuvent également augmenter, diminuer ou même supprimer la date de conservation.
- **Conservation légale** : L'application d'une conservation légale à une version d'objet verrouille immédiatement cet objet. Par exemple, vous pourriez avoir besoin de suspendre légalement un objet lié à une enquête ou à un litige juridique. Une conservation légale n'a pas de date d'expiration, mais reste en place jusqu'à ce qu'elle soit explicitement supprimée.

Le paramètre de conservation légale d'un objet est indépendant du mode de conservation et de la date de conservation. Si une version d'objet est soumise à une suspension légale, personne ne peut supprimer cette version.

Pour spécifier les paramètres de verrouillage d'objet S3 lors de l'ajout d'une version d'objet à un bucket, émettez un ["Mettre l'objet"](#), ["Copier l'objet"](#), ou ["Créer un téléchargement multi-parties"](#) demande.

Vous pouvez utiliser les éléments suivants :

- `x-amz-object-lock-mode`, qui peut être CONFORMITÉ ou GOUVERNANCE (sensible à la casse).



Si vous précisez `x-amz-object-lock-mode`, vous devez également spécifier `x-amz-object-lock-retain-until-date`.

- `x-amz-object-lock-retain-until-date`
 - La valeur de conservation jusqu'à la date doit être au format `2020-08-10T21:46:00Z`. Les fractions de secondes sont autorisées, mais seuls 3 chiffres décimaux sont conservés (précision en millisecondes). Les autres formats ISO 8601 ne sont pas autorisés.
 - La date de conservation doit être dans le futur.
- `x-amz-object-lock-legal-hold`

Si la conservation légale est activée (sensible à la casse), l'objet est placé sous conservation légale. Si la retenue légale est désactivée, aucune retenue légale n'est placée. Toute autre valeur entraîne une erreur 400 Bad Request (InvalidArgument).

Si vous utilisez l'un de ces en-têtes de requête, tenez compte de ces restrictions :

- Le `Content-MD5` l'en-tête de la demande est requis le cas échéant `x-amz-object-lock-*` l'en-tête de requête est présent dans la requête `PutObject`. `Content-MD5` n'est pas requis pour `CopyObject` ou `CreateMultipartUpload`.
- Si le compartiment n'a pas de verrouillage d'objet S3 activé et qu'un `x-amz-object-lock-*` l'en-tête de requête est présent, une erreur 400 Bad Request (InvalidRequest) est renvoyée.
- La requête `PutObject` prend en charge l'utilisation de `x-amz-storage-class: REDUCED_REDUNDANCY` pour correspondre au comportement d'AWS. Cependant, lorsqu'un objet est ingéré dans un bucket avec S3 Object Lock activé, StorageGRID effectuera toujours une ingestion à double validation.
- Une réponse de version `GET` ou `HeadObject` ultérieure inclura les en-têtes `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, et `x-amz-object-lock-legal-hold`, si configuré et si l'expéditeur de la requête a le bon `s3:Get*` autorisations.

Vous pouvez utiliser le `s3:object-lock-remaining-retention-days` clé de condition de politique pour limiter les périodes de conservation minimales et maximales autorisées pour vos objets.

Comment mettre à jour les paramètres de conservation d'un objet

Si vous devez mettre à jour les paramètres de conservation légale ou de rétention d'une version d'objet existante, vous pouvez effectuer les opérations de sous-ressources d'objet suivantes :

- `PutObjectLegalHold`

Si la nouvelle valeur de conservation légale est activée, l'objet est placé sous une conservation légale. Si la valeur de maintien légal est OFF, le maintien légal est levé.

- `PutObjectRetention`
 - La valeur du mode peut être COMPLIANCE ou GOVERNANCE (sensible à la casse).
 - La valeur de conservation jusqu'à la date doit être au format `2020-08-10T21:46:00Z`. Les fractions de secondes sont autorisées, mais seuls 3 chiffres décimaux sont conservés (précision en millisecondes). Les autres formats ISO 8601 ne sont pas autorisés.
 - Si une version d'objet possède une date de conservation existante, vous ne pouvez que l'augmenter. La nouvelle valeur doit être dans le futur.

Comment utiliser le mode GOUVERNANCE

Les utilisateurs qui ont le `s3:BypassGovernanceRetention` l'autorisation peut contourner les paramètres de conservation actifs d'un objet qui utilise le mode GOUVERNANCE. Toutes les opérations `DELETE` ou `PutObjectRetention` doivent inclure le `x-amz-bypass-governance-retention:true` en-tête de requête. Ces utilisateurs peuvent effectuer ces opérations supplémentaires :

- Exécutez les opérations `DeleteObject` ou `DeleteObjects` pour supprimer une version d'objet avant l'expiration de sa période de conservation.

Les objets faisant l'objet d'une suspension légale ne peuvent pas être supprimés. La retenue légale doit être désactivée.

- Exécutez des opérations `PutObjectRetention` qui modifient le mode de version d'un objet de GOUVERNANCE à CONFORMITÉ avant l'expiration de la période de conservation de l'objet.

Le passage du mode CONFORMITÉ au mode GOUVERNANCE n'est jamais autorisé.

- Exécutez des opérations PutObjectRetention pour augmenter, diminuer ou supprimer la période de conservation d'une version d'objet.

Informations connexes

- ["Gérer les objets avec S3 Object Lock"](#)
- ["Utilisez S3 Object Lock pour conserver les objets"](#)
- ["Guide de l'utilisateur d'Amazon Simple Storage Service : Verrouillage d'objets"](#)

Créer une configuration du cycle de vie S3

Vous pouvez créer une configuration de cycle de vie S3 pour contrôler le moment où des objets spécifiques sont supprimés du système StorageGRID .

L'exemple simple de cette section illustre comment une configuration de cycle de vie S3 peut contrôler le moment où certains objets sont supprimés (expirés) de compartiments S3 spécifiques. L'exemple dans cette section est fourni à titre d'illustration uniquement. Pour plus de détails sur la création de configurations de cycle de vie S3, consultez ["Guide de l'utilisateur d'Amazon Simple Storage Service : Gestion du cycle de vie des objets"](#) . Notez que StorageGRID prend uniquement en charge les actions d'expiration ; il ne prend pas en charge les actions de transition.

Quelle est la configuration du cycle de vie

Une configuration de cycle de vie est un ensemble de règles appliquées aux objets dans des compartiments S3 spécifiques. Chaque règle spécifie quels objets sont concernés et quand ces objets expireront (à une date spécifique ou après un certain nombre de jours).

StorageGRID prend en charge jusqu'à 1 000 règles de cycle de vie dans une configuration de cycle de vie. Chaque règle peut inclure les éléments XML suivants :

- Expiration : supprimez un objet lorsqu'une date spécifiée est atteinte ou lorsqu'un nombre de jours spécifié est atteint, à compter du moment où l'objet a été ingéré.
- NoncurrentVersionExpiration : supprimez un objet lorsqu'un nombre de jours spécifié est atteint, à compter du moment où l'objet est devenu non actuel.
- Filtre (préfixe, balise)
- Statut
- ID

Chaque objet suit les paramètres de conservation d'un cycle de vie de compartiment S3 ou d'une politique ILM. Lorsqu'un cycle de vie de compartiment S3 est configuré, les actions d'expiration du cycle de vie remplacent la stratégie ILM pour les objets correspondant au filtre de cycle de vie du compartiment. Les objets qui ne correspondent pas au filtre de cycle de vie du bucket utilisent les paramètres de conservation de la stratégie ILM. Si un objet correspond à un filtre de cycle de vie de compartiment et qu'aucune action d'expiration n'est explicitement spécifiée, les paramètres de conservation de la stratégie ILM ne sont pas utilisés et il est implicite que les versions d'objet sont conservées pour toujours. Voir ["Exemples de priorités pour le cycle de vie du bucket S3 et la politique ILM"](#) .

Par conséquent, un objet peut être supprimé de la grille même si les instructions de placement d'une règle ILM s'appliquent toujours à l'objet. Ou bien, un objet peut être conservé sur la grille même après l'expiration des instructions de placement ILM pour l'objet. Pour plus de détails, consultez la section ["Comment ILM fonctionne tout au long de la vie d'un objet"](#) .



La configuration du cycle de vie du bucket peut être utilisée avec les buckets pour lesquels le verrouillage d'objet S3 est activé, mais la configuration du cycle de vie du bucket n'est pas prise en charge pour les buckets conformes hérités.

StorageGRID prend en charge l'utilisation des opérations de bucket suivantes pour gérer les configurations du cycle de vie :

- Supprimer le cycle de vie du bucket
- GetBucketLifecycleConfiguration
- Configuration du cycle de vie de PutBucket

Créer une configuration du cycle de vie

Comme première étape de la création d'une configuration de cycle de vie, vous créez un fichier JSON qui inclut une ou plusieurs règles. Par exemple, ce fichier JSON comprend trois règles, comme suit :

1. La règle 1 s'applique uniquement aux objets qui correspondent au préfixe `category1 /` et qui ont un `key2` valeur de `tag2` . Le `Expiration` le paramètre spécifie que les objets correspondant au filtre expireront à minuit le 22 août 2020.
2. La règle 2 s'applique uniquement aux objets qui correspondent au préfixe `category2 /`. Le `Expiration` le paramètre spécifie que les objets correspondant au filtre expireront 100 jours après leur ingestion.



Les règles qui spécifient un nombre de jours sont relatives au moment où l'objet a été ingéré. Si la date actuelle dépasse la date d'ingestion plus le nombre de jours, certains objets peuvent être supprimés du bucket dès que la configuration du cycle de vie est appliquée.

3. La règle 3 s'applique uniquement aux objets qui correspondent au préfixe `category3 /`. Le `Expiration` le paramètre spécifie que toutes les versions non actuelles des objets correspondants expireront 50 jours après être devenues non actuelles.

```

{
  "Rules": [
    {
      "ID": "rule1",
      "Filter": {
        "And": {
          "Prefix": "category1/",
          "Tags": [
            {
              "Key": "key2",
              "Value": "tag2"
            }
          ]
        }
      },
      "Expiration": {
        "Date": "2020-08-22T00:00:00Z"
      },
      "Status": "Enabled"
    },
    {
      "ID": "rule2",
      "Filter": {
        "Prefix": "category2/"
      },
      "Expiration": {
        "Days": 100
      },
      "Status": "Enabled"
    },
    {
      "ID": "rule3",
      "Filter": {
        "Prefix": "category3/"
      },
      "NoncurrentVersionExpiration": {
        "NoncurrentDays": 50
      },
      "Status": "Enabled"
    }
  ]
}

```

Appliquer la configuration du cycle de vie au bucket

Après avoir créé le fichier de configuration du cycle de vie, vous l'appliquez à un bucket en émettant une requête `PutBucketLifecycleConfiguration`.

Cette requête applique la configuration du cycle de vie dans le fichier d'exemple aux objets d'un bucket nommé `testbucket`.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Pour valider qu'une configuration de cycle de vie a été correctement appliquée au bucket, émettez une demande `GetBucketLifecycleConfiguration`. Par exemple:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-configuration
--bucket testbucket
```

Une réponse réussie répertorie la configuration du cycle de vie que vous venez d'appliquer.

Valider que l'expiration du cycle de vie du bucket s'applique à l'objet

Vous pouvez déterminer si une règle d'expiration dans la configuration du cycle de vie s'applique à un objet spécifique lors de l'émission d'une demande `PutObject`, `HeadObject` ou `GetObject`. Si une règle s'applique, la réponse comprend une `Expiration` paramètre qui indique quand l'objet expire et quelle règle d'expiration a été respectée.



Étant donné que le cycle de vie du bucket remplace ILM, le `expiry-date` la date réelle à laquelle l'objet sera supprimé est indiquée. Pour plus de détails, consultez la section ["Comment la rétention d'objet est déterminée"](#).

Par exemple, cette requête `PutObject` a été émise le 22 juin 2020 et place un objet dans le `testbucket` seau.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

La réponse de réussite indique que l'objet expirera dans 100 jours (1er octobre 2020) et qu'il correspond à la règle 2 de la configuration du cycle de vie.

```
{
  "Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-id=\"rule2\"",
  "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

Par exemple, cette requête HeadObject a été utilisée pour obtenir des métadonnées pour le même objet dans le bucket testbucket.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

La réponse de réussite inclut les métadonnées de l'objet et indique que l'objet expirera dans 100 jours et qu'il correspond à la règle 2.

```
{
  "AcceptRanges": "bytes",
  "Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-id=\"rule2\"",
  "LastModified": "2020-06-23T09:07:48+00:00",
  "ContentLength": 921,
  "ETag": "\"9762f8a803bc34f5340579d4446076f7\"",
  "ContentType": "binary/octet-stream",
  "Metadata": {}
}
```



Pour les buckets avec contrôle de version activé, le x-amz-expiration l'en-tête de réponse s'applique uniquement aux versions actuelles des objets.

Recommandations pour la mise en œuvre de l'API REST S3

Vous devez suivre ces recommandations lors de l'implémentation de l'API REST S3 à utiliser avec StorageGRID.

Recommandations pour les HEADs vers des objets inexistants

Si votre application vérifie régulièrement si un objet existe dans un chemin où vous ne vous attendez pas à ce que l'objet existe réellement, vous devez utiliser l'option « Disponible » ["cohérence"](#) . Par exemple, vous devez utiliser la cohérence « Disponible » si votre application HEAD un emplacement avant d'y effectuer un PUT.

Dans le cas contraire, si l'opération HEAD ne trouve pas l'objet, vous risquez de recevoir un nombre élevé d'erreurs de serveur interne 500 si deux ou plusieurs nœuds de stockage sur le même site ne sont pas disponibles ou si un site distant est inaccessible.

Vous pouvez définir la cohérence « Disponible » pour chaque bucket à l'aide de l'["Cohérence du seau PUT"](#) demande, ou vous pouvez spécifier la cohérence dans l'en-tête de demande pour une opération API individuelle.

Recommandations pour les clés d'objet

Suivez ces recommandations pour les noms de clés d'objet, en fonction de la date de création initiale du bucket.

Buckets créés dans StorageGRID 11.4 ou version antérieure

- N'utilisez pas de valeurs aléatoires comme quatre premiers caractères des clés d'objet. Ceci est en contraste avec l'ancienne recommandation AWS pour les préfixes de clé. Utilisez plutôt des préfixes non aléatoires et non uniques, tels que `image`.
- Si vous suivez l'ancienne recommandation AWS d'utiliser des caractères aléatoires et uniques dans les préfixes de clé, préfixez les clés d'objet avec un nom de répertoire. C'est-à-dire, utilisez ce format :

```
mybucket/mydir/f8e3-image3132.jpg
```

Au lieu de ce format :

```
mybucket/f8e3-image3132.jpg
```

Buckets créés dans StorageGRID 11.4 ou version ultérieure

Il n'est pas nécessaire de restreindre les noms de clés d'objet pour respecter les meilleures pratiques en matière de performances. Dans la plupart des cas, vous pouvez utiliser des valeurs aléatoires pour les quatre premiers caractères des noms de clés d'objet.



Une exception à cette règle est une charge de travail S3 qui supprime en continu tous les objets après une courte période de temps. Pour minimiser l'impact sur les performances de ce cas d'utilisation, faites varier une partie initiale du nom de la clé tous les plusieurs milliers d'objets avec quelque chose comme la date. Par exemple, supposons qu'un client S3 écrit généralement 2 000 objets/seconde et que la politique de cycle de vie ILM ou bucket supprime tous les objets après trois jours. Pour minimiser l'impact sur les performances, vous pouvez nommer les clés en utilisant un modèle comme celui-ci :

```
/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg
```

Recommandations pour les « lectures de plage »

Si le "option globale pour compresser les objets stockés" est activé, les applications clientes S3 doivent éviter d'effectuer des opérations `GetObject` qui spécifient une plage d'octets à renvoyer. Ces opérations de « lecture de plage » sont inefficaces car StorageGRID doit décompresser efficacement les objets pour accéder aux octets demandés. Les opérations `GetObject` qui demandent une petite plage d'octets à partir d'un très grand objet sont particulièrement inefficaces ; par exemple, il est inefficace de lire une plage de 10 Mo à partir d'un objet compressé de 50 Go.

Si les plages sont lues à partir d'objets compressés, les demandes des clients peuvent expirer.



Si vous devez compresser des objets et que votre application cliente doit utiliser des lectures de plage, augmentez le délai d'expiration de lecture pour l'application.

Prise en charge de l'API REST Amazon S3

Détails d'implémentation de l'API REST S3

Le système StorageGRID implémente l'API Simple Storage Service (version API 2006-03-01) avec prise en charge de la plupart des opérations et avec certaines limitations. Vous devez comprendre les détails d'implémentation lorsque vous intégrez des applications clientes S3 REST API.

Le système StorageGRID prend en charge à la fois les demandes de type hébergé virtuel et les demandes de type chemin.

Gestion des dates

L'implémentation StorageGRID de l'API REST S3 prend uniquement en charge les formats de date HTTP valides.

Le système StorageGRID prend uniquement en charge les formats de date HTTP valides pour tous les en-têtes qui acceptent les valeurs de date. La partie horaire de la date peut être spécifiée au format Greenwich Mean Time (GMT) ou au format Universal Coordinated Time (UTC) sans décalage de fuseau horaire (+0000 doit être spécifié). Si vous incluez le `x-amz-date` en-tête de votre demande, il remplace toute valeur spécifiée dans l'en-tête de la demande Date. Lors de l'utilisation d'AWS Signature Version 4, le `x-amz-date` l'en-tête doit être présent dans la demande signée car l'en-tête de date n'est pas pris en charge.

En-têtes de requête courants

Le système StorageGRID prend en charge les en-têtes de requête courants définis par "[Référence de l'API Amazon Simple Storage Service : en-têtes de requête courants](#)", à une exception près.

En-tête de la requête	Mise en œuvre
Autorisation	Prise en charge complète d'AWS Signature Version 2 Prise en charge d'AWS Signature version 4, avec les exceptions suivantes : <ul style="list-style-type: none">Lorsque vous fournissez la valeur réelle de la somme de contrôle de la charge utile dans <code>x-amz-content-sha256</code>, la valeur est acceptée sans validation, comme si la valeur <code>UNSIGNED-PAYLOAD</code> avait été prévu pour l'en-tête. Lorsque vous fournissez un <code>x-amz-content-sha256</code> valeur d'en-tête qui implique <code>aws-chunked</code> en streaming (par exemple, <code>STREAMING-AWS4-HMAC-SHA256-PAYLOAD</code>), les signatures de bloc ne sont pas vérifiées par rapport aux données de bloc.
jeton de sécurité x-amz	Non implémenté. Retours <code>XNotImplemented</code> .

En-têtes de réponse courants

Le système StorageGRID prend en charge tous les en-têtes de réponse courants définis par la *Référence API du service de stockage simple*, à une exception près.

En-tête de réponse	Mise en œuvre
<code>x-amz-id-2</code>	Non utilisé

Authentifier les demandes

Le système StorageGRID prend en charge l'accès authentifié et anonyme aux objets à l'aide de l'API S3.

L'API S3 prend en charge les versions Signature 2 et Signature 4 pour l'authentification des requêtes API S3.

Les demandes authentifiées doivent être signées à l'aide de votre identifiant de clé d'accès et de votre clé

d'accès secrète.

Le système StorageGRID prend en charge deux méthodes d'authentification : HTTP Authorization en-tête et utilisation des paramètres de requête.

Utiliser l'en-tête d'autorisation HTTP

Le HTTP Authorization L'en-tête est utilisé par toutes les opérations API S3, à l'exception des demandes anonymes lorsque la politique de compartiment le permet. Le Authorization L'en-tête contient toutes les informations de signature requises pour authentifier une demande.

Utiliser les paramètres de requête

Vous pouvez utiliser des paramètres de requête pour ajouter des informations d'authentification à une URL. Ceci est connu sous le nom de présignature de l'URL, qui peut être utilisée pour accorder un accès temporaire à des ressources spécifiques. Les utilisateurs disposant de l'URL présignée n'ont pas besoin de connaître la clé d'accès secrète pour accéder à la ressource, ce qui vous permet de fournir un accès restreint à un tiers à une ressource.

Opérations sur le service

Le système StorageGRID prend en charge les opérations suivantes sur le service.

Opération	Mise en œuvre
Listes de seaux (anciennement nommé service GET)	Implémenté avec tous les comportements de l'API REST Amazon S3. Sous réserve de modifications sans préavis.
Utilisation du stockage GET	Le StorageGRID" Utilisation du stockage GET " La demande vous indique la quantité totale de stockage utilisée par un compte et pour chaque compartiment associé au compte. Il s'agit d'une opération sur le service avec un chemin de / et un paramètre de requête personnalisé(?x-ntap-sg-usage) ajouté.
OPTIONS /	Les applications clientes peuvent émettre OPTIONS / demandes adressées au port S3 sur un nœud de stockage, sans fournir les informations d'identification d'authentification S3, pour déterminer si le nœud de stockage est disponible. Vous pouvez utiliser cette demande pour la surveillance ou pour permettre aux équilibres de charge externes d'identifier quand un nœud de stockage est en panne.

Opérations sur les godets

Le système StorageGRID prend en charge un maximum de 5 000 buckets pour chaque compte de locataire S3.

Chaque grille peut contenir un maximum de 100 000 buckets.

Pour prendre en charge 5 000 buckets, chaque nœud de stockage de la grille doit disposer d'un minimum de 64 Go de RAM.

Les restrictions de nom de bucket suivent les restrictions régionales standard AWS US, mais vous devez les restreindre davantage aux conventions de dénomination DNS pour prendre en charge les demandes de style hébergé virtuel S3.

Pour plus d'informations, voir les éléments suivants :

- ["Guide de l'utilisateur d'Amazon Simple Storage Service : quotas, restrictions et limitations des buckets"](#)
- ["Configurer les noms de domaine des points de terminaison S3"](#)

Les opérations ListObjects (GET Bucket) et ListObjectVersions (versions d'objet GET Bucket) prennent en charge StorageGRID ["valeurs de cohérence"](#) .

Vous pouvez vérifier si les mises à jour de l'heure du dernier accès sont activées ou désactivées pour des compartiments individuels. Voir ["Heure du dernier accès au bucket GET"](#) .

Le tableau suivant décrit comment StorageGRID implémente les opérations de bucket S3 REST API. Pour effectuer l'une de ces opérations, les informations d'accès nécessaires doivent être fournies pour le compte.

