



Utiliser StorageGRID

StorageGRID

NetApp
November 04, 2025

This PDF was generated from <https://docs.netapp.com/fr-fr/storagegrid-117/tenant/index.html> on November 04, 2025. Always check docs.netapp.com for the latest.

Sommaire

Utiliser StorageGRID	1
Utilisez un compte de locataire	1
Utilisez un compte de locataire : présentation	1
Comment se connecter et se déconnecter	2
Présentation du tableau de bord du gestionnaire de locataires	7
API de gestion des locataires	10
Utiliser les connexions de fédération de grille	15
Gestion des groupes et des utilisateurs	28
Gestion des clés d'accès S3	47
Gestion des compartiments S3	53
Gérez les services de la plateforme S3	74
UTILISEZ L'API REST S3	117
Versions et mises à jour prises en charge par l'API REST S3	117
Référence rapide : demandes d'API S3 prises en charge	120
Configurez les comptes et les connexions des locataires	138
La prise en charge des services de plateforme StorageGRID	141
Implémentation de l'API REST S3 par StorageGRID	142
Prise en charge de l'API REST Amazon S3	160
Requêtes StorageGRID S3	210
Règles d'accès au compartiment et au groupe	231
Configuration de la sécurité pour l'API REST	257
Surveiller et auditer les opérations	259
Avantages des connexions HTTP actives, inactives et simultanées	262
Utiliser l'API REST de Swift (obsolète)	265
Utilisez l'API REST de Swift : présentation	265
Configurez les comptes et les connexions des locataires	268
Opérations prises en charge par l'API REST Swift	272
Opérations de l'API REST StorageGRID Swift	285
Configuration de la sécurité pour l'API REST	288
Surveiller et auditer les opérations	290

Utiliser StorageGRID

Utilisez un compte de locataire

Utilisez un compte de locataire : présentation

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

Qu'est-ce qu'un compte de locataire ?

Chaque compte de locataire possède ses propres groupes, utilisateurs, compartiments S3, conteneurs Swift et objets fédérés.

Les comptes de tenant peuvent être utilisés pour isoler les objets stockés par des entités différentes. Par exemple, vous pouvez utiliser plusieurs comptes locataires pour l'une de ces utilisations :

- **Utilisation en entreprise** : si le système StorageGRID est utilisé au sein d'une entreprise, le stockage objet de la grille peut être séparé par les différents services de l'organisation. Par exemple, il peut y avoir des comptes de tenant pour le service Marketing, le service Customer support, le service des ressources humaines, etc.



Si vous utilisez le protocole client S3, vous pouvez également utiliser des compartiments S3 et des règles de compartiment pour isoler les objets entre les différents départements d'une entreprise. Vous n'avez pas besoin de créer des comptes de locataire distincts. Voir les instructions de mise en œuvre "["Compartiments S3 et règles de compartiments"](#)" pour en savoir plus.

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

Comment créer un compte de locataire

Les comptes de locataire sont créés par un "["Administrateur du grid StorageGRID utilisant le gestionnaire de grille"](#)". Lors de la création d'un compte de locataire, l'administrateur de la grille spécifie ce qui suit :

- Informations de base comprenant le nom du locataire, le type de client (S3 ou Swift) et le quota de stockage facultatif.
- Autorisations pour le compte de locataire, par exemple si le compte de locataire peut utiliser les services de la plateforme S3, configurer son propre référentiel d'identité, utiliser S3 Select ou utiliser une connexion de fédération grid.
- Accès racine initial pour le locataire, selon que le système StorageGRID utilise des groupes et utilisateurs locaux, la fédération des identités ou l'authentification unique (SSO).

En outre, les administrateurs du grid peuvent activer le paramètre de verrouillage objet S3 pour le système StorageGRID si les comptes de locataires S3 doivent être conformes aux exigences réglementaires. Lorsque le verrouillage des objets S3 est activé, tous les comptes de locataires S3 peuvent créer et gérer des compartiments conformes.

Configurez les locataires S3

Après un "[Le compte de locataire S3 est créé](#)", Vous pouvez accéder au Gestionnaire de tenant pour effectuer des tâches telles que :

- Configurer la fédération des identités (sauf si le référentiel d'identité est partagé avec la grille)
- Gestion des groupes et des utilisateurs
- Utilisez la fédération grid pour le clone de compte et la réPLICATION inter-grid
- Gestion des clés d'accès S3
- Création et gestion de compartiments S3
- Utilisez les services de plateforme S3
- Utiliser S3 Select
- Contrôle de l'utilisation du stockage

 Même si vous pouvez créer et gérer des compartiments S3 avec le gestionnaire des locataires, vous devez utiliser un client S3 pour ingérer et gérer les objets. Voir "["UTILISEZ L'API REST S3"](#) pour plus d'informations.

Configurez les locataires Swift

Après un "[Le compte de locataire Swift est créé](#)", Vous pouvez accéder au Gestionnaire de tenant pour effectuer des tâches telles que :

- Configurer la fédération des identités (sauf si le référentiel d'identité est partagé avec la grille)
- Gestion des groupes et des utilisateurs
- Contrôle de l'utilisation du stockage

 Les utilisateurs Swift doivent disposer de l'autorisation d'accès racine pour accéder au Gestionnaire de locataires. Cependant, l'autorisation d'accès racine ne permet pas aux utilisateurs de s'authentifier dans "["API REST Swift"](#) pour créer des conteneurs et ingérer des objets. Les utilisateurs doivent disposer de l'autorisation Administrateur Swift pour s'authentifier dans l'API REST de Swift.

Comment se connecter et se déconnecter

Connectez-vous au Gestionnaire de locataires

Pour accéder au Gestionnaire de locataires, entrez l'URL du locataire dans la barre d'adresse d'un "[navigateur web pris en charge](#)".

Avant de commencer

- Vous disposez de vos identifiants de connexion.
- Vous disposez d'une URL permettant d'accéder au gestionnaire de locataires, fournie par votre administrateur de grille. L'URL se présente comme 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 haute disponibilité de nœuds d'administration. Il peut également inclure un numéro de port, l'ID de compte de 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 possède "[autorisations d'accès spécifiques](#)".

Étapes

1. Lancez un "[navigateur web pris en charge](#)".
2. Dans la barre d'adresse du navigateur, entrez l'URL d'accès au Gestionnaire de locataires.
3. Si vous êtes invité à recevoir une alerte de sécurité, installez le certificat à l'aide de l'assistant d'installation du navigateur.
4. Connectez-vous au Gestionnaire de locataires.

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

Pas d'utilisation de SSO

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

- Page de connexion de Grid Manager. Sélectionnez le lien **tenant sign-in**.

The screenshot shows the login interface for the NetApp StorageGRID Grid Manager. At the top, the NetApp logo and 'StorageGRID®' are displayed. Below that, the text 'Grid Manager' is centered. There are two input fields: 'Username' and 'Password', each containing a single vertical bar placeholder. A blue rectangular button labeled 'Sign in' is positioned below the password field. At the bottom of the page, there is a green-outlined link labeled 'Tenant sign in' and other links 'NetApp support' and 'NetApp.com'.

- Page de connexion du Gestionnaire de locataires. Le champ **compte** est peut-être déjà renseigné, comme indiqué ci-dessous.



Tenant Manager

Recent

Account

Username

Password

Sign in

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

i. Si l'ID de compte à 20 chiffres du locataire ne s'affiche pas, sélectionnez le nom du compte du locataire s'il apparaît dans la liste des comptes récents ou saisissez l'ID du compte.

ii. Saisissez votre nom d'utilisateur et votre mot de passe.

iii. Sélectionnez **connexion**.

Le tableau de bord du gestionnaire de locataires s'affiche.

iv. Si vous avez reçu un mot de passe initial de la part d'une autre personne, sélectionnez **username > change password** 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

Entrez vos informations d'identification SSO standard et sélectionnez **se connecter**.

- Page de connexion SSO du Gestionnaire de locataires.

NetApp StorageGRID®

Tenant Manager

Recent

Account

Sign in

[NetApp support | NetApp.com](#)

- i. Si l'ID de compte à 20 chiffres du locataire ne s'affiche pas, sélectionnez le nom du compte du locataire s'il apparaît dans la liste des comptes récents ou saisissez l'ID du compte.
- ii. Sélectionnez **connexion**.
- iii. Connectez-vous à l'aide de vos identifiants SSO standard sur la page de connexion SSO de votre entreprise.

Le tableau de bord du gestionnaire de locataires s'affiche.

Déconnectez-vous du Gestionnaire de locataires

Lorsque vous avez terminé de travailler avec le Gestionnaire de locataires, vous devez

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

Étapes

1. Localisez la liste déroulante 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 au 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 accédiez. La page de connexion StorageGRID s'affiche. Le nom du compte de locataire que vous venez d'accéder est indiqué par défaut dans la liste déroulante **comptes récents** et le **ID de compte** du locataire s'affiche.



Si SSO est activé et que vous êtes également connecté à Grid Manager, vous devez également vous déconnecter de Grid Manager pour vous déconnecter de SSO.

Présentation du tableau de bord du gestionnaire de locataires

Le tableau de bord du gestionnaire de locataires présente la configuration d'un compte de locataire et la quantité d'espace utilisée par les objets dans les compartiments du locataire (S3) ou les conteneurs (Swift). Si le locataire dispose d'un quota, le tableau de bord indique la part du quota utilisée et la quantité restante. En cas d'erreurs liées au compte de tenant, les erreurs s'affichent dans le tableau de bord.



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

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

Dashboard

16 Buckets
[View buckets](#)

2 Platform services endpoints
[View endpoints](#)

0 Groups
[View groups](#)

1 User
[View users](#)

Storage usage [?](#)

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

Total objects

8,418,886

objects

Tenant details [?](#)

Name: Tenant02

ID: 3341 1240 0546 8283 2208

Platform services enabled

Can use own identity source

S3 Select enabled

Récapitulatif du compte de locataire

La partie supérieure du tableau de bord contient les informations suivantes :

- Le nombre de compartiments ou de conteneurs configurés, de groupes et d'utilisateurs
- Le nombre de terminaux de services de plate-forme, le cas échéant, ont été configurés

Vous pouvez sélectionner les liens pour afficher les détails.

Le côté droit du tableau de bord contient les informations suivantes :

- Nombre total d'objets pour le locataire.

Pour un compte S3, si aucun objet n'a été ingéré et que vous disposez de l'autorisation d'accès racine, les directives de démarrage s'affichent à la place du nombre total d'objets.

- Détails du locataire, y compris le nom et l'ID du compte de locataire, et si le locataire peut l'utiliser "services de plateforme", "son propre référentiel d'identité", "fédération des grilles", ou "S3 Select" (seules les autorisations activées sont répertoriées).

Utilisation du stockage et des quotas

Le panneau utilisation du stockage contient les informations suivantes :

- Volume des données d'objet pour le locataire.



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

- Si un quota est défini, la quantité totale d'espace disponible pour les données d'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 charger des objets et rejette les nouvelles ingère si le locataire a dépassé le quota. Cependant, StorageGRID ne prend pas en compte la taille du téléchargement actuel lors de la détermination du dépassement du quota. Si des objets sont supprimés, un locataire peut temporairement empêcher le téléchargement de nouveaux objets jusqu'au recalcul de l'utilisation du quota. Le calcul de l'utilisation des quotas peut prendre 10 minutes ou plus.

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

Vous pouvez placer le curseur sur n'importe quel segment de graphique pour afficher l'espace total utilisé par ce compartiment ou ce conteneur.



- Pour correspondre au graphique à barres, une liste des plus grands seaux ou conteneurs, y compris la quantité totale de données d'objet et le nombre d'objets pour chaque godet 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 compartiments ou conteneurs, tous les autres compartiments 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 des quotas ont été activées dans Grid Manager, elles s'affichent 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 **usage du quota de locataire élevé** est déclenchée. Effectuez les actions recommandées pour l'alerte.



Only 0.6% of the quota is remaining. If the quota is exceeded, you can no longer upload new objects.

Si vous dépassiez votre quota, vous ne pouvez pas télécharger de nouveaux objets.



The quota has been met. You cannot upload new objects.

Erreurs de point final

Si vous avez utilisé le gestionnaire de grille pour configurer un ou plusieurs points de terminaison pour les services de plateforme, le tableau de bord du gestionnaire de locataires 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 afficher des détails sur "erreurs de noeud final des services de plate-forme", Sélectionnez **noeuds finaux** pour afficher la page noeuds finaux.

API de gestion des locataires

Compréhension de l'API de gestion des locataires

Vous pouvez effectuer des tâches de gestion du système via l'API REST de gestion des locataires plutôt que dans l'interface utilisateur du gestionnaire de locataires. Par exemple, vous pouvez utiliser l'API pour automatiser les opérations ou créer plusieurs entités plus rapidement (par exemple, les utilisateurs).

L'API de gestion des locataires :

- Utilise la plate-forme 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 swagger fournit des détails complets et de la documentation pour chaque opération API.
- Utilisations "gestion des versions pour prendre en charge les mises à niveau sans interruption".

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

1. Connectez-vous au Gestionnaire de locataires.
2. Dans le haut du Gestionnaire de locataires, sélectionnez l'icône d'aide et sélectionnez **documentation API**.

Opérations d'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 pour effectuer l'authentification de session utilisateur.

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

Pour plus d'informations sur l'amélioration de la sécurité d'authentification, reportez-vous à la section "[Protéger contre la contrefaçon de demandes intersites](#)".



Si l'authentification unique (SSO) est activée pour le système StorageGRID, vous devez effectuer différentes étapes pour l'authentification. Voir la "[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 lister la version du produit ainsi que les versions principales de l'API prises en charge par cette version.
- **Conteneurs** : opérations sur les compartiments S3 ou les conteneurs Swift.
- **Désactivé-features** : opérations permettant d'afficher les fonctions qui auraient pu être désactivées.
- **Noeuds finaux** : opérations pour gérer un noeud final. Les terminaux permettent à un compartiment 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 de grille transversale.
- **Groupes** : opérations de gestion des groupes de locataires locaux et de récupération des groupes de locataires fédérés à partir d'un référentiel d'identité externe.
- **Identity-source** : opérations permettant de configurer un référentiel d'identité externe et de synchroniser manuellement les informations relatives au groupe fédéré et à l'utilisateur.
- **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 pour afficher et gérer les utilisateurs locataires.

Détails de l'opération

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

groups Operations on groups

GET /org/groups Lists Tenant User Groups

Parameters

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	Example Value Model

```
[{"responseTime": "2018-02-01T16:22:31.066Z", "status": "success", "apiVersion": "2.3"}]
```

Émettre des requêtes API



Toutes les opérations d'API que vous effectuez à l'aide de la page Web API Docs 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 afficher les détails de la demande.

2. Déterminez si la demande nécessite des paramètres supplémentaires, tels qu'un ID de groupe ou d'utilisateur. Ensuite, obtenir ces valeurs. Vous devrez peut-être d'abord lancer une autre demande d'API pour obtenir les informations dont vous avez besoin.
3. Déterminez si vous devez modifier l'exemple de corps de la demande. Si c'est le cas, vous pouvez sélectionner **modèle** pour connaître les exigences de chaque champ.
4. Sélectionnez **essayez-le**.
5. Fournir tous les paramètres requis ou modifier le corps de la demande selon les besoins.
6. Sélectionnez **Exécuter**.
7. Vérifiez 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 la gestion des versions pour prendre en charge les mises à niveau sans interruption.

Par exemple, cette URL de demande spécifie la version 3 de l'API.

`https://hostname_or_ip_address/api/v3/authorize`

La version principale de l'API de gestion des locataires est incrémentée lorsque des modifications sont effectuées et que *non compatibles* sont apportées aux versions antérieures. La version mineure de l'API de gestion des locataires est incrémentée lorsque des modifications qui sont *compatibles* avec les versions antérieures sont effectuées. Les modifications compatibles incluent l'ajout de nouveaux noeuds finaux ou de nouvelles propriétés. L'exemple suivant illustre comment la version de l'API est incrémentée en fonction du type de modifications apportées.

Type de modification de l'API	Ancienne version	Nouvelle version
Compatible avec les versions plus anciennes	2.1	2.2
Non compatible avec les versions plus anciennes	2.1	3.0

Lors de la première installation du logiciel StorageGRID, seule la version la plus récente de l'API de gestion des locataires est activée. Cependant, lorsque StorageGRID est mis à niveau vers une nouvelle version de fonction, vous continuez à accéder à l'ancienne version de l'API pour au moins une version de StorageGRID.

Les requêtes obsolètes sont marquées comme obsolètes de l'une des manières suivantes :

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

Identification des versions d'API prises en charge dans la version actuelle

Utilisez la requête d'API suivante pour renvoyer une liste des versions principales de l'API prises en charge :

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

Spécifiez la version de l'API pour la demande

Vous pouvez spécifier la version de l'API à l'aide d'un paramètre de chemin d'accès (/api/v3) ou un en-tête (Api-Version: 3). Si vous indiquez les deux valeurs, la valeur de l'en-tête remplace la valeur du chemin d'accès.

```
curl https://<IP-Address>/api/v3/grid/accounts
```

```
curl -H "Api-Version: 3" https://<IP-Address>/api/grid/accounts
```

Protection contre la contrefaçon de demandes intersites (CSRF)

Vous pouvez vous protéger contre les attaques de contrefaçon de requêtes intersites (CSRF) contre StorageGRID en utilisant des jetons CSRF pour améliorer l'authentification qui utilise des cookies. Grid Manager et tenant Manager activent automatiquement cette fonction de sécurité ; les autres clients API peuvent choisir de l'activer lorsqu'ils se connectent.