Opération	Mise en œuvre
Créer un bucket	<p>Crée un nouveau bucket. En créant le bucket, vous devenez le propriétaire du bucket.</p> <ul style="list-style-type: none"> Les noms de bucket doivent respecter les règles suivantes : <ul style="list-style-type: none"> Doit être unique sur chaque système StorageGRID (pas seulement unique au sein du compte locataire). Doit être conforme au DNS. Doit contenir au moins 3 et pas plus de 63 caractères. Peut être une série d'une ou plusieurs étiquettes, avec des étiquettes adjacentes séparées par un point. Chaque étiquette doit commencer et se terminer par une lettre minuscule ou un chiffre et ne peut utiliser que des lettres minuscules, des chiffres et des traits d'union. Ne doit pas ressembler à une adresse IP au format texte. Ne doit pas utiliser de points dans les requêtes de style hébergé virtuellement. Les points entraîneront des problèmes avec la vérification du certificat générique du serveur. Par défaut, les buckets sont créés dans le <code>us-east-1</code> région; cependant, vous pouvez utiliser le <code>LocationConstraint</code> élément de demande dans le corps de la demande pour spécifier une région différente. Lors de l'utilisation du <code>LocationConstraint</code> élément, vous devez spécifier le nom exact d'une région qui a été définie à l'aide du gestionnaire de grille ou de l'API de gestion de grille. Contactez votre administrateur système si vous ne connaissez pas le nom de la région à utiliser. <p>Remarque : une erreur se produira si votre demande <code>CreateBucket</code> utilise une région qui n'a pas été définie dans StorageGRID.</p> <ul style="list-style-type: none"> Vous pouvez inclure le <code>x-amz-bucket-object-lock-enabled</code> en-tête de demande pour créer un bucket avec S3 Object Lock activé. Voir "Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3" . <p>Vous devez activer le verrouillage d'objet S3 lorsque vous créez le bucket. Vous ne pouvez pas ajouter ou désactiver le verrouillage d'objet S3 après la création d'un bucket. S3 Object Lock nécessite le contrôle de version du bucket, qui est activé automatiquement lorsque vous créez le bucket.</p>
Supprimer le bucket	Supprime le bucket.
SupprimerBucketCors	Supprime la configuration CORS pour le bucket.
Supprimer le chiffrement du bucket	Supprime le cryptage par défaut du bucket. Les objets chiffrés existants restent chiffrés, mais tous les nouveaux objets ajoutés au bucket ne sont pas chiffrés.
Supprimer le cycle de vie du bucket	Supprime la configuration du cycle de vie du bucket. Voir "Créer une configuration du cycle de vie S3" .

Opération	Mise en œuvre
Supprimer la politique de bucket	Supprime la politique attachée au bucket.
SupprimerBucketReplication	Supprime la configuration de réplication attachée au bucket.
Supprimer le balisage du bucket	<p>Utilise le <code>tagging</code> sous-ressource pour supprimer toutes les balises d'un bucket.</p> <p>Attention : Si une balise de politique ILM non par défaut est définie pour ce compartiment, il y aura un <code>NTAP-SG-ILM-BUCKET-TAG</code> balise de bucket avec une valeur qui lui est attribuée. N'émettez pas de demande <code>DeleteBucketTagging</code> s'il y a un <code>NTAP-SG-ILM-BUCKET-TAG</code> étiquette de seau. Au lieu de cela, émettez une requête <code>PutBucketTagging</code> avec uniquement le <code>NTAP-SG-ILM-BUCKET-TAG</code> balise et sa valeur attribuée pour supprimer toutes les autres balises du bucket. Ne pas modifier ni supprimer le <code>NTAP-SG-ILM-BUCKET-TAG</code> étiquette de seau.</p>
ObtenirBucketAcl	Renvoie une réponse positive et l'ID, le nom d'affichage et l'autorisation du propriétaire du bucket, indiquant que le propriétaire a un accès complet au bucket.
ObtenirBucketCors	Renvoie le <code>cors</code> configuration pour le bucket.
Obtenir le chiffrement du bucket	Renvoie la configuration de chiffrement par défaut pour le bucket.
GetBucketLifecycleConfiguration (anciennement appelé cycle de vie du bucket GET)	Renvoie la configuration du cycle de vie du bucket. Voir "Créer une configuration du cycle de vie S3" .
Obtenir l'emplacement du bucket	Renvoie la région qui a été définie à l'aide de <code>LocationConstraint</code> élément dans la requête <code>CreateBucket</code> . Si la région du bucket est <code>us-east-1</code> , une chaîne vide est renvoyée pour la région.
Configuration de GetBucketNotification (anciennement appelée notification GET Bucket)	Renvoie la configuration de notification attachée au bucket.
Obtenir la politique de Bucket	Renvoie la politique attachée au bucket.
Réplication GetBucket	Renvoie la configuration de réplication attachée au bucket.

Opération	Mise en œuvre
Obtenir le balisage du bucket	<p>Utilise le <code>tagging</code> sous-ressource pour renvoyer toutes les balises d'un bucket.</p> <p>Attention : Si une balise de politique ILM non par défaut est définie pour ce compartiment, il y aura un <code>NTAP-SG-ILM-BUCKET-TAG</code> balise de bucket avec une valeur qui lui est attribuée. Ne pas modifier ni supprimer cette balise.</p>
Obtenir la gestion des versions du bucket	<p>Cette implémentation utilise le <code>versioning</code> sous-ressource pour renvoyer l'état de version d'un bucket.</p> <ul style="list-style-type: none"> • <i>blank</i> : le contrôle de version n'a jamais été activé (le bucket est « Non versionné ») • Activé : le contrôle de version est activé • Suspendu : le contrôle de version était précédemment activé et est suspendu
Obtenir la configuration du verrouillage de l'objet	<p>Renvoie le mode de conservation par défaut du bucket et la période de conservation par défaut, si configurés.</p> <p>Voir "Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3" .</p>
Tête de godet	<p>Détermine si un bucket existe et si vous avez l'autorisation d'y accéder.</p> <p>Cette opération renvoie :</p> <ul style="list-style-type: none"> • <code>x-ntap-sg-bucket-id</code>: L'UUID du bucket au format UUID. • <code>x-ntap-sg-trace-id</code>: L'ID de trace unique de la demande associée.
ListObjects et ListObjectsV2 (anciennement nommé GET Bucket)	<p>Renvoie tout ou partie (jusqu'à 1 000) des objets d'un bucket. La classe de stockage des objets peut avoir l'une des deux valeurs, même si l'objet a été ingéré avec le <code>REDUCED_REDUNDANCY</code> option de classe de stockage :</p> <ul style="list-style-type: none"> • <code>STANDARD</code>, ce qui indique que l'objet est stocké dans un pool de stockage composé de nœuds de stockage. • <code>GLACIER</code>, ce qui indique que l'objet a été déplacé vers le bucket externe spécifié par le pool de stockage Cloud. <p>Si le compartiment contient un grand nombre de clés supprimées qui ont le même préfixe, la réponse peut inclure certaines <code>CommonPrefixes</code> qui ne contiennent pas de clés.</p>
ListObjectVersions (anciennement appelées versions d'objets GET Bucket)	<p>Avec un accès en <code>LECTURE</code> sur un bucket, en utilisant cette opération avec le <code>versions</code> la sous-ressource répertorie les métadonnées de toutes les versions des objets dans le bucket.</p>

Opération	Mise en œuvre
PutBucketCors	Définit la configuration CORS pour un bucket afin que celui-ci puisse traiter les demandes inter-origines. Le partage de ressources inter-origines (CORS) est un mécanisme de sécurité qui permet aux applications Web clientes d'un domaine d'accéder aux ressources d'un domaine différent. Par exemple, supposons que vous utilisiez un bucket S3 nommé <code>images</code> pour stocker des graphiques. En définissant la configuration CORS pour le <code>images</code> bucket, vous pouvez autoriser l'affichage des images de ce bucket sur le site Web <code>http://www.example.com</code> .
Cryptage PutBucket	<p>Définit l'état de cryptage par défaut d'un bucket existant. Lorsque le chiffrement au niveau du bucket est activé, tout nouvel objet ajouté au bucket est chiffré. StorageGRID prend en charge le chiffrement côté serveur avec des clés gérées par StorageGRID. Lors de la spécification de la règle de configuration de chiffrement côté serveur, définissez le <code>SSEAlgorithm</code> paramètre à <code>AES256</code>, et n'utilisez pas le <code>KMSMasterKeyID</code> paramètre.</p> <p>La configuration de chiffrement par défaut du bucket est ignorée si la demande de téléchargement d'objet spécifie déjà le chiffrement (c'est-à-dire si la demande inclut le <code>x-amz-server-side-encryption-*</code> en-tête de requête).</p>
Configuration du cycle de vie de PutBucket (anciennement appelé cycle de vie du bucket PUT)	<p>Crée une nouvelle configuration de cycle de vie pour le bucket ou remplace une configuration de cycle de vie existante. StorageGRID prend en charge jusqu'à 1 000 règles de cycle de vie dans une configuration de cycle de vie. Chaque règle peut inclure les éléments XML suivants :</p> <ul style="list-style-type: none"> • Expiration (jours, date, ExpiredObjectDeleteMarker) • NoncurrentVersionExpiration (NewerNoncurrentVersions, NoncurrentDays) • Filtre (préfixe, balise) • Statut • ID <p>StorageGRID ne prend pas en charge ces actions :</p> <ul style="list-style-type: none"> • AbandonnerTéléchargement multi-parties incomplet • Transition <p>Voir "Créer une configuration du cycle de vie S3". Pour comprendre comment l'action Expiration dans un cycle de vie de bucket interagit avec les instructions de placement ILM, voir "Comment ILM fonctionne tout au long de la vie d'un objet".</p> <p>Remarque : la configuration du cycle de vie du bucket peut être utilisée avec les buckets pour lesquels le verrouillage d'objet S3 est activé, mais la configuration du cycle de vie du bucket n'est pas prise en charge pour les buckets conformes hérités.</p>

Opération	Mise en œuvre
Configuration de PutBucketNotification (anciennement appelée notification PUT Bucket)	<p>Configure les notifications pour le bucket à l'aide du XML de configuration de notification inclus dans le corps de la demande. Vous devez être conscient des détails de mise en œuvre suivants :</p> <ul style="list-style-type: none"> • StorageGRID prend en charge les rubriques Amazon Simple Notification Service (Amazon SNS) ou Kafka comme destinations. Les points de terminaison Simple Queue Service (SQS) ou Amazon Lambda ne sont pas pris en charge. • La destination des notifications doit être spécifiée comme l'URN d'un point de terminaison StorageGRID . Les points de terminaison peuvent être créés à l'aide du gestionnaire de locataires ou de l'API de gestion des locataires. <p>Le point de terminaison doit exister pour que la configuration des notifications réussisse. Si le point de terminaison n'existe pas, un 400 Bad Request l'erreur est renvoyée avec le code InvalidArgument .</p> <ul style="list-style-type: none"> • Vous ne pouvez pas configurer de notification pour les types d'événements suivants. Ces types d'événements ne sont pas pris en charge. <ul style="list-style-type: none"> ◦ <code>s3:ReducedRedundancyLostObject</code> ◦ <code>s3:ObjectRestore:Completed</code> • Les notifications d'événements envoyées depuis StorageGRID utilisent le format JSON standard, sauf qu'elles n'incluent pas certaines clés et utilisent des valeurs spécifiques pour d'autres, comme indiqué dans la liste suivante : <ul style="list-style-type: none"> ◦ Source de l'événement <code>sgws:s3</code> ◦ awsRegion non inclus ◦ x-amz-id-2 non inclus ◦ arn <code>urn:sgws:s3:::bucket_name</code>
Politique de PutBucket	Définit la politique attachée au bucket. Voir "Utiliser des politiques d'accès aux buckets et aux groupes" .

Opération	Mise en œuvre
Réplication de PutBucket	<p>Configure "Réplication StorageGRID CloudMirror" pour le bucket utilisant la configuration de réplication XML fournie dans le corps de la demande. Pour la réplication CloudMirror, vous devez connaître les détails d'implémentation suivants :</p> <ul style="list-style-type: none"> • StorageGRID prend uniquement en charge la version V1 de la configuration de réplication. Cela signifie que StorageGRID ne prend pas en charge l'utilisation du <code>Filter</code> élément pour les règles et suit les conventions V1 pour la suppression des versions d'objet. Pour plus de détails, voir "Guide de l'utilisateur d'Amazon Simple Storage Service : Configuration de la réplication" . • La réplication de bucket peut être configurée sur des buckets versionnés ou non versionnés. • Vous pouvez spécifier un bucket de destination différent dans chaque règle du XML de configuration de réplication. Un bucket source peut être répliqué vers plusieurs buckets de destination. • Les buckets de destination doivent être spécifiés comme URN des points de terminaison StorageGRID comme spécifié dans le gestionnaire de locataires ou l'API de gestion des locataires. Voir "Configurer la réplication CloudMirror" . <p>Le point de terminaison doit exister pour que la configuration de la réplication réussisse. Si le point de terminaison n'existe pas, la demande échoue en tant que 400 Bad Request . Le message d'erreur indique : <code>Unable to save the replication policy. The specified endpoint URN does not exist: URN.</code></p> <ul style="list-style-type: none"> • Vous n'avez pas besoin de spécifier un <code>Role</code> dans la configuration XML. Cette valeur n'est pas utilisée par StorageGRID et sera ignorée si elle est soumise. • Si vous omettez la classe de stockage du XML de configuration, StorageGRID utilise le <code>STANDARD</code> classe de stockage par défaut. • Si vous supprimez un objet du bucket source ou si vous supprimez le bucket source lui-même, le comportement de la réplication inter-région est le suivant : <ul style="list-style-type: none"> ◦ Si vous supprimez l'objet ou le bucket avant qu'il ne soit répliqué, l'objet/bucket n'est pas répliqué et vous n'en êtes pas averti. ◦ Si vous supprimez l'objet ou le compartiment après sa réplication, StorageGRID suit le comportement de suppression standard d'Amazon S3 pour la V1 de la réplication inter-régions.

Opération	Mise en œuvre
Balisage de PutBucket	<p>Utilise le <code>tagging</code> sous-ressource pour ajouter ou mettre à jour un ensemble de balises pour un bucket. Lorsque vous ajoutez des balises de bucket, tenez compte des limitations suivantes :</p> <ul style="list-style-type: none"> • StorageGRID et Amazon S3 prennent en charge jusqu'à 50 balises pour chaque compartiment. • Les balises associées à un bucket doivent avoir des clés de balise uniques. Une clé de balise peut comporter jusqu'à 128 caractères Unicode. • Les valeurs des balises peuvent contenir jusqu'à 256 caractères Unicode. • La clé et les valeurs sont sensibles à la casse. <p>Attention : Si une balise de politique ILM non par défaut est définie pour ce compartiment, il y aura un <code>NTAP-SG-ILM-BUCKET-TAG</code> balise de bucket avec une valeur qui lui est attribuée. Assurez-vous que le <code>NTAP-SG-ILM-BUCKET-TAG</code> la balise de bucket est incluse avec la valeur attribuée dans toutes les requêtes <code>PutBucketTagging</code>. Ne pas modifier ni supprimer cette balise.</p> <p>Remarque : cette opération écrasera toutes les balises actuelles que le bucket possède déjà. Si des balises existantes sont omises de l'ensemble, ces balises seront supprimées pour le bucket.</p>
Gestion des versions de PutBucket	<p>Utilise le <code>versioning</code> sous-ressource pour définir l'état de version d'un bucket existant. Vous pouvez définir l'état de versionnage avec l'une des valeurs suivantes :</p> <ul style="list-style-type: none"> • Activé : active le contrôle de version pour les objets du bucket. Tous les objets ajoutés au bucket reçoivent un ID de version unique. • Suspendu : désactive le contrôle de version pour les objets du bucket. Tous les objets ajoutés au bucket reçoivent l'ID de version <code>null</code>.
Configuration de PutObjectLock	<p>Configure ou supprime le mode de conservation par défaut du bucket et la période de conservation par défaut.</p> <p>Si la période de conservation par défaut est modifiée, la date de conservation des versions d'objet existantes reste la même et n'est pas recalculée à l'aide de la nouvelle période de conservation par défaut.</p> <p>Voir "Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3" pour des informations détaillées.</p>

Opérations sur les objets

Opérations sur les objets

Cette section décrit comment le système StorageGRID implémente les opérations API REST S3 pour les objets.

Les conditions suivantes s'appliquent à toutes les opérations sur les objets :

- StorageGRID "**valeurs de cohérence**" sont pris en charge par toutes les opérations sur les objets, à l'exception des suivantes :
 - ObtenirObjectAcl
 - OPTIONS /
 - MettreObjetLegalHold
 - PutObjectRetention
 - Sélectionner le contenu de l'objet
- Les demandes client conflictuelles, telles que deux clients écrivant sur la même clé, sont résolues sur la base des « derniers gagnants ». Le moment de l'évaluation des « dernières victoires » est basé sur le moment où le système StorageGRID termine une demande donnée, et non sur le moment où les clients S3 commencent une opération.
- Tous les objets d'un bucket StorageGRID appartiennent au propriétaire du bucket, y compris les objets créés par un utilisateur anonyme ou par un autre compte.
- Les objets de données ingérés dans le système StorageGRID via Swift ne sont pas accessibles via S3.

Le tableau suivant décrit comment StorageGRID implémente les opérations d'objet S3 REST API.

Opération	Mise en œuvre
Supprimer l'objet	<p>Authentification multifacteur (MFA) et en-tête de réponse <code>x-amz-mfa</code> ne sont pas pris en charge.</p> <p>Lors du traitement d'une demande <code>DeleteObject</code>, StorageGRID tente de supprimer immédiatement toutes les copies de l'objet de tous les emplacements stockés. En cas de succès, StorageGRID renvoie immédiatement une réponse au client. Si toutes les copies ne peuvent pas être supprimées dans les 30 secondes (par exemple, parce qu'un emplacement est temporairement indisponible), StorageGRID met les copies en file d'attente pour suppression, puis indique la réussite au client.</p> <p>Gestion des versions</p> <p>Pour supprimer une version spécifique, le demandeur doit être le propriétaire du bucket et utiliser le <code>versionId</code> sous-ressource. L'utilisation de cette sous-ressource supprime définitivement la version. Si le <code>versionId</code> correspond à un marqueur de suppression, l'en-tête de réponse <code>x-amz-delete-marker</code> est renvoyé défini sur <code>true</code>.</p> <ul style="list-style-type: none"> • Si un objet est supprimé sans le <code>versionId</code> sous-ressource sur un bucket avec le contrôle de version activé, cela entraîne la génération d'un marqueur de suppression. Le <code>versionId</code> pour le marqueur de suppression est renvoyé en utilisant le <code>x-amz-version-id</code> en-tête de réponse et le <code>x-amz-delete-marker</code> l'en-tête de réponse est renvoyé défini sur <code>true</code>. • Si un objet est supprimé sans le <code>versionId</code> sous-ressource sur un bucket avec contrôle de version suspendu, cela entraîne une suppression permanente d'une version « null » déjà existante ou d'un marqueur de suppression « null », et la génération d'un nouveau marqueur de suppression « null ». Le <code>x-amz-delete-marker</code> l'en-tête de réponse est renvoyé défini sur <code>true</code>. <p>Remarque : Dans certains cas, plusieurs marqueurs de suppression peuvent exister pour un objet.</p> <p>Voir "Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3" pour savoir comment supprimer des versions d'objets en mode GOUVERNANCE.</p>
Supprimer les objets (précédemment nommé SUPPRIMER plusieurs objets)	<p>Authentification multifacteur (MFA) et en-tête de réponse <code>x-amz-mfa</code> ne sont pas pris en charge.</p> <p>Plusieurs objets peuvent être supprimés dans le même message de demande.</p> <p>Voir "Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3" pour savoir comment supprimer des versions d'objets en mode GOUVERNANCE.</p>

Opération	Mise en œuvre
Supprimer l'étiquetage des objets	<p>Utilise le <code>tagging</code> sous-ressource pour supprimer toutes les balises d'un objet.</p> <p>Gestion des versions</p> <p>Si le <code>versionId</code> si le paramètre de requête n'est pas spécifié dans la requête, l'opération supprime toutes les balises de la version la plus récente de l'objet dans un bucket versionné. Si la version actuelle de l'objet est un marqueur de suppression, un statut « <code>MethodNotAllowed</code> » est renvoyé avec le <code>x-amz-delete-marker</code> en-tête de réponse défini sur <code>true</code>.</p>
Obtenir l'objet	"Obtenir l'objet"
GetObjectAcl	Si les informations d'identification d'accès nécessaires sont fournies pour le compte, l'opération renvoie une réponse positive et l'ID, le nom d'affichage et l'autorisation du propriétaire de l'objet, indiquant que le propriétaire dispose d'un accès complet à l'objet.
Obtenir la conservation légale de l'objet	"Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"
Obtenir la rétention d'objet	"Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"
Obtenir l'étiquetage des objets	<p>Utilise le <code>tagging</code> sous-ressource pour renvoyer toutes les balises d'un objet.</p> <p>Gestion des versions</p> <p>Si le <code>versionId</code> si le paramètre de requête n'est pas spécifié dans la requête, l'opération renvoie toutes les balises de la version la plus récente de l'objet dans un bucket versionné. Si la version actuelle de l'objet est un marqueur de suppression, un statut « <code>MethodNotAllowed</code> » est renvoyé avec le <code>x-amz-delete-marker</code> en-tête de réponse défini sur <code>true</code>.</p>
HeadObject	"HeadObject"
Restaurer l'objet	"Restaurer l'objet"
Mettre l'objet	"Mettre l'objet"
Copier l'objet (précédemment nommé PUT Object - Copy)	"Copier l'objet"
MettreObjetLegalHold	"Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"

Opération	Mise en œuvre
PutObjectRetention	"Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"
Balises d'objets	<p>Utilise le <code>tagging</code> sous-ressource pour ajouter un ensemble de balises à un objet existant.</p> <p>Limites des balises d'objet</p> <p>Vous pouvez ajouter des balises aux nouveaux objets lorsque vous les téléchargez, ou vous pouvez les ajouter aux objets existants. StorageGRID et Amazon S3 prennent en charge jusqu'à 10 balises pour chaque objet. Les balises associées à un objet doivent avoir des clés de balise uniques. Une clé de balise peut contenir jusqu'à 128 caractères Unicode et les valeurs de balise peuvent contenir jusqu'à 256 caractères Unicode. La clé et les valeurs sont sensibles à la casse.</p> <p>Mises à jour des balises et comportement d'ingestion</p> <p>Lorsque vous utilisez PutObjectTagging pour mettre à jour les balises d'un objet, StorageGRID ne réingère pas l'objet. Cela signifie que l'option pour le comportement d'ingestion spécifiée dans la règle ILM correspondante n'est pas utilisée. Toutes les modifications apportées au placement des objets déclenchées par la mise à jour sont effectuées lorsque ILM est réévalué par les processus ILM d'arrière-plan normaux.</p> <p>Cela signifie que si la règle ILM utilise l'option Strict pour le comportement d'ingestion, aucune action n'est entreprise si les placements d'objets requis ne peuvent pas être effectués (par exemple, parce qu'un emplacement nouvellement requis n'est pas disponible). L'objet mis à jour conserve son emplacement actuel jusqu'à ce que le placement requis soit possible.</p> <p>Résoudre les conflits</p> <p>Les demandes client conflictuelles, telles que deux clients écrivant sur la même clé, sont résolues sur la base des « derniers gagnants ». Le moment de l'évaluation des « dernières victoires » est basé sur le moment où le système StorageGRID termine une demande donnée, et non sur le moment où les clients S3 commencent une opération.</p> <p>Gestion des versions</p> <p>Si le <code>versionId</code> le paramètre de requête n'est pas spécifié dans la requête, l'opération ajoute des balises à la version la plus récente de l'objet dans un bucket versionné. Si la version actuelle de l'objet est un marqueur de suppression, un statut « MethodNotAllowed » est renvoyé avec le <code>x-amz-delete-marker</code> en-tête de réponse défini sur <code>true</code>.</p>
Sélectionner le contenu de l'objet	"Sélectionner le contenu de l'objet"

StorageGRID prend en charge les clauses, types de données et opérateurs Amazon S3 Select suivants pour le ["Commande SelectObjectContent"](#) .



Tous les éléments non répertoriés ne sont pas pris en charge.

Pour la syntaxe, voir ["Sélectionner le contenu de l'objet"](#) . Pour plus d'informations sur S3 Select, consultez le ["Documentation AWS pour S3 Select"](#) .

Seuls les comptes locataires pour lesquels S3 Select est activé peuvent émettre des requêtes SelectObjectContent. Voir le ["considérations et exigences pour l'utilisation de S3 Select"](#) .

Clauses

- Liste SELECT
- Clause FROM
- Clause WHERE
- Clause LIMIT

Types de données

- booléen
- entier
- chaîne
- flotter
- décimal, numérique
- horodatage

Opérateurs

Opérateurs logiques

- ET
- PAS
- OU

Opérateurs de comparaison

- <
- >
- <=
- >=
- =
- =
- <>

- !=
- ENTRE
- DANS

Opérateurs de recherche de motifs

- COMME
- _
- %

opérateurs unitaires

- EST NUL
- N'EST PAS NUL

opérateurs mathématiques

- +
- -
- *
- /
- %

StorageGRID suit la priorité de l'opérateur Amazon S3 Select.

Fonctions d'agrégation

- MOYENNE()
- COMPTE(*)
- MAX()
- MIN()
- SOMME()

Fonctions conditionnelles

- CAS
- SE FONDRE
- NULLIF

Fonctions de conversion

- CAST (pour le type de données pris en charge)

Fonctions de date

- DATE_ADD
- DATE_DIFF

- EXTRAIT
- TO_STRING
- À_HORODATAGE
- UTCNOW

Fonctions de chaîne

- LONGUEUR_CARACTÈRE, LONGUEUR_CARACTÈRE
- INFÉRIEUR
- SOUS-CHAÎNE
- GARNITURE
- SUPÉRIEUR

Utiliser le cryptage côté serveur

Le chiffrement côté serveur vous permet de protéger vos données d'objet au repos. StorageGRID crypte les données lorsqu'il écrit l'objet et déchiffre les données lorsque vous accédez à l'objet.

Si vous souhaitez utiliser le chiffrement côté serveur, vous pouvez choisir l'une des deux options mutuellement exclusives, en fonction de la manière dont les clés de chiffrement sont gérées :

- **SSE (chiffrement côté serveur avec clés gérées par StorageGRID)** : lorsque vous émettez une demande S3 pour stocker un objet, StorageGRID chiffre l'objet avec une clé unique. Lorsque vous émettez une demande S3 pour récupérer l'objet, StorageGRID utilise la clé stockée pour déchiffrer l'objet.
- **SSE-C (chiffrement côté serveur avec clés fournies par le client)** : lorsque vous émettez une demande S3 pour stocker un objet, vous fournissez votre propre clé de chiffrement. Lorsque vous récupérez un objet, vous fournissez la même clé de chiffrement dans le cadre de votre demande. Si les deux clés de chiffrement correspondent, l'objet est déchiffré et vos données d'objet sont renvoyées.

Bien que StorageGRID gère toutes les opérations de chiffrement et de déchiffrement d'objets, vous devez gérer les clés de chiffrement que vous fournissez.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant.



Si un objet est chiffré avec SSE ou SSE-C, tous les paramètres de chiffrement au niveau du bucket ou de la grille sont ignorés.

Utiliser SSE

Pour chiffrer un objet avec une clé unique gérée par StorageGRID, vous utilisez l'en-tête de requête suivant :

```
x-amz-server-side-encryption
```

L'en-tête de requête SSE est pris en charge par les opérations d'objet suivantes :

- ["Mettre l'objet"](#)

- ["Copier l'objet"](#)
- ["Créer un téléchargement multi-parties"](#)

Utiliser SSE-C

Pour crypter un objet avec une clé unique que vous gérez, vous utilisez trois en-têtes de requête :

En-tête de la requête	Description
x-amz-server-side-encryption-customer-algorithm	Spécifiez l'algorithme de cryptage. La valeur de l'en-tête doit être AES256 .
x-amz-server-side-encryption-customer-key	Spécifiez la clé de chiffrement qui sera utilisée pour chiffrer ou déchiffrer l'objet. La valeur de la clé doit être de 256 bits, codée en base64.
x-amz-server-side-encryption-customer-key-MD5	Spécifiez le condensé MD5 de la clé de chiffrement conformément à la RFC 1321, qui est utilisé pour garantir que la clé de chiffrement a été transmise sans erreur. La valeur du condensé MD5 doit être codée en base64 sur 128 bits.

Les en-têtes de requête SSE-C sont pris en charge par les opérations d'objet suivantes :

- ["Obtenir l'objet"](#)
- ["HeadObject"](#)
- ["Mettre l'objet"](#)
- ["Copier l'objet"](#)
- ["Créer un téléchargement multi-parties"](#)
- ["Télécharger une partie"](#)
- ["TéléchargerPartCopy"](#)

Considérations relatives à l'utilisation du chiffrement côté serveur avec des clés fournies par le client (SSE-C)

Avant d'utiliser SSE-C, tenez compte des considérations suivantes :

- Vous devez utiliser https.



StorageGRID rejette toute requête effectuée via http lors de l'utilisation de SSE-C. Pour des raisons de sécurité, il est important de considérer que toute clé envoyée accidentellement via http est compromise. Jetez la clé et faites-la tourner comme il convient.

- L'ETag dans la réponse n'est pas le MD5 des données de l'objet.
- Vous devez gérer le mappage des clés de chiffrement aux objets. StorageGRID ne stocke pas les clés de chiffrement. Vous êtes responsable du suivi de la clé de cryptage que vous fournissez pour chaque objet.
- Si votre bucket est compatible avec le contrôle de version, chaque version d'objet doit avoir sa propre clé de chiffrement. Vous êtes responsable du suivi de la clé de chiffrement utilisée pour chaque version d'objet.

- Étant donné que vous gérez les clés de chiffrement côté client, vous devez également gérer toutes les mesures de protection supplémentaires, telles que la rotation des clés, côté client.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant.

- Si la réplication inter-grille ou la réplication CloudMirror est configurée pour le bucket, vous ne pouvez pas ingérer d'objets SSE-C. L'opération d'ingestion échouera.

Informations connexes

["Guide de l'utilisateur Amazon S3 : Utilisation du chiffrement côté serveur avec les clés fournies par le client \(SSE-C\)"](#)

Copier l'objet

Vous pouvez utiliser la requête S3 CopyObject pour créer une copie d'un objet déjà stocké dans S3. Une opération CopyObject revient à exécuter GetObject suivi de PutObject.

Résoudre les conflits

Les demandes client conflictuelles, telles que deux clients écrivant sur la même clé, sont résolues sur la base des « derniers gagnants ». Le moment de l'évaluation des « dernières victoires » est basé sur le moment où le système StorageGRID termine une demande donnée, et non sur le moment où les clients S3 commencent une opération.

Taille de l'objet

La taille maximale *recommandée* pour une seule opération PutObject est de 5 Gio (5 368 709 120 octets). Si vous avez des objets dont la taille est supérieure à 5 Gio, utilisez ["téléchargement en plusieurs parties"](#) plutôt.

La taille maximale *prise en charge* pour une seule opération PutObject est de 5 Tio (5 497 558 138 880 octets).



Si vous avez effectué une mise à niveau à partir de StorageGRID 11.6 ou d'une version antérieure, l'alerte S3 PUT La taille de l'objet est trop grande sera déclenchée si vous tentez de télécharger un objet dépassant 5 Gio. Si vous disposez d'une nouvelle installation de StorageGRID 11.7 ou 11.8, l'alerte ne sera pas déclenchée dans ce cas. Cependant, pour s'aligner sur la norme AWS S3, les futures versions de StorageGRID ne prendront pas en charge les téléchargements d'objets supérieurs à 5 Gio.

Caractères UTF-8 dans les métadonnées utilisateur

Si une demande inclut des valeurs UTF-8 (non échappées) dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur, le comportement de StorageGRID n'est pas défini.

StorageGRID n'analyse ni n'interprète les caractères UTF-8 échappés inclus dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur. Les caractères UTF-8 échappés sont traités comme des caractères ASCII :

- Les requêtes réussissent si les métadonnées définies par l'utilisateur incluent des caractères UTF-8 échappés.

- StorageGRID ne renvoie pas le `x-amz-missing-meta` en-tête si la valeur interprétée du nom ou de la valeur de la clé inclut des caractères non imprimables.

En-têtes de requête pris en charge

Les en-têtes de requête suivants sont pris en charge :

- `Content-Type`
- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`, suivi d'une paire nom-valeur contenant des métadonnées définies par l'utilisateur
- `x-amz-metadata-directive`: La valeur par défaut est `COPY` , qui vous permet de copier l'objet et les métadonnées associées.

Vous pouvez spécifier `REPLACE` pour écraser les métadonnées existantes lors de la copie de l'objet, ou pour mettre à jour les métadonnées de l'objet.

- `x-amz-storage-class`
- `x-amz-tagging-directive`: La valeur par défaut est `COPY` , qui vous permet de copier l'objet et toutes les balises.

Vous pouvez spécifier `REPLACE` pour écraser les balises existantes lors de la copie de l'objet, ou pour mettre à jour les balises.

- En-têtes de demande de verrouillage d'objet S3 :

- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`

Si une demande est effectuée sans ces en-têtes, les paramètres de conservation par défaut du bucket sont utilisés pour calculer le mode de version de l'objet et la date de conservation. Voir ["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#) .

- En-têtes de requête SSE :

- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`
- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-server-side-encryption-customer-key`

- `x-amz-server-side-encryption-customer-algorithm`

Voir [En-têtes de requête pour le chiffrement côté serveur](#)

En-têtes de requête non pris en charge

Les en-têtes de requête suivants ne sont pas pris en charge :

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`

Lorsque vous copiez un objet, si l'objet source possède une somme de contrôle, StorageGRID ne copie pas cette valeur de somme de contrôle dans le nouvel objet. Ce comportement s'applique que vous essayiez ou non d'utiliser `x-amz-checksum-algorithm` dans la demande d'objet.

- `x-amz-website-redirect-location`

Options de classe de stockage

Le `x-amz-storage-class` L'en-tête de requête est pris en charge et affecte le nombre de copies d'objets créées par StorageGRID si la règle ILM correspondante utilise la validation double ou équilibrée ["option d'ingestion"](#) .

- `STANDARD`

(Par défaut) Spécifie une opération d'ingestion à double validation lorsque la règle ILM utilise l'option Double validation ou lorsque l'option Équilibré revient à la création de copies intermédiaires.

- `REDUCED_REDUNDANCY`

Spécifie une opération d'ingestion à validation unique lorsque la règle ILM utilise l'option de validation double ou lorsque l'option Équilibré revient à la création de copies intermédiaires.



Si vous ingérez un objet dans un bucket avec le verrouillage d'objet S3 activé, le `REDUCED_REDUNDANCY` l'option est ignorée. Si vous ingérez un objet dans un bucket conforme hérité, le `REDUCED_REDUNDANCY` l'option renvoie une erreur. StorageGRID effectuera toujours une ingestion à double validation pour garantir que les exigences de conformité sont satisfaites.

Utilisation de `x-amz-copy-source` dans `CopyObject`

Si le bucket source et la clé, spécifiés dans le `x-amz-copy-source` en-tête, sont différents du bucket et de la clé de destination, une copie des données de l'objet source est écrite dans la destination.

Si la source et la destination correspondent, et que le `x-amz-metadata-directive` l'en-tête est spécifié

comme `REPLACE`, les métadonnées de l'objet sont mises à jour avec les valeurs de métadonnées fournies dans la demande. Dans ce cas, StorageGRID ne réingère pas l'objet. Cela a deux conséquences importantes :

- Vous ne pouvez pas utiliser `CopyObject` pour crypter un objet existant sur place ou pour modifier le cryptage d'un objet existant sur place. Si vous fournissez le `x-amz-server-side-encryption` en-tête ou le `x-amz-server-side-encryption-customer-algorithm` en-tête, StorageGRID rejette la demande et renvoie `XNotImplemented`.
- L'option pour le comportement d'ingestion spécifiée dans la règle ILM correspondante n'est pas utilisée. Toutes les modifications apportées au placement des objets déclenchées par la mise à jour sont effectuées lorsque ILM est réévalué par les processus ILM d'arrière-plan normaux.

Cela signifie que si la règle ILM utilise l'option `Strict` pour le comportement d'ingestion, aucune action n'est entreprise si les placements d'objets requis ne peuvent pas être effectués (par exemple, parce qu'un emplacement nouvellement requis n'est pas disponible). L'objet mis à jour conserve son emplacement actuel jusqu'à ce que le placement requis soit possible.

En-têtes de requête pour le chiffrement côté serveur

Si tu [utilises le cryptage côté serveur](#), les en-têtes de requête que vous fournissez dépendent du fait que l'objet source est chiffré ou non et du fait que vous prévoyez de chiffrer l'objet cible.

- Si l'objet source est chiffré à l'aide d'une clé fournie par le client (SSE-C), vous devez inclure les trois en-têtes suivants dans la demande `CopyObject`, afin que l'objet puisse être déchiffré puis copié :
 - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Préciser `AES256`.
 - `x-amz-copy-source-server-side-encryption-customer-key`: Spécifiez la clé de chiffrement que vous avez fournie lors de la création de l'objet source.
 - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Spécifiez le condensé MD5 que vous avez fourni lors de la création de l'objet source.
- Si vous souhaitez crypter l'objet cible (la copie) avec une clé unique que vous fournissez et gérez, incluez les trois en-têtes suivants :
 - `x-amz-server-side-encryption-customer-algorithm`: Préciser `AES256`.
 - `x-amz-server-side-encryption-customer-key`: Spécifiez une nouvelle clé de chiffrement pour l'objet cible.
 - `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le condensé MD5 de la nouvelle clé de chiffrement.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser les clés fournies par le client pour sécuriser les données d'objet, examinez les considérations relatives ["en utilisant le cryptage côté serveur"](#).

- Si vous souhaitez crypter l'objet cible (la copie) avec une clé unique gérée par StorageGRID (SSE), incluez cet en-tête dans la requête `CopyObject` :
 - `x-amz-server-side-encryption`



Le `server-side-encryption` la valeur de l'objet ne peut pas être mise à jour. Au lieu de cela, faites une copie avec un nouveau `server-side-encryption` valeur en utilisant `x-amz-metadata-directive: REPLACE`.

Gestion des versions

Si le bucket source est versionné, vous pouvez utiliser le `x-amz-copy-source` en-tête pour copier la dernière version d'un objet. Pour copier une version spécifique d'un objet, vous devez spécifier explicitement la version à copier à l'aide de la commande `versionId` sous-ressource. Si le bucket de destination est versionné, la version générée est renvoyée dans le `x-amz-version-id` en-tête de réponse. Si le contrôle de version est suspendu pour le bucket cible, alors `x-amz-version-id` renvoie une valeur « null ».

Obtenir l'objet

Vous pouvez utiliser la requête S3 `GetObject` pour récupérer un objet d'un bucket S3.

GetObject et objets multipartites

Vous pouvez utiliser le `partNumber` paramètre de requête pour récupérer une partie spécifique d'un objet en plusieurs parties ou segmenté. Le `x-amz-mp-parts-count` L'élément de réponse indique le nombre de parties que contient l'objet.

Vous pouvez définir `partNumber` à 1 pour les objets segmentés/multipartites et les objets non segmentés/non multipartites ; cependant, le `x-amz-mp-parts-count` L'élément de réponse n'est renvoyé que pour les objets segmentés ou en plusieurs parties.

Caractères UTF-8 dans les métadonnées utilisateur

StorageGRID n'analyse ni n'interprète les caractères UTF-8 échappés dans les métadonnées définies par l'utilisateur. Les requêtes GET pour un objet avec des caractères UTF-8 échappés dans les métadonnées définies par l'utilisateur ne renvoient pas le `x-amz-missing-meta` en-tête si le nom ou la valeur de la clé inclut des caractères non imprimables.

En-tête de requête pris en charge

L'en-tête de requête suivant est pris en charge :

- `x-amz-checksum-mode`: Préciser `ENABLED`

Le Range l'en-tête n'est pas pris en charge avec `x-amz-checksum-mode` pour `GetObject`. Lorsque vous incluez Range dans la demande avec `x-amz-checksum-mode` activé, StorageGRID ne renvoie pas de valeur de somme de contrôle dans la réponse.

En-tête de requête non pris en charge

L'en-tête de requête suivant n'est pas pris en charge et renvoie `XNotImplemented` :

- `x-amz-website-redirect-location`


Gestion des versions

Si un `versionId` la sous-ressource n'est pas spécifiée, l'opération récupère la version la plus récente de l'objet dans un bucket versionné. Si la version actuelle de l'objet est un marqueur de suppression, un statut « Non trouvé » est renvoyé avec le `x-amz-delete-marker` en-tête de réponse défini sur `true` .

En-têtes de requête pour le chiffrement côté serveur avec les clés de chiffrement fournies par le client (SSE-C)

Utilisez les trois en-têtes si l'objet est chiffré avec une clé unique que vous avez fournie.


- `x-amz-server-side-encryption-customer-algorithm`: Préciser AES256 .
- `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de chiffrement pour l'objet.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le condensé MD5 de la clé de chiffrement de l'objet.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser les clés fournies par le client pour sécuriser les données d'objet, examinez les considérations dans ["Utiliser le cryptage côté serveur"](#) .

Comportement de GetObject pour les objets Cloud Storage Pool

Si un objet a été stocké dans un ["Pool de stockage cloud"](#) , le comportement d'une requête GetObject dépend de l'état de l'objet. Voir ["HeadObject"](#) pour plus de détails.



Si un objet est stocké dans un pool de stockage cloud et qu'une ou plusieurs copies de l'objet existent également sur la grille, les requêtes GetObject tenteront de récupérer les données de la grille, avant de les récupérer du pool de stockage cloud.

État de l'objet	Comportement de GetObject
Objet ingéré dans StorageGRID mais pas encore évalué par ILM, ou objet stocké dans un pool de stockage traditionnel ou utilisant un codage d'effacement	200 OK Une copie de l'objet est récupérée.
Objet dans le pool de stockage cloud, mais pas encore passé à un état non récupérable	200 OK Une copie de l'objet est récupérée.
Objet passé à un état non récupérable	403 Forbidden , InvalidObjectState Utiliser un "Restaurer l'objet" demande de restauration de l'objet à un état récupérable.
Objet en cours de restauration à partir d'un état non récupérable	403 Forbidden , InvalidObjectState Attendez que la demande RestoreObject soit terminée.
Objet entièrement restauré dans le pool de stockage cloud	200 OK Une copie de l'objet est récupérée.

Objets multipartites ou segmentés dans un pool de stockage cloud

Si vous avez téléchargé un objet en plusieurs parties ou si StorageGRID a divisé un objet volumineux en segments, StorageGRID détermine si l'objet est disponible dans le pool de stockage cloud en échantillonnant un sous-ensemble des parties ou des segments de l'objet. Dans certains cas, une requête `GetObject` peut renvoyer de manière incorrecte `200 OK` lorsque certaines parties de l'objet ont déjà été transférées vers un état non récupérable ou lorsque certaines parties de l'objet n'ont pas encore été restaurées.

Dans ces cas :

- La requête `GetObject` peut renvoyer des données mais s'arrêter à mi-chemin du transfert.
- Une requête `GetObject` ultérieure peut renvoyer `403 Forbidden`.

GetObject et réplication inter-grille

Si vous utilisez "[fédération de réseau](#)" et "[réplication inter-réseaux](#)" est activé pour un bucket, le client S3 peut vérifier l'état de réplication d'un objet en émettant une requête `GetObject`. La réponse inclut le StorageGRID spécifique `x-ntap-sg-cgr-replication-status` en-tête de réponse, qui aura l'une des valeurs suivantes :

Grille	État de réplication
Source	<ul style="list-style-type: none">• TERMINÉ : La réplication a réussi.• EN ATTENTE : L'objet n'a pas encore été répliqué.• ÉCHEC : La réplication a échoué avec un échec permanent. Un utilisateur doit résoudre l'erreur.
Destination	RÉPLIQUE : L'objet a été répliqué à partir de la grille source.



StorageGRID ne prend pas en charge le `x-amz-replication-status` en-tête.

HeadObject

Vous pouvez utiliser la requête S3 `HeadObject` pour récupérer les métadonnées d'un objet sans renvoyer l'objet lui-même. Si l'objet est stocké dans un pool de stockage cloud, vous pouvez utiliser `HeadObject` pour déterminer l'état de transition de l'objet.

HeadObject et objets multipartites

Vous pouvez utiliser le `partNumber` paramètre de demande pour récupérer les métadonnées d'une partie spécifique d'un objet en plusieurs parties ou segmenté. Le `x-amz-mp-parts-count` L'élément de réponse indique le nombre de parties que contient l'objet.

Vous pouvez définir `partNumber` à 1 pour les objets segmentés/multipartites et les objets non segmentés/non multipartites ; cependant, le `x-amz-mp-parts-count` L'élément de réponse n'est renvoyé que pour les objets segmentés ou en plusieurs parties.

Caractères UTF-8 dans les métadonnées utilisateur

StorageGRID n'analyse ni n'interprète les caractères UTF-8 échappés dans les métadonnées définies par

l'utilisateur. Les requêtes HEAD pour un objet avec des caractères UTF-8 échappés dans les métadonnées définies par l'utilisateur ne renvoient pas le `x-amz-missing-meta` en-tête si le nom ou la valeur de la clé inclut des caractères non imprimables.

En-tête de requête pris en charge

L'en-tête de requête suivant est pris en charge :

- `x-amz-checksum-mode`

Le `partNumber` paramètre et `Range` les en-têtes ne sont pas pris en charge avec `x-amz-checksum-mode` pour `HeadObject`. Lorsque vous les incluez dans la demande avec `x-amz-checksum-mode` activé, `StorageGRID` ne renvoie pas de valeur de somme de contrôle dans la réponse.

En-tête de requête non pris en charge

L'en-tête de requête suivant n'est pas pris en charge et renvoie `XNotImplemented` :

- `x-amz-website-redirect-location`

Gestion des versions

Si un `versionId` la sous-ressource n'est pas spécifiée, l'opération récupère la version la plus récente de l'objet dans un bucket versionné. Si la version actuelle de l'objet est un marqueur de suppression, un statut « Non trouvé » est renvoyé avec le `x-amz-delete-marker` en-tête de réponse défini sur `true` .

En-têtes de requête pour le chiffrement côté serveur avec les clés de chiffrement fournies par le client (SSE-C)

Utilisez ces trois en-têtes si l'objet est chiffré avec une clé unique que vous avez fournie.