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

StorageGRID contribue à la protection contre les attaques CSRF en utilisant des jetons CSRF. Lorsque cette option 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 fonction, définissez l' `csrfToken` paramètre à `true` pendant 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"
```

Si vrai, un GridCsrfToken Le cookie est défini avec une valeur aléatoire pour les connexions dans Grid Manager et dans AccountCsrfToken Le cookie est défini avec une valeur aléatoire pour les connexions au Gestionnaire de locataires.

Si le cookie est présent, toutes les demandes pouvant modifier l'état du système (POST, PUT, PATCH, DELETE) doivent inclure l'une des options suivantes :

- Le X-Csrf-Token En-tête, avec la valeur de l'en-tête définie sur la valeur du cookie de jeton CSRF.
- Pour les noeuds finaux qui acceptent un corps codé par formulaire : a csrfToken paramètre corps de demande codé par formulaire.

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



Les demandes disposant d'un jeu de cookies de jeton CSRF appliquent également le "Content-Type: application/json" En-tête pour toute demande qui attend un corps de requête JSON comme une protection supplémentaire contre les attaques CSRF.

Utiliser les connexions de fédération de grille

Cloner des groupes de locataires et des utilisateurs

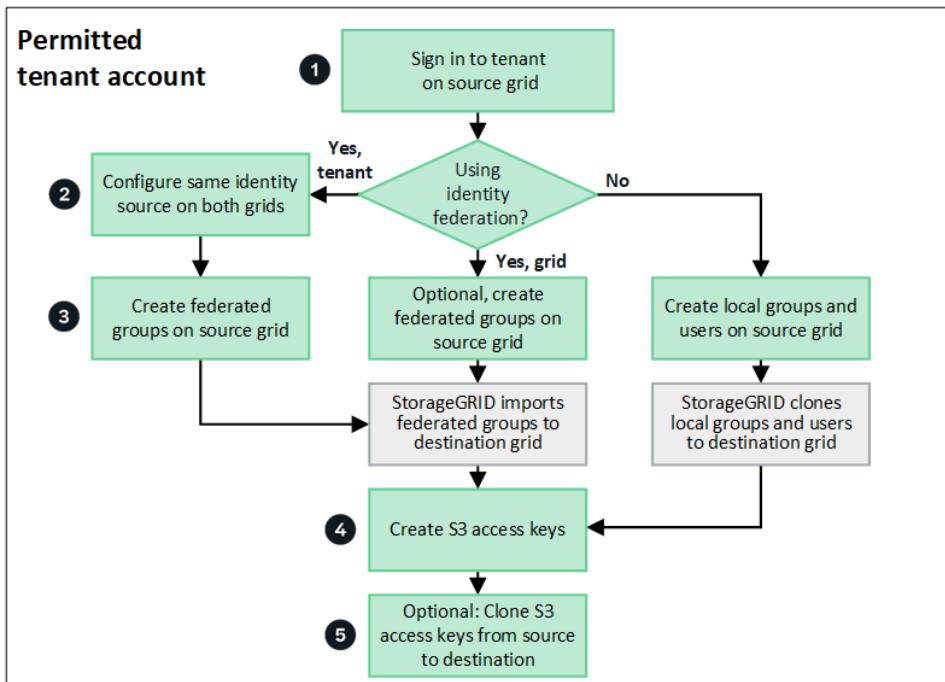
Si un nouveau locataire est autorisé à utiliser une connexion de fédération de grille, ce dernier est répliqué d'un système StorageGRID vers un autre système StorageGRID lors de sa création. Une fois le locataire répliqué, tous les groupes et utilisateurs ajoutés au locataire source sont clonés dans le locataire de destination.

Le système StorageGRID dans lequel le tenant est créé à l'origine est *source GRID* du tenant. Le système StorageGRID dans lequel le locataire est répliqué est la *grille de destination* du locataire. Les deux comptes de tenant possèdent les mêmes ID de compte, nom, description, quota de stockage et 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 clone de compte](#)" et "[Gérer les locataires autorisés](#)".

Le clonage des informations de compte de locataire est requis pour "[réPLICATION ENTRE PLUSIEURS GRILLES](#)" d'objets de compartiment. Le fait de disposer des mêmes groupes de locataires et utilisateurs sur les deux grilles vous permet d'accéder aux compartiments et objets correspondants sur l'une ou l'autre grille.

Workflow des locataires pour le clone de compte

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



Voici les principales étapes du flux de travail :

1

Connectez-vous au locataire

Connectez-vous au compte de locataire sur la grille source (la grille dans laquelle le locataire a été initialement créé).

2

Vous pouvez également configurer la fédération des identités

Si votre compte de tenant dispose de l'autorisation **utiliser son propre référentiel d'identité** pour utiliser des groupes et des utilisateurs fédérés, configurez le même référentiel d'identité (avec les mêmes paramètres) pour les comptes de tenant source et de destination. Les groupes et utilisateurs fédérés ne peuvent pas être clonés à moins que les deux grilles n'utilisent le même référentiel d'identité. Pour obtenir des instructions, reportez-vous à la section "[Utiliser la fédération des identités](#)".

3

Créer des groupes et des utilisateurs

Lorsque vous créez des groupes et des utilisateurs, commencez toujours par la grille source du locataire. Lorsque vous ajoutez un nouveau groupe, StorageGRID le clone automatiquement dans la grille de destination.

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

4

Création de clés d'accès S3

C'est possible "[créez vos propres clés d'accès](#)" ou à "[créez les clés d'accès d'un autre utilisateur](#)" sur la grille source ou de destination pour accéder aux compartiments de cette grille.

5

Vous pouvez également cloner les clés d'accès S3

Si vous avez besoin d'accéder à des compartiments avec les mêmes clés d'accès sur les deux grilles, créez les clés d'accès sur la grille source, puis utilisez l'API du gestionnaire de locataires pour les cloner manuellement dans la grille de destination. Pour obtenir des instructions, reportez-vous à la section "["Cloner les clés d'accès S3 à l'aide de l'API"](#)".

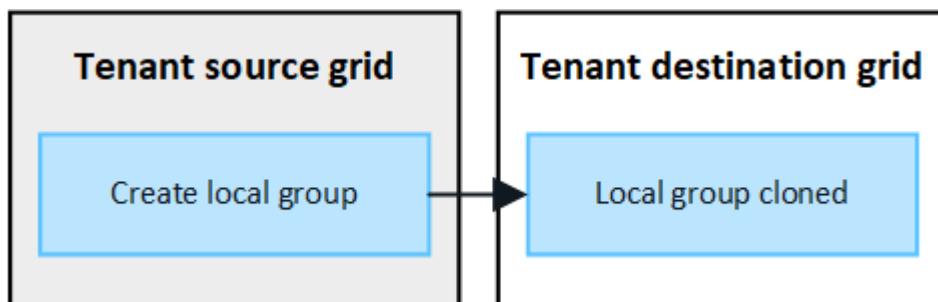
Comment les groupes, les utilisateurs et les clés d'accès S3 sont-ils clonés ?

Dans cette section, vous apprendrez comment les groupes, les utilisateurs et les clés d'accès S3 sont clonés entre la grille source des locataires et la grille de destination des locataires.

Les groupes locaux créés dans 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 dans la grille de destination du locataire.

Le groupe d'origine et le clone disposent des mêmes mode d'accès, autorisations de groupe et règles de groupe S3. Pour obtenir des instructions, reportez-vous à la section "["Créez des groupes pour les locataires S3"](#)".

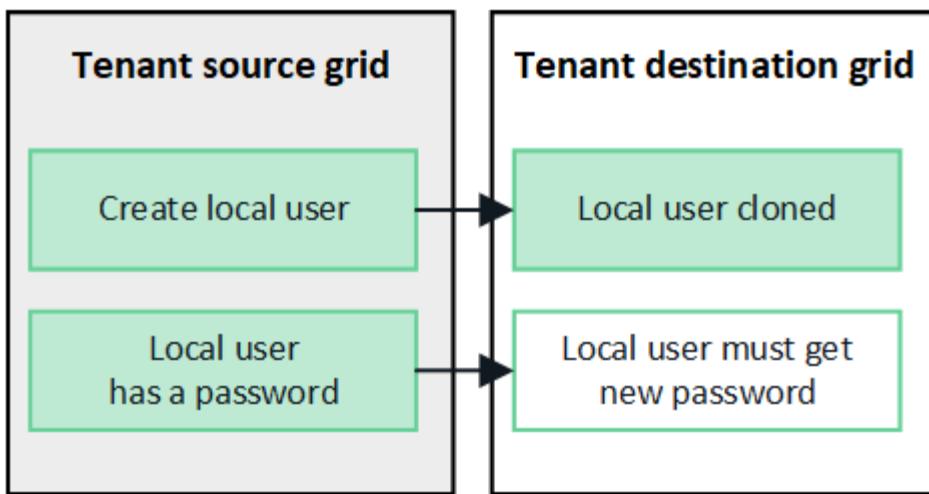


Tous les utilisateurs sélectionnés lors de la création d'un groupe local sur la grille source ne sont pas inclus lorsque le groupe est cloné dans la grille de destination. Pour cette raison, ne sélectionnez pas d'utilisateurs lorsque vous créez le groupe. Sélectionnez plutôt le groupe lorsque vous créez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

Les utilisateurs locaux créés dans la grille source sont clonés

Lorsque vous créez un utilisateur local sur la grille source, StorageGRID le clone automatiquement dans la grille de destination. L'utilisateur d'origine et son clone ont tous les deux le même nom complet, le même nom d'utilisateur et le même paramètre **deny Access**. Les deux utilisateurs appartiennent également aux mêmes groupes. Pour obtenir des instructions, reportez-vous à la section "["Gérez 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 au gestionnaire de locataires sur la grille de destination, l'utilisateur root du compte de locataire doit ajouter un mot de passe pour cet utilisateur sur la grille de destination. Pour obtenir des instructions, reportez-vous à la section "["Gérez les utilisateurs locaux"](#)".

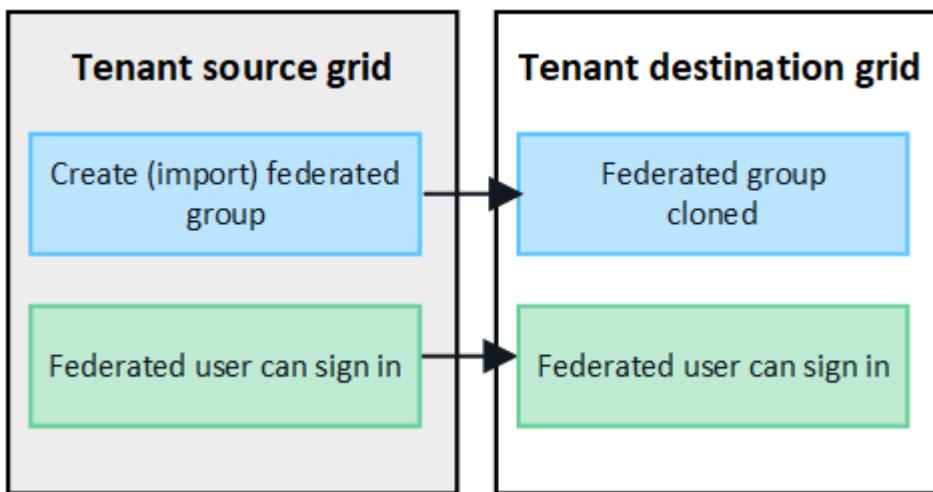


Les groupes fédérés créés dans la grille source sont clonés

Suppose les conditions requises pour l'utilisation du clone du compte avec "[authentification unique](#)" et "[fédération des identités](#)" ont été réunis, les groupes fédérés que vous créez (importez) pour le locataire sur la grille source sont automatiquement clonés dans le locataire sur la grille de destination.

Les deux groupes disposent des mêmes mode d'accès, autorisations de groupe et règles de groupe S3.

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

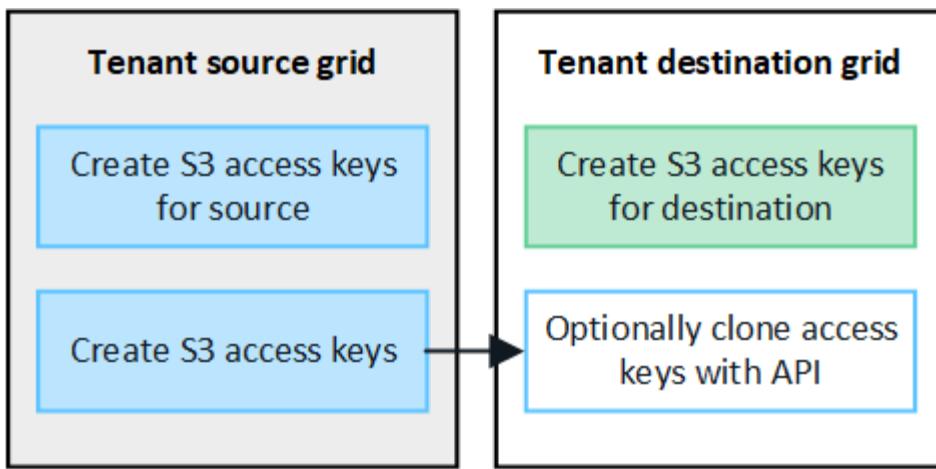


Les clés d'accès S3 peuvent être clonées manuellement

StorageGRID ne clone pas automatiquement les clés d'accès S3, car la sécurité est améliorée grâce à l'utilisation de clés différentes sur chaque grille.

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

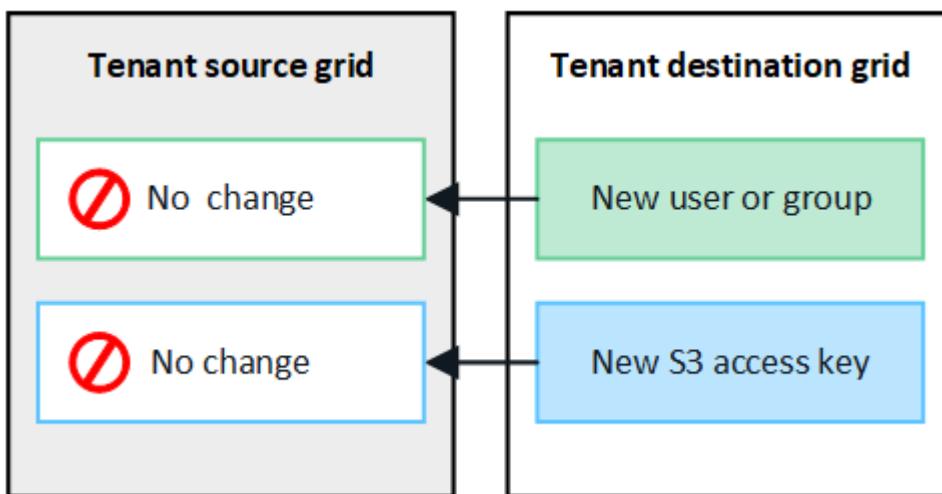
- Si vous n'avez pas besoin d'utiliser les mêmes touches pour chaque grille, vous pouvez le faire "[créez vos propres clés d'accès](#)" ou "[créez les clés d'accès d'un autre utilisateur](#)" sur chaque grille.
- Si vous devez utiliser les mêmes clés sur les deux grilles, vous pouvez créer des clés sur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



Lorsque vous clonez les clés d'accès S3 d'un utilisateur fédéré, ces deux clés sont clonées dans le locataire de destination.

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

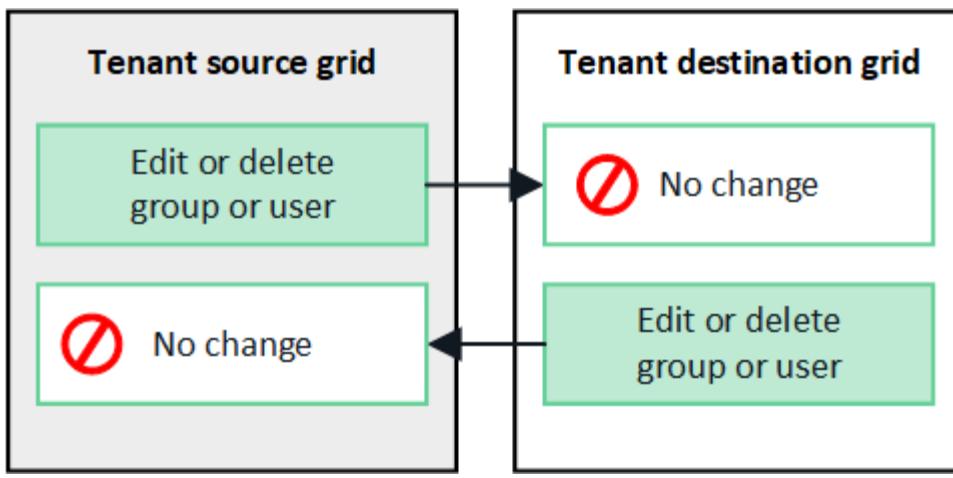
Le clonage s'effectue uniquement depuis la grille source du locataire vers la grille de destination du locataire. Si vous créez ou importez des groupes et des utilisateurs sur la grille de destination du locataire, StorageGRID ne les clone pas dans la grille source du locataire.



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

Le clonage a lieu 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 de fédération grid**, vous pouvez utiliser l'API de gestion des locataires pour cloner manuellement les clés d'accès S3 du locataire de la grille source vers le locataire de la grille de destination.

Avant de commencer

- Le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille**.
- La connexion de fédération de grille a un **état 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 autorisations d'accès racine](#)".
- Si vous clonez des clés d'accès pour un utilisateur local, l'utilisateur existe déjà sur les deux grilles.



Lorsque vous clonez les clés d'accès S3 d'un utilisateur fédéré, ces deux clés sont ajoutées 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

- À l'aide du gestionnaire de locataires sur la grille source, "[créez vos propres clés d'accès](#)" et téléchargez le .csv fichier.
- Dans le haut du Gestionnaire de locataires, sélectionnez l'icône d'aide et sélectionnez **documentation API**.
- Dans la section **s3**, sélectionnez le noeud final 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 **essayez-le**.
5. Dans la zone de texte **body**, remplacez les entrées d'exemple pour **accesskey** et **secretAccessKey** par les valeurs du fichier **.csv** que vous avez téléchargé.

Veuillez à conserver les guillemets doubles autour de chaque chaîne.

```
{
  "accessKey": "AKIAIOSFODNN7EXAMPLE",
  "secretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
  "expires": "2028-09-04T00:00:00.000Z"
}
```

6. Si la clé expire, remplacez l'exemple de **expire** par la date et l'heure d'expiration sous forme de chaîne au format de données 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. Vérifiez que le code de réponse du serveur est **204**, ce qui indique que la clé a été correctement clonée dans 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. À l'aide du gestionnaire de locataires sur la grille source, "[Créez les clés d'accès S3 de l'autre utilisateur](#)" et téléchargez le **.csv** fichier.
2. Dans le haut du Gestionnaire de locataires, sélectionnez l'icône d'aide et sélectionnez **documentation API**.
3. Obtenez l'ID utilisateur. Vous aurez besoin de cette valeur pour cloner les clés d'accès des autres utilisateurs.
 - a. Dans la section **Users**, sélectionnez le noeud final suivant :