- `x-amz-server-side-encryption-customer-algorithm`: Préciser AES256 .
- `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de chiffrement pour l'objet.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le condensé MD5 de la clé de chiffrement de l'objet.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser les clés fournies par le client pour sécuriser les données d'objet, examinez les considérations dans ["Utiliser le cryptage côté serveur"](#) .

Réponses `HeadObject` pour les objets `Cloud Storage Pool`

Si l'objet est stocké dans un ["Pool de stockage cloud"](#) , les en-têtes de réponse suivants sont renvoyés :

- `x-amz-storage-class`: GLACIER
- `x-amz-restore`

Les en-têtes de réponse fournissent des informations sur l'état d'un objet lorsqu'il est déplacé vers un pool de stockage cloud, éventuellement transféré vers un état non récupérable et restauré.

État de l'objet	Réponse à HeadObject
Objet ingéré dans StorageGRID mais pas encore évalué par ILM, ou objet stocké dans un pool de stockage traditionnel ou utilisant un codage d'effacement	200 OK(Aucun en-tête de réponse spécial n'est renvoyé.)
Objet dans le pool de stockage cloud, mais pas encore passé à un état non récupérable	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>Jusqu'à ce que l'objet soit transféré vers un état non récupérable, la valeur de <code>expiry-date</code> se déroule à une époque lointaine dans le futur. L'heure exacte de la transition n'est pas contrôlée par le système StorageGRID .</p>
L'objet est passé à un état non récupérable, mais au moins une copie existe également sur la grille	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>La valeur pour <code>expiry-date</code> se déroule à une époque lointaine dans le futur.</p> <p>Remarque : Si la copie sur la grille n'est pas disponible (par exemple, un nœud de stockage est en panne), vous devez émettre un "Restaurer l'objet" demandez à restaurer la copie à partir du pool de stockage cloud avant de pouvoir récupérer l'objet avec succès.</p>
L'objet est passé à un état non récupérable et aucune copie n'existe sur la grille	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p>
Objet en cours de restauration à partir d'un état non récupérable	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="true"</p>

État de l'objet	Réponse à HeadObject
Objet entièrement restauré dans le pool de stockage cloud	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 2018 00:00:00 GMT"</p> <p>Le expiry-date indique quand l'objet dans le pool de stockage cloud sera renvoyé à un état non récupérable.</p>

Objets multipartites ou segmentés dans le pool de stockage cloud

Si vous avez téléchargé un objet en plusieurs parties ou si StorageGRID a divisé un objet volumineux en segments, StorageGRID détermine si l'objet est disponible dans le pool de stockage cloud en échantillonnant un sous-ensemble des parties ou des segments de l'objet. Dans certains cas, une requête HeadObject peut renvoyer de manière incorrecte `x-amz-restore: ongoing-request="false"` lorsque certaines parties de l'objet ont déjà été transférées vers un état non récupérable ou lorsque certaines parties de l'objet n'ont pas encore été restaurées.

Réplication HeadObject et inter-grille

Si vous utilisez ["fédération de réseau"](#) et ["réplication inter-réseaux"](#) est activé pour un bucket, le client S3 peut vérifier l'état de réplication d'un objet en émettant une demande HeadObject. La réponse inclut le StorageGRID spécifique `x-ntap-sg-cgr-replication-status` en-tête de réponse, qui aura l'une des valeurs suivantes :

Grille	État de réplication
Source	<ul style="list-style-type: none"> • TERMINÉ : La réplication a réussi. • EN ATTENTE : L'objet n'a pas encore été répliqué. • ÉCHEC : La réplication a échoué avec un échec permanent. Un utilisateur doit résoudre l'erreur.
Destination	RÉPLIQUE : L'objet a été répliqué à partir de la grille source.



StorageGRID ne prend pas en charge le `x-amz-replication-status` en-tête.

Mettre l'objet

Vous pouvez utiliser la requête S3 PutObject pour ajouter un objet à un bucket.

Résoudre les conflits

Les demandes client conflictuelles, telles que deux clients écrivant sur la même clé, sont résolues sur la base des « derniers gagnants ». Le moment de l'évaluation des « dernières victoires » est basé sur le moment où le système StorageGRID termine une demande donnée, et non sur le moment où les clients S3 commencent une

opération.

Taille de l'objet

La taille maximale *recommandée* pour une seule opération PutObject est de 5 Gio (5 368 709 120 octets). Si vous avez des objets dont la taille est supérieure à 5 Gio, utilisez ["téléchargement en plusieurs parties"](#) plutôt.

La taille maximale *prise en charge* pour une seule opération PutObject est de 5 Tio (5 497 558 138 880 octets).



Si vous avez effectué une mise à niveau à partir de StorageGRID 11.6 ou d'une version antérieure, l'alerte S3 PUT La taille de l'objet est trop grande sera déclenchée si vous tentez de télécharger un objet dépassant 5 Gio. Si vous disposez d'une nouvelle installation de StorageGRID 11.7 ou 11.8, l'alerte ne sera pas déclenchée dans ce cas. Cependant, pour s'aligner sur la norme AWS S3, les futures versions de StorageGRID ne prendront pas en charge les téléchargements d'objets supérieurs à 5 Gio.

Taille des métadonnées utilisateur

Amazon S3 limite la taille des métadonnées définies par l'utilisateur dans chaque en-tête de requête PUT à 2 Ko. StorageGRID limite les métadonnées utilisateur à 24 Ko. La taille des métadonnées définies par l'utilisateur est mesurée en prenant la somme du nombre d'octets dans l'encodage UTF-8 de chaque clé et valeur.

Caractères UTF-8 dans les métadonnées utilisateur

Si une demande inclut des valeurs UTF-8 (non échappées) dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur, le comportement de StorageGRID n'est pas défini.

StorageGRID n'analyse ni n'interprète les caractères UTF-8 échappés inclus dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur. Les caractères UTF-8 échappés sont traités comme des caractères ASCII :

- Les requêtes PutObject, CopyObject, GetObject et HeadObject réussissent si les métadonnées définies par l'utilisateur incluent des caractères UTF-8 échappés.
- StorageGRID ne renvoie pas le `x-amz-missing-meta` en-tête si la valeur interprétée du nom ou de la valeur de la clé inclut des caractères non imprimables.

Limites des balises d'objet

Vous pouvez ajouter des balises aux nouveaux objets lorsque vous les téléchargez, ou vous pouvez les ajouter aux objets existants. StorageGRID et Amazon S3 prennent en charge jusqu'à 10 balises pour chaque objet. Les balises associées à un objet doivent avoir des clés de balise uniques. Une clé de balise peut contenir jusqu'à 128 caractères Unicode et les valeurs de balise peuvent contenir jusqu'à 256 caractères Unicode. La clé et les valeurs sont sensibles à la casse.

Propriété de l'objet

Dans StorageGRID, tous les objets appartiennent au compte propriétaire du bucket, y compris les objets créés par un compte non propriétaire ou un utilisateur anonyme.

En-têtes de requête pris en charge

Les en-têtes de requête suivants sont pris en charge :

- Cache-Control
- Content-Disposition
- Content-Encoding

Lorsque vous spécifiez `aws-chunked` pour `Content-Encoding` StorageGRID ne vérifie pas les éléments suivants :

- StorageGRID ne vérifie pas le `chunk-signature` par rapport aux données du bloc.
- StorageGRID ne vérifie pas la valeur que vous fournissez pour `x-amz-decoded-content-length` contre l'objet.

- Content-Language
- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

L'encodage de transfert fragmenté est pris en charge si `aws-chunked` la signature de la charge utile est également utilisée.

- `x-amz-checksum-sha256`
- `x-amz-meta-`, suivi d'une paire nom-valeur contenant des métadonnées définies par l'utilisateur.

Lors de la spécification de la paire nom-valeur pour les métadonnées définies par l'utilisateur, utilisez ce format général :

```
x-amz-meta-name: value
```

Si vous souhaitez utiliser l'option **Heure de création définie par l'utilisateur** comme heure de référence pour une règle ILM, vous devez utiliser `creation-time` comme le nom des métadonnées qui enregistrent quand l'objet a été créé. Par exemple:

```
x-amz-meta-creation-time: 1443399726
```

La valeur pour `creation-time` est évalué en secondes depuis le 1er janvier 1970.



Une règle ILM ne peut pas utiliser à la fois une **heure de création définie par l'utilisateur** pour l'heure de référence et l'option d'ingestion équilibrée ou stricte. Une erreur est renvoyée lors de la création de la règle ILM.

- `x-amz-tagging`
- En-têtes de demande de verrouillage d'objet S3
 - `x-amz-object-lock-mode`
 - `x-amz-object-lock-retain-until-date`
 - `x-amz-object-lock-legal-hold`

Si une demande est effectuée sans ces en-têtes, les paramètres de conservation par défaut du bucket sont utilisés pour calculer le mode de version de l'objet et la date de conservation. Voir ["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#) .

- En-têtes de requête SSE :
 - `x-amz-server-side-encryption`
 - `x-amz-server-side-encryption-customer-key-MD5`
 - `x-amz-server-side-encryption-customer-key`
 - `x-amz-server-side-encryption-customer-algorithm`

Voir [En-têtes de requête pour le chiffrement côté serveur](#)

En-têtes de requête non pris en charge

Les en-têtes de requête suivants ne sont pas pris en charge :

- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

Le `x-amz-website-redirect-location` retourne d'en-tête `XNotImplemented` .

Options de classe de stockage

Le `x-amz-storage-class` l'en-tête de requête est pris en charge. La valeur soumise pour `x-amz-storage-class` affecte la manière dont StorageGRID protège les données de l'objet pendant l'ingestion et non le nombre de copies persistantes de l'objet stockées dans le système StorageGRID (qui est déterminé par ILM).

Si la règle ILM correspondant à un objet ingéré utilise l'option d'ingestion stricte, le `x-amz-storage-class` l'en-tête n'a aucun effet.

Les valeurs suivantes peuvent être utilisées pour `x-amz-storage-class` :

- STANDARD(Défaut)
 - **Double validation** : si la règle ILM spécifie l'option Double validation pour le comportement d'ingestion, dès qu'un objet est ingéré, une deuxième copie de cet objet est créée et distribuée à un autre nœud de stockage (double validation). Lorsque l'ILM est évalué, StorageGRID détermine si ces copies intermédiaires initiales satisfont aux instructions de placement de la règle. Si ce n'est pas le

cas, de nouvelles copies d'objets devront peut-être être réalisées à des emplacements différents et les copies intermédiaires initiales devront peut-être être supprimées.

- **Équilibré** : si la règle ILM spécifie l'option Équilibré et que StorageGRID ne peut pas effectuer immédiatement toutes les copies spécifiées dans la règle, StorageGRID effectue deux copies intermédiaires sur différents nœuds de stockage.

Si StorageGRID peut créer immédiatement toutes les copies d'objets spécifiées dans la règle ILM (placement synchrone), le `x-amz-storage-class` l'en-tête n'a aucun effet.

- **REDUCED_REDUNDANCY**

- *** Double validation *** : si la règle ILM spécifie l'option Double validation pour le comportement d'ingestion, StorageGRID crée une copie intermédiaire unique lorsque l'objet est ingéré (validation unique).
- **Équilibré** : si la règle ILM spécifie l'option Équilibré, StorageGRID effectue une seule copie intermédiaire uniquement si le système ne peut pas effectuer immédiatement toutes les copies spécifiées dans la règle. Si StorageGRID peut effectuer un placement synchrone, cet en-tête n'a aucun effet. Le `REDUCED_REDUNDANCY` L'option est mieux utilisée lorsque la règle ILM qui correspond à l'objet crée une seule copie répliquée. Dans ce cas, en utilisant `REDUCED_REDUNDANCY` élimine la création et la suppression inutiles d'une copie d'objet supplémentaire pour chaque opération d'ingestion.

En utilisant le `REDUCED_REDUNDANCY` Cette option n'est pas recommandée dans d'autres circonstances. `REDUCED_REDUNDANCY` augmente le risque de perte de données d'objet lors de l'ingestion. Par exemple, vous risquez de perdre des données si la copie unique est initialement stockée sur un nœud de stockage qui échoue avant que l'évaluation ILM puisse avoir lieu.



Le fait de n'avoir qu'une seule copie répliquée pendant une période donnée expose les données à un risque de perte permanente. Si une seule copie répliquée d'un objet existe, cet objet est perdu si un nœud de stockage échoue ou présente une erreur importante. Vous perdez également temporairement l'accès à l'objet pendant les procédures de maintenance telles que les mises à niveau.

Spécification `REDUCED_REDUNDANCY` affecte uniquement le nombre de copies créées lorsqu'un objet est ingéré pour la première fois. Cela n'affecte pas le nombre de copies de l'objet effectuées lorsque l'objet est évalué par les stratégies ILM actives et n'entraîne pas le stockage des données à des niveaux de redondance inférieurs dans le système StorageGRID .



Si vous ingérez un objet dans un bucket avec le verrouillage d'objet S3 activé, le `REDUCED_REDUNDANCY` l'option est ignorée. Si vous ingérez un objet dans un bucket conforme hérité, le `REDUCED_REDUNDANCY` l'option renvoie une erreur. StorageGRID effectuera toujours une ingestion à double validation pour garantir que les exigences de conformité sont satisfaites.

En-têtes de requête pour le chiffrement côté serveur

Vous pouvez utiliser les en-têtes de requête suivants pour crypter un objet avec un cryptage côté serveur. Les options SSE et SSE-C s'excluent mutuellement.

- **SSE** : utilisez l'en-tête suivant si vous souhaitez chiffrer l'objet avec une clé unique gérée par StorageGRID.
 - `x-amz-server-side-encryption`

Quand le `x-amz-server-side-encryption` l'en-tête n'est pas inclus dans la requête `PutObject`, la grille entière "[paramètre de cryptage des objets stockés](#)" est omis de la réponse `PutObject`.

- **SSE-C** : utilisez ces trois en-têtes si vous souhaitez chiffrer l'objet avec une clé unique que vous fournissez et gérez.
 - `x-amz-server-side-encryption-customer-algorithm`: Préciser AES256 .
 - `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de chiffrement pour le nouvel objet.
 - `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le condensé MD5 de la clé de chiffrement du nouvel objet.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser les clés fournies par le client pour sécuriser les données d'objet, examinez les considérations relatives "[en utilisant le cryptage côté serveur](#)".



Si un objet est chiffré avec SSE ou SSE-C, tous les paramètres de chiffrement au niveau du bucket ou de la grille sont ignorés.

Gestion des versions

Si le contrôle de version est activé pour un bucket, un `versionId` est généré automatiquement pour la version de l'objet stocké. Ce `versionId` est également renvoyé dans la réponse en utilisant le `x-amz-version-id` en-tête de réponse.

Si le contrôle de version est suspendu, la version de l'objet est stockée avec une valeur nulle `versionId` et si une version nulle existe déjà, elle sera écrasée.

Calculs de signature pour l'en-tête d'autorisation

Lors de l'utilisation du `Authorization` en-tête pour authentifier les requêtes, StorageGRID diffère d'AWS des manières suivantes :

- StorageGRID ne nécessite pas `host` en-têtes à inclure dans `CanonicalHeaders` .
- StorageGRID ne nécessite pas `Content-Type` à inclure dans `CanonicalHeaders` .
- StorageGRID ne nécessite pas `x-amz-*` en-têtes à inclure dans `CanonicalHeaders` .



En règle générale, incluez toujours ces en-têtes dans `CanonicalHeaders` pour garantir qu'ils sont vérifiés ; cependant, si vous excluez ces en-têtes, StorageGRID ne renvoie pas d'erreur.

Pour plus de détails, reportez-vous à "[Calculs de signature pour l'en-tête d'autorisation : transfert de charge utile en un seul bloc \(AWS Signature Version 4\)](#)".

Informations connexes

- "[Gérer les objets avec ILM](#)"
- "[Référence de l'API Amazon Simple Storage Service : PutObject](#)"

Restaurer l'objet

Vous pouvez utiliser la demande S3 RestoreObject pour restaurer un objet stocké dans un pool de stockage cloud.

Type de demande pris en charge

StorageGRID prend uniquement en charge les requêtes RestoreObject pour restaurer un objet. Il ne prend pas en charge le SELECT type de restauration. Sélectionnez les demandes de retour XNotImplemented .

Gestion des versions

En option, précisez `versionId` pour restaurer une version spécifique d'un objet dans un bucket versionné. Si vous ne précisez pas `versionId` , la version la plus récente de l'objet est restaurée

Comportement de RestoreObject sur les objets du pool de stockage cloud

Si un objet a été stocké dans un "Pool de stockage cloud" , une demande RestoreObject a le comportement suivant, en fonction de l'état de l'objet. Voir "HeadObject" pour plus de détails.



Si un objet est stocké dans un pool de stockage cloud et qu'une ou plusieurs copies de l'objet existent également sur la grille, il n'est pas nécessaire de restaurer l'objet en émettant une demande RestoreObject. Au lieu de cela, la copie locale peut être récupérée directement, à l'aide d'une requête GetObject.

État de l'objet	Comportement de RestoreObject
Objet ingéré dans StorageGRID mais pas encore évalué par ILM, ou l'objet ne se trouve pas dans un pool de stockage cloud	403 Forbidden , InvalidObjectState
Objet dans le pool de stockage cloud, mais pas encore passé à un état non récupérable	<code>`200 OK`</code> Aucune modification n'est apportée. Remarque : Avant qu'un objet ne soit passé à un état non récupérable, vous ne pouvez pas modifier son <code>expiry-date</code> .

État de l'objet	Comportement de RestoreObject
Objet passé à un état non récupérable	<p>`202 Accepted` Restaure une copie récupérable de l'objet dans le pool de stockage cloud pendant le nombre de jours spécifié dans le corps de la demande. À la fin de cette période, l'objet est remis dans un état non récupérable.</p> <p>En option, utilisez le <code>Tier</code> élément de demande pour déterminer combien de temps la tâche de restauration prendra pour se terminer (<code>Expedited</code>, <code>Standard</code>, ou <code>Bulk</code>). Si vous ne précisez pas <code>Tier</code>, le <code>Standard</code> le niveau est utilisé.</p> <p>Important : Si un objet a été transféré vers S3 Glacier Deep Archive ou si le pool de stockage cloud utilise le stockage Azure Blob, vous ne pouvez pas le restaurer à l'aide de <code>Expedited</code> étage. L'erreur suivante est renvoyée <code>403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class</code>.</p>
Objet en cours de restauration à partir d'un état non récupérable	<code>409 Conflict, RestoreAlreadyInProgress</code>
Objet entièrement restauré dans le pool de stockage cloud	<p><code>200 OK</code></p> <p>Remarque : si un objet a été restauré dans un état récupérable, vous pouvez modifier son <code>expiry-date</code> en réémettant la requête <code>RestoreObject</code> avec une nouvelle valeur pour <code>Days</code>. La date de restauration est mise à jour par rapport à l'heure de la demande.</p>

Sélectionner le contenu de l'objet

Vous pouvez utiliser la requête `S3 SelectObjectContent` pour filtrer le contenu d'un objet S3 en fonction d'une simple instruction SQL.

Pour plus d'informations, voir ["Référence de l'API Amazon Simple Storage Service : SelectObjectContent"](#).

Avant de commencer

- Le compte locataire dispose de l'autorisation `S3 Select`.
- Tu as `s3:GetObject` autorisation pour l'objet que vous souhaitez interroger.
- L'objet que vous souhaitez interroger doit être dans l'un des formats suivants :
 - **CSV**. Peut être utilisé tel quel ou compressé dans des archives GZIP ou BZIP2.
 - **Parquet**. Exigences supplémentaires pour les objets Parquet :
 - S3 Select prend uniquement en charge la compression en colonnes à l'aide de GZIP ou Snappy. S3 Select ne prend pas en charge la compression d'objets entiers pour les objets Parquet.
 - S3 Select ne prend pas en charge la sortie Parquet. Vous devez spécifier le format de sortie au format CSV ou JSON.
 - La taille maximale du groupe de lignes non compressé est de 512 Mo.
 - Vous devez utiliser les types de données spécifiés dans le schéma de l'objet.

- Vous ne pouvez pas utiliser les types logiques INTERVAL, JSON, LIST, TIME ou UUID.
- Votre expression SQL a une longueur maximale de 256 Ko.
- Tout enregistrement dans l'entrée ou les résultats a une longueur maximale de 1 Mio.

Exemple de syntaxe de requête CSV

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <CSV>
      <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
      <Comments>#</Comments>
      <FieldDelimiter>\t</FieldDelimiter>
      <FileHeaderInfo>USE</FileHeaderInfo>
      <QuoteCharacter>'</QuoteCharacter>
      <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
      <RecordDelimiter>\n</RecordDelimiter>
    </CSV>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>
```

Exemple de syntaxe de demande de parquet

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <PARQUET>
    </PARQUET>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>
```

Exemple de requête SQL

Cette requête obtient le nom de l'État, les populations de 2010, les populations estimées de 2015 et le pourcentage de changement à partir des données du recensement américain. Les enregistrements du fichier qui ne sont pas des états sont ignorés.

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

Les premières lignes du fichier à interroger, SUB-EST2020_ALL.csv , ressemble à ceci :

```
SUMLEV, STATE, COUNTY, PLACE, COUSUB, CONCIT, PRIMGEO_FLAG, FUNCSTAT, NAME, STNAME,
CENSUS2010POP,
ESTIMATESBASE2010, POPESTIMATE2010, POPESTIMATE2011, POPESTIMATE2012, POPESTIM
ATE2013, POPESTIMATE2014,
POPESTIMATE2015, POPESTIMATE2016, POPESTIMATE2017, POPESTIMATE2018, POPESTIMAT
E2019, POPESTIMATE042020,
POPESTIMATE2020
040, 01, 000, 00000, 00000, 00000, 0, A, Alabama, Alabama, 4779736, 4780118, 4785514, 4
799642, 4816632, 4831586,
4843737, 4854803, 4866824, 4877989, 4891628, 4907965, 4920706, 4921532
162, 01, 000, 00124, 00000, 00000, 0, A, Abbeville
city, Alabama, 2688, 2705, 2699, 2694, 2645, 2629, 2610, 2602,
2587, 2578, 2565, 2555, 2555, 2553
162, 01, 000, 00460, 00000, 00000, 0, A, Adamsville
city, Alabama, 4522, 4487, 4481, 4474, 4453, 4430, 4399, 4371,
4335, 4304, 4285, 4254, 4224, 4211
162, 01, 000, 00484, 00000, 00000, 0, A, Addison
town, Alabama, 758, 754, 751, 750, 745, 744, 742, 734, 734, 728,
725, 723, 719, 717
```

Exemple d'utilisation d'AWS-CLI (CSV)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

Les premières lignes du fichier de sortie, changes.csv, ressemble à ceci :

```
Alabama, 4779736, 4854803, 1.5705260708959658022953568983726297854
Alaska, 710231, 738430, 3.9703983633493891424057806544631253775
Arizona, 6392017, 6832810, 6.8959922978928247531256565807005832431
Arkansas, 2915918, 2979732, 2.1884703204959810255295244928012378949
California, 37253956, 38904296, 4.4299724839960620557988526104449148971
Colorado, 5029196, 5454328, 8.4532796097030221132761578590295546246
```

Exemple d'utilisation d'AWS-CLI (Parquet)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}' --output-serialization
'{"CSV":{}}' changes.csv
```

Les premières lignes du fichier de sortie, changes.csv, ressemblent à ceci :

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

Opérations pour les téléchargements en plusieurs parties

Opérations pour les téléchargements en plusieurs parties

Cette section décrit comment StorageGRID prend en charge les opérations de téléchargement en plusieurs parties.

Les conditions et notes suivantes s'appliquent à toutes les opérations de téléchargement en plusieurs parties :

- Vous ne devez pas dépasser 1 000 téléchargements multipartites simultanés vers un seul bucket, car les résultats des requêtes ListMultipartUploads pour ce bucket peuvent renvoyer des résultats incomplets.
- StorageGRID applique les limites de taille AWS pour les parties en plusieurs parties. Les clients S3 doivent suivre ces directives :
 - Chaque partie d'un téléchargement en plusieurs parties doit être comprise entre 5 Mio (5 242 880 octets) et 5 Gio (5 368 709 120 octets).
 - La dernière partie peut être inférieure à 5 Mio (5 242 880 octets).
 - En général, les tailles des pièces doivent être aussi grandes que possible. Par exemple, utilisez des tailles de partie de 5 Gio pour un objet de 100 Gio. Étant donné que chaque partie est considérée comme un objet unique, l'utilisation de grandes tailles de partie réduit la surcharge des métadonnées StorageGRID .
 - Pour les objets inférieurs à 5 Gio, envisagez plutôt d'utiliser un téléchargement non multipartite.
- L'ILM est évalué pour chaque partie d'un objet multipartite au fur et à mesure de son ingestion et pour l'objet dans son ensemble lorsque le téléchargement multipartite est terminé, si la règle ILM utilise l'option Équilibré ou Strict ["option d'ingestion"](#) . Vous devez être conscient de la manière dont cela affecte le placement des objets et des pièces :
 - Si l'ILM change pendant qu'un téléchargement multipartite S3 est en cours, certaines parties de l'objet

peuvent ne pas répondre aux exigences ILM actuelles une fois le téléchargement multipartie terminé. Toute pièce qui n'est pas placée correctement est mise en file d'attente pour une réévaluation ILM et déplacée vers l'emplacement correct ultérieurement.

- Lors de l'évaluation de l'ILM pour une pièce, StorageGRID filtre sur la taille de la pièce, et non sur la taille de l'objet. Cela signifie que des parties d'un objet peuvent être stockées dans des emplacements qui ne répondent pas aux exigences ILM pour l'objet dans son ensemble. Par exemple, si une règle spécifie que tous les objets de 10 Go ou plus sont stockés sur DC1 tandis que tous les objets plus petits sont stockés sur DC2, chaque partie de 1 Go d'un téléchargement multipartie en 10 parties est stockée sur DC2 lors de l'ingestion. Cependant, lorsque l'ILM est évalué pour l'objet dans son ensemble, toutes les parties de l'objet sont déplacées vers DC1.
- Toutes les opérations de téléchargement en plusieurs parties prennent en charge StorageGRID ["valeurs de cohérence"](#) .
- Lorsqu'un objet est ingéré à l'aide d'un téléchargement en plusieurs parties, le ["seuil de segmentation des objets \(1 Gio\)"](#) n'est pas appliqué.
- Selon vos besoins, vous pouvez utiliser ["chiffrement côté serveur"](#) avec des téléchargements en plusieurs parties. Pour utiliser SSE (chiffrement côté serveur avec clés gérées par StorageGRID), vous incluez le `x-amz-server-side-encryption` en-tête de demande dans la demande CreateMultipartUpload uniquement. Pour utiliser SSE-C (chiffrement côté serveur avec clés fournies par le client), vous spécifiez les trois mêmes en-têtes de demande de clé de chiffrement dans la demande CreateMultipartUpload et dans chaque demande UploadPart ultérieure.

Opération	Mise en œuvre
Abandonner le téléchargement en plusieurs parties	Implémenté avec tous les comportements de l'API REST Amazon S3. Sous réserve de modifications sans préavis.
Téléchargement complet en plusieurs parties	Voir "Téléchargement complet en plusieurs parties"
Créer un téléchargement multi-parties (anciennement appelé Initiate Multipart Upload)	Voir "Créer un téléchargement multi-parties"
ListeMultipartUploads	Voir "ListeMultipartUploads"
Liste des pièces	Implémenté avec tous les comportements de l'API REST Amazon S3. Sous réserve de modifications sans préavis.
Télécharger une partie	Voir "Télécharger une partie"
TéléchargerPartCopy	Voir "TéléchargerPartCopy"

Téléchargement complet en plusieurs parties

L'opération CompleteMultipartUpload termine un téléchargement en plusieurs parties d'un objet en assemblant les parties précédemment téléchargées.



StorageGRID prend en charge les valeurs non consécutives dans l'ordre croissant pour le `partNumber` paramètre de demande avec `CompleteMultipartUpload`. Le paramètre peut commencer par n'importe quelle valeur.

Résoudre les conflits

Les demandes client conflictuelles, telles que deux clients écrivant sur la même clé, sont résolues sur la base des « derniers gagnants ». Le moment de l'évaluation des « dernières victoires » est basé sur le moment où le système StorageGRID termine une demande donnée, et non sur le moment où les clients S3 commencent une opération.

En-têtes de requête pris en charge

Les en-têtes de requête suivants sont pris en charge :

- `x-amz-checksum-sha256`
- `x-amz-storage-class`

Le `x-amz-storage-class` l'en-tête affecte le nombre de copies d'objets créées par StorageGRID si la règle ILM correspondante spécifie le ["Option de double validation ou d'ingestion équilibrée"](#) .

- STANDARD

(Par défaut) Spécifie une opération d'ingestion à double validation lorsque la règle ILM utilise l'option Double validation ou lorsque l'option Équilibré revient à la création de copies intermédiaires.

- REDUCED_REDUNDANCY

Spécifie une opération d'ingestion à validation unique lorsque la règle ILM utilise l'option de validation double ou lorsque l'option Équilibré revient à la création de copies intermédiaires.



Si vous ingérez un objet dans un bucket avec le verrouillage d'objet S3 activé, le REDUCED_REDUNDANCY l'option est ignorée. Si vous ingérez un objet dans un bucket conforme hérité, le REDUCED_REDUNDANCY l'option renvoie une erreur. StorageGRID effectuera toujours une ingestion à double validation pour garantir que les exigences de conformité sont satisfaites.



Si un téléchargement en plusieurs parties n'est pas terminé dans les 15 jours, l'opération est marquée comme inactive et toutes les données associées sont supprimées du système.



Le ETag la valeur renvoyée n'est pas une somme MD5 des données, mais suit l'implémentation de l'API Amazon S3 de la ETag valeur pour les objets en plusieurs parties.

En-têtes de requête non pris en charge

Les en-têtes de requête suivants ne sont pas pris en charge :

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Gestion des versions

Cette opération termine un téléchargement en plusieurs parties. Si le contrôle de version est activé pour un bucket, la version de l'objet est créée une fois le téléchargement en plusieurs parties terminé.

Si le contrôle de version est activé pour un bucket, un `versionId` est généré automatiquement pour la version de l'objet stocké. Ce `versionId` est également renvoyé dans la réponse en utilisant le `x-amz-version-id` en-tête de réponse.

Si le contrôle de version est suspendu, la version de l'objet est stockée avec une valeur nulle `versionId` et si une version nulle existe déjà, elle sera écrasée.



Lorsque le contrôle de version est activé pour un bucket, l'exécution d'un téléchargement en plusieurs parties crée toujours une nouvelle version, même s'il existe des téléchargements en plusieurs parties simultanés effectués sur la même clé d'objet. Lorsque le contrôle de version n'est pas activé pour un bucket, il est possible de lancer un téléchargement en plusieurs parties, puis de lancer et de terminer un autre téléchargement en plusieurs parties sur la même clé d'objet. Sur les buckets non versionnés, le téléchargement en plusieurs parties qui se termine en dernier est prioritaire.

Échec de la réplication, de la notification ou de la notification des métadonnées

Si le bucket dans lequel le téléchargement en plusieurs parties se produit est configuré pour un service de plateforme, le téléchargement en plusieurs parties réussit même si l'action de réplication ou de notification associée échoue.

Un locataire peut déclencher la réplication ou la notification ayant échoué en mettant à jour les métadonnées ou les balises de l'objet. Un locataire peut soumettre à nouveau les valeurs existantes pour éviter d'apporter des modifications indésirables.

["Dépanner les services de la plateforme"](#) .

Créer un téléchargement multi-parties

L'opération `CreateMultipartUpload` (précédemment nommée `Initiate Multipart Upload`) lance un téléchargement en plusieurs parties pour un objet et renvoie un ID de téléchargement.

Le `x-amz-storage-class` l'en-tête de requête est pris en charge. La valeur soumise pour `x-amz-storage-class` affecte la manière dont `StorageGRID` protège les données de l'objet pendant l'ingestion et non le nombre de copies persistantes de l'objet stockées dans le système `StorageGRID` (qui est déterminé par ILM).

Si la règle ILM correspondant à un objet ingéré utilise le Strict "[option d'ingestion](#)", le `x-amz-storage-class` l'en-tête n'a aucun effet.

Les valeurs suivantes peuvent être utilisées pour `x-amz-storage-class` :

- **STANDARD**(Défaut)
 - **Double validation** : si la règle ILM spécifie l'option d'ingestion `Double validation`, dès qu'un objet est ingéré, une deuxième copie de cet objet est créée et distribuée à un autre nœud de stockage (double validation). Lorsque l'ILM est évalué, `StorageGRID` détermine si ces copies intermédiaires initiales satisfont aux instructions de placement de la règle. Si ce n'est pas le cas, de nouvelles copies d'objets

devront peut-être être réalisées à des emplacements différents et les copies intermédiaires initiales devront peut-être être supprimées.

- **Équilibré** : si la règle ILM spécifie l'option Équilibré et que StorageGRID ne peut pas effectuer immédiatement toutes les copies spécifiées dans la règle, StorageGRID effectue deux copies intermédiaires sur différents nœuds de stockage.

Si StorageGRID peut créer immédiatement toutes les copies d'objets spécifiées dans la règle ILM (placement synchrone), le `x-amz-storage-class` l'en-tête n'a aucun effet.

- **REDUCED_REDUNDANCY**

- **Double validation** : si la règle ILM spécifie l'option Double validation, StorageGRID crée une seule copie intermédiaire lorsque l'objet est ingéré (validation unique).
- **Équilibré** : si la règle ILM spécifie l'option Équilibré, StorageGRID effectue une seule copie intermédiaire uniquement si le système ne peut pas effectuer immédiatement toutes les copies spécifiées dans la règle. Si StorageGRID peut effectuer un placement synchrone, cet en-tête n'a aucun effet. Le **REDUCED_REDUNDANCY** L'option est mieux utilisée lorsque la règle ILM qui correspond à l'objet crée une seule copie répliquée. Dans ce cas, en utilisant **REDUCED_REDUNDANCY** élimine la création et la suppression inutiles d'une copie d'objet supplémentaire pour chaque opération d'ingestion.

En utilisant le **REDUCED_REDUNDANCY** Cette option n'est pas recommandée dans d'autres circonstances. **REDUCED_REDUNDANCY** augmente le risque de perte de données d'objet lors de l'ingestion. Par exemple, vous risquez de perdre des données si la copie unique est initialement stockée sur un nœud de stockage qui échoue avant que l'évaluation ILM puisse avoir lieu.



Le fait de n'avoir qu'une seule copie répliquée pendant une période donnée expose les données à un risque de perte permanente. Si une seule copie répliquée d'un objet existe, cet objet est perdu si un nœud de stockage échoue ou présente une erreur importante. Vous perdez également temporairement l'accès à l'objet pendant les procédures de maintenance telles que les mises à niveau.

Spécification **REDUCED_REDUNDANCY** affecte uniquement le nombre de copies créées lorsqu'un objet est ingéré pour la première fois. Cela n'affecte pas le nombre de copies de l'objet effectuées lorsque l'objet est évalué par les stratégies ILM actives et n'entraîne pas le stockage des données à des niveaux de redondance inférieurs dans le système StorageGRID .



Si vous ingérez un objet dans un bucket avec le verrouillage d'objet S3 activé, le **REDUCED_REDUNDANCY** l'option est ignorée. Si vous ingérez un objet dans un bucket conforme hérité, le **REDUCED_REDUNDANCY** l'option renvoie une erreur. StorageGRID effectuera toujours une ingestion à double validation pour garantir que les exigences de conformité sont satisfaites.

En-têtes de requête pris en charge

Les en-têtes de requête suivants sont pris en charge :

- Content-Type
- x-amz-checksum-algorithm

Actuellement, seule la valeur SHA256 pour `x-amz-checksum-algorithm` est pris en charge.

- `x-amz-meta-`, suivi d'une paire nom-valeur contenant des métadonnées définies par l'utilisateur

Lors de la spécification de la paire nom-valeur pour les métadonnées définies par l'utilisateur, utilisez ce format général :

```
x-amz-meta-_name_: `value`
```

Si vous souhaitez utiliser l'option **Heure de création définie par l'utilisateur** comme heure de référence pour une règle ILM, vous devez utiliser `creation-time` comme le nom des métadonnées qui enregistrent quand l'objet a été créé. Par exemple:

```
x-amz-meta-creation-time: 1443399726
```

La valeur pour `creation-time` est évalué en secondes depuis le 1er janvier 1970.



Ajout `creation-time` car les métadonnées définies par l'utilisateur ne sont pas autorisées si vous ajoutez un objet à un bucket pour lequel la conformité héritée est activée. Une erreur sera renvoyée.

- En-têtes de demande de verrouillage d'objet S3 :

- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`

Si une demande est effectuée sans ces en-têtes, les paramètres de conservation par défaut du bucket sont utilisés pour calculer la date de conservation de la version de l'objet.

["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#)

- En-têtes de requête SSE :

- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-algorithm`

[En-têtes de requête pour le chiffrement côté serveur](#)



Pour plus d'informations sur la façon dont StorageGRID gère les caractères UTF-8, consultez ["Mettre l'objet"](#) .

En-têtes de requête pour le chiffrement côté serveur

Vous pouvez utiliser les en-têtes de requête suivants pour chiffrer un objet en plusieurs parties avec un chiffrement côté serveur. Les options SSE et SSE-C s'excluent mutuellement.

- **SSE** : utilisez l'en-tête suivant dans la demande `CreateMultipartUpload` si vous souhaitez chiffrer l'objet avec une clé unique gérée par `StorageGRID`. Ne spécifiez pas cet en-tête dans aucune des requêtes `UploadPart`.
 - `x-amz-server-side-encryption`
- **SSE-C** : utilisez ces trois en-têtes dans la demande `CreateMultipartUpload` (et dans chaque demande `UploadPart` ultérieure) si vous souhaitez crypter l'objet avec une clé unique que vous fournissez et gérez.
 - `x-amz-server-side-encryption-customer-algorithm`: Préciser `AES256` .
 - `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de chiffrement pour le nouvel objet.
 - `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le condensé MD5 de la clé de chiffrement du nouvel objet.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser les clés fournies par le client pour sécuriser les données d'objet, examinez les considérations relatives ["en utilisant le cryptage côté serveur"](#) .

En-têtes de requête non pris en charge

L'en-tête de requête suivant n'est pas pris en charge :

- `x-amz-website-redirect-location`

Le `x-amz-website-redirect-location` retourne d'en-tête `XNotImplemented` .

Gestion des versions

Le téléchargement en plusieurs parties consiste en des opérations distinctes pour lancer le téléchargement, répertorier les téléchargements, télécharger des parties, assembler les parties téléchargées et terminer le téléchargement. Les objets sont créés (et versionnés si applicable) lorsque l'opération `CompleteMultipartUpload` est effectuée.

ListeMultipartUploads

L'opération `ListMultipartUploads` répertorie les téléchargements multipartites en cours pour un bucket.

Les paramètres de requête suivants sont pris en charge :

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`
- `Host`
- `Date`

- Authorization

Gestion des versions

Le téléchargement en plusieurs parties consiste en des opérations distinctes pour lancer le téléchargement, répertorier les téléchargements, télécharger des parties, assembler les parties téléchargées et terminer le téléchargement. Les objets sont créés (et versionnés si applicable) lorsque l'opération CompleteMultipartUpload est effectuée.

Télécharger une partie

L'opération UploadPart télécharge une partie dans un téléchargement en plusieurs parties pour un objet.

En-têtes de requête pris en charge

Les en-têtes de requête suivants sont pris en charge :

- x-amz-checksum-sha256
- Content-Length
- Content-MD5

En-têtes de requête pour le chiffrement côté serveur

Si vous avez spécifié le chiffrement SSE-C pour la demande CreateMultipartUpload, vous devez également inclure les en-têtes de demande suivants dans chaque demande UploadPart :

- x-amz-server-side-encryption-customer-algorithm: Préciser AES256 .
- x-amz-server-side-encryption-customer-key: Spécifiez la même clé de chiffrement que celle que vous avez fournie dans la demande CreateMultipartUpload.
- x-amz-server-side-encryption-customer-key-MD5: Spécifiez le même condensé MD5 que celui que vous avez fourni dans la demande CreateMultipartUpload.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser les clés fournies par le client pour sécuriser les données d'objet, examinez les considérations dans ["Utiliser le cryptage côté serveur"](#) .

Si vous avez spécifié une somme de contrôle SHA-256 lors de la demande CreateMultipartUpload, vous devez également inclure l'en-tête de demande suivant dans chaque demande UploadPart :

- x-amz-checksum-sha256: Spécifiez la somme de contrôle SHA-256 pour cette partie.

En-têtes de requête non pris en charge

Les en-têtes de requête suivants ne sont pas pris en charge :

- x-amz-sdk-checksum-algorithm
- x-amz-trailer

Gestion des versions

Le téléchargement en plusieurs parties consiste en des opérations distinctes pour lancer le téléchargement, répertorier les téléchargements, télécharger des parties, assembler les parties téléchargées et terminer le téléchargement. Les objets sont créés (et versionnés si applicable) lorsque l'opération `CompleteMultipartUpload` est effectuée.

TéléchargerPartCopy

L'opération `UploadPartCopy` télécharge une partie d'un objet en copiant les données d'un objet existant comme source de données.

L'opération `UploadPartCopy` est implémentée avec tout le comportement de l'API REST Amazon S3. Sous réserve de modifications sans préavis.

Cette requête lit et écrit les données d'objet spécifiées dans `x-amz-copy-source-range` au sein du système `StorageGRID`.

Les en-têtes de requête suivants sont pris en charge :

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

En-têtes de requête pour le chiffrement côté serveur

Si vous avez spécifié le chiffrement SSE-C pour la demande `CreateMultipartUpload`, vous devez également inclure les en-têtes de demande suivants dans chaque demande `UploadPartCopy` :

- `x-amz-server-side-encryption-customer-algorithm`: Préciser AES256.
- `x-amz-server-side-encryption-customer-key`: Spécifiez la même clé de chiffrement que celle que vous avez fournie dans la demande `CreateMultipartUpload`.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le même condensé MD5 que celui que vous avez fourni dans la demande `CreateMultipartUpload`.

Si l'objet source est chiffré à l'aide d'une clé fournie par le client (SSE-C), vous devez inclure les trois en-têtes suivants dans la demande `UploadPartCopy`, afin que l'objet puisse être déchiffré puis copié :

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Préciser AES256.
- `x-amz-copy-source-server-side-encryption-customer-key`: Spécifiez la clé de chiffrement que vous avez fournie lors de la création de l'objet source.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Spécifiez le condensé MD5 que vous avez fourni lors de la création de l'objet source.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser les clés fournies par le client pour sécuriser les données d'objet, examinez les considérations dans ["Utiliser le cryptage côté serveur"](#).

Gestion des versions

Le téléchargement en plusieurs parties consiste en des opérations distinctes pour lancer le téléchargement, répertorier les téléchargements, télécharger des parties, assembler les parties téléchargées et terminer le téléchargement. Les objets sont créés (et versionnés si applicable) lorsque l'opération CompleteMultipartUpload est effectuée.

Réponses d'erreur

Le système StorageGRID prend en charge toutes les réponses d'erreur standard de l'API REST S3 qui s'appliquent. De plus, l'implémentation StorageGRID ajoute plusieurs réponses personnalisées.

Codes d'erreur de l'API S3 pris en charge

Nom	Statut HTTP
Accès refusé	403 Interdit
BadDigest	400 Mauvaise requête
BucketExisteDéjà	409 Conflit
Seau non vide	409 Conflit
Corps incomplet	400 Mauvaise requête
Erreur interne	Erreur interne du serveur 500
ID de clé d'accès non valide	403 Interdit
Argument invalide	400 Mauvaise requête
Nom de bucket invalide	400 Mauvaise requête
État du bucket invalide	409 Conflit
InvalidDigest	400 Mauvaise requête
Erreur d'algorithme de chiffrement invalide	400 Mauvaise requête
Partie invalide	400 Mauvaise requête
Commande de pièces invalide	400 Mauvaise requête
Plage invalide	416 Plage demandée non satisfaisante

Nom	Statut HTTP
Demande invalide	400 Mauvaise requête
Classe de stockage invalide	400 Mauvaise requête
Balise invalide	400 Mauvaise requête
URI invalide	400 Mauvaise requête
Clé trop longue	400 Mauvaise requête
XML malformé	400 Mauvaise requête
Métadonnées trop volumineuses	400 Mauvaise requête
Méthode non autorisée	Méthode 405 non autorisée
Longueur du contenu manquant	411 Longueur requise
Erreur de corps de demande manquante	400 Mauvaise requête
En-tête de sécurité manquant	400 Mauvaise requête
Aucun seau de ce type	404 non trouvé
Aucune clé de ce type	404 non trouvé
Aucun téléchargement de ce type	404 non trouvé
Non implémenté	501 non implémenté
Politique NoSuchBucket	404 non trouvé
Erreur de configuration de verrouillage d'objet non trouvée	404 non trouvé
Précondition échouée	412 Échec de la condition préalable
RequestTimeTooSkewed	403 Interdit
Service non disponible	Service 503 indisponible
La signature ne correspond pas	403 Interdit

Nom	Statut HTTP
Trop de seaux	400 Mauvaise requête
La clé utilisateur doit être spécifiée	400 Mauvaise requête

Codes d'erreur personnalisés StorageGRID

Nom	Description	Statut HTTP
XBucketLifecycleNon autorisé	La configuration du cycle de vie du bucket n'est pas autorisée dans un bucket conforme hérité	400 Mauvaise requête
Exception d'analyse de politique XBucket	Échec de l'analyse de la politique de bucket JSON reçue.	400 Mauvaise requête
Conflit de conformité X	Opération refusée en raison de paramètres de conformité hérités.	403 Interdit
XComplianceRéduitRedondanceInterdit	La redondance réduite n'est pas autorisée dans le bucket conforme hérité	400 Mauvaise requête
XMaxBucketPolicyLengthDépassé	Votre politique dépasse la durée maximale autorisée pour la politique de compartiment.	400 Mauvaise requête
En-tête de demande interne XMissing	Il manque un en-tête d'une requête interne.	400 Mauvaise requête
XNoSuchBucketCompliance	La conformité héritée n'est pas activée pour le bucket spécifié.	404 non trouvé
XNonAcceptable	La demande contient un ou plusieurs en-têtes d'acceptation qui n'ont pas pu être satisfaits.	406 Non acceptable
XNonImplémenté	La demande que vous avez fournie implique une fonctionnalité qui n'est pas implémentée.	501 non implémenté

Opérations personnalisées StorageGRID

Opérations personnalisées StorageGRID

Le système StorageGRID prend en charge les opérations personnalisées qui sont ajoutées à l'API REST S3.

Le tableau suivant répertorie les opérations personnalisées prises en charge par StorageGRID.

Opération	Description
"Cohérence du bucket GET"	Renvoie la cohérence appliquée à un bucket particulier.
"Cohérence du seau PUT"	Définit la cohérence appliquée à un bucket particulier.
"Heure du dernier accès au bucket GET"	Renvoie si les dernières mises à jour de l'heure d'accès sont activées ou désactivées pour un bucket particulier.
"Heure du dernier accès au bucket PUT"	Vous permet d'activer ou de désactiver les mises à jour de l'heure du dernier accès pour un bucket particulier.
"SUPPRIMER la configuration de notification des métadonnées du bucket"	Supprime la configuration XML de notification de métadonnées associée à un bucket particulier.
"Configuration de la notification des métadonnées du bucket GET"	Renvoie la configuration XML de notification de métadonnées associée à un bucket particulier.
"Configuration des notifications de métadonnées du compartiment PUT"	Configure le service de notification de métadonnées pour un bucket.
"Utilisation du stockage GET"	Vous indique la quantité totale de stockage utilisée par un compte et pour chaque bucket associé au compte.
"Obsolète : CreateBucket avec paramètres de conformité"	Obsolète et non pris en charge : vous ne pouvez plus créer de nouveaux buckets avec la conformité activée.
"Obsolète : conformité du bucket GET"	Obsolète mais pris en charge : renvoie les paramètres de conformité actuellement en vigueur pour un bucket conforme hérité existant.
"Obsolète : conformité du compartiment PUT"	Obsolète mais pris en charge : vous permet de modifier les paramètres de conformité d'un bucket conforme hérité existant.

Cohérence du bucket GET

La demande de cohérence GET Bucket vous permet de déterminer la cohérence appliquée à un bucket particulier.

La cohérence par défaut est définie pour garantir la lecture après écriture des objets nouvellement créés.

Vous devez disposer de l'autorisation `s3:GetBucketConsistency` ou être root du compte pour terminer cette opération.

Exemple de demande

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Réponse

Dans la réponse XML, <Consistency> renverra l'une des valeurs suivantes :

Cohérence	Description
tous	Tous les nœuds reçoivent les données immédiatement, sinon la demande échouera.
fort-mondial	Garantit la cohérence de lecture après écriture pour toutes les demandes client sur tous les sites.
site fort	Garantit la cohérence de lecture après écriture pour toutes les demandes client au sein d'un site.
lecture après nouvelle écriture	(Par défaut) Fournit une cohérence de lecture après écriture pour les nouveaux objets et une cohérence éventuelle pour les mises à jour d'objets. Offre des garanties de haute disponibilité et de protection des données. Recommandé dans la plupart des cas.
disponible	Assure une cohérence éventuelle pour les nouveaux objets et les mises à jour d'objets. Pour les buckets S3, utilisez-les uniquement si nécessaire (par exemple, pour un bucket contenant des valeurs de journal rarement lues ou pour des opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les buckets S3 FabricPool .

Exemple de réponse

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

Informations connexes

["Valeurs de cohérence"](#)

Cohérence du seau PUT

La demande de cohérence PUT Bucket vous permet de spécifier la cohérence à appliquer aux opérations effectuées sur un bucket.

La cohérence par défaut est définie pour garantir la lecture après écriture des objets nouvellement créés.

Avant de commencer

Vous devez disposer de l'autorisation `s3:PutBucketConsistency` ou être root du compte pour terminer cette opération.

Demande

Le `x-ntap-sg-consistency` le paramètre doit contenir l'une des valeurs suivantes :

Cohérence	Description
tous	Tous les nœuds reçoivent les données immédiatement, sinon la demande échouera.
fort-mondial	Garantit la cohérence de lecture après écriture pour toutes les demandes client sur tous les sites.
site fort	Garantit la cohérence de lecture après écriture pour toutes les demandes client au sein d'un site.
lecture après nouvelle écriture	(Par défaut) Fournit une cohérence de lecture après écriture pour les nouveaux objets et une cohérence éventuelle pour les mises à jour d'objets. Offre des garanties de haute disponibilité et de protection des données. Recommandé dans la plupart des cas.

Cohérence	Description
disponible	Assure une cohérence éventuelle pour les nouveaux objets et les mises à jour d'objets. Pour les buckets S3, utilisez-les uniquement si nécessaire (par exemple, pour un bucket contenant des valeurs de journal rarement lues ou pour des opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les buckets S3 FabricPool .

Remarque : En général, vous devez utiliser la cohérence « Lecture après nouvelle écriture ». Si les requêtes ne fonctionnent pas correctement, modifiez le comportement du client de l'application si possible. Ou configurez le client pour spécifier la cohérence de chaque demande d'API. Définissez la consistance au niveau du seau uniquement en dernier recours.

Exemple de demande

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Informations connexes

["Valeurs de cohérence"](#)

Heure du dernier accès au bucket GET

La demande d'heure du dernier accès au bucket GET vous permet de déterminer si les mises à jour de l'heure du dernier accès sont activées ou désactivées pour les buckets individuels.

Vous devez disposer de l'autorisation `s3:GetBucketLastAccessTime` ou être root du compte pour terminer cette opération.

Exemple de demande

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemple de réponse

Cet exemple montre que les mises à jour de l'heure du dernier accès sont activées pour le bucket.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

Heure du dernier accès au bucket PUT

La demande d'heure du dernier accès au bucket PUT vous permet d'activer ou de désactiver les mises à jour de l'heure du dernier accès pour des buckets individuels. La désactivation des mises à jour de l'heure du dernier accès améliore les performances et constitue le paramètre par défaut pour tous les buckets créés avec la version 10.3.0 ou ultérieure.

Vous devez disposer de l'autorisation `s3:PutBucketLastAccessTime` pour un bucket ou être root du compte pour terminer cette opération.



À partir de la version 10.3 de StorageGRID, les mises à jour de l'heure du dernier accès sont désactivées par défaut pour tous les nouveaux buckets. Si vous disposez de buckets créés à l'aide d'une version antérieure de StorageGRID et que vous souhaitez appliquer le nouveau comportement par défaut, vous devez désactiver explicitement les mises à jour de l'heure du dernier accès pour chacun de ces buckets antérieurs. Vous pouvez activer ou désactiver les mises à jour de l'heure du dernier accès à l'aide de la demande d'heure du dernier accès au bucket PUT ou à partir de la page de détails d'un bucket dans le gestionnaire de locataires. Voir ["Activer ou désactiver les mises à jour de l'heure du dernier accès"](#).

Si les mises à jour de l'heure du dernier accès sont désactivées pour un bucket, le comportement suivant est appliqué aux opérations sur le bucket :

- Les requêtes `GetObject`, `GetObjectAcl`, `GetObjectTagging` et `HeadObject` ne mettent pas à jour l'heure du dernier accès. L'objet n'est pas ajouté aux files d'attente pour l'évaluation de la gestion du cycle de vie des informations (ILM).
- Les requêtes `CopyObject` et `PutObjectTagging` qui mettent à jour uniquement les métadonnées mettent également à jour l'heure du dernier accès. L'objet est ajouté aux files d'attente pour l'évaluation ILM.
- Si les mises à jour de l'heure du dernier accès sont désactivées pour le bucket source, les demandes `CopyObject` ne mettent pas à jour l'heure du dernier accès pour le bucket source. L'objet qui a été copié n'est pas ajouté aux files d'attente pour l'évaluation ILM pour le bucket source. Cependant, pour la destination, les demandes `CopyObject` mettent toujours à jour l'heure du dernier accès. La copie de l'objet est ajoutée aux files d'attente pour l'évaluation ILM.
- Les demandes `CompleteMultipartUpload` mettent à jour l'heure du dernier accès. L'objet terminé est ajouté aux files d'attente pour l'évaluation ILM.

Exemples de demandes

Cet exemple active l'heure du dernier accès à un bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Cet exemple désactive l'heure du dernier accès à un bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

SUPPRIMER la configuration de notification des métadonnées du bucket

La demande de configuration de notification des métadonnées DELETE Bucket vous permet de désactiver le service d'intégration de recherche pour des buckets individuels en supprimant le XML de configuration.

Vous devez disposer de l'autorisation `s3:DeleteBucketMetadataNotification` pour un bucket ou être root du compte pour terminer cette opération.

Exemple de demande

Cet exemple montre la désactivation du service d'intégration de recherche pour un bucket.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Configuration de la notification des métadonnées du bucket GET

La demande de configuration de notification de métadonnées GET Bucket vous permet de récupérer le XML de configuration utilisé pour configurer l'intégration de la recherche pour des buckets individuels.

Vous devez disposer de l'autorisation `s3:GetBucketMetadataNotification` ou être root du compte pour terminer cette opération.

Exemple de demande

Cette requête récupère la configuration de notification des métadonnées pour le bucket nommé `bucket`.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Réponse

Le corps de la réponse inclut la configuration de notification de métadonnées pour le bucket. La configuration de notification des métadonnées vous permet de déterminer comment le bucket est configuré pour l'intégration de la recherche. Autrement dit, il vous permet de déterminer quels objets sont indexés et à quels points de terminaison leurs métadonnées d'objet sont envoyées.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>
```