```
GET /org/users
```

 - b. Sélectionnez **essayez-le**.
 - 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 noeud final suivant :

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

POST </org/users/{userId}/replicate-s3-access-key> Clone an S3 key to the other grids.

5. Sélectionnez **essayez-le**.
6. Dans la zone de texte **userid**, collez l'ID utilisateur que vous avez copié.
7. Dans la zone de texte **body**, remplacez les entrées d'exemple pour **example Access key** et **secret Access key** par les valeurs du fichier **.csv** pour cet utilisateur.

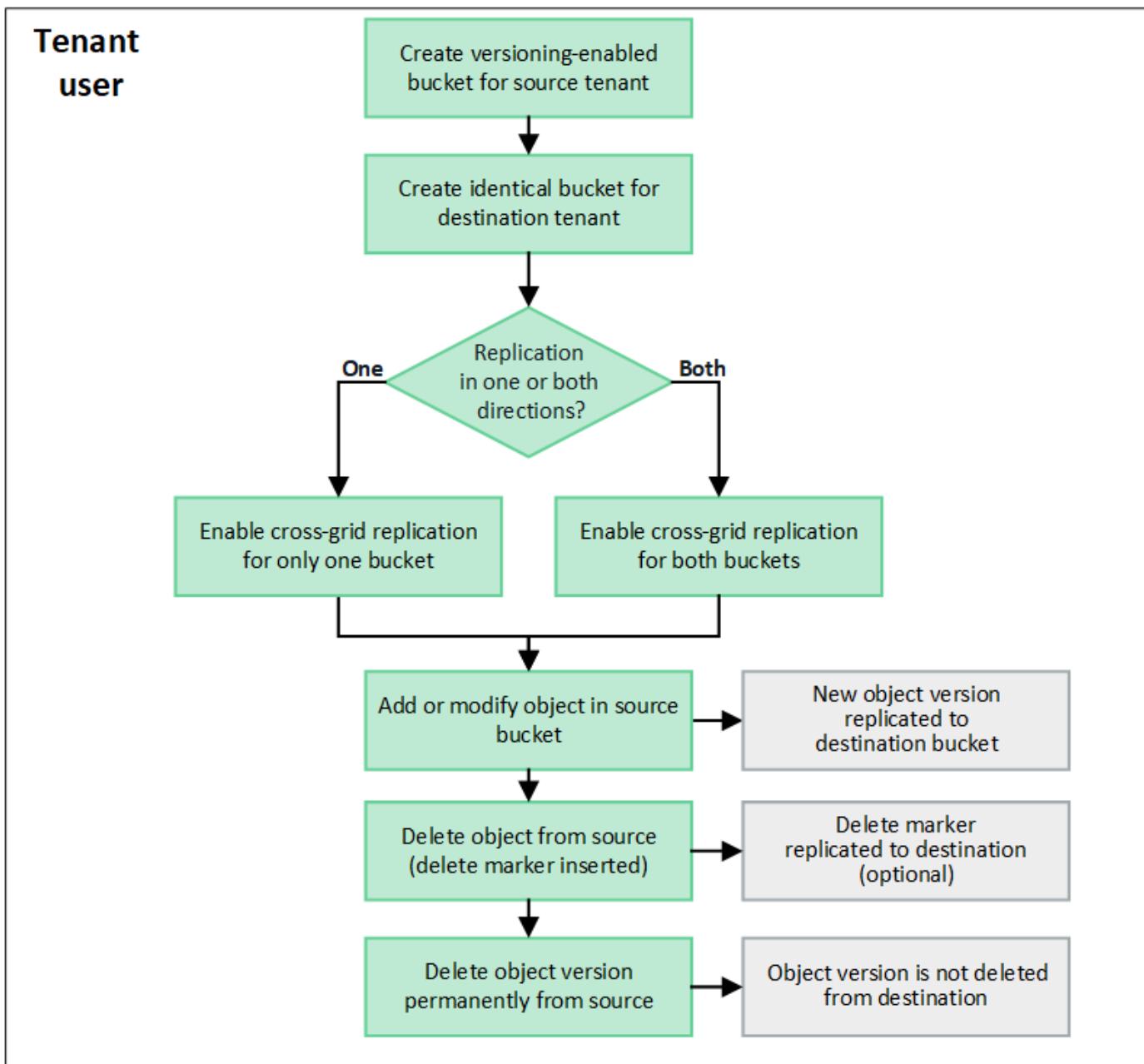
Veillez à conserver les guillemets doubles autour de la chaîne.
8. Si la clé expire, remplacez l'exemple de **expire** par la date et l'heure d'expiration sous forme de chaîne au format de données ISO 8601 (par exemple, 2023-02-28T22:46:33-08:00). Si la clé n'expire pas, entrez **null** comme valeur pour l'entrée **Expires** (ou supprimez la ligne **Expires** et la virgule précédente).
9. Sélectionnez **Exécuter**.
10. Vérifiez que le code de réponse du serveur est **204**, ce qui indique que la clé a été correctement clonée dans la grille de destination.

Gérer la réPLICATION entre les grilles

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

Flux de production pour la réPLICATION entre les grilles

Le diagramme de flux de travail récapitule les étapes que vous allez effectuer pour configurer la réPLICATION inter-grille entre les compartiments sur deux grilles. Ces étapes sont décrites plus en détail ci-dessous.



Configurer la réplication entre les grilles

Avant de pouvoir utiliser la réplication multigrille, vous devez vous connecter aux comptes de locataires correspondants sur chaque grille et créer des compartiments identiques. Vous pouvez ensuite activer la réplication entre les grilles sur l'un ou l'autre des compartiments, ou sur les deux.

Avant de commencer

- Vous avez examiné les exigences relatives à la réplication intergrid. Voir "[Qu'est-ce que la réplication cross-grid](#)".
- Vous utilisez un "[navigateur web pris en charge](#)".
- Le compte de tenant possède l'autorisation **utiliser la connexion de fédération de grille** et des comptes de tenant identiques existent sur les deux grilles. Voir "[Gérez les locataires autorisés pour la connexion de fédération de grille](#)".
- L'utilisateur locataire auquel vous vous connectez, car il existe déjà sur les deux grilles et appartient à un groupe d'utilisateurs qui possède le "[Autorisation d'accès racine](#)".

- 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 compartiments identiques

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

Étapes

1. En commençant à partir de l'une des grilles de la connexion de fédération de grille, créez un nouveau compartiment :
 - a. Connectez-vous au compte de tenant à l'aide des informations d'identification d'un utilisateur de tenant 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, vérifiez que l'utilisateur root du compte locataire a défini un mot de passe pour votre compte utilisateur.

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

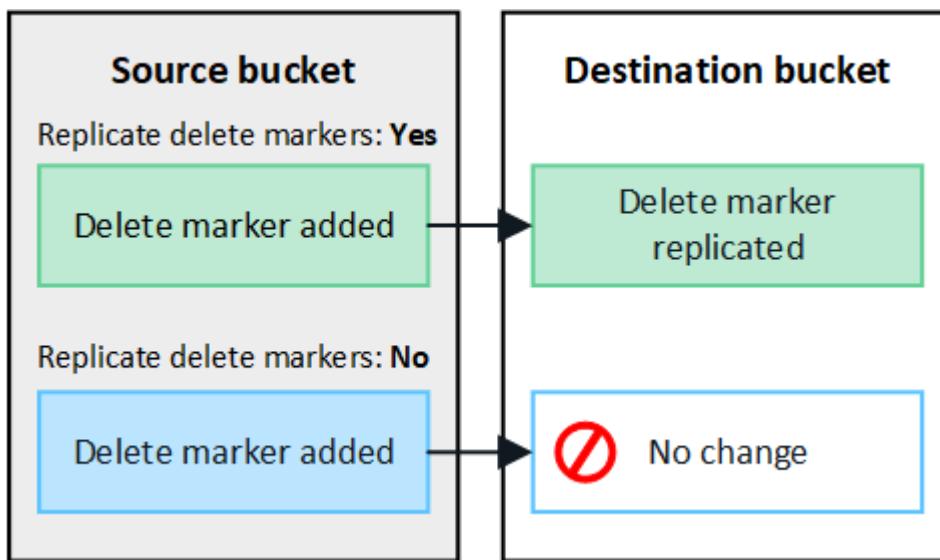
Activer la réPLICATION entre les grilles

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

Étapes

1. À partir d'une grille dont vous souhaitez répliquer les objets, activez "[réPLICATION multigrille dans une direction](#)":
 - a. Connectez-vous au compte du locataire pour le compartiment.
 - b. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Compartiments**.
 - c. Sélectionnez le nom du compartiment dans le tableau pour accéder à la page de détails du compartiment.
 - d. Sélectionnez l'onglet **RéPLICATION multigrille**.
 - e. Sélectionnez **Activer** et consultez la liste des exigences.
 - f. Si toutes les exigences ont été satisfaites, sélectionnez la connexion de fédération de grille que vous souhaitez utiliser.
 - g. Vous pouvez également modifier le paramètre **replicate delete markers** pour déterminer ce qui se passe sur la grille de destination si un client S3 envoie une demande de suppression à la grille source qui n'inclut pas d'ID de version :

- Si **Yes** (par défaut), un marqueur de suppression est ajouté au compartiment source et répliqué dans le compartiment de destination.
- Si **non**, un marqueur de suppression est ajouté au compartiment source mais n'est pas répliqué dans le compartiment de destination.



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

Voir "[Qu'est-ce que la réPLICATION cross-grid](#)" pour plus d'informations.

- a. Vérifiez vos sélections. Vous ne pouvez pas modifier ces paramètres à moins que les deux compartiments ne soient vides.
- b. Sélectionnez **Activer et tester**.

Après quelques instants, un message de réussite s'affiche. Les objets ajoutés à ce compartiment seront désormais automatiquement répliqués sur l'autre grille. **La réPLICATION multigrille** est affichée sous la forme d'une fonction activée sur la page de détails du compartiment.

2. Si vous le souhaitez, accédez au compartiment correspondant sur l'autre grille et "[activez la réPLICATION entre les grilles dans les deux sens](#)".

Tester la réPLICATION entre les grilles

Si la réPLICATION inter-grid est activée pour un compartiment, vous devrez peut-être vérifier que la connexion et la réPLICATION inter-grid fonctionnent correctement et que les compartiments source et de destination répondent toujours à toutes les exigences (par exemple, la gestion des versions est toujours activée).

Avant de commencer

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

Étapes

1. Connectez-vous au compte du locataire pour le compartiment.

2. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.
3. Sélectionnez le nom du compartiment dans le tableau pour accéder à la page de détails du compartiment.
4. Sélectionnez l'onglet **réPLICATION multigrille**.
5. Sélectionnez **Tester la connexion**.

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

6. Si la réPLICATION inter-grille est configurée pour se produire dans les deux sens, allez dans le compartiment 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 entre les grilles

Vous pouvez arrêter définitivement la réPLICATION multigrille si vous ne souhaitez plus copier d'objets sur l'autre grille.

Avant de désactiver la réPLICATION multigrille, notez ce qui suit :

- La désactivation de la réPLICATION multigrille ne supprime pas les objets qui ont déjà été copiés entre les grilles. Par exemple, les objets dans my-bucket Sur la grille 1 qui a été copiée dans my-bucket Sur la grille 2 ne sont pas supprimés si vous désactivez la réPLICATION inter-grid pour ce compartiment. Si vous souhaitez supprimer ces objets, vous devez les supprimer manuellement.
- Si la réPLICATION inter-grid a été activée pour chacun des compartiments (c'est-à-dire si la réPLICATION se produit dans les deux directions), vous pouvez désactiver la réPLICATION inter-grid pour l'un ou les deux compartiments. Par exemple, vous pouvez 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 à partir de my-bucket Sur la grille 2 à my-bucket Sur la grille 1.
- Vous devez désactiver la réPLICATION multigrille 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-grid pour un compartiment contenant des objets, vous ne pourrez pas réactiver la réPLICATION inter-grid à moins de supprimer tous les objets des compartiments source et de destination.



Vous ne pouvez pas réactiver la réPLICATION sauf si les deux compartiments sont 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 racine"](#)".

Étapes

1. Depuis la grille dont vous ne souhaitez plus répliquer les objets, arrêtez la réPLICATION inter-grid pour le compartiment :
 - a. Connectez-vous au compte du locataire pour le compartiment.
 - b. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.

- c. Sélectionnez le nom du compartiment dans le tableau pour accéder à la page de détails du compartiment.
- d. Sélectionnez l'onglet **réPLICATION multigrille**.
- e. Sélectionnez **Désactiver la réPLICATION**.
- f. Si vous êtes sûr de vouloir désactiver la réPLICATION inter-grille pour ce compartiment, tapez **Yes** dans la zone de texte et sélectionnez **Disable**.

Après quelques instants, un message de réussite s'affiche. Les nouveaux objets ajoutés à ce compartiment ne peuvent plus être automatiquement répliqués sur l'autre grille. **La réPLICATION multigrille** n'est plus affichée comme fonction activée sur la page Compartiments.

2. Si la réPLICATION inter-grille a été configurée pour se produire dans les deux directions, allez dans le compartiment correspondant sur l'autre grille et arrêtez la réPLICATION inter-grille dans l'autre direction.

Afficher les connexions de fédération de grille

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

Avant de commencer

- Le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille**.
- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Autorisation d'accès racine](#)".

Étapes

1. Sélectionnez **STORAGE (S3) > Grid federation connections**.

La page de connexion de fédération de grille s'affiche et comprend un tableau qui résume les informations suivantes :

Colonne	Description
Nom de la connexion	Les connexions de fédération de grille que ce locataire a l'autorisation d'utiliser.
Compartiments avec réPLICATION inter-grid	Pour chaque connexion de fédération de grid, les compartiments de locataire pour lesquels la réPLICATION inter-grid est activée. Les objets ajoutés à ces compartiments seront répliqués sur l'autre grille de la connexion.
Dernière erreur	Pour chaque connexion de fédération de grille, l'erreur la plus récente se produit, le cas échéant, lors de la réPLICATION des données vers l'autre grille. Voir Effacez la dernière erreur .

2. Si vous le souhaitez, sélectionnez un nom de compartiment "[afficher les détails du compartiment](#)".

[effacez la dernière erreur](#)

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

- La version de l'objet source est introuvable.
- Le compartiment source est introuvable.
- Le compartiment de destination a été supprimé.
- Le compartiment de destination a été recréé par un autre compte.
- La gestion des versions du compartiment de destination est suspendue.
- Le compartiment de destination a été recréé par le même compte, mais il n'est plus versionné.



Cette colonne affiche uniquement la dernière erreur de réPLICATION inter-grille à se produire ; les erreurs précédentes qui se sont peut-être produites 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 compartiment de destination de la réPLICATION inter-grid était dans un état non valide, probablement parce que la gestion de version a été suspendue ou que le verrouillage d'objet S3 a été activé.

The screenshot shows a table titled "Grid federation connections" with one row of data. The columns are "Connection name", "Buckets with cross-grid replication", and "Last error". The "Connection name" column contains "Grid 1-Grid 2". The "Buckets with cross-grid replication" column contains "my-cgr-bucket". The "Last error" column contains the following text:

```

2022-12-07 16:02:20 MST
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)

```

2. Effectuez toutes les actions recommandées. Par exemple, si la gestion des versions a été suspendue dans le compartiment de destination pour la réPLICATION inter-grid, réactivez la gestion des versions pour ce compartiment.
3. Sélectionnez la connexion dans le tableau.
4. Sélectionnez **Effacer erreur**.
5. Sélectionnez **Oui** pour effacer le message et mettre à jour l'état du système.
6. Patiencez 5-6 minutes, puis ingérer un nouvel objet dans le compartiment. 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 dans le message avant d'ingérer un nouvel objet.

7. Pour déterminer si des objets n'ont pas pu être répliqués en raison d'une erreur de compartiment, reportez-vous à la section "[Identifier et réessayer les opérations de réPLICATION ayant échoué](#)".

Gestion des groupes et des utilisateurs

Utiliser la fédération des identités

L'utilisation de la fédération des identités accélère la configuration des groupes de locataires et des utilisateurs, et permet aux utilisateurs de se connecter au compte du locataire à l'aide des identifiants familiers.

Configurez la fédération des identités pour le gestionnaire des locataires

Vous pouvez configurer la fédération des identités pour le Gestionnaire de locataires si vous souhaitez que les groupes et les utilisateurs de locataires 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 Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Autorisation d'accès racine](#)".
- Vous utilisez Active Directory, Azure AD, OpenLDAP ou Oracle Directory Server comme fournisseur d'identité.



Si vous souhaitez utiliser un service LDAP v3 non répertorié, contactez le support technique.

- Si vous avez l'intention d'utiliser OpenLDAP, vous devez configurer le serveur OpenLDAP. Voir [Instructions de configuration du serveur OpenLDAP](#).
- Si vous prévoyez d'utiliser TLS (transport Layer Security) pour les communications avec le serveur LDAP, le fournisseur d'identité doit utiliser TLS 1.2 ou 1.3. Voir "[Chiffrement pris en charge pour les connexions TLS sortantes](#)".

Description de la tâche

La configuration d'un service de fédération des identités pour votre locataire dépend de la configuration de votre compte locataire. Votre locataire peut partager le service de fédération des identités configuré pour Grid Manager. Si ce message s'affiche lorsque vous accédez à la page Fédération des identités, vous ne pouvez pas configurer un référentiel d'identité fédéré distinct 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.

Entrez la configuration

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

Étapes

1. Sélectionnez **ACCESS MANAGEMENT > identity federation**.
2. Sélectionnez **Activer la fédération d'identités**.
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.

- Si vous avez sélectionné **autre**, renseignez les champs de la section attributs LDAP. Dans le cas contraire, passez à l'étape suivante.

- Nom unique utilisateur** : 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 d'utilisateur** : 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 de groupe** : 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** : nom de l'attribut qui contient l'identificateur 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.

- Pour tous les types de services LDAP, entrez les informations de connexion réseau et de serveur LDAP 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** : port utilisé pour se connecter au serveur LDAP.



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

- Nom d'utilisateur** : 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 bas niveau ou le nom principal d'utilisateur.

L'utilisateur spécifié doit être autorisé à répertorier les groupes et les utilisateurs et à accéder aux attributs suivants :

- `sAMAccountName` ou `uid`

- objectGUID, entryUUID, ou nsuniqueid
- cn
- memberOf ou isMemberOf
- **Active Directory** : objectSid, primaryGroupID, userAccountControl, et userPrincipalName
- **Azure**: accountEnabled et userPrincipalName
- **Mot de passe** : mot de passe associé au nom d'utilisateur.
- **DN de base de groupe** : chemin complet du nom distinctif (DN) pour une sous-arborescence LDAP que vous voulez 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=exemple,DC=com) peuvent être utilisés comme groupes fédérés.



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

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



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

- **Bind username format** (facultatif) : le nom d'utilisateur par défaut StorageGRID devrait utiliser si le modèle ne peut pas être déterminé automatiquement.

Il est recommandé de fournir le format **Bind username** car il peut permettre aux utilisateurs de se connecter si StorageGRID ne parvient pas à se lier avec le compte de service.

Entrez l'un des motifs suivants :

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

Inclure **[NOM D'UTILISATEUR]** exactement comme écrit.

6. Dans la section transport Layer Security (TLS), sélectionnez un paramètre de sécurité.

- **Utilisez 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.
- **Utilisez 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.

- **Utilisez le certificat CA du système d'exploitation** : utilisez le certificat CA de la grille par défaut installé sur le système d'exploitation pour sécuriser les connexions.
- **Utilisez un certificat d'autorité de certification 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 de l'autorité de certification.

Testez la connexion et enregistrez 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 de nom d'utilisateur BIND, 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 connexion réussie » s'affiche si les paramètres de connexion sont valides. Sélectionnez **Enregistrer** pour enregistrer la configuration.
 - Un message « Impossible d'établir la connexion test » s'affiche si les paramètres de connexion ne sont pas valides. Sélectionnez **Fermer**. Ensuite, résolvez tout problème et testez à nouveau la connexion.
3. Si vous avez fourni un format de nom d'utilisateur BIND, entrez le nom d'utilisateur et le mot de passe d'un utilisateur fédéré valide.

Par exemple, entrez votre nom d'utilisateur et votre mot de passe. N'incluez pas de caractères spéciaux dans le nom d'utilisateur, tels que @ ou /.

The screenshot shows a 'Test Connection' dialog box. At the top, it says 'Test Connection' and has a close button. Below that, there's a note: '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.' There are two input fields: 'Test username' containing 'myusername' and 'Test password' containing redacted text. Below the password field is a visibility toggle icon. At the bottom, there are 'Cancel' and 'Test Connection' buttons.

- Un message « Test connexion réussie » 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 du test sont incorrects. Résolvez tout problème et testez à nouveau la connexion.

Forcer la synchronisation avec le référentiel d'identité

Le système StorageGRID synchronise régulièrement les groupes fédérés et les utilisateurs à partir du référentiel d'identité. Vous pouvez forcer la synchronisation à démarrer si vous souhaitez activer ou restreindre les autorisations utilisateur le plus rapidement possible.

Étapes

1. Accédez à la page fédération des identités.
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 synchronisation de la fédération d'identités** est déclenchée en cas de problème de synchronisation des groupes fédérés et des utilisateurs à partir du référentiel d'identité.

Désactiver la fédération des identités

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

Description de la tâche

Avant de désactiver la fédération des identités, vous devez prendre connaissance des points suivants :

- Les utilisateurs fédérés ne pourront pas se connecter.
- Les utilisateurs fédérés qui sont actuellement connectés conservent 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 le référentiel d'identité ne se produira pas et des alertes ou des alarmes ne seront pas émises pour les comptes qui n'ont pas été synchronisés.
- La case **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 connexion unique doit être **désactivé** avant de pouvoir désactiver la fédération d'identités. Voir "["Désactiver l'authentification unique"](#)".

Étapes

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

Instructions de configuration du serveur OpenLDAP

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



Pour les référentiels 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 les clés S3 de l'utilisateur ou supprimez l'utilisateur de tous les groupes.

Recouvrements de memberOf et de raffint

Les recouvrements de membre et de raffinement doivent être activés. Pour plus d'informations, reportez-vous aux instructions relatives à la maintenance de l'adhésion au groupe inverse dans le <http://www.openldap.org/doc/admin24/index.html>["Documentation OpenLDAP : version 2.4 - Guide de l'administrateur"].

Indexation

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.

Reportez-vous aux informations relatives à la maintenance de l'adhésion au groupe inverse dans le <http://www.openldap.org/doc/admin24/index.html>["Documentation OpenLDAP : version 2.4 - Guide de l'administrateur"].

Gestion des groupes de locataires

Créez 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 Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Autorisation d'accès racine](#)".
- Si vous prévoyez d'importer un groupe fédéré, vous avez "[fédération des identités configurée](#)", et le groupe fédéré existe déjà dans le référentiel d'identité configuré.
- Si votre compte locataire dispose de l'autorisation **utiliser la connexion de 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.

Accédez à l'assistant de création de groupe

Pour la première étape, accédez à l'assistant de création de groupe.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT > Groups**.
2. Si votre compte locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, vérifiez qu'une bannière bleue s'affiche, 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 pouvez être connecté à la grille de destination du locataire.

Groups

Create and manage local and federated groups. Set group permissions to control access to specific pages and features.

0 groups

Create group

Actions ▾

i This tenant has **Use grid federation connection** permission for connection Grid 1 to Grid 2. New local tenant groups will be automatically cloned to the same tenant on the other grid in the connection. If you edit or remove a group, your changes will not be synced to the other grid.

3. Sélectionnez **Créer 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 du référentiel d'identité configuré précédemment.

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 les applications client pour gérer les ressources du locataire, en fonction des autorisations de groupe.

2. Entrez le nom du groupe.

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



Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, une erreur de clonage se produit 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 à l' `sAMAccountName` attribut. Pour OpenLDAP, le nom unique est le nom associé à `uid` attribut.

3. Sélectionnez **Continuer**.

Gérer les autorisations de groupe

Les autorisations de groupe contrôlent les tâches que les utilisateurs peuvent effectuer dans le Gestionnaire de locataires et l'API de gestion des locataires.

Étapes

1. Pour **Access mode**, sélectionnez l'une des options suivantes :

- **Lecture-écriture** (par défaut) : les utilisateurs peuvent se connecter au gestionnaire de locataires et gérer la configuration du locataire.

- **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent pas apporter de modifications ni exécuter d'opérations dans le gestionnaire de locataires ou l'API de gestion des locataires. 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 dispose d'un accès en lecture seule à tous les paramètres et fonctions sélectionnés.

2. Sélectionnez une ou plusieurs autorisations pour ce groupe.

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

3. Sélectionnez **Continuer**.

Définissez la règle de groupe S3

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

Étapes

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

Stratégie de groupe	Description
Aucun accès à S3	Par défaut. Les utilisateurs de ce groupe n'ont pas accès aux ressources S3, sauf si l'accès est accordé avec une règle de compartiment. Si vous sélectionnez cette option, seul l'utilisateur root peut accéder aux ressources S3 par défaut.
Accès en lecture seule	Les utilisateurs de ce groupe disposent d'un accès en lecture seule aux ressources S3. Par exemple, les utilisateurs de ce groupe peuvent afficher la liste des objets et lire les données d'objet, les métadonnées et les balises. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe en lecture seule s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
Accès complet	Les utilisateurs de ce groupe bénéficient d'un accès complet aux ressources S3, y compris les compartiments. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe à accès complet s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.

Stratégie de groupe	Description
Réduction des ransomwares	<p>Cet exemple de règle s'applique à toutes les compartiments pour ce locataire. Les utilisateurs de ce groupe peuvent effectuer des actions courantes, mais ne peuvent pas supprimer définitivement des objets des compartiments pour lesquels la gestion des versions d'objet est activée.</p> <p>Les utilisateurs de tenant Manager disposant 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), le cas échéant.</p>
Personnalisées	Les utilisateurs du groupe se voient accorder les autorisations que vous spécifiez dans la zone de texte.

- Si vous avez sélectionné **personnalisé**, entrez la stratégie de groupe. Chaque stratégie de groupe a une taille limite de 5,120 octets. Vous devez entrer une chaîne au format JSON valide.

Pour plus d'informations sur les stratégies de groupe, notamment la syntaxe de la langue et des exemples, reportez-vous à la section "[Exemples de stratégies de groupe](#)".

- Si vous créez un groupe local, sélectionnez **Continuer**. Si vous créez un groupe fédéré, sélectionnez **Créer 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 qui existent déjà.

 Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de 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 dans 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

- Vous pouvez également sélectionner un ou plusieurs utilisateurs locaux pour ce groupe.
- Sélectionnez **Créer 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 de fédération de grille** et que vous êtes sur la grille source du locataire, le nouveau groupe est cloné dans la grille de destination du locataire. **Succès** apparaît comme l'état **clonage** dans la section vue d'ensemble de la page de détails du groupe.

Créez des groupes pour un locataire Swift

Vous pouvez gérer les autorisations d'accès pour un compte de 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 de locataire Swift.



La prise en charge des applications du client Swift a été obsolète et sera supprimée dans une prochaine version.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "["Autorisation d'accès racine"](#)".
- Si vous prévoyez d'importer un groupe fédéré, vous avez "["fédération des identités configurée"](#)", et le groupe fédéré existe déjà dans le référentiel d'identité configuré.

Accédez à l'assistant de création de groupe

Étapes

Pour la première étape, accédez à l'assistant de création de groupe.

1. Sélectionnez **ACCESS MANAGEMENT > Groups**.
2. Sélectionnez **Créer 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 du référentiel d'identité configuré précédemment.

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 les applications client pour gérer les ressources du locataire, en fonction des autorisations de groupe.

2. Entrez le nom du groupe.
 - **Groupe local** : saisissez à la fois 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 à l' `sAMAccountName` attribut. Pour OpenLDAP, le nom unique est le nom associé à `uid` attribut.
3. Sélectionnez **Continuer**.

Gérer les autorisations de groupe

Les autorisations de groupe contrôlent les tâches que les utilisateurs peuvent effectuer dans le Gestionnaire de locataires et l'API de gestion des locataires.

Étapes

1. Pour **Access mode**, sélectionnez l'une des options suivantes :
 - **Lecture-écriture** (par défaut) : les utilisateurs peuvent se connecter au gestionnaire de locataires et

gérer la configuration du locataire.

- **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent pas apporter de modifications ni exécuter d'opérations dans le gestionnaire de locataires ou l'API de gestion des locataires. 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 dispose d'un accès en lecture seule à tous les paramètres et fonctions sélectionnés.

2. Cochez la case **accès racine** si les utilisateurs du groupe doivent se connecter à l'API tenant Manager ou tenant Management.
3. Sélectionnez **Continuer**.

Définissez la stratégie de groupe Swift

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

1. Cochez la case **Swift Administrator** 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 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 qui existent déjà.

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 "[Gérez les utilisateurs locaux](#)".

2. Sélectionnez **Créer 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, tenez compte des 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 vous 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 autorisés à se connecter peuvent effectuer les tâches suivantes :

- Afficher le tableau de bord
- Modifier son 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 ne peuvent afficher que les paramètres et les fonctions associés.



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

Vous pouvez attribuer les autorisations suivantes à un groupe. Notez que les locataires S3 et Swift disposent d'autorisations de groupe différentes.

Autorisations	Description
Accès racine	<p>Donne un accès complet au gestionnaire des locataires et à l'API de gestion des locataires.</p> <p>Remarque : les utilisateurs Swift doivent disposer d'une autorisation d'accès racine pour se connecter au compte locataire.</p>
Administrateur	<p>Les locataires Swift uniquement. Fournit un accès complet aux conteneurs et objets Swift pour ce compte de locataire</p> <p>Remarque : les utilisateurs de Swift doivent disposer de l'autorisation Administrateur Swift pour effectuer toutes les opérations avec l'API REST Swift.</p>
Gérez vos identifiants S3	<p>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 STORAGE (S3) > My S3 Access keys.</p>
Gestion de 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 gérer les paramètres de tous les compartiments S3 du compte, indépendamment des règles du compartiment S3 ou du groupe. <p>Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu rubriques.</p> <ul style="list-style-type: none"> Locataires Swift : permet aux utilisateurs Swift de contrôler le niveau de cohérence des conteneurs Swift à l'aide de l'API de gestion des locataires. <p>Remarque : vous ne pouvez attribuer l'autorisation gérer tous les compartiments aux groupes Swift qu'à partir de l'API de gestion des locataires. Vous ne pouvez pas attribuer cette autorisation à des groupes Swift à l'aide du Gestionnaire de locataires.</p>

Autorisations	Description
Gestion des terminaux	<p>Permet aux utilisateurs d'utiliser le gestionnaire de locataires ou l'API de gestion des locataires pour créer ou modifier des terminaux de service de plateforme, qui sont utilisés comme destination pour les services de plateforme StorageGRID.</p> <p>Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu Platform Services Endpoints.</p>
Gestion des objets avec la console S3	<p>Associé à l'autorisation gérer tous les compartiments, permet aux utilisateurs d'accéder à la console S3 expérimentale à partir de la page compartiments. Les utilisateurs qui disposent de cette autorisation mais qui ne disposent pas de l'autorisation gérer tous les compartiments peuvent toujours naviguer directement vers la console S3 expérimentale.</p>

Gérer les groupes

Vous pouvez afficher un groupe, modifier le nom, les autorisations, les stratégies et les utilisateurs d'un groupe, dupliquer un groupe ; ou supprimer un groupe.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "["Autorisation d'accès racine"](#)".

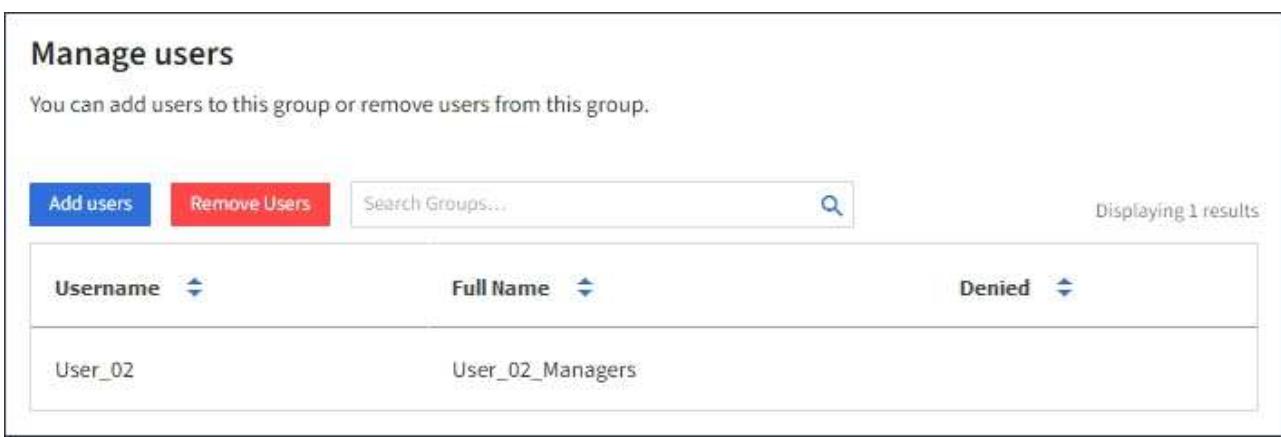
Afficher ou modifier un groupe

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

Étapes

1. Sélectionnez **ACCESS MANAGEMENT > Groups**.
2. Consultez les informations fournies sur la page groupes, qui répertorie les informations de base pour tous les groupes locaux et fédérés pour ce compte de tenant.
- Si le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous affichez des groupes sur la grille source du locataire, une bannière bleue indique que si vous modifiez ou supprimez un groupe, vos modifications ne seront pas synchronisées avec l'autre grille. Voir "["Cloner des groupes de locataires et des utilisateurs"](#)".
3. Si vous souhaitez modifier le nom du groupe :
 - a. Cochez la case du groupe.
 - b. Sélectionnez **actions > Modifier le nom du groupe**.
 - c. Saisissez 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 du groupe et sélectionnez **actions > Afficher les détails du groupe**.
5. Consultez la section Présentation, qui présente les informations suivantes pour chaque groupe :

- Nom d'affichage
 - Nom unique
 - Type
 - Mode d'accès
 - Autorisations
 - Règle S3
 - Nombre d'utilisateurs dans ce groupe
 - Champs supplémentaires si le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous affichez le groupe sur la grille source du locataire :
 - État de 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 de groupe selon vos besoins. Voir "[Créez des groupes pour un locataire S3](#)" et "[Créez des groupes pour un locataire Swift](#)" pour plus d'informations sur ce que vous devez saisir.
- a. Dans la section vue d'ensemble, 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 une règle de groupe S3 différente ou entrez la chaîne JSON pour une règle personnalisée, si nécessaire.
 - Si vous modifiez un groupe Swift, cochez ou décochez la case **Administrateur Swift**.
7. Pour ajouter un ou plusieurs utilisateurs locaux existants au groupe :
- a. Sélectionnez l'onglet utilisateurs.



The screenshot shows a 'Manage users' interface. At the top, there's a message: 'You can add users to this group or remove users from this group.' Below this are two buttons: 'Add users' (blue) and 'Remove Users' (red). To the right are a search bar with 'Search Groups...' and a magnifying glass icon, and a text field showing 'Displaying 1 results'. A table follows, with columns: 'Username' (sorted by 'Full Name'), 'Full Name' (sorted by 'Denied'), and 'Denied' (sorted by 'Username'). There is one row in the table: 'User_02' under 'Username', 'User_02_Managers' under 'Full Name', and 'Denied' under 'Denied'.

- b. Sélectionnez **Ajouter des utilisateurs**.
 - c. Sélectionnez les utilisateurs existants que vous souhaitez ajouter, puis sélectionnez **Ajouter des utilisateurs**.
- Un message de réussite s'affiche en haut à droite.
8. Pour supprimer des utilisateurs locaux du groupe :

- a. Sélectionnez l'onglet utilisateurs.
- b. Sélectionnez **Supprimer utilisateurs**.
- c. Sélectionnez les utilisateurs que vous souhaitez supprimer, puis sélectionnez **Supprimer utilisateurs**.

Un message de réussite s'affiche en haut à droite.

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

Dupliquer le groupe

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



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

Étapes

1. Sélectionnez **ACCESS MANAGEMENT > Groups**.
2. Cochez la case du groupe que vous souhaitez dupliquer.
3. Sélectionnez **actions > Dupliquer le groupe**.
4. Voir "[Créez des groupes pour un locataire S3](#)" ou "[Créez des groupes pour un locataire Swift](#)" pour plus d'informations sur ce que vous devez saisir.
5. Sélectionnez **Créer groupe**.

Supprimer un ou plusieurs groupes

Vous pouvez supprimer un ou plusieurs groupes. Les utilisateurs qui appartiennent uniquement à un groupe supprimé ne pourront plus se connecter au gestionnaire de tenant ni utiliser le compte de tenant.



Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de 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 **ACCESS MANAGEMENT > Groups**.
2. Cochez la case correspondant à chaque groupe à supprimer.
3. Sélectionnez **actions > Supprimer groupe** ou **actions > Supprimer groupes**.

Une boîte de dialogue de confirmation s'affiche.

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

Gérez les utilisateurs locaux

Vous pouvez créer des utilisateurs locaux et les affecter à des groupes locaux pour déterminer les fonctions 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 racine.



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 Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Autorisation d'accès racine](#)".
- Si votre compte locataire dispose de l'autorisation **utiliser la connexion de 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.

Créez un utilisateur local

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

Les utilisateurs S3 qui n'appartiennent à aucun groupe ne disposent pas d'autorisations de gestion ni de règles de groupe S3 qui leur sont appliquées. Il est possible que les utilisateurs bénéficient d'un accès par compartiment S3 accordé via une règle de compartiment.

Les utilisateurs Swift qui n'appartiennent à aucun groupe ne disposent d'aucune autorisation de gestion ou d'un accès au conteneur Swift.

Accédez à l'assistant de création d'utilisateur

Étapes

1. Sélectionnez **ACCESS MANAGEMENT > Users**.

Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de 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 dans l'autre grille de la connexion.

Users