Chaque configuration de notification de métadonnées comprend une ou plusieurs règles. Chaque règle spécifie les objets auxquels elle s'applique et la destination vers laquelle StorageGRID doit envoyer les métadonnées de l'objet. Les destinations doivent être spécifiées à l'aide de l'URN d'un point de terminaison StorageGRID .

Nom	Description	Obligatoire
Configuration des notifications de métadonnées	Balise de conteneur pour les règles utilisées pour spécifier les objets et la destination des notifications de métadonnées. Contient un ou plusieurs éléments de règle.	Oui

Nom	Description	Obligatoire
Règle	<p>Balise de conteneur pour une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié.</p> <p>Les règles avec des préfixes qui se chevauchent sont rejetées.</p> <p>Inclus dans l'élément <code>MetadataNotificationConfiguration</code>.</p>	Oui
ID	<p>Identifiant unique de la règle.</p> <p>Inclus dans l'élément Règle.</p>	Non
Statut	<p>Le statut peut être « Activé » ou « Désactivé ».</p> <p>Aucune action n'est entreprise pour les règles désactivées.</p> <p>Inclus dans l'élément Règle.</p>	Oui
Préfixe	<p>Les objets qui correspondent au préfixe sont affectés par la règle et leurs métadonnées sont envoyées à la destination spécifiée.</p> <p>Pour faire correspondre tous les objets, spécifiez un préfixe vide.</p> <p>Inclus dans l'élément Règle.</p>	Oui
Destination	<p>Balise de conteneur pour la destination d'une règle.</p> <p>Inclus dans l'élément Règle.</p>	Oui

Nom	Description	Obligatoire
Urne	<p>URN de la destination où les métadonnées de l'objet sont envoyées. Doit être l'URN d'un point de terminaison StorageGRID avec les propriétés suivantes :</p> <ul style="list-style-type: none"> • `es` doit être le troisième élément. • L'URN doit se terminer par l'index et le type où les métadonnées sont stockées, sous la forme <code>domain-name/myindex/mytype</code> . <p>Les points de terminaison sont configurés à l'aide de l'API Tenant Manager ou Tenant Management. Ils prennent la forme suivante :</p> <ul style="list-style-type: none"> • <code>arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> <p>Le point de terminaison doit être configuré avant que le XML de configuration ne soit soumis, sinon la configuration échouera avec une erreur 404.</p> <p>L'urne est incluse dans l'élément Destination.</p>	Oui

Exemple de réponse

Le XML inclus entre le

`<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` Les balises montrent comment l'intégration avec un point de terminaison d'intégration de recherche est configurée pour le bucket. Dans cet exemple, les métadonnées de l'objet sont envoyées à un index Elasticsearch nommé `current` et le type nommé `2017` qui est hébergé dans un domaine AWS nommé `records` .

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix>2017</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:33333333:domain/records/current/2017</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Informations connexes

["Utiliser un compte locataire"](#)

Configuration des notifications de métadonnées du compartiment PUT

La demande de configuration de notification des métadonnées PUT Bucket vous permet d'activer le service d'intégration de recherche pour des buckets individuels. La configuration XML de notification de métadonnées que vous fournissez dans le corps de la demande spécifie les objets dont les métadonnées sont envoyées à l'index de recherche de destination.

Vous devez disposer de l'autorisation `s3:PutBucketMetadataNotification` pour un bucket ou être root du compte pour terminer cette opération.

Demande

La demande doit inclure la configuration de notification des métadonnées dans le corps de la demande. Chaque configuration de notification de métadonnées comprend une ou plusieurs règles. Chaque règle spécifie les objets auxquels elle s'applique et la destination vers laquelle StorageGRID doit envoyer les métadonnées de l'objet.

Les objets peuvent être filtrés sur le préfixe du nom de l'objet. Par exemple, vous pouvez envoyer des métadonnées pour des objets avec le préfixe `/images` vers une destination et les objets avec le préfixe `/videos` à un autre.

Les configurations dont les préfixes se chevauchent ne sont pas valides et sont rejetées lorsqu'elles sont soumises. Par exemple, une configuration qui incluait une règle pour les objets avec le préfixe `test` et une deuxième règle pour les objets avec le préfixe `test2` ne serait pas autorisé.

Les destinations doivent être spécifiées à l'aide de l'URN d'un point de terminaison StorageGRID . Le point de terminaison doit exister lorsque la configuration de notification des métadonnées est soumise, sinon la demande échoue en tant que 400 Bad Request . Le message d'erreur indique : Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: *URN*.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>
```

Le tableau décrit les éléments du XML de configuration de notification de métadonnées.

Nom	Description	Obligatoire
Configuration des notifications de métadonnées	Balise de conteneur pour les règles utilisées pour spécifier les objets et la destination des notifications de métadonnées. Contient un ou plusieurs éléments de règle.	Oui
Règle	Balise de conteneur pour une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié. Les règles avec des préfixes qui se chevauchent sont rejetées. Inclus dans l'élément MetadataNotificationConfiguration.	Oui
ID	Identifiant unique de la règle. Inclus dans l'élément Règle.	Non

Nom	Description	Obligatoire
Statut	<p>Le statut peut être « Activé » ou « Désactivé ». Aucune action n'est entreprise pour les règles désactivées.</p> <p>Inclus dans l'élément Règle.</p>	Oui
Préfixe	<p>Les objets qui correspondent au préfixe sont affectés par la règle et leurs métadonnées sont envoyées à la destination spécifiée.</p> <p>Pour faire correspondre tous les objets, spécifiez un préfixe vide.</p> <p>Inclus dans l'élément Règle.</p>	Oui
Destination	<p>Balise de conteneur pour la destination d'une règle.</p> <p>Inclus dans l'élément Règle.</p>	Oui
Urne	<p>URN de la destination où les métadonnées de l'objet sont envoyées. Doit être l'URN d'un point de terminaison StorageGRID avec les propriétés suivantes :</p> <ul style="list-style-type: none"> • `es` doit être le troisième élément. • L'URN doit se terminer par l'index et le type où les métadonnées sont stockées, sous la forme <code>domain-name/myindex/mytype</code>. <p>Les points de terminaison sont configurés à l'aide de l'API Tenant Manager ou Tenant Management. Ils prennent la forme suivante :</p> <ul style="list-style-type: none"> • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> <p>Le point de terminaison doit être configuré avant que le XML de configuration ne soit soumis, sinon la configuration échouera avec une erreur 404.</p> <p>L'urne est incluse dans l'élément Destination.</p>	Oui

Exemples de demandes

Cet exemple montre l'activation de l'intégration de la recherche pour un bucket. Dans cet exemple, les métadonnées d'objet pour tous les objets sont envoyées vers la même destination.

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Dans cet exemple, les métadonnées d'objet pour les objets qui correspondent au préfixe `/images` est envoyé à une destination, tandis que les métadonnées d'objet pour les objets qui correspondent au préfixe `/videos` est envoyé vers une deuxième destination.

```

PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:33333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

JSON généré par le service d'intégration de recherche

Lorsque vous activez le service d'intégration de recherche pour un bucket, un document JSON est généré et envoyé au point de terminaison de destination chaque fois que des métadonnées ou des balises d'objet sont ajoutées, mises à jour ou supprimées.

Cet exemple montre un exemple de JSON qui pourrait être généré lorsqu'un objet avec la clé `SGWS/Tagging.txt` est créé dans un bucket nommé `test`. Le `test` le bucket n'est pas versionné, donc le `versionId` la balise est vide.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region": "us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Métadonnées d'objet incluses dans les notifications de métadonnées

Le tableau répertorie tous les champs inclus dans le document JSON envoyé au point de terminaison de destination lorsque l'intégration de la recherche est activée.

Le nom du document inclut le nom du bucket, le nom de l'objet et l'ID de version s'il est présent.

Type	Nom de l'article	Description
Informations sur le bucket et l'objet	seau	Nom du seau
Informations sur le bucket et l'objet	clé	Nom de la clé de l'objet
Informations sur le bucket et l'objet	ID de version	Version de l'objet, pour les objets dans les buckets versionnés
Informations sur le bucket et l'objet	région	Région de bucket, par exemple us-east-1
Métadonnées du système	taille	Taille de l'objet (en octets) telle que visible par un client HTTP
Métadonnées du système	md5	Hachage d'objet
Métadonnées de l'utilisateur	métadonnées <i>key:value</i>	Toutes les métadonnées utilisateur pour l'objet, sous forme de paires clé-valeur

Type	Nom de l'article	Description
Mots-clés	balises <i>key:value</i>	Toutes les balises d'objet définies pour l'objet, sous forme de paires clé-valeur



Pour les balises et les métadonnées utilisateur, StorageGRID transmet des dates et des nombres à Elasticsearch sous forme de chaînes ou de notifications d'événements S3. Pour configurer Elasticsearch afin d'interpréter ces chaînes comme des dates ou des nombres, suivez les instructions Elasticsearch pour le mappage de champs dynamiques et pour le mappage des formats de date. Vous devez activer les mappages de champs dynamiques sur l'index avant de configurer le service d'intégration de recherche. Une fois qu'un document est indexé, vous ne pouvez pas modifier les types de champs du document dans l'index.

Informations connexes

["Utiliser un compte locataire"](#)

Demande d'utilisation du stockage GET

La demande GET Storage Usage vous indique la quantité totale de stockage utilisée par un compte et pour chaque bucket associé au compte.

La quantité de stockage utilisée par un compte et ses buckets peut être obtenue par une requête ListBuckets modifiée avec le `x-ntap-sg-usage` paramètre de requête. L'utilisation du stockage du bucket est suivie séparément des requêtes PUT et DELETE traitées par le système. Il peut y avoir un certain délai avant que les valeurs d'utilisation correspondent aux valeurs attendues en fonction du traitement des demandes, en particulier si le système est soumis à une charge importante.

Par défaut, StorageGRID tente de récupérer les informations d'utilisation à l'aide d'une cohérence globale forte. Si une cohérence globale forte ne peut pas être obtenue, StorageGRID tente de récupérer les informations d'utilisation avec une cohérence de site forte.

Vous devez disposer de l'autorisation `s3:ListAllMyBuckets` ou être root du compte pour terminer cette opération.

Exemple de demande

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemple de réponse

Cet exemple montre un compte qui comporte quatre objets et 12 octets de données dans deux compartiments. Chaque compartiment contient deux objets et six octets de données.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

Gestion des versions

Chaque version d'objet stockée contribuera à la `ObjectCount` et `DataBytes` valeurs dans la réponse. Les marqueurs de suppression ne sont pas ajoutés au `ObjectCount` total.

Informations connexes

["Valeurs de cohérence"](#)

Demandes de bucket obsolètes pour la conformité héritée

Demandes de bucket obsolètes pour la conformité héritée

Vous devrez peut-être utiliser l'API REST StorageGRID S3 pour gérer les buckets créés à l'aide de la fonctionnalité de conformité héritée.

Fonctionnalité de conformité obsolète

La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes de StorageGRID est obsolète et a été remplacée par S3 Object Lock.

Si vous avez précédemment activé le paramètre de conformité global, le paramètre de verrouillage d'objet S3 global est activé dans StorageGRID 11.6. Vous ne pouvez plus créer de nouveaux buckets avec la conformité activée ; toutefois, si nécessaire, vous pouvez utiliser l'API REST StorageGRID S3 pour gérer tous les buckets conformes existants.

- ["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#)
- ["Gérer les objets avec ILM"](#)
- ["Base de connaissances NetApp : Gestion des buckets compatibles hérités dans StorageGRID 11.5"](#)

Demandes de conformité obsolètes :

- ["Obsolète - Modifications de la demande PUT Bucket pour la conformité"](#)

L'élément XML SGCompliance est obsolète. Auparavant, vous pouviez inclure cet élément personnalisé StorageGRID dans le corps de la requête XML facultatif des requêtes PUT Bucket pour créer un bucket conforme.

- ["Obsolète - Conformité du bucket GET"](#)

La demande de conformité GET Bucket est obsolète. Toutefois, vous pouvez continuer à utiliser cette demande pour déterminer les paramètres de conformité actuellement en vigueur pour un bucket conforme hérité existant.

- ["Obsolète - Conformité du compartiment PUT"](#)

La demande de conformité PUT Bucket est obsolète. Toutefois, vous pouvez continuer à utiliser cette demande pour modifier les paramètres de conformité d'un bucket conforme hérité existant. Par exemple, vous pouvez placer un bucket existant en attente légale ou augmenter sa période de conservation.

Obsolète : CreateBucket demande des modifications pour la conformité

L'élément XML SGCompliance est obsolète. Auparavant, vous pouviez inclure cet élément personnalisé StorageGRID dans le corps de la requête XML facultatif des requêtes CreateBucket pour créer un bucket conforme.



La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes de StorageGRID est obsolète et a été remplacée par S3 Object Lock. Voir ce qui suit pour plus de détails :

- ["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#)
- ["Base de connaissances NetApp : Gestion des buckets compatibles hérités dans StorageGRID 11.5"](#)

Vous ne pouvez plus créer de nouveaux buckets avec la conformité activée. Le message d'erreur suivant est renvoyé si vous tentez d'utiliser les modifications de demande CreateBucket pour la conformité afin de créer un nouveau bucket conforme :

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

Obsolète : demande de conformité GET Bucket

La demande de conformité GET Bucket est obsolète. Toutefois, vous pouvez continuer à utiliser cette demande pour déterminer les paramètres de conformité actuellement en vigueur pour un bucket conforme hérité existant.



La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes de StorageGRID est obsolète et a été remplacée par S3 Object Lock. Voir ce qui suit pour plus de détails :

- ["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#)
- ["Base de connaissances NetApp : Gestion des buckets compatibles hérités dans StorageGRID 11.5"](#)

Vous devez disposer de l'autorisation `s3:GetBucketCompliance` ou être root du compte pour terminer cette opération.