View local and federated users. Edit properties and group membership of local users.

1 user

[Create user](#)

[Actions](#) ▾



This tenant has **Use grid federation connection** permission for connection Grid 1 to Grid 2. New local tenant users will be automatically cloned to the same tenant on the other grid in the connection. If you edit or remove a group, your changes will not be synced to the other grid..

2. Sélectionnez **Créer utilisateur**.

Entrez les informations d'identification

Étapes

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

Champ	Description
Nom complet	Le nom complet de cet utilisateur, par exemple le prénom et le nom d'une personne ou le nom d'une application.
Nom d'utilisateur	Nom que cet utilisateur utilisera pour se connecter. Les noms d'utilisateur doivent être uniques et ne peuvent pas être modifiés. Remarque : si votre compte locataire dispose de l'autorisation utiliser la connexion de fédération de grille , une erreur de clonage se produit si le même Nom d'utilisateur existe déjà pour le locataire sur la grille de destination.
Mot de passe et confirmer le mot de passe	Le mot de passe que l'utilisateur utilisera lors de sa connexion.
Refuser l'accès	Sélectionnez Oui pour empêcher cet utilisateur de se connecter au compte de tenant, même s'il appartient toujours à un ou plusieurs groupes. Par exemple, sélectionnez Oui pour suspendre temporairement la capacité d'un utilisateur à se connecter.

2. Sélectionnez **Continuer**.

Affecter à des groupes

Étapes

1. Attribuez l'utilisateur à un ou plusieurs groupes locaux pour déterminer les tâches qu'ils peuvent effectuer.

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

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

2. Sélectionnez **Créer utilisateur**.

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

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

Afficher ou modifier un utilisateur local

Étapes

1. Sélectionnez **ACCESS MANAGEMENT > Users**.
2. Consultez les informations fournies sur la page utilisateurs, qui répertorie les informations de base pour tous les utilisateurs locaux et fédérés pour ce compte de tenant.

Si le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous affichez l'utilisateur sur la grille source du locataire, une bannière bleue indique que si vous modifiez ou supprimez l'utilisateur, vos modifications ne seront pas synchronisées avec l'autre grille.
3. Si vous souhaitez modifier le nom complet de l'utilisateur :
 - a. Cochez la case de l'utilisateur.
 - b. Sélectionnez **actions > Modifier le nom complet**.
 - c. Saisissez 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 de l'utilisateur et sélectionnez **actions > Afficher les détails de l'utilisateur**.
5. Consultez la section Présentation, qui présente les informations suivantes pour chaque utilisateur :
 - Nom complet
 - Nom d'utilisateur
 - Type d'utilisateur
 - Accès refusé
 - Mode d'accès
 - Appartenance à un groupe
 - Champs supplémentaires si le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous affichez l'utilisateur sur la grille source du locataire :
 - État de 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 d'informations sur ce que vous devez saisir.
 - a. Dans la section vue d'ensemble, modifiez le nom complet en sélectionnant le nom ou l'icône de modification .
 - Vous ne pouvez pas modifier 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 permettre à l'utilisateur de se connecter ou sélectionnez **Oui** pour empêcher l'utilisateur de se connecter. Sélectionnez ensuite **Enregistrer les modifications**.
 - d. Dans l'onglet **clés d'accès**, sélectionnez **Créer une clé** et suivez les instructions de "[Création des clés d'accès S3 d'un autre utilisateur](#)".

- e. Dans l'onglet **groupes**, sélectionnez **Modifier les groupes** pour ajouter l'utilisateur à des groupes ou supprimer l'utilisateur des groupes. Sélectionnez ensuite **Enregistrer les modifications**.
7. Confirmez que vous avez sélectionné **Enregistrer les modifications** pour chaque section que vous avez modifiée.

Dupliquer l'utilisateur local

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



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

Étapes

1. Sélectionnez **ACCESS MANAGEMENT > Users**.
2. Cochez la case correspondant à l'utilisateur que vous souhaitez dupliquer.
3. Sélectionnez **actions > Dupliquer utilisateur**.
4. Voir [Créer un utilisateur local](#) pour plus d'informations sur ce que vous devez saisir.
5. Sélectionnez **Créer utilisateur**.

Supprimez un ou plusieurs utilisateurs locaux

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



Si votre compte de tenant dispose de l'autorisation **utiliser la connexion de 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 le référentiel d'identité fédéré pour supprimer des utilisateurs fédérés.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT > Users**.
2. Cochez la case correspondant à chaque utilisateur à supprimer.
3. Sélectionnez **actions > Supprimer utilisateur** ou **actions > Supprimer utilisateurs**.

Une boîte de dialogue de confirmation s'affiche.

4. Sélectionnez **Supprimer utilisateur** ou **Supprimer utilisateurs**.

Gestion des clés d'accès S3

Présentation de la gestion des clés d'accès S3

Chaque utilisateur d'un compte de 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 de la manière suivante :

- 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 **Root Access** peuvent gérer les clés d'accès du compte root S3 et de tous les autres utilisateurs. Les clés d'accès racine offrent un accès complet à toutes les compartiments et objets du locataire, sauf si une règle de compartiment est explicitement désactivée.

StorageGRID prend en charge l'authentification Signature version 2 et Signature version 4. L'accès entre comptes n'est pas autorisé sauf si cette règle est explicitement activée par une règle 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 compartiments et objets.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires 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 autorisations d'accès racine](#)".

Description de la tâche

Vous pouvez créer une ou plusieurs clés d'accès S3 qui vous permettent de créer et de gérer des compartiments pour votre compte de 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 que vous êtes sur le point d'expirer, créez une nouvelle clé avant l'expiration de l'ancienne, puis supprimez l'ancienne.

Chaque clé peut avoir une heure d'expiration spécifique ou pas d'expiration. Suivez les directives ci-dessous pour l'heure d'expiration :

- Définissez une durée 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 le risque si votre ID de clé d'accès et votre clé secrète sont exposés accidentellement. 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 régulièrement de nouvelles clés, vous n'avez pas besoin de définir une heure d'expiration pour vos clés. Si vous décidez plus tard de créer de nouvelles clés, supprimez les anciennes clés manuellement.

 Vous pouvez accéder aux compartiments S3 et aux objets appartenant à votre compte à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour votre compte dans le Gestionnaire des locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

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

La page Mes touches d'accès s'affiche et répertorie toutes les clés d'accès existantes.

2. Sélectionnez **Créer clé**.
3. Effectuez l'une des opérations suivantes :
 - Sélectionnez **ne définissez pas d'heure d'expiration** pour créer une clé qui n'expire pas. (Valeur par défaut)
 - Sélectionnez **définissez 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. La durée 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, avec la liste de votre ID de clé d'accès et de votre clé secrète d'accès.

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



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 de clés après la fermeture de la boîte de dialogue.

6. Sélectionnez **Terminer**.

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

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

Affichez vos clés d'accès S3

Si vous utilisez un locataire S3 et que vous disposez des autorisations appropriées, vous pouvez afficher la liste de vos clés d'accès S3. Vous pouvez trier la liste en fonction de l'heure d'expiration afin de déterminer quelles clés vont bientôt expirer. Si nécessaire, c'est possible "["créer de nouvelles clés"](#) ou "["supprimer les clés"](#) que vous n'utilisez plus.



Vous pouvez accéder aux compartiments S3 et aux objets appartenant à votre compte à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour votre compte dans le Gestionnaire des locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs disposant des informations d'identification [Manage your own S3 "permission"](#).

Étapes

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

2. À partir de la page Mes clés d'accès, triez toutes les clés d'accès existantes par **heure d'expiration** ou **ID de clé d'accès**.
3. Au besoin, créez de nouvelles clés ou supprimez les clés 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 des autorisations appropriées, vous pouvez supprimer vos propres clés d'accès S3. Une fois la clé d'accès supprimée, elle ne peut plus être utilisée pour accéder aux objets et aux compartiments du compte du locataire.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous disposez de l'autorisation gérer vos propres informations d'identification S3. Voir "[Autorisations de gestion des locataires](#)".

 Vous pouvez accéder aux compartiments S3 et aux objets appartenant à votre compte à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour votre compte dans le Gestionnaire des locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **STORAGE (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 **Supprimer la touche**.
4. Dans la boîte de dialogue de confirmation, sélectionnez **touche Suppr**.

Un message de confirmation s'affiche dans le coin supérieur droit de la page.

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

Si vous utilisez un locataire S3 avec l'autorisation appropriée, vous pouvez créer des clés d'accès S3 pour d'autres utilisateurs, comme les applications qui ont besoin d'accéder à des compartiments et des objets.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Autorisation d'accès racine](#)".

Description de la tâche

Vous pouvez créer une ou plusieurs clés d'accès S3 pour les autres utilisateurs afin qu'ils puissent créer et

gérer des compartiments pour leur compte de 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 les besoins de l'utilisateur et supprimez les clés qui ne sont pas utilisées. Si vous n'avez qu'une seule clé et que vous êtes sur le point d'expirer, créez une nouvelle clé avant l'expiration de l'ancienne, puis supprimez l'ancienne.

Chaque clé peut avoir une heure d'expiration spécifique ou pas d'expiration. Suivez les directives ci-dessous pour l'heure 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 le risque si l'ID de clé d'accès et la clé secrète sont exposés accidentellement. 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 régulièrement de nouvelles clés, vous n'avez pas besoin de définir une heure d'expiration pour les clés. Si vous décidez plus tard de créer de nouvelles clés, supprimez les anciennes clés manuellement.

 Les compartiments S3 et les objets appartenant à un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé secrète affichée 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 pivoter les clés d'accès régulièrement, supprimez les clés inutilisées du compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT > Users**.
2. Sélectionnez l'utilisateur dont vous souhaitez gérer les clés d'accès S3.

La page de détails utilisateur s'affiche.

3. Sélectionnez **touches d'accès**, puis **touche Créeer**.
4. Effectuez l'une des opérations suivantes :

- Sélectionnez **ne pas définir de délai d'expiration** pour créer une clé qui n'expire pas. (Valeur par défaut)
- Sélectionnez **définissez 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. La durée 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, avec la liste de l'ID de clé d'accès et de la clé secrète.

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



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 de clés après la fermeture de la boîte de dialogue.

7. Sélectionnez **Terminer**.

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

- Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération grid**, vous pouvez utiliser l'API de gestion des locataires pour cloner manuellement les clés d'accès S3 du locataire de la grille source vers le locataire de 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 pour déterminer quelles clés vont bientôt expirer. Au besoin, vous pouvez créer de nouvelles clés et supprimer des clés qui ne sont plus utilisées.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous disposez de l'autorisation d'accès racine.

 Les compartiments S3 et les objets appartenant à un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé secrète affichée 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 pivoter les clés d'accès régulièrement, supprimez les clés inutilisées du compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

- Selectionnez **ACCESS MANAGEMENT > Users**.
- Sur la page utilisateurs, sélectionnez l'utilisateur dont vous souhaitez afficher les clés d'accès S3.
- Dans la page Détails de l'utilisateur, sélectionnez **touches d'accès**.
- Trier les clés par **heure d'expiration** ou **ID de clé d'accès**.
- Si nécessaire, créez de nouvelles clés et supprimez manuellement les clés que le n'est plus utilisé.

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 associées

["Créez les clés d'accès S3 d'un autre utilisateur"](#)

["Supprimez les clés d'accès S3 d'un autre utilisateur"](#)

Supprimez 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 la clé d'accès supprimée, elle ne peut plus être utilisée pour accéder aux objets et aux compartiments du compte du locataire.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous disposez de l'autorisation d'accès racine. Voir "[Autorisations de gestion des locataires](#)".



Les compartiments S3 et les objets appartenant à un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé secrète affichée 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 pivoter les clés d'accès régulièrement, supprimez les clés inutilisées du compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT > Users**.
2. Sur la page utilisateurs, sélectionnez l'utilisateur dont vous souhaitez gérer les clés d'accès S3.
3. Sur la page Détails de l'utilisateur, sélectionnez **touches d'accès**, puis cochez la case correspondant à chaque clé d'accès que vous souhaitez supprimer.
4. Sélectionnez **actions > Supprimer la touche sélectionnée**.
5. Dans la boîte de dialogue de confirmation, sélectionnez **touche Suppr.**

Un message de confirmation s'affiche dans le coin supérieur droit de la page.

Gestion des compartiments S3

Créer un compartiment S3

Vous pouvez utiliser le Gestionnaire des locataires pour créer des compartiments S3 pour les données d'objet.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs disposant de l'accès racine ou de la fonction gérer tous les compartiments "[permission](#)". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.



Les autorisations 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 règle de groupe](#)".

- Si vous prévoyez d'activer le verrouillage objet S3 pour un compartiment, un administrateur du grid a activé le paramètre de verrouillage objet S3 global pour le système StorageGRID. Vous avez également passé en revue les exigences relatives aux compartiments et aux objets S3 Object Lock. Voir "[Utilisez le verrouillage d'objet S3 pour conserver les objets](#)".

Accéder à l'assistant

Étapes

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

Entrez les détails

Étapes

1. Entrez les détails du compartiment.

Champ	Description
Nom du compartiment	<p>Nom du compartiment conforme aux règles suivantes :</p> <ul style="list-style-type: none">• Il doit être unique sur chaque système StorageGRID (et pas seulement au sein du compte du locataire).• Doit être conforme DNS.• Doit contenir au moins 3 caractères et pas plus de 63 caractères.• Chaque étiquette doit commencer et se terminer par une lettre ou un chiffre en minuscules et ne peut utiliser que des lettres minuscules, des chiffres et des tirets.• Ne doit pas utiliser de périodes dans des demandes de type hébergement virtuel. Les périodes provoquera des problèmes avec la vérification du certificat générique du serveur. <p>Pour plus d'informations, reportez-vous à la section "Documentation Amazon Web Services (AWS) sur les règles d'attribution de nom de compartiment".</p> <p>Remarque : vous ne pouvez pas modifier le nom du compartiment après avoir créé le compartiment.</p>
Région	<p>La région du godet.</p> <p>L'administrateur StorageGRID gère les régions disponibles. Ce compartiment peut affecter la règle de protection des données appliquée aux objets. Par défaut, tous les compartiments sont créés dans le us-east-1 région.</p> <p>Remarque : vous ne pouvez pas modifier la région après avoir créé le compartiment.</p>

2. Sélectionnez Continuer.

Gestion des paramètres d'objet

Étapes

1. Activez éventuellement le contrôle de version d'objet pour le compartiment.

Activez la gestion des versions d'objet si vous souhaitez stocker chaque version de chaque objet dans ce compartiment. Vous pouvez ensuite récupérer les versions précédentes d'un objet si nécessaire. Vous devez activer la gestion des versions d'objet si le compartiment est utilisé pour la réPLICATION entre plusieurs grilles.

2. Si le paramètre global S3 Object Lock est activé, activez éventuellement S3 Object Lock pour que le compartiment stocke des objets à l'aide d'un modèle WORM (Write-once-read-many).

Activez le verrouillage des objets S3 pour un compartiment uniquement si vous devez conserver les objets pendant une durée fixe, par exemple, pour répondre à certaines exigences réglementaires. Le verrouillage

objet S3 est un paramètre permanent qui vous permet d'empêcher la suppression ou l'écrasement d'objets pendant une durée fixe ou indéfiniment.



Une fois le paramètre S3 Object Lock activé pour un compartiment, il ne peut pas être désactivé. Toute personne disposant des autorisations appropriées peut ajouter à ce compartiment des objets qui ne peuvent pas être modifiés. Il se peut que vous ne puissiez pas supprimer ces objets ou le compartiment lui-même.

Si vous activez le verrouillage des objets S3 pour un compartiment, le contrôle de version des compartiments est automatiquement activé.

3. Si vous avez sélectionné **Activer le verrouillage d'objet S3**, vous pouvez activer **rétention par défaut** pour ce compartiment.

Lorsque **Default Retention** est activé, les nouveaux objets ajoutés au compartiment sont automatiquement protégés contre la suppression ou l'écrasement. Le paramètre **rétention par défaut** ne s'applique pas aux objets qui ont leurs propres périodes de rétention.

- a. Si **Default Retention** est activé, spécifiez un **mode de rétention par défaut** pour le compartiment.

Mode de rétention par défaut	Description
La conformité	<ul style="list-style-type: none">L'objet ne peut pas être supprimé tant que sa date de conservation jusqu'à n'est pas atteinte.La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être réduite.La date de conservation de l'objet jusqu'à ne peut pas être supprimée tant que cette date n'est pas atteinte.
La gouvernance	<ul style="list-style-type: none">Utilisateurs avec le <code>s3:BypassGovernanceRetention</code> l'autorisation peut utiliser le <code>x-amz-bypass-governance-retention: true</code> demander à l'en-tête de contourner les paramètres de rétention.Ces utilisateurs peuvent supprimer une version d'objet avant d'atteindre sa date de conservation jusqu'à.Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

- b. Si **Default Retention** est activé, spécifiez la **période de rétention par défaut** pour le compartiment.

La **période de conservation par défaut** indique la durée pendant laquelle les nouveaux objets ajoutés à ce compartiment doivent être conservés, à partir du moment où ils sont ingérés. Spécifiez une valeur comprise entre 1 et 36,500 jours ou entre 1 et 100 ans.

4. Sélectionnez **Créer un compartiment**.

Le godet est créé et ajouté au tableau sur la page godets.

5. Si vous le souhaitez, sélectionnez **aller à la page des détails du compartiment** à "afficher les détails du compartiment" et effectuer une configuration supplémentaire.

Afficher les détails du compartiment

Vous pouvez afficher les compartiments de votre compte de locataire.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".

Étapes

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

La page compartiments s'affiche.

2. Passez en revue les informations récapitulatives pour chaque compartiment.

Si nécessaire, vous pouvez trier les informations par colonne, ou vous pouvez avancer et revenir à la liste.



Les valeurs nombre d'objets et espace utilisé affichées sont des estimations. Ces estimations sont affectées par le moment de l'ingestion, la connectivité réseau et l'état des nœuds. Si la gestion des versions des compartiments est activée, les versions des objets supprimés sont incluses dans le nombre d'objets.

Colonne	Description
Nom	Nom unique du compartiment, qui ne peut pas être modifié.
Fonctionnalités activées	Liste des fonctions activées pour le compartiment.
Verrouillage d'objet S3	Indique si le verrouillage d'objet S3 est activé pour le compartiment. Cette colonne apparaît uniquement si le verrouillage objet S3 est activé pour la grille. Cette colonne affiche également des informations pour tous les compartiments conformes existants.
Région	La région du compartiment, qui ne peut pas être modifiée.
Nombre d'objets	Nombre d'objets dans ce compartiment. Lorsque des objets sont ajoutés ou supprimés, il est possible que cette valeur ne soit pas mise à jour immédiatement. Si la gestion des versions des compartiments est activée, les versions d'objets non actuelles sont incluses dans cette valeur.
Espace utilisé	Taille logique de tous les objets du compartiment. La taille logique n'inclut pas l'espace réel requis pour les copies répliquées ou avec code d'effacement, ni pour les métadonnées d'objet.
Date de création	Date et heure de création du compartiment.

3. Pour afficher les détails d'un compartiment spécifique, sélectionnez le nom du compartiment dans le tableau.

La page des détails du compartiment s'affiche. À partir de cette page, vous pouvez effectuer les tâches

suivantes :

- Configurez et gérez des options de compartiment, notamment "[niveau de cohérence](#)", "[mises à jour de l'heure du dernier accès](#)", "[gestion des versions d'objets](#)", "[Verrouillage d'objet S3](#)" et "[rétenzione de compartiments par défaut](#)"
- Configurez l'accès au compartiment, par exemple "[Partage des ressources d'origine croisée \(CORS\)](#)"
- Gérez "[services de plateforme](#)" (si autorisé pour le locataire), y compris la réPLICATION, les notifications d'événements et l'intégration de la recherche
- Activer et "[gérer la réPLICATION entre les grilles](#)" (Si le locataire est autorisé) pour répliquer les objets ingérés dans ce compartiment vers un autre système StorageGRID
- Accédez au "[Console S3 expérimentale](#)" pour gérer les objets dans le compartiment
- "[Supprime tous les objets d'un compartiment](#)"
- "[Supprimer un compartiment](#)" c'est déjà vide

Modifiez le niveau de cohérence d'un compartiment

Si vous utilisez un locataire S3, vous pouvez modifier le niveau de cohérence des opérations effectuées sur les objets dans des compartiments S3.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Gérez tous les compartiments ou l'autorisation d'accès racine](#)". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.

Description de la tâche

Les contrôles de cohérence assurent un équilibre entre la disponibilité des objets et la cohérence de ces objets entre plusieurs nœuds de stockage et sites. En général, vous devez utiliser le niveau de cohérence **Read-After-New-write** pour vos compartiments.

Si le niveau de cohérence **Read-After-New-write** ne répond pas aux exigences de l'application client, vous pouvez modifier le niveau de cohérence en définissant le niveau de cohérence du compartiment ou en utilisant le **Consistency-Control** en-tête. Le **Consistency-Control** le cueilleur remplace le niveau de cohérence du godet.



Lorsque vous modifiez le niveau de cohérence d'un compartiment, seuls les objets ingérées après la modification sont garantis pour satisfaire le niveau révisé.

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.
 2. Sélectionnez le nom du compartiment dans la table.
- La page des détails du compartiment s'affiche.
3. Dans l'onglet **Bucket options**, sélectionnez l'accordéon **Consistency level**.
 4. Sélectionnez un niveau de cohérence pour les opérations effectuées sur les objets de ce compartiment.
 - **Tous** : fournit le plus haut niveau de cohérence. Tous les nœuds reçoivent les données immédiatement, sinon la requête échoue.

- **Strong-global** : garantit la cohérence lecture après écriture pour toutes les demandes client sur tous les sites.
- **Strong-site** : garantit la cohérence lecture après écriture pour toutes les demandes client au sein d'un site.
- **Read-After-New-write** (par défaut) : fournit une cohérence lecture-après-écriture pour les nouveaux objets et une cohérence éventuelle pour les mises à jour d'objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.
- **Disponible** : assure la cohérence finale pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.

5. Sélectionnez **Enregistrer les modifications**.

Activez ou désactivez les mises à jour de l'heure du dernier accès

Les administrateurs du grid créent les règles de gestion du cycle de vie des informations d'un système StorageGRID. Ils ont la possibilité de spécifier la date d'accès de dernier objet afin de déterminer si celui-ci doit être déplacé vers un autre emplacement de stockage. Si vous utilisez un locataire S3, vous pouvez activer ces règles en activant les mises à jour de l'heure du dernier accès pour les objets dans un compartiment S3.

Ces instructions s'appliquent uniquement aux systèmes StorageGRID qui incluent au moins une règle ILM utilisant l'option **Last Access Time** 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 d'informations.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "["Gérez tous les compartiments ou l'autorisation d'accès racine"](#)". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.

Description de la tâche

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

Par exemple, pour s'assurer que les objets récemment affichés restent dans un stockage plus rapide, un administrateur du grid peut créer une règle ILM spécifiant ce qui suit :

- 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 dernier mois 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 **Last Access Time** et que vous souhaitez que cette option s'applique aux objets de ce compartiment, vous devez activer les mises à jour de l'heure du dernier accès pour les compartiments S3 spécifiés dans cette règle.



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

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

- Mettre à jour les objets avec de nouveaux horodatages
- Ajoutez ces objets à la file d'attente ILM pour une réévaluation des règles et règles ILM actuelles

Le tableau récapitule 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	
	Heure du dernier accès mise à jour ?	Objet ajouté à la file d'attente d'évaluation ILM ?	Heure du dernier 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.
Demander de copier un objet d'un compartiment 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
Demander de terminer un téléchargement partitionné	Oui, pour l'objet assemblé			

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.
2. Sélectionnez le nom du compartiment dans la table.

La page des détails du compartiment s'affiche.

3. Dans l'onglet **Bucket options**, sélectionnez l'accordéon **Last Access Time Updates**.
4. Activer ou désactiver les mises à jour des heures du dernier accès.
5. Sélectionnez **Enregistrer les modifications**.

Modifiez le contrôle de version d'objet pour un compartiment

Si vous utilisez un locataire S3, vous pouvez modifier l'état de gestion des versions des compartiments S3.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Gérez tous les compartiments ou l'autorisation d'accès racine](#)". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.

Description de la tâche

Vous pouvez activer ou suspendre la gestion des versions d'objet pour un compartiment. Une fois que vous avez activé la gestion des versions pour un compartiment, il ne peut plus revenir à un état sans version. Toutefois, vous pouvez suspendre le contrôle de version du compartiment.

- Désactivé : le contrôle de version n'a jamais été activé
- Activé : la gestion des versions est activée
- Suspendu : la gestion des versions a déjà été activée et est suspendue

Pour plus d'informations, reportez-vous aux sections suivantes :

- "[Gestion des versions d'objet](#)"
- "[Règles et règles ILM pour les objets avec version S3 \(exemple 4\)](#)"
- "[Comment supprimer les objets](#)"

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.
2. Sélectionnez le nom du compartiment dans la table.

La page des détails du compartiment s'affiche.

3. Dans l'onglet **Bucket options**, sélectionnez l'accordéon **Object multiversion**.
4. Sélectionnez un état de gestion des versions pour les objets de ce compartiment.

La gestion des versions d'objet doit rester activée pour un compartiment utilisé pour la réplication entre plusieurs grilles. Si le verrouillage d'objet S3 ou la conformité héritée est activée, les options **Object versionnage** sont désactivées.

Option	Description
Activez le contrôle des versions	<p>Activez la gestion des versions d'objet si vous souhaitez stocker chaque version de chaque objet dans ce compartiment. Vous pouvez ensuite récupérer les versions précédentes d'un objet si nécessaire.</p> <p>Les objets qui se trouvent déjà dans le compartiment sont avec gestion de version lorsqu'ils sont modifiés par l'utilisateur.</p>
Suspendre la gestion des versions	Suspendre la gestion des versions d'objet si vous ne souhaitez plus créer de nouvelles versions d'objet. Vous pouvez toujours récupérer toutes les versions d'objet existantes.

5. Sélectionnez **Enregistrer les modifications**.

Utilisez le verrouillage d'objet S3 pour conserver les objets

Vous pouvez utiliser le verrouillage objet S3 si les compartiments et les objets doivent respecter les exigences réglementaires en matière de conservation des données.

Qu'est-ce que le verrouillage objet S3 ?

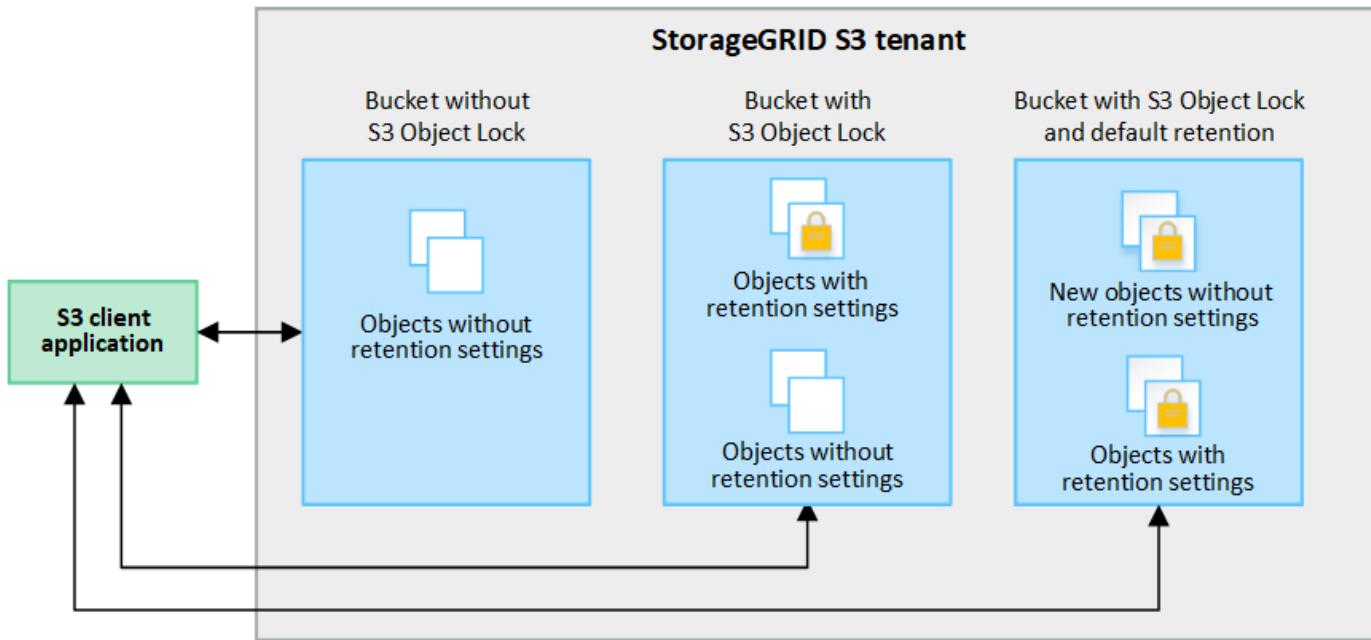
La fonctionnalité de verrouillage objet StorageGRID S3 est une solution de protection des objets équivalente au verrouillage objet S3 dans Amazon simple Storage Service (Amazon S3).

Comme illustré dans la figure, lorsque le paramètre global de verrouillage d'objet S3 est activé pour un système StorageGRID, un compte de locataire S3 peut créer des compartiments avec ou sans verrouillage d'objet S3 activé. Si le verrouillage objet S3 est activé pour un compartiment, la gestion des versions de compartiment est requise et elle est automatiquement activée.

Si le verrouillage objet S3 est activé dans un compartiment, les applications client S3 peuvent spécifier des paramètres de conservation pour toute version d'objet enregistrée dans ce compartiment.

En outre, un compartiment dans lequel le verrouillage objet S3 est activé peut choisir entre un mode de conservation et une période de conservation par défaut. Les paramètres par défaut s'appliquent uniquement aux objets ajoutés au compartiment sans leurs propres paramètres de conservation.

StorageGRID with S3 Object Lock setting enabled



Modes de rétention

La fonction 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 conservation Amazon S3.

- En mode conformité :
 - L'objet ne peut pas être supprimé tant que sa date de conservation jusqu'à n'est pas atteinte.
 - La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être réduite.
 - La date de conservation de l'objet jusqu'à 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 d'atteindre sa date de conservation jusqu'à.
 - 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 objet S3 activé, les utilisateurs peuvent utiliser l'application client S3 pour spécifier éventuellement les paramètres de conservation suivants pour chaque objet ajouté au compartiment :

- **Mode de conservation** : conformité ou gouvernance.
- **Conserver-jusqu'à-date**: Si la date de conservation d'une version d'objet est dans le futur, l'objet peut être récupéré, mais il ne peut pas être supprimé.
- **Mise en garde légale** : l'application d'une mise en garde légale à une version d'objet verrouille immédiatement cet objet. Par exemple, vous devrez peut-être mettre une obligation légale sur un objet lié

à une enquête ou à un litige juridique. Une obligation légale n'a pas de date d'expiration, mais reste en place jusqu'à ce qu'elle soit explicitement supprimée. Les dispositions légales sont indépendantes de la date de conservation.



Si un objet fait l'objet d'une conservation légale, personne ne peut le supprimer, quel que soit son mode de conservation.

Pour plus d'informations sur les paramètres d'objet, reportez-vous à la section "["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#)".

Paramètre de rétention par défaut pour les compartiments

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

- **Mode de rétention par défaut** : conformité ou gouvernance.
- **Période de rétention par défaut** : durée pendant laquelle les nouvelles versions d'objets ajoutées à ce compartiment doivent être conservées, à partir du jour où elles sont ajoutées.

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.

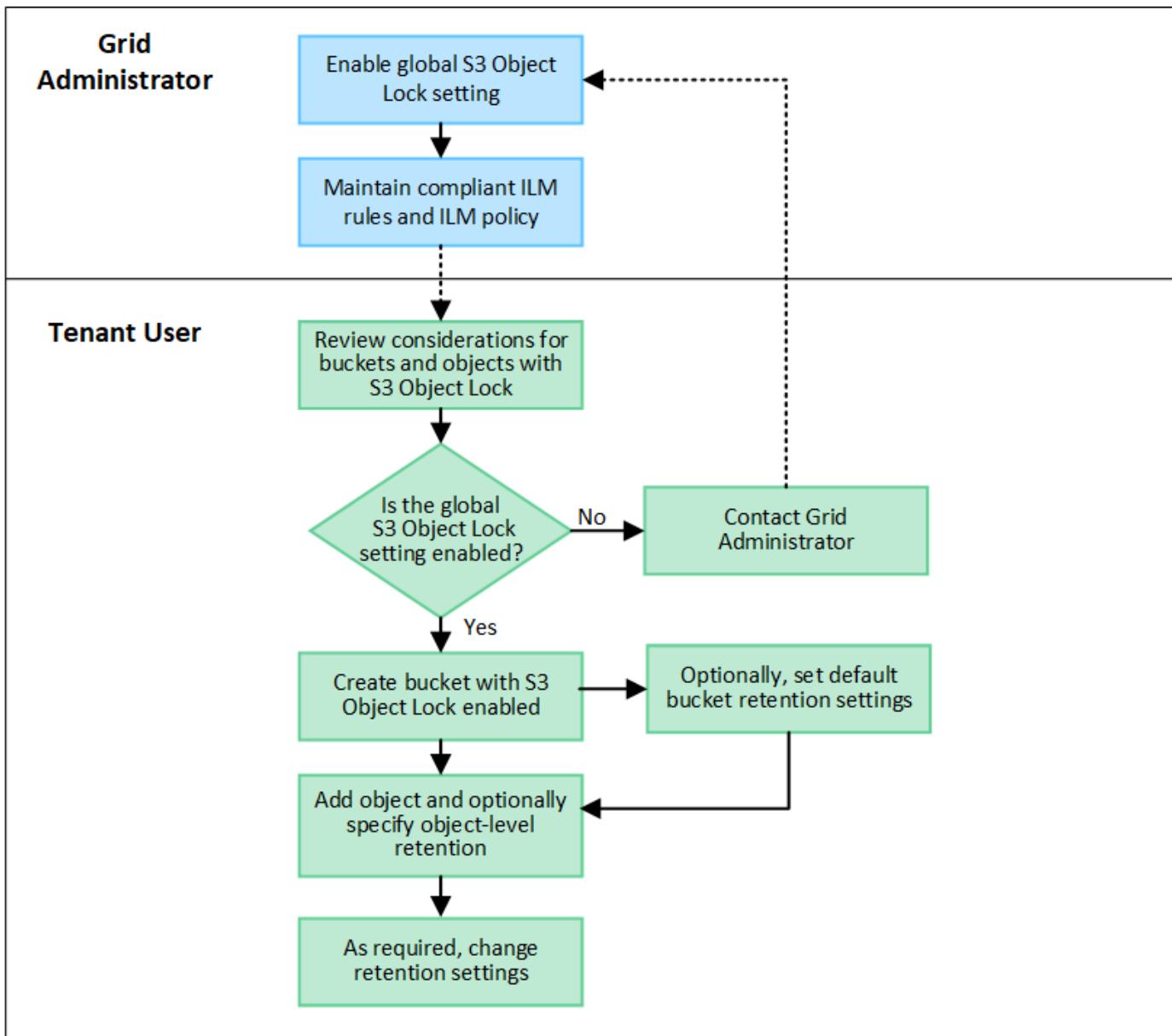
Voir "[Créer un compartiment S3](#)" et "[Mettre à jour la conservation par défaut du verrouillage d'objet S3](#)".

Workflow de verrouillage d'objet S3

Le schéma de workflow montre les étapes générales d'utilisation de la fonction de verrouillage d'objet S3 dans StorageGRID.

Avant de créer des compartiments avec le verrouillage d'objet S3 activé, l'administrateur de la grille doit activer le paramètre de verrouillage d'objet S3 global pour l'ensemble du système StorageGRID. L'administrateur du grid doit également s'assurer que la politique de gestion du cycle de vie de l'information est « conforme ». Elle doit répondre aux exigences des compartiments lorsque le verrouillage objet S3 est activé. Pour plus de détails, contactez votre administrateur de grille ou consultez les instructions de "[Gestion des objets avec le verrouillage objet S3](#)".

Une fois le paramètre global S3 Object Lock activé, vous pouvez créer des compartiments avec S3 Object Lock activé et spécifier éventuellement des paramètres de conservation par défaut pour chaque compartiment. En outre, vous pouvez utiliser l'application client S3 pour spécifier des paramètres de conservation pour chaque version d'objet.



Conditions requises pour les compartiments avec verrouillage objet S3 activé

- Si le paramètre global de verrouillage 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 compartiments avec le verrouillage objet S3 activé.
- Si vous prévoyez d'utiliser le verrouillage d'objet S3, vous devez activer le verrouillage d'objet S3 lors de la création du compartiment. Vous ne pouvez pas activer le verrouillage objet S3 pour un compartiment existant.
- Lorsque le verrouillage d'objet S3 est activé pour un compartiment, StorageGRID active automatiquement le contrôle de version pour ce compartiment. Vous ne pouvez pas désactiver le verrouillage objet S3 ou suspendre la gestion des versions pour le compartiment.
- Vous pouvez également spécifier un mode de conservation et une période de conservation par défaut pour chaque compartiment à l'aide du gestionnaire des locataires, de l'API de gestion des locataires ou de l'API REST S3. Les paramètres de conservation par défaut du compartiment s'appliquent uniquement aux nouveaux objets ajoutés au compartiment 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 jusqu'à pour chaque version d'objet lors du téléchargement.

- La configuration du cycle de vie des compartiments est prise en charge pour les compartiments avec le verrouillage objet S3 activé.
- La réPLICATION CloudMirror n'est pas prise en charge pour les compartiments avec le verrouillage objet S3 activé.

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

- Pour protéger une version d'objet, vous pouvez spécifier les paramètres de conservation par défaut du compartiment ou les paramètres de conservation pour chaque version d'objet. Les paramètres de conservation au niveau objet peuvent être spécifiés à l'aide de l'application client 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 un paramètre de conservation à la date et un paramètre de conservation légal, l'un mais pas l'autre, ou l'autre. La spécification d'un paramètre de conservation à la date ou d'un paramètre de conservation légal 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 des compartiments avec verrouillage objet S3 activé

Chaque objet enregistré dans un compartiment lorsque le verrouillage objet S3 est activé passe par les étapes suivantes :

1. Entrée d'objet

Lors de l'ajout d'une version d'objet à un compartiment pour lequel S3 Object Lock est activé, les paramètres de conservation sont appliqués comme suit :

- Si des paramètres de rétention sont spécifiés pour l'objet, les paramètres de niveau objet sont appliqués. Tous les paramètres de compartiment 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 le verrouillage objet S3.

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

2. Conservation et suppression d'objets

StorageGRID stocke plusieurs copies de chaque objet protégé pendant la période de conservation spécifiée. Le nombre et le type exacts de copies d'objet et d'emplacements de stockage sont déterminés par les règles de conformité de la politique ILM active. La possibilité de supprimer un objet protégé avant d'atteindre sa date de conservation jusqu'à dépend de son mode de conservation.

- Si un objet fait l'objet d'une conservation légale, personne ne peut le supprimer, quel que soit son mode de conservation.

Est-il toujours possible de gérer des compartiments existants conformes ?

La fonction de verrouillage d'objet S3 remplace la fonction de conformité disponible dans les versions StorageGRID précédentes. Si vous avez créé des compartiments conformes à l'aide d'une version précédente de StorageGRID, vous pouvez continuer à gérer les paramètres de ces compartiments. Toutefois, vous ne pouvez plus créer de compartiments conformes. Pour obtenir des instructions, reportez-vous à la section 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 : comment

gérer des compartiments conformes aux anciennes générations dans StorageGRID 11.5" ^].

Mettre à jour la conservation par défaut du verrouillage d'objet S3

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

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Gérez tous les compartiments ou l'autorisation d'accès racine](#)". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.
- 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 compartiment. Voir "[Utilisez le verrouillage d'objet S3 pour conserver les objets](#)".

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.
2. Sélectionnez le nom du compartiment dans la table.
La page des détails du compartiment s'affiche.
3. Dans l'onglet **Bucket options**, sélectionnez l'accordéon **S3 Object Lock**.
4. En option, activez ou désactivez **rétention par défaut** pour ce compartiment.

Les modifications de ce paramètre ne s'appliquent pas aux objets qui se trouvent déjà dans le compartiment ni aux objets qui peuvent avoir leurs propres périodes de conservation.

5. Si **Default Retention** est activé, spécifiez un **mode de rétention par défaut** pour le compartiment.

Mode de rétention par défaut	Description
La conformité	<ul style="list-style-type: none">• L'objet ne peut pas être supprimé tant que sa date de conservation jusqu'à n'est pas atteinte.• La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être réduite.• La date de conservation de l'objet jusqu'à ne peut pas être supprimée tant que cette date n'est pas atteinte.

Mode de rétention par défaut	Description
La gouvernance	<ul style="list-style-type: none"> Utilisateurs avec le <code>s3:BypassGovernanceRetention</code> l'autorisation peut utiliser le <code>x-amz-bypass-governance-retention: true</code> demander à l'en-tête de contourner les paramètres de rétention. Ces utilisateurs peuvent supprimer une version d'objet avant d'atteindre sa date de conservation jusqu'à. Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

6. Si **Default Retention** est activé, spécifiez la **période de rétention par défaut** pour le compartiment.

La **période de conservation par défaut** indique la durée pendant laquelle les nouveaux objets ajoutés à ce compartiment doivent être conservés, à partir du moment où ils sont ingérés. Spécifiez une valeur comprise entre 1 et 36,500 jours ou entre 1 et 100 ans.

7. Sélectionnez **Enregistrer les modifications**.

Configurer le partage de ressources inter-sources (CORS)

Vous pouvez configurer le partage de ressources entre sources (CORS) pour un compartiment S3 si vous souhaitez que ce compartiment et ces objets soient accessibles aux applications web d'autres domaines.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Gérez tous les compartiments ou l'autorisation d'accès racine](#)". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.

Description de la tâche

Le partage de ressources d'origine croisée (CORS) est un mécanisme de sécurité qui permet aux applications Web clientes d'un domaine d'accéder aux ressources d'un domaine différent. Supposons par exemple que vous utilisez un compartiment S3 nommé `Images` pour stocker des graphiques. En configurant CORS pour l'`Images` le champ permet d'afficher les images de ce compartiment sur le site web `http://www.example.com`.

Activer le CORS pour un godet

Étapes

1. Utilisez un éditeur de texte pour créer le fichier XML requis.

Cet exemple montre le code XML utilisé pour activer le code commande pour un compartiment S3. Ce XML permet à n'importe quel domaine d'envoyer des requêtes GET au compartiment, mais il n'autorise que le `http://www.example.com` Domaine pour envoyer des demandes POST et DE SUPPRESSION. Tous les en-têtes de demande 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 du développeur Amazon simple Storage Service"](#).

2. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.
 3. Sélectionnez le nom du compartiment dans la table.
- La page des détails du compartiment s'affiche.
4. Dans l'onglet **Bucket Access**, sélectionnez l'accordéon **Cross-Origin Resource Sharing (CORS)**.
 5. Cochez la case **Activer CORS**.
 6. Collez le fichier 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**.

Supprime les objets du compartiment

Vous pouvez utiliser le Gestionnaire de locataires pour supprimer les objets d'une ou de plusieurs compartiments.

Considérations et exigences

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

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



Un compartiment qui utilise le verrouillage d'objet S3 restera à 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 mises en suspens légales soient supprimées.

- Pendant la suppression des objets, l'état du compartiment est **Suppression d'objets : lecture seule**. Dans cet état, vous ne pouvez pas ajouter de nouveaux objets au compartiment.
- Une fois tous les objets supprimés, le compartiment reste à l'état en lecture seule. Vous pouvez effectuer l'une des opérations suivantes :
 - Ramener le compartiment en mode écriture et le réutiliser pour de nouveaux objets
 - Supprimez le compartiment
 - Conservez le compartiment en mode lecture seule pour réserver son nom pour une utilisation ultérieure
- Si la gestion des versions d'un objet est activée dans un compartiment, les marqueurs de suppression qui se trouvent dans le compartiment au démarrage de ces étapes ne seront pas supprimés par l'opération de suppression d'objets. Si vous souhaitez supprimer un compartiment versionné après la suppression de tous les objets, vous devez supprimer tous les marqueurs de suppression préexistants.
- Si vous utilisez "[réPLICATION entre plusieurs grilles](#)", noter ce qui suit :
 - L'utilisation de cette option ne supprime aucun objet du compartiment de l'autre grille.
 - Si vous sélectionnez cette option pour le compartiment source, l'alerte **échec de réPLICATION multigrille** est déclenchée si vous ajoutez des objets au compartiment de destination sur l'autre grille. Si vous ne pouvez pas garantir que personne n'ajoutera d'objets au compartiment de l'autre grille, "[désactiver la réPLICATION entre les grilles](#)" ce compartiment avant la suppression de tous les objets de compartiment.

Avant de commencer

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

Étapes

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

La page compartiments s'affiche et affiche tous les compartiments S3 existants.

2. Utilisez le menu **actions** ou la page de détails pour un compartiment spécifique.

Menu actions

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

Page de détails

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

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.

Au bout de quelques minutes :

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

The screenshot shows the AWS S3 Bucket details page for 'my-bucket'. The bucket name is highlighted in yellow. Key details shown include:

- Region: us-east-1
- Date created: 2022-12-14 10:09:50 MST
- Object count: 3

Below these details is a link to 'View bucket contents in Experimental S3 Console' with a magnifying glass icon. A 'Delete bucket' button is also present.

A prominent yellow warning box at the bottom left states: "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." It includes a progress bar indicating 0% completion and a 'Stop deleting objects' button.

A green success message box at the top right says: "Success Starting to delete objects from one bucket." with a close button.

5. Si nécessaire pendant l'exécution de l'opération, sélectionnez **Arrêter la suppression d'objets** pour arrêter le processus. Sélectionnez ensuite **Supprimer les objets dans le compartiment** pour reprendre le processus.

Lorsque vous sélectionnez **Arrêter la suppression d'objets**, le compartiment est remis en mode écriture ; cependant, vous ne pouvez pas accéder aux objets qui ont été supprimés ni les restaurer.

6. Attendez la fin de l'opération.

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

Buckets > my-bucket

my-bucket (read-only)

Region: us-east-1

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

Object count: 0

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

Delete bucket

Bucket is empty but is still read-only.

This bucket is now empty.

- To remove this bucket, select **Delete bucket**.
- To return this bucket to write mode so it can be reused, select **Stop deleting objects**.

Stop deleting objects

7. Effectuez l'une des opérations suivantes :

- Quittez la page pour garder le compartiment en mode lecture seule. Par exemple, vous pouvez conserver un compartiment vide en mode lecture seule afin de réserver le nom du compartiment pour une utilisation ultérieure.
- Supprimer le compartiment. Vous pouvez sélectionner **Supprimer un compartiment** pour supprimer un seul compartiment ou retourner à la page compartiments et sélectionner **actions > Supprimer** compartiments pour supprimer plusieurs compartiments.



Si vous ne pouvez pas supprimer un compartiment multiversion après la suppression de tous les objets, les marqueurs de suppression peuvent rester. Pour supprimer le godet, vous devez supprimer tous les marqueurs de suppression restants.

- Ramenez le compartiment en mode écriture et réutilisez-le éventuellement pour de nouveaux objets. Vous pouvez sélectionner **Arrêter la suppression d'objets** pour un seul compartiment ou revenir à la page compartiments et sélectionner **action > Arrêter la suppression d'objets** pour plusieurs compartiments.

Supprimez le compartiment S3

Vous pouvez utiliser le Gestionnaire de locataires pour supprimer une ou plusieurs compartiments S3 vides.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".

- Vous appartenez à un groupe d'utilisateurs qui possède le "[Gérez tous les compartiments ou l'autorisation d'accès racine](#)". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.
- Les compartiments à supprimer sont vides.

Description de la tâche

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

Vous ne pouvez pas supprimer un compartiment S3 s'il contient des objets, des versions d'objets non actuelles ou des marqueurs de suppression. Pour plus d'informations sur la suppression des objets avec version S3, reportez-vous à la section "[Comment supprimer les objets](#)".

Étapes

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

La page compartiments s'affiche et affiche tous les compartiments S3 existants.

2. Utilisez le menu **actions** ou la page de détails pour un compartiment spécifique.

Menu actions

- a. Cochez la case correspondant à chaque compartiment à supprimer.
- b. Sélectionnez **actions > Supprimer des compartiments**.

Page de détails

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

3. Lorsque la boîte de dialogue de confirmation s'affiche, sélectionnez **Oui**.

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

Si un compartiment n'est pas vide, un message d'erreur s'affiche. Vous devez supprimer tous les objets et tous les marqueurs de suppression du compartiment avant de pouvoir le supprimer.

Utilisation de la console Experimental S3

Vous pouvez utiliser la console S3 pour afficher les objets d'un compartiment S3.

Vous pouvez également utiliser la console S3 pour :

- Ajouter et supprimer des objets, des versions d'objet et des dossiers
- Renommez les objets
- Déplacer et copier des objets entre des compartiments et des dossiers
- Gérer les balises d'objet

- Afficher les métadonnées d'objet
- Télécharger des objets

 La console S3 est marquée comme « expérimentale » car elle n'est pas encore complète ou approuvée pour une utilisation dans un environnement de production. Les locataires ne doivent utiliser la console S3 que lors de l'exécution de fonctions sur un petit nombre d'objets, par exemple lors du chargement d'objets pour simuler une nouvelle règle ILM, pour résoudre les problèmes d'ingestion ou via des grilles de validation technique ou non-production.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs disposant de l'autorisation d'accès racine ou disposant à la fois des options gérer tous les compartiments et gérer les objets avec la console S3 "[autorisations](#)".



Les utilisateurs disposant de l'autorisation gérer les objets avec la console S3, mais qui ne disposent pas de l'autorisation gérer tous les compartiments, peuvent toujours naviguer directement vers la console S3 expérimentale.

- Vous avez créé un compartiment.
- Une règle de groupe S3 ou de compartiment a été configurée pour l'utilisateur.
- Vous connaissez l'ID de clé d'accès de l'utilisateur et la clé d'accès secrète. Si vous le souhaitez, vous avez un `.csv` fichier contenant ces informations. Voir la "[instructions pour la création de clés d'accès](#)".

Étapes

1. Sélectionnez **godets**.
2. Sélectionnez **Experimental S3 Console**  . Vous pouvez également accéder à ce lien à partir de la page des détails du compartiment.
3. Sur la page de connexion de la console Experimental S3, collez l'ID de clé d'accès et la clé secrète dans les champs. Sinon, sélectionnez **Télécharger les touches d'accès** et sélectionnez votre `.csv` fichier.
4. Sélectionnez **connexion**.
5. Gérez les objets selon vos besoins.

Name	Logical space used	Last modified on