Exemple de demande

Cet exemple de requête vous permet de déterminer les paramètres de conformité pour le bucket nommé `mybucket`.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemple de réponse

Dans la réponse XML, `<SGCompliance>` répertorie les paramètres de conformité en vigueur pour le bucket. Cet exemple de réponse montre les paramètres de conformité d'un bucket dans lequel chaque objet sera conservé pendant un an (525 600 minutes), à compter du moment où l'objet est ingéré dans la grille. Il n'y a actuellement aucune retenue légale sur ce bucket. Chaque objet sera automatiquement supprimé après un an.

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nom	Description
Durée de conservation (minutes)	Durée de la période de conservation des objets ajoutés à ce bucket, en minutes. La période de conservation commence lorsque l'objet est ingéré dans la grille.
Conservation légale	<ul style="list-style-type: none"> • Vrai : ce bucket est actuellement sous une suspension légale. Les objets de ce compartiment ne peuvent pas être supprimés tant que la conservation légale n'est pas levée, même si leur période de conservation a expiré. • Faux : Ce bucket n'est actuellement pas soumis à une suspension légale. Les objets de ce compartiment peuvent être supprimés lorsque leur période de conservation expire.
Suppression automatique	<ul style="list-style-type: none"> • Vrai : les objets de ce compartiment seront supprimés automatiquement à l'expiration de leur période de conservation, sauf si le compartiment est soumis à une suspension légale. • Faux : les objets de ce bucket ne seront pas supprimés automatiquement à l'expiration de la période de conservation. Vous devez supprimer ces objets manuellement si vous devez les supprimer.

Réponses d'erreur

Si le bucket n'a pas été créé pour être conforme, le code d'état HTTP de la réponse est 404 Not Found, avec un code d'erreur S3 de `XNoSuchBucketCompliance`.

Obsolète : demande de conformité du compartiment PUT

La demande de conformité PUT Bucket est obsolète. Toutefois, vous pouvez continuer à utiliser cette demande pour modifier les paramètres de conformité d'un bucket conforme hérité existant. Par exemple, vous pouvez placer un bucket existant en attente légale ou augmenter sa période de conservation.



La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes de StorageGRID est obsolète et a été remplacée par S3 Object Lock. Voir ce qui suit pour plus de détails :

- ["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#)
- ["Base de connaissances NetApp : Gestion des buckets compatibles hérités dans StorageGRID 11.5"](#)

Vous devez disposer de l'autorisation `s3:PutBucketCompliance` ou être root du compte pour terminer cette opération.

Vous devez spécifier une valeur pour chaque champ des paramètres de conformité lors de l'émission d'une demande de conformité PUT Bucket.

Exemple de demande

Cet exemple de requête modifie les paramètres de conformité pour le bucket nommé `mybucket`. Dans cet exemple, les objets dans `mybucket` seront désormais conservés pendant deux ans (1 051 200 minutes) au lieu d'un an, à compter de la date d'ingestion de l'objet dans la grille. Il n'y a aucune retenue légale sur ce seau. Chaque objet sera automatiquement supprimé après deux ans.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nom	Description
Durée de conservation (minutes)	<p>Durée de la période de conservation des objets ajoutés à ce bucket, en minutes. La période de conservation commence lorsque l'objet est ingéré dans la grille.</p> <p>Important Lorsque vous spécifiez une nouvelle valeur pour <code>RetentionPeriodMinutes</code>, vous devez spécifier une valeur égale ou supérieure à la période de rétention actuelle du bucket. Une fois la période de conservation du bucket définie, vous ne pouvez pas diminuer cette valeur ; vous pouvez uniquement l'augmenter.</p>
Conservation légale	<ul style="list-style-type: none">• Vrai : ce bucket est actuellement sous une suspension légale. Les objets de ce compartiment ne peuvent pas être supprimés tant que la conservation légale n'est pas levée, même si leur période de conservation a expiré.• Faux : Ce bucket n'est actuellement pas soumis à une suspension légale. Les objets de ce compartiment peuvent être supprimés lorsque leur période de conservation expire.
Suppression automatique	<ul style="list-style-type: none">• Vrai : les objets de ce compartiment seront supprimés automatiquement à l'expiration de leur période de conservation, sauf si le compartiment est soumis à une suspension légale.• Faux : les objets de ce bucket ne seront pas supprimés automatiquement à l'expiration de la période de conservation. Vous devez supprimer ces objets manuellement si vous devez les supprimer.

Cohérence des paramètres de conformité

Lorsque vous mettez à jour les paramètres de conformité d'un bucket S3 avec une demande de conformité PUT Bucket, StorageGRID tente de mettre à jour les métadonnées du bucket sur la grille. Par défaut, StorageGRID utilise la cohérence **Strong-global** pour garantir que tous les sites de centre de données et tous les nœuds de stockage contenant des métadonnées de bucket ont une cohérence de lecture après écriture pour les paramètres de conformité modifiés.

Si StorageGRID ne peut pas atteindre la cohérence **Strong-global** parce qu'un site de centre de données ou plusieurs nœuds de stockage sur un site ne sont pas disponibles, le code d'état HTTP de la réponse est 503 Service Unavailable.

Si vous recevez cette réponse, vous devez contacter l'administrateur du réseau pour vous assurer que les services de stockage requis sont mis à disposition dès que possible. Si l'administrateur du réseau ne parvient pas à rendre disponibles suffisamment de nœuds de stockage sur chaque site, le support technique peut vous demander de réessayer la demande ayant échoué en forçant la cohérence **Strong-site**.



Ne forcez jamais la cohérence **Strong-site** pour la conformité du bucket PUT, sauf si le support technique vous l'a demandé et si vous comprenez les conséquences potentielles de l'utilisation de ce niveau.

Lorsque la cohérence est réduite à **Strong-site**, StorageGRID garantit que les paramètres de conformité mis à jour auront une cohérence de lecture après écriture uniquement pour les demandes client au sein d'un site. Cela signifie que le système StorageGRID peut temporairement avoir plusieurs paramètres incohérents pour ce bucket jusqu'à ce que tous les sites et nœuds de stockage soient disponibles. Les paramètres incohérents peuvent entraîner un comportement inattendu et indésirable. Par exemple, si vous placez un bucket sous une suspension légale et que vous forcez une cohérence inférieure, les paramètres de conformité précédents du bucket (c'est-à-dire la suspension légale) peuvent continuer à être en vigueur sur certains sites de centres de données. Par conséquent, les objets que vous pensez être en attente légale peuvent être supprimés à l'expiration de leur période de conservation, soit par l'utilisateur, soit par la suppression automatique, si cette option est activée.

Pour forcer l'utilisation de la cohérence **Strong-site**, réémettez la demande de conformité PUT Bucket et incluez le Consistency-Control En-tête de requête HTTP, comme suit :

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Réponses d'erreur

- Si le bucket n'a pas été créé pour être conforme, le code d'état HTTP de la réponse est 404 Not Found .
- Si RetentionPeriodMinutes si la demande est inférieure à la période de conservation actuelle du bucket, le code d'état HTTP est 400 Bad Request .

Informations connexes

["Obsolète : Modifications de la demande PUT Bucket pour la conformité"](#)

Politiques d'accès aux buckets et aux groupes

Utiliser des politiques d'accès aux buckets et aux groupes

StorageGRID utilise le langage de stratégie Amazon Web Services (AWS) pour permettre aux locataires S3 de contrôler l'accès aux buckets et aux objets au sein de ces buckets. Le système StorageGRID implémente un sous-ensemble du langage de politique de l'API REST S3. Les politiques d'accès pour l'API S3 sont écrites en JSON.

Aperçu de la politique d'accès

Il existe deux types de politiques d'accès prises en charge par StorageGRID.

- **Stratégies de bucket**, qui sont gérées à l'aide des opérations API S3 GetBucketPolicy, PutBucketPolicy et DeleteBucketPolicy ou de l'API Tenant Manager ou Tenant Management. Les stratégies de bucket sont attachées aux buckets, elles sont donc configurées pour contrôler l'accès des utilisateurs du compte propriétaire du bucket ou d'autres comptes au bucket et aux objets qu'il contient. Une politique de bucket s'applique à un seul bucket et éventuellement à plusieurs groupes.
- **Stratégies de groupe**, qui sont configurées à l'aide de Tenant Manager ou de l'API Tenant Management. Les stratégies de groupe sont attachées à un groupe dans le compte, elles sont donc configurées pour permettre à ce groupe d'accéder à des ressources spécifiques appartenant à ce compte. Une stratégie de groupe s'applique à un seul groupe et éventuellement à plusieurs compartiments.



Il n'y a aucune différence de priorité entre les politiques de groupe et de compartiment.

Les stratégies de bucket et de groupe StorageGRID suivent une grammaire spécifique définie par Amazon. À l'intérieur de chaque politique se trouve un ensemble d'énoncés de politique, et chaque énoncé contient les éléments suivants :

- ID de relevé (Sid) (facultatif)
- Effet
- Principal/Non principal
- Ressource/PasRessource
- Action/Pas d'action
- Condition (facultatif)

Les instructions de politique sont construites à l'aide de cette structure pour spécifier les autorisations : Accorder <Effet> pour autoriser/refuser à <Principal> d'effectuer <Action> sur <Ressource> lorsque <Condition> s'applique.

Chaque élément de politique est utilisé pour une fonction spécifique :

Élément	Description
Sid	L'élément Sid est facultatif. Le Sid est uniquement destiné à servir de description pour l'utilisateur. Il est stocké mais non interprété par le système StorageGRID .

Élément	Description
Effet	Utilisez l'élément Effet pour déterminer si les opérations spécifiées sont autorisées ou refusées. Vous devez identifier les opérations que vous autorisez (ou refusez) sur les buckets ou les objets à l'aide des mots-clés d'élément Action pris en charge.
Principal/Non principal	<p>Vous pouvez autoriser les utilisateurs, les groupes et les comptes à accéder à des ressources spécifiques et à effectuer des actions spécifiques. Si aucune signature S3 n'est incluse dans la demande, l'accès anonyme est autorisé en spécifiant le caractère générique (*) comme principal. Par défaut, seul le root du compte a accès aux ressources appartenant au compte.</p> <p>Il vous suffit de spécifier l'élément Principal dans une stratégie de bucket. Pour les stratégies de groupe, le groupe auquel la stratégie est attachée est l'élément principal implicite.</p>
Ressource/PasRessource	L'élément Ressource identifie les buckets et les objets. Vous pouvez autoriser ou refuser des autorisations sur des buckets et des objets à l'aide du nom de ressource Amazon (ARN) pour identifier la ressource.
Action/Pas d'action	Les éléments Action et Effet sont les deux composants des autorisations. Lorsqu'un groupe demande une ressource, l'accès à cette ressource lui est accordé ou refusé. L'accès est refusé à moins que vous n'attribuiez spécifiquement des autorisations, mais vous pouvez utiliser un refus explicite pour remplacer une autorisation accordée par une autre politique.
Condition	L'élément Condition est facultatif. Les conditions vous permettent de créer des expressions pour déterminer quand une politique doit être appliquée.

Dans l'élément Action, vous pouvez utiliser le caractère générique (*) pour spécifier toutes les opérations ou un sous-ensemble d'opérations. Par exemple, cette action correspond aux autorisations telles que s3:GetObject, s3:PutObject et s3:DeleteObject.

```
s3:*Object
```

Dans l'élément Ressource, vous pouvez utiliser les caractères génériques (*) et (?). Alors que l'astérisque (*) correspond à 0 ou plusieurs caractères, le point d'interrogation (?) correspond à n'importe quel caractère unique.

Dans l'élément Principal, les caractères génériques ne sont pas pris en charge, sauf pour définir un accès anonyme, qui accorde une autorisation à tout le monde. Par exemple, vous définissez le caractère générique (*) comme valeur principale.

```
"Principal": "*"

```

```
"Principal":{"AWS":"*"}
```

Dans l'exemple suivant, l'instruction utilise les éléments Effet, Principal, Action et Ressource. Cet exemple montre une déclaration de politique de compartiment complète qui utilise l'effet « Autoriser » pour donner aux principaux, le groupe d'administrateurs `federated-group/admin` et le groupe financier `federated-group/finance`, autorisations pour effectuer l'action `s3:ListBucket` sur le seau nommé `mybucket` et l'action `s3:GetObject` sur tous les objets à l'intérieur de ce seau.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

La politique de compartiment a une limite de taille de 20 480 octets et la politique de groupe a une limite de taille de 5 120 octets.

Cohérence des politiques

Par défaut, toutes les mises à jour que vous apportez aux stratégies de groupe sont finalement cohérentes. Lorsqu'une stratégie de groupe devient cohérente, les modifications peuvent prendre 15 minutes supplémentaires pour prendre effet, en raison de la mise en cache des stratégies. Par défaut, toutes les mises à jour que vous apportez aux stratégies de compartiment sont fortement cohérentes.

Si nécessaire, vous pouvez modifier les garanties de cohérence pour les mises à jour de la stratégie de compartiment. Par exemple, vous souhaitez peut-être qu'une modification apportée à une stratégie de compartiment soit disponible en cas de panne du site.

Dans ce cas, vous pouvez soit définir le `Consistency-Control` en-tête dans la demande `PutBucketPolicy`, ou vous pouvez utiliser la demande de cohérence `PUT Bucket`. Lorsqu'une stratégie de compartiment devient cohérente, les modifications peuvent prendre 8 secondes supplémentaires pour prendre effet, en raison de la

mise en cache de la stratégie.



Si vous définissez la cohérence sur une valeur différente pour contourner une situation temporaire, assurez-vous de redéfinir le paramètre au niveau du bucket sur sa valeur d'origine lorsque vous avez terminé. Dans le cas contraire, toutes les futures demandes de bucket utiliseront le paramètre modifié.

Utiliser l'ARN dans les déclarations de politique

Dans les déclarations de politique, l'ARN est utilisé dans les éléments Principal et Ressource.

- Utilisez cette syntaxe pour spécifier l'ARN de la ressource S3 :

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- Utilisez cette syntaxe pour spécifier l'ARN de la ressource d'identité (utilisateurs et groupes) :

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

Autres considérations :

- Vous pouvez utiliser l'astérisque (*) comme caractère générique pour faire correspondre zéro ou plusieurs caractères à l'intérieur de la clé d'objet.
- Les caractères internationaux, qui peuvent être spécifiés dans la clé d'objet, doivent être codés à l'aide de JSON UTF-8 ou à l'aide de séquences d'échappement JSON \u. Le codage en pourcentage n'est pas pris en charge.

"Syntaxe URN RFC 2141"

Le corps de la requête HTTP pour l'opération PutBucketPolicy doit être codé avec charset=UTF-8.

Spécifier les ressources dans une politique

Dans les instructions de politique, vous pouvez utiliser l'élément Ressource pour spécifier le compartiment ou l'objet pour lequel les autorisations sont accordées ou refusées.

- Chaque déclaration de politique nécessite un élément Ressource. Dans une politique, les ressources sont désignées par l'élément `Resource`, ou alternativement, `NotResource` pour l'exclusion.
- Vous spécifiez les ressources avec un ARN de ressource S3. Par exemple:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- Vous pouvez également utiliser des variables de politique à l'intérieur de la clé d'objet. Par exemple:

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- La valeur de la ressource peut spécifier un compartiment qui n'existe pas encore lors de la création d'une stratégie de groupe.

Spécifier les principaux dans une politique

Utilisez l'élément Principal pour identifier le compte d'utilisateur, de groupe ou de locataire auquel l'accès à la ressource est autorisé/refusé par l'instruction de stratégie.

- Chaque déclaration de politique dans une politique de compartiment doit inclure un élément Principal. Les instructions de politique dans une politique de groupe n'ont pas besoin de l'élément Principal car le groupe est considéré comme le principal.
- Dans une politique, les mandants sont désignés par l'élément « Principal » ou « NotPrincipal » pour l'exclusion.
- Les identités basées sur un compte doivent être spécifiées à l'aide d'un ID ou d'un ARN :

```
"Principal": { "AWS": "account_id"}  
"Principal": { "AWS": "identity_arn" }
```

- Cet exemple utilise l'ID de compte locataire 27233906934684427525, qui inclut la racine du compte et tous les utilisateurs du compte :

```
"Principal": { "AWS": "27233906934684427525" }
```

- Vous pouvez spécifier uniquement la racine du compte :

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- Vous pouvez spécifier un utilisateur fédéré spécifique (« Alex ») :

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-  
user/Alex" }
```

- Vous pouvez spécifier un groupe fédéré spécifique (« Managers ») :

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-  
group/Managers" }
```

- Vous pouvez spécifier un principal anonyme :

```
"Principal": ""
```

- Pour éviter toute ambiguïté, vous pouvez utiliser l'UUID de l'utilisateur au lieu du nom d'utilisateur :

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-  
eb6b9e546013
```

Par exemple, supposons qu'Alex quitte l'organisation et le nom d'utilisateur `Alex` est supprimé. Si un nouvel Alex rejoint l'organisation et se voit attribuer le même `Alex` nom d'utilisateur, le nouvel utilisateur peut hériter involontairement des autorisations accordées à l'utilisateur d'origine.

- La valeur principale peut spécifier un nom de groupe/utilisateur qui n'existe pas encore lors de la création d'une stratégie de compartiment.

Spécifier les autorisations dans une politique

Dans une politique, l'élément Action est utilisé pour autoriser/refuser des autorisations à une ressource. Il existe un ensemble d'autorisations que vous pouvez spécifier dans une politique, qui sont indiquées par l'élément « Action » ou, alternativement, « NotAction » pour l'exclusion. Chacun de ces éléments correspond à des opérations spécifiques de l'API REST S3.

Les tableaux répertorient les autorisations qui s'appliquent aux buckets et les autorisations qui s'appliquent aux objets.



Amazon S3 utilise désormais l'autorisation `s3:PutReplicationConfiguration` pour les actions `PutBucketReplication` et `DeleteBucketReplication`. StorageGRID utilise des autorisations distinctes pour chaque action, ce qui correspond à la spécification Amazon S3 d'origine.



Une suppression est effectuée lorsqu'un put est utilisé pour écraser une valeur existante.

Autorisations qui s'appliquent aux buckets

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3:Créer un bucket	Créer un bucket	Oui. Remarque : À utiliser uniquement dans la stratégie de groupe.
s3 : Supprimer le bucket	Supprimer le bucket	
s3 : Supprimer la notification des métadonnées du bucket	SUPPRIMER la configuration de notification des métadonnées du bucket	Oui

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3 : Supprimer la politique de bucket	Supprimer la politique de bucket	
s3 : Supprimer la configuration de réplication	SupprimerBucketReplication	Oui, des autorisations distinctes pour PUT et DELETE
s3 : Obtenir l'Acl du bucket	ObtenirBucketAcl	
s3 : Obtenir la conformité du bucket	Conformité du bucket GET (obsolète)	Oui
s3 : GetBucketConsistency	Cohérence du bucket GET	Oui
s3:Obtenir le bucket CORS	ObtenirBucketCors	
s3 : Obtenir la configuration du chiffrement	Obtenir le chiffrement du bucket	
s3 : Obtenir l'heure du dernier accès au bucket	Heure du dernier accès au bucket GET	Oui
s3 : Obtenir l'emplacement du bucket	Obtenir l'emplacement du bucket	
s3 : GetBucketMetadataNotification	Configuration de la notification des métadonnées du bucket GET	Oui
s3 : Obtenir une notification de bucket	Configuration de GetBucketNotification	
s3 : GetBucketObjectLockConfiguration	Obtenir la configuration du verrouillage de l'objet	
s3 : Obtenir la politique du bucket	Obtenir la politique de Bucket	
s3 : Obtenir le balisage du bucket	Obtenir le balisage du bucket	
s3 : Obtenir la gestion des versions du bucket	Obtenir la gestion des versions du bucket	
s3 : Obtenir la configuration du cycle de vie	GetBucketLifecycleConfiguration	
s3 : Obtenir la configuration de réplication	Réplication GetBucket	

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3 : ListeTousMesSeaux	<ul style="list-style-type: none"> Listes de seaux Utilisation du stockage GET 	<p>Oui, pour l'utilisation du stockage GET.</p> <p>Remarque : À utiliser uniquement dans la stratégie de groupe.</p>
s3:ListBucket	<ul style="list-style-type: none"> Liste d'objets Tête de godet Restaurer l'objet 	
s3 : ListBucketMultipartUploads	<ul style="list-style-type: none"> ListeMultipartUploads Restaurer l'objet 	
s3 : ListBucketVersions	Versions du bucket GET	
s3 : PutBucketCompliance	Conformité du compartiment PUT (obsolète)	Oui
s3 : PutBucketConsistency	Cohérence du seau PUT	Oui
s3:PutBucketCORS	<ul style="list-style-type: none"> SupprimerBucketCors† PutBucketCors 	
s3 : PutEncryptionConfiguration	<ul style="list-style-type: none"> Supprimer le chiffrement du bucket Cryptage PutBucket 	
s3 : PutBucketLastAccessTime	Heure du dernier accès au bucket PUT	Oui
s3 : PutBucketMetadataNotification	Configuration des notifications de métadonnées du compartiment PUT	Oui
s3 : PutBucketNotification	Configuration de PutBucketNotification	
s3 : PutBucketObjectLockConfiguration	<ul style="list-style-type: none"> CreateBucket avec le <code>x-amz-bucket-object-lock-enabled: true</code> en-tête de requête (nécessite également l'autorisation <code>s3:CreateBucket</code>) Configuration de PutObjectLock 	
s3 : PutBucketPolicy	Politique de PutBucket	

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3 : Mettre en place le balisage du bucket	<ul style="list-style-type: none"> Supprimer le balisage du bucket† Balisage de PutBucket 	
s3 : PutBucketVersioning	Gestion des versions de PutBucket	
s3 : PutLifecycleConfiguration	<ul style="list-style-type: none"> Supprimer le cycle de vie du bucket† Configuration du cycle de vie de PutBucket 	
s3 : PutReplicationConfiguration	Réplication de PutBucket	Oui, des autorisations distinctes pour PUT et DELETE

Autorisations qui s'appliquent aux objets

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3 : Abandonner le téléchargement en plusieurs parties	<ul style="list-style-type: none"> Abandonner le téléchargement en plusieurs parties Restaurer l'objet 	
s3 : Contournement de la gouvernance et de la rétention	<ul style="list-style-type: none"> Supprimer l'objet Supprimer les objets PutObjectRetention 	
s3:Supprimer l'objet	<ul style="list-style-type: none"> Supprimer l'objet Supprimer les objets Restaurer l'objet 	
s3 : Supprimer le balisage d'objet	Supprimer l'étiquetage des objets	
s3 : Supprimer le balisage de version d'objet	DeleteObjectTagging (une version spécifique de l'objet)	
s3 : Supprimer la version de l'objet	DeleteObject (une version spécifique de l'objet)	

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3:Obtenir l'objet	<ul style="list-style-type: none"> • Obtenir l'objet • HeadObject • Restaurer l'objet • Sélectionner le contenu de l'objet 	
s3:GetObjectAcl	ObtenirObjectAcl	
s3 : GetObjectLegalHold	Obtenir la conservation légale de l'objet	
s3 : Obtenir la rétention d'objet	Obtenir la rétention d'objet	
s3 : Obtenir le balisage des objets	Obtenir l'étiquetage des objets	
s3 : Obtenir le balisage de la version de l'objet	GetObjectTagging (une version spécifique de l'objet)	
s3 : Obtenir la version de l'objet	GetObject (une version spécifique de l'objet)	
s3 : ListeMultipartUploadParts	ListParts, RestoreObject	
s3:PutObject	<ul style="list-style-type: none"> • Mettre l'objet • Copier l'objet • Restaurer l'objet • Créer un téléchargement multi-parties • Téléchargement complet en plusieurs parties • Télécharger une partie • TéléchargerPartCopy 	
s3 : PutObjectLegalHold	MettreObjetLegalHold	
s3 : PutObjectRetention	PutObjectRetention	
s3 : Mettre en place un balisage d'objet	Balisage d'objets	
s3 : Mettre en place la version de l'objet	PutObjectTagging (une version spécifique de l'objet)	

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3 : PutOverwriteObject	<ul style="list-style-type: none"> • Mettre l'objet • Copier l'objet • Balisage d'objets • Supprimer l'étiquetage des objets • Téléchargement complet en plusieurs parties 	Oui
s3:RestoreObject	Restaurer l'objet	

Utiliser l'autorisation PutOverwriteObject

L'autorisation s3:PutOverwriteObject est une autorisation StorageGRID personnalisée qui s'applique aux opérations qui créent ou mettent à jour des objets. Le paramètre de cette autorisation détermine si le client peut écraser les données d'un objet, les métadonnées définies par l'utilisateur ou le balisage d'un objet S3.

Les paramètres possibles pour cette autorisation incluent :

- **Autoriser**: Le client peut écraser un objet. Il s'agit du paramètre par défaut.
- **Refuser** : Le client ne peut pas écraser un objet. Lorsqu'elle est définie sur Refuser, l'autorisation PutOverwriteObject fonctionne comme suit :
 - Si un objet existant est trouvé sur le même chemin :
 - Les données de l'objet, les métadonnées définies par l'utilisateur ou le balisage de l'objet S3 ne peuvent pas être écrasés.
 - Toutes les opérations d'ingestion en cours sont annulées et une erreur est renvoyée.
 - Si le contrôle de version S3 est activé, le paramètre Refuser empêche les opérations PutObjectTagging ou DeleteObjectTagging de modifier le TagSet d'un objet et ses versions non actuelles.
 - Si aucun objet existant n'est trouvé, cette autorisation n'a aucun effet.
- Lorsque cette autorisation n'est pas présente, l'effet est le même que si Autoriser était défini.



Si la stratégie S3 actuelle autorise l'écrasement et que l'autorisation PutOverwriteObject est définie sur Refuser, le client ne peut pas écraser les données d'un objet, les métadonnées définies par l'utilisateur ou le balisage d'un objet. De plus, si la case à cocher **Empêcher la modification du client** est sélectionnée (**CONFIGURATION > Paramètres de sécurité > Réseau et objets**), ce paramètre remplace le paramètre de l'autorisation PutOverwriteObject.

Spécifier les conditions dans une politique

Les conditions définissent quand une politique sera en vigueur. Les conditions sont constituées d'opérateurs et de paires clé-valeur.

Les conditions utilisent des paires clé-valeur pour l'évaluation. Un élément Condition peut contenir plusieurs conditions, et chaque condition peut contenir plusieurs paires clé-valeur. Le bloc de condition utilise le format suivant :

```
Condition: {
  condition_type: {
    condition_key: condition_values
```

Dans l'exemple suivant, la condition `IpAddress` utilise la clé de condition `SourceIp`.

```
"Condition": {
  "IpAddress": {
    "aws:SourceIp": "54.240.143.0/24"
    ...
  },
  ...
```

Opérateurs de condition pris en charge

Les opérateurs de condition sont classés comme suit :

- Chaîne
- Numérique
- Booléen
- adresse IP
- Vérification nulle

Opérateurs de condition	Description
Chaîne égale	Compare une clé à une valeur de chaîne en fonction d'une correspondance exacte (sensible à la casse).
Chaîne non égale	Compare une clé à une valeur de chaîne en fonction d'une correspondance négative (sensible à la casse).
Chaîne égale à Ignorer la casse	Compare une clé à une valeur de chaîne en fonction d'une correspondance exacte (ignore la casse).
Chaîne non égale à ignorer la casse	Compare une clé à une valeur de chaîne en fonction d'une correspondance négative (ignore la casse).
Comme une chaîne	Compare une clé à une valeur de chaîne en fonction d'une correspondance exacte (sensible à la casse). Peut inclure les caractères génériques * et ?.
ChaînePasComme	Compare une clé à une valeur de chaîne en fonction d'une correspondance négative (sensible à la casse). Peut inclure les caractères génériques * et ?.

Opérateurs de condition	Description
NumériqueÉgal	Compare une clé à une valeur numérique en fonction d'une correspondance exacte.
NumériqueNonÉgal	Compare une clé à une valeur numérique en fonction d'une correspondance négative.
Numérique supérieur à	Compare une clé à une valeur numérique en fonction d'une correspondance « supérieure à ».
Numérique supérieur à égal	Compare une clé à une valeur numérique en fonction d'une correspondance « supérieure ou égale ».
NumériqueInférieurÀ	Compare une clé à une valeur numérique en fonction d'une correspondance « inférieure à ».
NumériqueInférieurÀÉgal	Compare une clé à une valeur numérique en fonction d'une correspondance « inférieure ou égale ».
Booléen	Compare une clé à une valeur booléenne en fonction d'une correspondance « vrai ou faux ».
Adresse IP	Compare une clé à une adresse IP ou à une plage d'adresses IP.
Pas d'adresse IP	Compare une clé à une adresse IP ou à une plage d'adresses IP en fonction d'une correspondance négative.
Nul	Vérifie si une clé de condition est présente dans le contexte de la demande actuelle.

Clés de condition prises en charge

Clés de condition	Actions	Description
aws:SourceIP	opérateurs IP	<p>Sera comparé à l'adresse IP à partir de laquelle la demande a été envoyée. Peut être utilisé pour les opérations de bucket ou d'objet.</p> <p>Remarque : si la requête S3 a été envoyée via le service d'équilibrage de charge sur les nœuds d'administration et les nœuds de passerelle, elle sera comparée à l'adresse IP en amont du service d'équilibrage de charge.</p> <p>Remarque : si un équilibreur de charge tiers non transparent est utilisé, cela sera comparé à l'adresse IP de cet équilibreur de charge. N'importe lequel <code>X-Forwarded-For</code> l'en-tête sera ignoré car sa validité ne peut pas être vérifiée.</p>
aws:nom d'utilisateur	Ressource/Identité	Sera comparé au nom d'utilisateur de l'expéditeur à partir duquel la demande a été envoyée. Peut être utilisé pour les opérations de bucket ou d'objet.
s3:délimiteur	s3:ListBucket et s3:Authorisations ListBucketVersions	Sera comparé au paramètre délimiteur spécifié dans une demande ListObjects ou ListObjectVersions.

Clés de condition	Actions	Description
s3:ExistingObjectTag/<clé-balise>	s3 : Supprimer le balisage d'objet s3 : Supprimer le balisage de version d'objet s3:Obtenir l'objet s3:GetObjectAcl 3 : Obtenir le balisage des objets s3 : Obtenir la version de l'objet s3 : ObtenirObjectVersionAcl s3 : Obtenir le balisage de la version de l'objet s3:PutObjectAcl s3 : Mettre en place un balisage d'objet s3:PutObjectVersionAcl s3 : Mettre en place la version de l'objet	Nécessitera que l'objet existant possède la clé et la valeur de balise spécifiques.
s3:max-clés	s3:ListBucket et s3:Autorisations ListBucketVersions	Sera comparé au paramètre max-keys spécifié dans une requête ListObjects ou ListObjectVersions.
s3 : jours de conservation restants pour le verrouillage d'objet	s3:PutObject	Comparable à la date de conservation spécifiée dans le x-amz-object-lock-retain-until-date en-tête de demande ou période de conservation par défaut calculée à partir du compartiment pour garantir que ces valeurs se situent dans la plage autorisée pour les demandes suivantes : <ul style="list-style-type: none"> • Mettre l'objet • Copier l'objet • Créer un téléchargement multi-parties

Clés de condition	Actions	Description
s3 : jours de conservation restants pour le verrouillage d'objet	s3 : PutObjectRetention	Compare la date de conservation spécifiée dans la demande PutObjectRetention pour garantir qu'elle se situe dans la plage autorisée.
s3:préfixe	s3:ListBucket et s3:Autorisations ListBucketVersions	Sera comparé au paramètre de préfixe spécifié dans une demande ListObjects ou ListObjectVersions.
s3:RequestObjectTag/<clé-balise>	s3:PutObject s3 : Mettre en place un balisage d'objet s3 : Mettre en place la version de l'objet	Nécessitera une clé et une valeur de balise spécifiques lorsque la demande d'objet inclut le balisage.

Spécifier les variables dans une politique

Vous pouvez utiliser des variables dans les politiques pour renseigner les informations de politique lorsqu'elles sont disponibles. Vous pouvez utiliser des variables de politique dans le `Resource` élément et dans les comparaisons de chaînes dans le `Condition` élément.

Dans cet exemple, la variable `${aws:username}` fait partie de l'élément `Ressource` :

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

Dans cet exemple, la variable `${aws:username}` fait partie de la valeur de condition dans le bloc de condition :

```
"Condition": {
  "StringLike": {
    "s3:prefix": "${aws:username}/*"
    ...
  },
  ...
}
```

Variable	Description
<code>\${aws:SourceIp}</code>	Utilise la clé <code>SourceIp</code> comme variable fournie.
<code>\${aws:username}</code>	Utilise la clé du nom d'utilisateur comme variable fournie.
<code>\${s3:prefix}</code>	Utilise la clé de préfixe spécifique au service comme variable fournie.

Variable	Description
<code>\$ { s3 : max - keys }</code>	Utilise la clé max-keys spécifique au service comme variable fournie.
<code>\$ { * }</code>	Caractère spécial. Utilise le caractère comme un caractère * littéral.
<code>\$ { ? }</code>	Caractère spécial. Utilise le caractère comme un caractère ? littéral.
<code>\$ { \$ }</code>	Caractère spécial. Utilise le caractère comme un caractère \$ littéral.

Créer des politiques nécessitant un traitement spécial

Parfois, une politique peut accorder des autorisations dangereuses pour la sécurité ou pour la poursuite des opérations, comme le verrouillage de l'utilisateur root du compte. L'implémentation de l'API REST StorageGRID S3 est moins restrictive lors de la validation des politiques qu'Amazon, mais tout aussi stricte lors de l'évaluation des politiques.

Description de la politique	Type de politique	Comportement d'Amazon	Comportement de StorageGRID
Refuser toute autorisation sur le compte root	Seau	Valide et appliqué, mais le compte utilisateur root conserve l'autorisation pour toutes les opérations de stratégie de compartiment S3	Même
Se refuser toute autorisation d'utilisateur/groupe	Groupe	Valide et appliqué	Même
Autoriser un groupe de comptes étrangers à accorder n'importe quelle autorisation	Seau	Principal invalide	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 Méthode non autorisée lorsqu'elles sont autorisées par une stratégie
Autoriser un compte root ou un utilisateur étranger à accéder à n'importe quelle autorisation	Seau	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 Méthode non autorisée lorsqu'elles sont autorisées par une stratégie	Même

Description de la politique	Type de politique	Comportement d'Amazon	Comportement de StorageGRID
Accorder à tout le monde des autorisations pour toutes les actions	Seau	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 Méthode non autorisée pour la racine du compte étranger et les utilisateurs	Même
Refuser à tout le monde les autorisations pour toutes les actions	Seau	Valide et appliqué, mais le compte utilisateur root conserve l'autorisation pour toutes les opérations de stratégie de compartiment S3	Même
Le principal est un utilisateur ou un groupe inexistant	Seau	Principal invalide	Valide
La ressource est un bucket S3 inexistant	Groupe	Valide	Même
Principal est un groupe local	Seau	Principal invalide	Valide
La politique accorde à un compte non propriétaire (y compris les comptes anonymes) des autorisations pour placer des objets.	Seau	Valide. Les objets appartiennent au compte créateur et la politique de compartiment ne s'applique pas. Le compte créateur doit accorder des autorisations d'accès à l'objet à l'aide des listes de contrôle d'accès (ACL) d'objet.	Valide. Les objets appartiennent au compte propriétaire du bucket. La politique des seaux s'applique.

Protection WORM (écriture unique, lecture multiple)

Vous pouvez créer des buckets WORM (Write-Once-Read-Many) pour protéger les données, les métadonnées d'objet définies par l'utilisateur et le balisage d'objet S3. Vous configurez les buckets WORM pour permettre la création de nouveaux objets et pour empêcher l'écrasement ou la suppression du contenu existant. Utilisez l'une des approches décrites ici.

Pour garantir que les écrasements sont toujours refusés, vous pouvez :

- Depuis le Gestionnaire de grille, accédez à **CONFIGURATION > Sécurité > Paramètres de sécurité > Réseau et objets**, puis cochez la case **Empêcher la modification du client**.
- Appliquez les règles et politiques S3 suivantes :
 - Ajoutez une opération PutOverwriteObject DENY à la stratégie S3.
 - Ajoutez une opération DeleteObject DENY à la stratégie S3.
 - Ajoutez une opération PutObject ALLOW à la stratégie S3.



La définition de DeleteObject sur DENY dans une stratégie S3 n'empêche pas ILM de supprimer des objets lorsqu'une règle telle que « zéro copie après 30 jours » existe.



Même lorsque toutes ces règles et politiques sont appliquées, elles ne protègent pas contre les écritures simultanées (voir situation A). Ils protègent contre les écrasements séquentiels terminés (voir situation B).

Situation A : Écritures simultanées (non protégées)

```
/mybucket/important.doc  
PUT#1 ---> OK  
PUT#2 -----> OK
```

Situation B : Écrasements séquentiels terminés (protégés contre)

```
/mybucket/important.doc  
PUT#1 -----> PUT#2 ---X (denied)
```

Informations connexes

- ["Comment les règles ILM de StorageGRID gèrent les objets"](#)
- ["Exemples de politiques de compartiment"](#)
- ["Exemples de stratégies de groupe"](#)
- ["Gérer les objets avec ILM"](#)
- ["Utiliser un compte locataire"](#)

Exemples de politiques de compartiment

Utilisez les exemples de cette section pour créer des politiques d'accès StorageGRID pour les buckets.

Les stratégies de compartiment spécifient les autorisations d'accès pour le compartiment auquel la stratégie est attachée. Vous configurez une stratégie de bucket en utilisant l'API S3 PutBucketPolicy via l'un de ces outils :

- ["Gestionnaire de locataires"](#) .
- AWS CLI utilisant cette commande (reportez-vous à ["Opérations sur les godets"](#)) :

```
> aws s3api put-bucket-policy --bucket examplebucket --policy  
file://policy.json
```

Exemple : autoriser tout le monde à accéder en lecture seule à un bucket

Dans cet exemple, tout le monde, y compris les personnes anonymes, est autorisé à répertorier les objets du bucket et à effectuer des opérations GetObject sur tous les objets du bucket. Toutes les autres opérations

seront refusées. Notez que cette politique peut ne pas être particulièrement utile car personne, à l'exception de la racine du compte, n'a l'autorisation d'écrire dans le bucket.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
[ "arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*" ]
    }
  ]
}
```

Exemple : autoriser tous les utilisateurs d'un compte à accéder pleinement à un bucket et tous les utilisateurs d'un autre compte à accéder en lecture seule à un bucket.

Dans cet exemple, toutes les personnes d'un compte spécifié sont autorisées à accéder pleinement à un compartiment, tandis que toutes les personnes d'un autre compte spécifié sont uniquement autorisées à répertorier le compartiment et à effectuer des opérations GetObject sur les objets du compartiment commençant par le `shared/` préfixe de clé d'objet.



Dans StorageGRID, les objets créés par un compte non propriétaire (y compris les comptes anonymes) appartiennent au compte propriétaire du bucket. La politique de bucket s'applique à ces objets.

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}

```

Exemple : autoriser tout le monde à accéder en lecture seule à un compartiment et à accorder un accès complet au groupe spécifié

Dans cet exemple, tout le monde, y compris les anonymes, est autorisé à répertorier le bucket et à effectuer des opérations `GetObject` sur tous les objets du bucket, tandis que seuls les utilisateurs appartenant au groupe `Marketing` dans le compte spécifié, un accès complet est autorisé.

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket", "s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

Exemple : autoriser tout le monde à accéder en lecture et en écriture à un bucket si le client se trouve dans la plage d'adresses IP

Dans cet exemple, tout le monde, y compris les personnes anonymes, est autorisé à répertorier le bucket et à effectuer toutes les opérations d'objet sur tous les objets du bucket, à condition que les demandes proviennent d'une plage d'adresses IP spécifiée (54.240.143.0 à 54.240.143.255, sauf 54.240.143.188). Toutes les autres opérations seront refusées et toutes les demandes en dehors de la plage IP seront refusées.

```

{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
[ "arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*" ],
      "Condition": {
        "IpAddress": { "aws:SourceIp": "54.240.143.0/24" },
        "NotIpAddress": { "aws:SourceIp": "54.240.143.188" }
      }
    }
  ]
}

```

Exemple : autoriser l'accès complet à un bucket exclusivement par un utilisateur fédéré spécifié

Dans cet exemple, l'utilisateur fédéré Alex est autorisé à accéder pleinement au `examplebucket` seau et ses objets. Tous les autres utilisateurs, y compris « root », se voient explicitement refuser toutes les opérations. Notez cependant que « root » ne se voit jamais refuser les autorisations pour `Put/Get/DeleteBucketPolicy`.

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

Exemple : autorisation PutOverwriteObject

Dans cet exemple, le `Deny` L'effet pour `PutOverwriteObject` et `DeleteObject` garantit que personne ne peut écraser ou supprimer les données de l'objet, les métadonnées définies par l'utilisateur et le balisage de l'objet S3.

```

{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}

```

Exemples de stratégies de groupe

Utilisez les exemples de cette section pour créer des politiques d'accès StorageGRID pour les groupes.

Les stratégies de groupe spécifient les autorisations d'accès pour le groupe auquel la stratégie est attachée. Il n'y a pas de `Principal` élément de la politique car il est implicite. Les stratégies de groupe sont configurées à l'aide du gestionnaire de locataires ou de l'API.

Exemple : définir une stratégie de groupe à l'aide de Tenant Manager

Lorsque vous ajoutez ou modifiez un groupe dans le gestionnaire de locataires, vous pouvez sélectionner une stratégie de groupe pour déterminer les autorisations d'accès S3 dont disposeront les membres de ce groupe. Voir ["Créer des groupes pour un locataire S3"](#).

- **Pas d'accès S3** : option par défaut. Les utilisateurs de ce groupe n'ont pas accès aux ressources S3, sauf si l'accès est accordé avec une stratégie de compartiment. Si vous sélectionnez cette option, seul l'utilisateur root aura accès aux ressources S3 par défaut.
- **Accès en lecture seule** : les utilisateurs de ce groupe ont un accès en lecture seule aux ressources S3. Par exemple, les utilisateurs de ce groupe peuvent répertorier les objets et lire les données, les métadonnées et les balises des objets. Lorsque vous sélectionnez cette option, la chaîne JSON d'une stratégie de groupe en lecture seule apparaît dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Accès complet** : les utilisateurs de ce groupe ont un accès complet aux ressources S3, y compris aux buckets. Lorsque vous sélectionnez cette option, la chaîne JSON d'une stratégie de groupe à accès complet apparaît dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Atténuation des ransomwares** : cet exemple de politique s'applique à tous les compartiments de ce locataire. Les utilisateurs de ce groupe peuvent effectuer des actions courantes, mais ne peuvent pas supprimer définitivement les objets des buckets pour lesquels le contrôle de version des objets est activé.

Les utilisateurs de Tenant Manager qui disposent de l'autorisation Gérer tous les compartiments peuvent remplacer cette stratégie de groupe. Limitez l'autorisation Gérer tous les compartiments aux utilisateurs de confiance et utilisez l'authentification multifactor (MFA) lorsqu'elle est disponible.

- **Personnalisé** : les utilisateurs du groupe bénéficient des autorisations que vous spécifiez dans la zone de texte.

Exemple : autoriser le groupe à accéder à tous les compartiments

Dans cet exemple, tous les membres du groupe sont autorisés à accéder pleinement à tous les compartiments appartenant au compte locataire, sauf si cela est explicitement refusé par la politique de compartiment.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Exemple : autoriser l'accès en lecture seule du groupe à tous les compartiments

Dans cet exemple, tous les membres du groupe ont un accès en lecture seule aux ressources S3, sauf si cela est explicitement refusé par la politique de bucket. Par exemple, les utilisateurs de ce groupe peuvent répertorier les objets et lire les données d'objet, les métadonnées et les balises.

```

{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}

```

Exemple : autoriser les membres du groupe à accéder pleinement à leur « dossier » dans un compartiment

Dans cet exemple, les membres du groupe sont uniquement autorisés à répertorier et à accéder à leur dossier spécifique (préfixe de clé) dans le compartiment spécifié. Notez que les autorisations d'accès provenant d'autres stratégies de groupe et de la stratégie de compartiment doivent être prises en compte lors de la détermination de la confidentialité de ces dossiers.

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

Opérations S3 suivies dans les journaux d'audit

Les messages d'audit sont générés par les services StorageGRID et stockés dans des fichiers journaux texte. Vous pouvez consulter les messages d'audit spécifiques à S3 dans le journal d'audit pour obtenir des détails sur les opérations de bucket et d'objet.

Opérations de bucket suivies dans les journaux d'audit

- Créer un bucket
- Supprimer le bucket
- Supprimer le balisage du bucket
- Supprimer les objets
- Obtenir le balisage du bucket
- Tête de godet
- Liste d'objets
- ListObjectVersions
- Conformité du compartiment PUT
- Balisage de PutBucket
- Gestion des versions de PutBucket

Opérations sur les objets suivies dans les journaux d'audit

- Téléchargement complet en plusieurs parties
- Copier l'objet
- Supprimer l'objet
- Obtenir l'objet
- HeadObject
- Mettre l'objet
- Restaurer l'objet
- Sélectionner un objet
- UploadPart (lorsqu'une règle ILM utilise une ingestion équilibrée ou stricte)
- UploadPartCopy (lorsqu'une règle ILM utilise une ingestion équilibrée ou stricte)

Informations connexes

- ["Accéder au fichier journal d'audit"](#)
- ["Le client écrit des messages d'audit"](#)
- ["Le client lit les messages d'audit"](#)

Utiliser l'API REST Swift (fin de vie)

Utiliser l'API REST Swift

La prise en charge de l'API Swift a atteint sa fin de vie et sera supprimée dans une prochaine version.



Les détails Swift ont été supprimés de cette version du site de documentation. Voir ["StorageGRID 11.8 : utiliser l'API REST Swift"](#).

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.