03_Grid_Primer_11.5.pdf	2.73 MB	2021-12-03 09:43:26 MST
04_Tenant_Users_Guide_11.5.pdf	1.07 MB	2021-12-03 09:44:24 MST
06_Tenant_Users_Guide_11.5.pdf	1.25 MB	2021-12-03 09:44:27 MST
08_Tenant_Users_Guide_11.5.pdf	1.25 MB	2021-12-03 09:44:27 MST
09_Tenant_Users_Guide_11.5.pdf	1.25 MB	2021-12-03 09:44:26 MST
10_Grid_Primer_11.5.pdf	2.8 MB	2021-12-03 09:43:27 MST

Select an object or folder to view its details.

Displaying 16 objects
Selected 0 objects

Gérez les services de la plateforme S3

Qu'est-ce que les services de plateforme ?

Les services de plateforme StorageGRID vous aident 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'objet à des destinations externes.

Si l'utilisation des services de plateforme est autorisée pour votre compte de locataire, vous pouvez configurer les services suivants pour n'importe quel compartiment S3 :

- **RéPLICATION CloudMirror** : utilisation "[Service de réplication StorageGRID CloudMirror](#)" Pour mettre en miroir des objets spécifiques d'un compartiment StorageGRID vers une destination externe spécifiée.

Vous pouvez, par exemple, utiliser la réplication CloudMirror pour mettre en miroir des enregistrements client spécifiques dans Amazon S3, puis exploiter les services AWS pour analyser vos données.



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

- **Notifications**: Utilisation "[notifications d'événement par compartiment](#)" Pour envoyer des notifications sur

des actions spécifiques effectuées sur des objets à un service Amazon simple notification Service™ (SNS) externe spécifié.

Par exemple, vous pouvez configurer l'envoi d'alertes aux administrateurs pour chaque objet ajouté à un compartiment, où les objets représentent les fichiers de journal associés à un événement système critique.



Bien que la notification d'événement puisse être configurée sur un compartiment avec l'option de verrouillage d'objet S3 activée, les métadonnées S3 Object Lock (conservation jusqu'à la date et état de conservation légale) des objets ne seront pas incluses dans les messages de notification.

- **Service d'intégration de recherche** : utilisez le "[service d'intégration de la recherche](#)" Permet d'envoyer des métadonnées d'objet S3 à un index Elasticsearch spécifié pour rechercher ou analyser les métadonnées à l'aide du service externe.

Vous pouvez, par exemple, configurer des compartiments pour envoyer les métadonnées d'objet S3 vers un service Elasticsearch distant. Vous pouvez ensuite utiliser Elasticsearch pour effectuer des recherches dans des compartiments et effectuer des analyses sophistiquées des modèles présents dans les métadonnées de l'objet.



Bien que l'intégration avec Elasticsearch puisse être configurée sur un compartiment avec l'option S3 Object Lock activée, les métadonnées S3 Object Lock (conservation jusqu'à la date et état de conservation légale) des objets ne seront pas incluses dans les messages de notification.

L'emplacement cible des services de plateforme étant généralement externe à votre déploiement StorageGRID, les services de plateforme vous offrent la puissance et la flexibilité offertes par l'utilisation de ressources de stockage externes, de services de notification et de services de recherche ou d'analyse pour vos données.

Toute combinaison de services de plateforme peut être configurée pour un seul compartiment S3. Par exemple, vous pouvez configurer le service CloudMirror et les notifications sur un compartiment StorageGRID S3 afin de pouvoir mettre en miroir des objets spécifiques sur Amazon simple Storage Service, 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 la plateforme doit être activée pour chaque compte de locataire par un administrateur StorageGRID à l'aide de Grid Manager ou de l'API de gestion du grid.

Configuration des services de plate-forme

Les services de plateforme communiquent avec les terminaux externes que vous configurez à l'aide de "[Gestionnaire de locataires](#)" ou le "[API de gestion des locataires](#)". Chaque terminal représente une destination externe, par exemple un compartiment StorageGRID S3, un compartiment Amazon Web Services, un sujet SNS (simple notification Service) ou un cluster Elasticsearch hébergé localement, dans AWS ou ailleurs.

Après avoir créé un noeud final externe, vous pouvez activer un service de plate-forme pour un compartiment en ajoutant une configuration XML au compartiment. La configuration XML identifie les objets sur lesquels le compartiment doit agir, l'action que le compartiment doit effectuer et le point de terminaison que le compartiment doit utiliser pour le service.

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

- Si vous souhaitez que tous les objets dont les clés commencent par /images Pour la réPLICATION vers un compartiment Amazon S3, vous devez ajouter une configuration de réPLICATION dans le compartiment source.
- Si vous souhaitez également envoyer des notifications lorsque ces objets sont stockés dans le compartiment, vous devez ajouter une configuration de notifications.
- Enfin, si vous voulez 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 mettre en œuvre les services de plateforme StorageGRID :

Service de plateforme	L'API REST S3
"RéPLICATION CloudMirror"	<ul style="list-style-type: none"> • RÉPLICATION des compartiments • RÉPLICATION des compartiments
"Notifications"	<ul style="list-style-type: none"> • GET Bucket notification • PUT Bucket notification
"Intégration de la recherche"	<ul style="list-style-type: none"> • CONFIGURATION DES notifications de métadonnées de compartiment • CONFIGURATION de notification des métadonnées de compartiment <p>Ces opérations sont personnalisées pour StorageGRID.</p>

Informations associées

["Considérations relatives aux services de plateforme"](#)

["UTILISEZ L'API REST S3"](#)

Service de réPLICATION CloudMirror

Vous pouvez activer la réPLICATION CloudMirror pour un compartiment S3 si vous souhaitez que StorageGRID réplique des objets spécifiés ajoutés au compartiment dans un ou plusieurs compartiments de destination.

La réPLICATION CloudMirror fonctionne indépendamment de la règle ILM active de la grille. Le service CloudMirror réplique les objets au fur et à mesure qu'ils sont stockés dans le compartiment source et les fournit au compartiment de destination dès que possible. La livraison des objets répliqués est déclenchée lors de la réussite de l'acquisition de l'objet.



La réPLICATION CloudMirror présente des similarités et des différences importantes avec la fonction de réPLICATION multigrille. Pour en savoir plus, voir "["Comparez la réPLICATION entre les grilles et la réPLICATION CloudMirror"](#)".

Si vous activez la réPLICATION CloudMirror pour un compartiment existant, seuls les nouveaux objets ajoutés à ce compartiment sont répliqués. Les objets existants dans le compartiment 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 la 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.

Dans StorageGRID, vous pouvez répliquer les objets dans un compartiment unique vers plusieurs compartiments de destination. Pour ce faire, spécifiez la destination de chaque règle dans le XML de configuration de réPLICATION. Vous ne pouvez pas répliquer un objet dans plusieurs compartiments en même temps.

En outre, vous pouvez configurer la réPLICATION CloudMirror pour les compartiments avec version ou sans version, et spécifier un compartiment avec version ou sans version comme destination. Vous pouvez utiliser n'importe quelle combinaison de compartiments avec version et sans version. Par exemple, vous pouvez spécifier un compartiment avec version comme destination pour un compartiment source sans version, ou vice-versa. Vous pouvez également répliquer les compartiments sans version.

Le comportement de suppression du service de réPLICATION CloudMirror est identique au comportement de suppression du service CRR (Cross Region Replication) fourni par Amazon S3 — la suppression d'un objet dans un compartiment source ne supprime jamais un objet répliqué dans la destination. Si le compartiment source et le compartiment de destination sont multiversion, le marqueur de suppression est répliqué. Si le compartiment de destination n'est pas multiversion, la suppression d'un objet du compartiment source ne réplique pas le marqueur de suppression vers le compartiment de destination ou supprime l'objet de destination.

Lors de la réPLICATION des objets dans le compartiment de destination, StorageGRID les désigne par « duplIcaas ». Un compartiment StorageGRID de destination ne réplique pas les objets marqués comme répliques, ce qui vous protège des boucles de réPLICATION accidentelles. Ce marquage de réPLICATION est interne à StorageGRID et ne vous empêche pas d'utiliser 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.

L'unicité et l'ordre des événements dans le compartiment de destination ne sont pas garantis. Plusieurs copies identiques d'un objet source peuvent être livrées à la destination du fait des opérations effectuées pour garantir le succès de la livraison. Dans de rares cas, lorsque le même objet est mis à jour simultanément depuis deux sites StorageGRID ou plus, il peut ne pas correspondre au ordre d'événements du compartiment source.

La réPLICATION CloudMirror est généralement configurée pour utiliser un compartiment S3 externe comme destination. Vous pouvez cependant également configurer la réPLICATION afin d'utiliser un autre déploiement StorageGRID ou tout service compatible S3.

Description des notifications pour les compartiments

Vous pouvez activer la notification des événements pour un compartiment S3 si vous souhaitez que StorageGRID envoie des notifications sur les événements spécifiés à un service Amazon simple notification Service (SNS) de destination.

C'est possible "[configurer les notifications d'événements](#)" En associant XML de configuration de notification à un compartiment source. Le XML de configuration de notification respecte les conventions S3 pour la

configuration des notifications de compartiment, avec la rubrique SNS de destination spécifiée comme URN d'un terminal.

Les notifications d'événements sont créées au niveau du compartiment source, comme indiqué dans la configuration de la notification, et sont envoyées vers le compartiment de destination. Si un événement associé à un objet réussit, une notification concernant cet événement est créée et mise en file d'attente pour la livraison.

L'unicité et l'ordre des notifications ne sont pas garantis. Plusieurs notifications d'événement peuvent être envoyées vers la destination après les opérations effectuées pour garantir la réussite de la livraison. La livraison étant asynchrone, l'ordre dans le temps des notifications au niveau de la destination n'est pas garanti correspondant à l'ordre des événements dans le compartiment source, en particulier pour les opérations provenant de différents sites StorageGRID. Vous pouvez utiliser le sequencer Key dans le message d'événement pour déterminer l'ordre des événements pour un objet particulier, tel que décrit dans la documentation Amazon S3.

Notifications et messages pris en charge

Les notifications d'événements StorageGRID suivent l'API Amazon S3 avec quelques limitations :

- Les types d'événements suivants sont pris en charge :
 - s3:ObjectCreated:*
 - s3:ObjectCreated:put
 - s3:ObjectCreated:Post
 - s3:ObjectCreated:Copier
 - s3:ObjectCreated:CompleteMultipartUpload
 - s3:ObjectRemoved:*
 - s3:ObjectRemoved:Supprimer
 - s3:ObjectRemoved:DeleteMarkerCreated
 - s3:ObjectRestore:Post
- Les notifications d'événements envoyées par StorageGRID utilisent le format JSON standard, mais n'incluent pas certaines clés et utilisent des valeurs spécifiques pour d'autres, comme illustré dans le tableau :

Nom de la clé	Valeur ajoutée de StorageGRID
Source d'événements	sgws:s3
Région de l'awsRegion	non inclus
x-amz-id-2	non inclus
arn	urn:sgws:s3:::bucket_name

Comprendre le service d'intégration de la recherche

Si vous souhaitez utiliser un service externe de recherche et d'analyse de données pour

vos métadonnées d'objet, vous pouvez activer l'intégration de la recherche pour un compartiment S3.

Le service d'intégration de recherche est un service StorageGRID personnalisé qui envoie automatiquement et de manière asynchrone des métadonnées d'objet S3 vers un terminal de destination lors de la mise à jour d'un objet ou de ses métadonnées. Vous pouvez ensuite utiliser des outils sophistiqués de recherche, d'analyse de données, de visualisation ou de machine learning proposés par le service de destination pour rechercher, analyser et obtenir des informations exploitables à partir de vos données d'objet.

Vous pouvez activer le service d'intégration de la recherche pour tout compartiment avec version ou sans version. L'intégration des recherches est configurée en associant le XML de configuration des notifications de métadonnées au compartiment qui spécifie les objets à utiliser et la destination des métadonnées de l'objet.

Les notifications sont générées sous la forme d'un document JSON nommé avec le nom de compartiment, 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 de toutes les métadonnées utilisateur.

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

Les notifications sont générées et mises en file d'attente pour livraison chaque fois que :

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

Après avoir ajouté le XML de configuration de notification des métadonnées à un compartiment, des notifications sont envoyées pour tout nouvel objet que vous créez et pour tout objet que vous modifiez en mettant à jour ses données, métadonnées utilisateur ou balises. Cependant, aucune notification n'est envoyée pour les objets qui se trouvaient déjà dans le compartiment. Pour vous assurer que les métadonnées d'objet de tous les objets du compartiment sont envoyées à la destination, effectuez l'une des opérations suivantes :

- Configurez le service d'intégration de la recherche immédiatement après avoir créé le compartiment et avant d'ajouter des objets.
- Exécutez une action sur tous les objets déjà dans le compartiment pour déclencher un message de notification des métadonnées à envoyer à la destination.

Le service d'intégration de recherche StorageGRID prend en charge un cluster Elasticsearch. Comme pour les autres services de plate-forme, la destination est spécifiée dans le noeud final dont l'URN est utilisé dans le XML de configuration du service. Utilisez le "["Matrice d'interopérabilité NetApp"](#)" Afin de déterminer les versions prises en charge par Elasticsearch.

Informations associées

["XML de configuration pour l'intégration de la recherche"](#)

"Métadonnées d'objet incluses dans les notifications de métadonnées"

"JSON généré par le service d'intégration de la recherche"

"Configurez le service d'intégration de la recherche"

Considérations relatives aux services de plateforme

Avant de mettre en œuvre des services de plateforme, examinez les recommandations et les considérations relatives à l'utilisation de ces services.

Pour plus d'informations sur S3, reportez-vous à la section "["UTILISEZ L'API REST S3"](#)".

Considérations relatives à l'utilisation des services de plate-forme

Réflexion	Détails
Surveillance des terminaux de destination	<p>Vous devez surveiller la disponibilité de chaque point final de destination. Si la connexion au point final de destination est perdue pendant une période prolongée et qu'il existe un important retard de requêtes, les demandes client supplémentaires (telles QUE LES requêtes ENVOYÉES) à StorageGRID échoueront. Vous devez réessayer ces demandes ayant échoué lorsque le noeud final devient accessible.</p>
Limitation du terminal de destination	<p>Le logiciel StorageGRID peut canaliser les demandes S3 entrantes pour un compartiment si le taux d'envoi des demandes dépasse le taux à partir duquel le terminal de destination peut recevoir les demandes. La restriction ne se produit que lorsqu'il existe un arriéré de demandes en attente d'envoi vers le noeud final de destination.</p> <p>Le seul effet visible est que les requêtes S3 entrantes prennent plus de temps à s'exécuter. Si vous commencez à détecter les performances beaucoup plus lentes, vous devez réduire le taux d'entrée ou utiliser un terminal avec une capacité plus élevée. Si l' carnet de commandes des requêtes continue d'augmenter, les opérations S3 des clients (par EXEMPLE, LES requêtes PUT) finiront par échouer.</p> <p>Les demandes CloudMirror sont plus susceptibles d'être affectées par les performances du terminal de destination, car ces demandes impliquent généralement plus de transfert de données que les demandes d'intégration de recherche ou de notification d'événements.</p>
Garanties de commande	<p>StorageGRID garantit l'ordre des opérations sur un objet d'un site. Tant que toutes les opérations relatives à un objet se trouvent sur le même site, l'état final de l'objet (pour la réPLICATION) sera toujours égal à l'état dans StorageGRID.</p> <p>StorageGRID tente également de commander des demandes lorsque des opérations sont effectuées sur des sites StorageGRID. Par exemple, si vous écrivez un objet initialement sur le site A, puis que vous le remplacez par un autre objet au niveau du site B, le dernier objet répliqué par CloudMirror vers le compartiment de destination n'est pas garanti que ce nouvel objet soit.</p>

Réflexion	Détails
Suppressions d'objets basées sur des règles ILM	<p>Pour correspondre au comportement de suppression des services CRR et SNS d'AWS, les requêtes CloudMirror et de notification d'événement ne sont pas envoyées lorsqu'un objet du compartiment source est supprimé en raison des règles ILM de StorageGRID. Par exemple, aucune demande de notification de CloudMirror ou d'événement n'est envoyée si une règle ILM supprime un objet au bout de 14 jours.</p> <p>Au contraire, les demandes d'intégration de la recherche sont envoyées lorsque les objets sont supprimés du fait de ILM.</p>

Considérations relatives à l'utilisation du service de réPLICATION CloudMirror

Réflexion	Détails
État de la réPLICATION	StorageGRID ne prend pas en charge le <code>x-amz-replication-status</code> en-tête.
Taille de l'objet	<p>La taille maximale des objets qui peuvent être répliqués dans un compartiment de destination par le service de réPLICATION CloudMirror est de 5 Tio, soit la même que la taille maximale de l'objet <i>pris en charge</i>.</p> <p>Remarque : la taille maximale recommandée pour une opération d'objet PUT simple est de 5 Gio (5,368,709,120 octets). Si vos objets sont supérieurs à 5 Gio, utilisez le téléchargement partitionné.</p>
Gestion des versions du compartiment et ID de version	<p>Si le compartiment S3 source de StorageGRID est activé pour la gestion des versions, vous devez également activer la gestion des versions pour le compartiment de destination.</p> <p>Lors de l'utilisation du contrôle de version, notez que l'ordre des versions d'objet dans le compartiment de destination est meilleur effort et n'est pas garanti par le service CloudMirror, en raison des limites du protocole S3.</p> <p>Remarque : les ID de version du compartiment source dans StorageGRID ne sont pas liés aux ID de version du compartiment de destination.</p>
Balisage des versions d'objets	<p>Le service CloudMirror ne réplique pas les demandes DE balisage d'objets PUT ou DELETE Object tagging qui fournissent 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'est pas possible de s'assurer qu'une mise à jour de balise vers un ID de version spécifique sera répliquée.</p> <p>En revanche, le service CloudMirror réplique les demandes DE balisage D'objets PUT ou SUPPRIME les demandes de balisage d'objets qui ne spécifient pas d'ID de version. Ces demandes mettent à jour les balises pour la clé la plus récente (ou la dernière version si le compartiment est versionné). Les ings normaux avec des étiquettes (et non les mises à jour de marquage) sont également répliqués.</p>

Réflexion	Détails
Téléchargements partitionnés et ETag valeurs	Lors de la mise en miroir d'objets qui ont été téléchargés à l'aide d'un téléchargement partitionné, le service CloudMirror ne conserve pas les pièces. En conséquence, le ETag la valeur de l'objet symétrique sera différente de la ETag valeur de l'objet d'origine.
Chiffrement des objets avec SSE-C (chiffrement côté serveur avec clés fournies par le client)	Le service CloudMirror ne prend pas en charge les objets chiffrés avec SSE-C. Si vous tentez d'ingérer un objet dans le compartiment source pour la réPLICATION CloudMirror et que la demande inclut les en-têtes de requête SSE-C, l'opération échoue.
Compartiment avec verrouillage objet S3 activé	Si le compartiment S3 de destination pour la réPLICATION CloudMirror est activé pour le verrouillage des objets S3, la tentative de configuration de la réPLICATION de compartiment (RÉPLICATION PUT bucket) échoue avec une erreur AccessDenied.

Configurer les terminaux des services de plateforme

Avant de pouvoir configurer un service de plateforme pour un compartiment, vous devez configurer au moins un point de terminaison afin qu'il soit la destination du service de plateforme.

L'accès aux services de plateforme est activé par locataire par administrateur StorageGRID. Pour créer ou utiliser un noeud final de services de plate-forme, vous devez être un utilisateur locataire disposant de l'autorisation gérer les noeuds finaux ou accès racine, dans une grille dont la mise en réseau a été configurée pour permettre aux noeuds de stockage d'accéder aux ressources de noeuds finaux externes. Pour plus d'informations, contactez votre administrateur StorageGRID.

Qu'est-ce qu'un terminal de services de plateforme ?

Lorsque vous créez un noeud final de services de plate-forme, vous spécifiez les informations dont StorageGRID a besoin pour accéder à la destination externe.

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

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

Vous pouvez utiliser le même point final que la destination pour plusieurs compartiments source. Par exemple, vous pouvez configurer plusieurs compartiments source pour envoyer les métadonnées d'objet vers le même point de terminaison d'intégration de la recherche, afin d'effectuer des recherches dans plusieurs compartiments. Vous pouvez également configurer un compartiment source pour utiliser plusieurs points de terminaison comme cible, ce qui vous permet d'envoyer des notifications sur la création d'objet à une rubrique SNS et des notifications sur la suppression d'objet à une autre rubrique SNS.

Terminaux pour la réPLICATION CloudMirror

StorageGRID prend en charge les terminaux de réPLICATION qui représentent des compartiments S3. Ces compartiments peuvent être hébergés sur Amazon Web Services, sur le même déploiement StorageGRID, sur un autre service ou sur un autre déploiement à distance.

Terminaux pour les notifications

StorageGRID prend en charge les terminaux SNS (simple notification Service). Les terminaux SQS (simple Queue Service) ou Lambda d'AWS ne sont pas pris en charge.

Points d'extrémité du service d'intégration de la recherche

StorageGRID prend en charge des terminaux d'intégration de recherche représentant les clusters Elasticsearch. Ces clusters Elasticsearch peuvent se trouver dans un data Center local ou être hébergés dans un cloud AWS ou ailleurs.

Le point final de l'intégration de la recherche fait référence à un index et à un type Elasticsearch spécifiques. Vous devez créer l'index dans Elasticsearch avant la création du noeud final dans StorageGRID, sinon la création du noeud final échouera. Il n'est pas nécessaire de créer le type avant de créer le noeud final. StorageGRID crée le type si nécessaire lors de l'envoi de métadonnées d'objet au terminal.

Informations associées

["Administrer StorageGRID"](#)

Spécifiez l'URN du terminal des services de plateforme

Lorsque vous créez un noeud final de services de plate-forme, vous devez spécifier un Nom de ressource unique (URN). Vous utiliserez l'URN pour référencer le noeud final lorsque vous créez un XML de configuration pour le service de plate-forme. L'URN de chaque terminal doit être unique.

StorageGRID valide les terminaux de services de plateforme lors de leur création. Avant de créer un noeud final de services de plate-forme, vérifiez que la ressource spécifiée dans le noeud final existe et qu'elle peut être atteinte.

Éléments DE RETOUR

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

- Si ce service est hébergé sur Amazon Web Services (AWS), utilisez `arn:aws`.
- Si ce 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 pour un terminal CloudMirror hébergé sur StorageGRID, il peut commencer par l'URN `urn:sgws`.

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

Service	Type
RéPLICATION CloudMirror	s3
Notifications	sns
Intégration de la recherche	es

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

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

Service	Ressource spécifique
RéPLICATION CloudMirror	nom du compartiment
Notifications	nom-rubrique-sns
Intégration de la recherche	domain-name/index-name/type-name Remarque : si le cluster Elasticsearch est NOT configuré pour créer automatiquement des index, vous devez créer l'index manuellement avant de créer le noeud final.

Urns 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 terminal d'intégration de recherche AWS, le `domain-name` doit inclure la chaîne littérale `domain/`, comme indiqué ici.

Urnes pour des services hébergés localement

Lors de l'utilisation de services hébergés localement au lieu de services cloud, vous pouvez spécifier l'URN de toute façon qui crée un URN valide et unique, tant que l'URN inclut les éléments requis dans les troisième et dernière positions. Vous pouvez laisser les éléments indiqués en blanc facultatif, ou vous pouvez les spécifier de quelque manière que ce soit pour vous aider à identifier la ressource et à rendre l'URN unique. Par exemple :

- RéPLICATION CloudMirror :

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

Pour un terminal CloudMirror hébergé sur StorageGRID, vous pouvez spécifier un URN valide commençant par `urn:sgws:`

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

- Notifications :

```
urn:mysite:sns:optional:optional:sns-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 domaine `name` L'élément peut être n'importe quelle chaîne tant que l'URN du terminal est unique.

Créer un terminal de services de plate-forme

Vous devez créer au moins un noeud final du type correct avant d'activer un service de plate-forme.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Les services de plateforme ont été activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Gestion des noeuds finaux ou des autorisations d'accès racine](#)".
- La ressource référencée par le noeud final des services de plate-forme a été créée :
 - RéPLICATION CloudMirror : compartiment S3
 - Notification d'événement : rubrique SNS
 - Notification de recherche : index Elasticsearch, si le cluster de destination n'est pas configuré pour

créer automatiquement des index.

- Vous disposez des informations relatives à la ressource de destination :

- Hôte et port pour l'URI (Uniform Resource identifier)



Si vous prévoyez d'utiliser un compartiment 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)

["Spécifiez l'URN du terminal des services de plateforme"](#)

- Informations d'authentification (si nécessaire) :
 - Clé d'accès : ID de clé d'accès et clé d'accès secrète
 - HTTP de base : nom d'utilisateur et mot de passe
 - CAP (C2S Access Portal) : URL d'informations d'identification temporaires, certificats de serveur et de client, clés client et phrase de passe de clé privée de client facultative.
 - Certificat de sécurité (en cas d'utilisation d'un certificat d'autorité de certification personnalisé)
- Si les fonctions de sécurité de Elasticsearch sont activées, vous disposez du privilège Monitor cluster pour les tests de connectivité et du privilège write index ou des priviléges index and delete index pour les mises à jour de documents.

Étapes

1. Sélectionnez **STORAGE (S3) > Platform services Endpoints**.

La page noeuds finaux des services de plate-forme s'affiche.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

0 endpoints

[Create endpoint](#)

[Delete endpoint](#)

Display name ? ▾

Last error ? ▾

Type ? ▾

URI ? ▾

URN ? ▾

No endpoints found

[Create endpoint](#)

2. Sélectionnez **Créer un noeud final**.

Create endpoint

1 Enter details 2 Select authentication type 3 Verify server

Optional Optional

Enter endpoint details

Enter the endpoint's display name, URI, and URN.

Display name ?

URI ?

URN ?

Cancel

Continue

3. Entrez un nom d'affichage pour décrire brièvement le point final et son objectif.

Le type de service de plate-forme pris en charge par le noeud final est affiché à côté du nom du noeud final lorsqu'il est répertorié sur la page noeuds finaux, de sorte que vous n'avez pas besoin d'inclure ces informations dans le nom.

4. Dans le champ **URI**, spécifiez l'identificateur de ressource unique (URI) du noeud final.

Utilisez l'un des formats suivants :

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

Si vous ne spécifiez pas de port, le port 443 est utilisé pour les URI HTTPS et le port 80 est utilisé pour les URI HTTP.

Par exemple, l'URI d'un compartiment hébergé sur StorageGRID peut être :

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

Dans cet exemple, s3.example.com Représente l'entrée DNS pour l'adresse IP virtuelle (VIP) du groupe

haute disponibilité StorageGRID, et 10443 représente le port défini dans le noeud final de l'équilibrer de charge.



Si possible, vous devez vous connecter à un groupe haute disponibilité de nœuds d'équilibrage de la charge pour éviter un point de défaillance unique.

De la même manière, l'URI d'un compartiment hébergé sur AWS peut être :

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



Si le noeud final est utilisé pour le service de réPLICATION CloudMirror, n'incluez pas le nom de compartiment dans l'URI. Vous incluez le nom du compartiment dans le champ **URN**.

5. Entrez le nom de ressource unique (URN) du noeud final.



Vous ne pouvez pas modifier l'URN d'un noeud final après sa création.

6. Sélectionnez **Continuer**.

7. Sélectionnez une valeur pour **Type d'authentification**, puis saisissez ou téléchargez les informations d'identification requises.

Create endpoint

1 Enter details 2 Select authentication type 3 Verify server

Authentication type ?

Select the method used to authenticate connections to the endpoint.

Anonymous

Anonymous
Access Key
Basic HTTP
CAP (C2S Access Portal)

Previous Continue

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 terminaux dont la sécurité est désactivée.	Pas d'authentification.
Clé d'accès	Utilise des identifiants de style AWS pour authentifier les connexions avec la destination.	<ul style="list-style-type: none"> ID de 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
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 autorité de certification du serveur (téléchargement de fichiers PEM) Certificat client (téléchargement de fichier PEM) Clé privée client (téléchargement de fichiers PEM, format crypté OpenSSL ou format de clé privée non crypté) Phrase de passe de clé privée du client (facultatif)

8. Sélectionnez **Continuer**.

9. Sélectionnez un bouton radio pour **Verify Server** pour choisir la manière dont la connexion TLS au noeud final est vérifiée.

Create endpoint

Enter details Select authentication type Verify server

Verify server

Use this method to validate the certificate for TLS connections to the endpoint resource. If you select "Use custom CA certificate," copy and paste the custom security certificate in the text box.

Use custom CA certificate

Use operating system CA certificate

Do not verify certificate

```
-----BEGIN CERTIFICATE-----
abcdefgijkl123456780ABCDEFGHIJKLM
123456/7890ABCDEFabcdefgijkl1ABCD
-----END CERTIFICATE-----
```

Previous [Test and create endpoint](#)

Type de vérification du certificat	Description
Utiliser un certificat d'autorité de certification 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 d'autorité de certification Grid par défaut installé sur le système d'exploitation pour sécuriser les connexions.
Ne vérifiez pas le certificat	Le certificat utilisé pour la connexion TLS n'est pas vérifié. Cette option n'est pas sécurisée.

10. Sélectionnez Test et Créer un noeud final.

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



La création du terminal échoue si les services de plate-forme ne sont pas activés pour votre compte de locataire. Veuillez contacter votre administrateur StorageGRID.

Après avoir configuré un noeud final, vous pouvez utiliser son URN pour configurer un service de plate-forme.

Informations associées

"[Spécifiez l'URN du terminal des services de plateforme](#)"

"[Configurez la réPLICATION CloudMirror](#)"

"[Configurer les notifications d'événements](#)"

"[Configurez le service d'intégration de la recherche](#)"

Tester la connexion pour le point final des services de plate-forme

Si la connexion à un service de plate-forme a changé, vous pouvez tester la connexion du noeud final pour vérifier que la ressource de destination existe et qu'elle peut être atteinte à l'aide des informations d'identification que vous avez spécifiées.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Gestion des noeuds finaux ou des autorisations d'accès racine](#)".

Description de la tâche

StorageGRID ne vérifie pas que les informations d'identification disposent des autorisations appropriées.

Étapes

1. Sélectionnez **STORAGE (S3) > Platform services Endpoints**.

La page noeuds finaux des services de plate-forme s'affiche et affiche la liste des noeuds finaux des services de plate-forme déjà configurés.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints

Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name	Last error	Type	URI	URN
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	✖ 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

2. Sélectionnez le noeud final dont vous souhaitez tester la connexion.

La page des détails du point final s'affiche.

Overview

Display name: [my-endpoint-1](#) 

Type: [S3 Bucket](#)

URI: <http://10.96.104.167:10443>

URN: [urn:sgws:s3:::bucket1](#)

[Connection](#) [Configuration](#)

Verify connection

Some errors might continue to appear after they are resolved. To see if an error is current or to force the removal of a resolved error, select **Test connection**.

[Test connection](#)

3. Sélectionnez **Tester la connexion**.

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

Modifier le point final des services de plate-forme

Vous pouvez modifier la configuration d'un point de terminaison de services de plate-forme pour modifier son nom, son URI ou d'autres détails. Par exemple, vous devrez peut-être mettre à jour les informations d'identification expirées ou modifier l'URI pour qu'il pointe vers un index Elasticsearch de sauvegarde pour le basculement. Vous ne pouvez pas modifier l'URN d'un terminal de services de plate-forme.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Gestion des noeuds finaux ou des autorisations d'accès racine](#)".

Étapes

1. Sélectionnez **STORAGE (S3) > Platform services Endpoints**.

La page noeuds finaux des services de plate-forme s'affiche et affiche la liste des noeuds finaux des services de plate-forme déjà configurés.

Platform services endpoints																								
A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.																								
4 endpoints																								
Create endpoint				Delete endpoint																				
<input type="checkbox"/> Display name <small>?</small> <small>▲</small> <input type="checkbox"/> Last error <small>?</small> <small>▲</small> <input type="checkbox"/> Type <small>?</small> <small>▲</small> <input type="checkbox"/> URI <small>?</small> <small>▲</small> <input type="checkbox"/> URN <small>?</small> <small>▲</small>																								
<table border="1"> <tr> <td><input type="checkbox"/></td> <td>my-endpoint-1</td> <td>S3 Bucket</td> <td>http://10.96.104.167:10443</td> <td>urn:sgws:s3:::bucket1</td> </tr> <tr> <td><input type="checkbox"/></td> <td>my-endpoint-2</td> <td>Search</td> <td>http://10.96.104.30:9200</td> <td>urn:sgws:es:::mydomain/sveloso/_doc</td> </tr> <tr> <td><input type="checkbox"/></td> <td>my-endpoint-3</td> <td>Notifications</td> <td>http://10.96.104.202:8080/</td> <td>arn:aws:sns:us-west-2::example1</td> </tr> <tr> <td><input type="checkbox"/></td> <td>my-endpoint-4</td> <td>S3 Bucket</td> <td>http://10.96.104.167:10443</td> <td>urn:sgws:s3:::bucket2</td> </tr> </table>					<input type="checkbox"/>	my-endpoint-1	S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1	<input type="checkbox"/>	my-endpoint-2	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc	<input type="checkbox"/>	my-endpoint-3	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1	<input type="checkbox"/>	my-endpoint-4	S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2
<input type="checkbox"/>	my-endpoint-1	S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1																				
<input type="checkbox"/>	my-endpoint-2	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc																				
<input type="checkbox"/>	my-endpoint-3	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1																				
<input type="checkbox"/>	my-endpoint-4	S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2																				

2. Sélectionnez le point final que vous souhaitez modifier.

La page des détails du point final s'affiche.

3. Sélectionnez **Configuration**.

Overview

Display name:	my-endpoint-3
Type:	Notifications
URI:	http://10.96.104.202:8080/
URN:	arn:aws:sns:us-west-2::example1

Connection

Configuration

Edit configuration

Endpoint details

URI

http://10.96.104.202:8080/

URN

arn:aws:sns:us-west-2::example1

Authentication type

Basic HTTP

Username

testme

Password

[Edit password](#)

Verify server

Use custom CA certificate

Use operating system CA certificate

Do not verify certificate

```
-----BEGIN CERTIFICATE-----  
abcdefghijklmnopqrstuvwxyz0ABCDEFGHIJKLMNOPQRSTUVWXYZ  
-----END CERTIFICATE-----
```

[Test and save changes](#)

4. Modifiez la configuration du noeud final selon les besoins.



Vous ne pouvez pas modifier l'URN d'un noeud final après sa création.

- a. Pour modifier le nom d'affichage du noeud final, sélectionnez l'icône d'édition
- b. Modifiez l'URI si nécessaire.
- c. Si nécessaire, modifiez le type d'authentification.
 - Pour l'authentification par clé d'accès, modifiez la clé selon vos besoins en sélectionnant **Modifier la clé S3** et en collant une nouvelle ID de clé d'accès et une nouvelle clé d'accès secrète. Si vous devez annuler vos modifications, sélectionnez **Revert S3 key edit**.
 - Pour l'authentification HTTP de base, modifiez le nom d'utilisateur si nécessaire. Modifiez le mot de passe selon vos besoins en sélectionnant **Modifier le mot de passe** et en saisissant le nouveau mot de passe. Si vous devez annuler vos modifications, sélectionnez **Revert password edit**.
 - Pour l'authentification CAP (C2S Access Portal), modifiez l'URL des informations d'identification temporaires ou la phrase de passe de la clé privée du client facultative et téléchargez de nouveaux certificats et fichiers de clés selon les besoins.



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

- 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 noeud final peut être atteint à l'aide des informations d'identification spécifiées. La connexion au noeud final est vérifiée à partir d'un noeud sur chaque site.
- Un message d'erreur s'affiche si la validation du noeud final échoue. Modifiez le noeud final pour corriger l'erreur, puis sélectionnez **Test et enregistrer les modifications**.

Supprimer le noeud final des services de plate-forme

Vous pouvez supprimer un noeud final si vous ne souhaitez plus utiliser le service de plate-forme associé.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "[navigateur web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Gestion des noeuds finaux ou des autorisations d'accès racine](#)".

Étapes

1. Sélectionnez **STORAGE (S3) > Platform services Endpoints**.

La page noeuds finaux des services de plate-forme s'affiche et affiche la liste des noeuds finaux des services de plate-forme déjà configurés.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints

Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name	Last error	Type	URI	URN
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	✖ 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

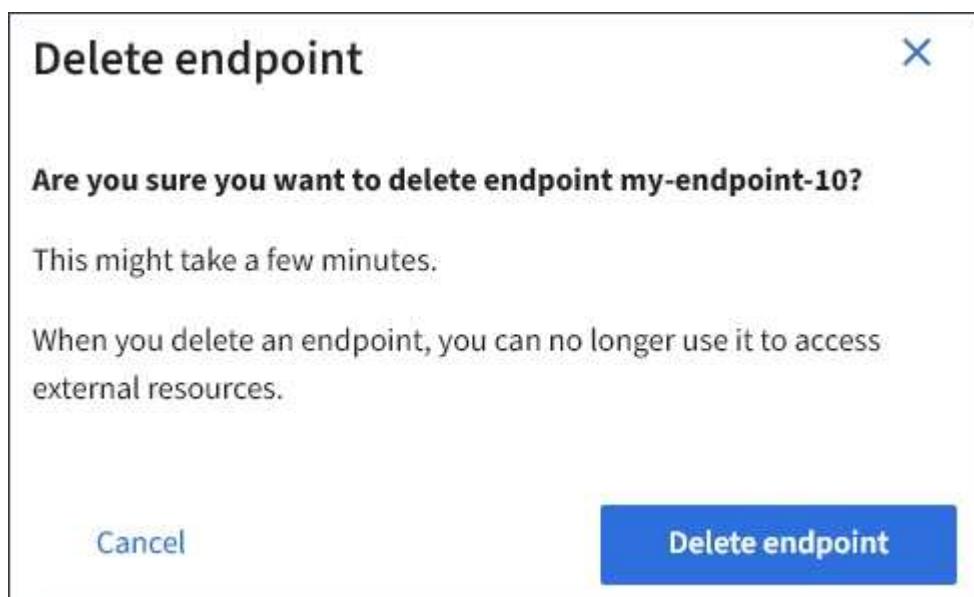
2. Cochez la case correspondant à chaque point final à supprimer.



Si vous supprimez un noeud final de services de plate-forme en cours d'utilisation, le service de plate-forme associé sera désactivé pour tous les compartiments qui utilisent le noeud final. Toutes les demandes qui n'ont pas encore été traitées seront supprimées. Toutes les nouvelles demandes seront toujours générées jusqu'à ce que vous modifiez la configuration de compartiment pour ne plus référencer l'URN supprimé. StorageGRID signale ces demandes comme des erreurs irrécupérables.

3. Sélectionnez **actions > Supprimer le point final**.

Un message de confirmation s'affiche.



4. Sélectionnez Supprimer le point final.

Dépanner les erreurs de point final des services de plate-forme

Si une erreur se produit lorsque StorageGRID tente de communiquer avec un noeud final de services de plate-forme, un message s'affiche sur le tableau de bord. Sur la page noeuds finaux des services de plate-forme, la colonne dernière erreur indique il y a combien de temps l'erreur s'est produite. Aucune erreur ne s'affiche si les autorisations associées aux informations d'identification d'un noeud final sont incorrectes.

Déterminez si l'erreur s'est produite

Si des erreurs de noeud final de 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 noeuds finaux des services de plate-forme pour obtenir 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 s'affiche sur le tableau de bord s'affiche également en haut de la page noeuds finaux Platform Services. Pour afficher un message d'erreur plus détaillé :

Étapes

1. Dans la liste des noeuds finaux, sélectionnez le noeud final qui contient l'erreur.
2. Sur la page des détails du noeud final, sélectionnez **connexion**. Cet onglet affiche uniquement l'erreur la plus récente pour un noeud final et indique il y a combien de temps l'erreur s'est produite. Erreurs incluant l'icône X rouge  s'est produit au cours des 7 derniers jours.

Overview

Display name:	my-endpoint-2 
Type:	Search
URI:	http://10.96.104.30:9200
URN:	urn:sgws:es:::mydomain/sveloso/_doc

[Connection](#)

[Configuration](#)

Verify connection

Some errors might continue to appear after they are resolved. To see if an error is current or to force the removal of a resolved error, select **Test connection**.

[Test connection](#)

Last error details

 2 hours ago

Endpoint failure: Endpont has an AWS failure: RequestError: send request failed; caused by: url.Error; caused by: net:OpError; caused by: os.SyscallError (logID: 143H5UDUUKMGDRWJ)

Vérifiez si l'erreur est toujours à jour

Certaines erreurs peuvent continuer à s'afficher dans la colonne **dernière erreur**, même après leur résolution. Pour voir si une erreur est active ou pour forcer la suppression d'une erreur résolue du tableau :

Étapes

1. Sélectionnez l'extrémité.

La page des détails du point final s'affiche.

2. Sélectionnez **connexion > Tester la connexion**.

La sélection de **Test Connection** permet à StorageGRID de valider l'existence du noeud final des services de plate-forme et de l'atteindre avec les informations d'identification actuelles. La connexion au noeud final est validée à partir d'un nœud sur chaque site.

Résoudre les erreurs de point final

Vous pouvez utiliser le message **dernière erreur** sur la page des détails du noeud final pour déterminer ce qui est à l'origine de l'erreur. Certaines erreurs peuvent vous obliger à modifier le noeud final pour résoudre le

problème. Par exemple, une erreur CloudMirroring peut se produire si StorageGRID ne parvient pas à accéder au compartiment S3 de destination, car il ne dispose pas des autorisations d'accès correctes ou si la clé d'accès a expiré. Le message est ""les identifiants de point de terminaison ou l'accès de destination doivent être mis à jour", et les détails sont "AccessDenied" ou "InvalidAccessKeyId."".

Si vous devez modifier le noeud final pour résoudre une erreur, la sélection de **Test et enregistrer les modifications** fait que StorageGRID valide le noeud final mis à jour et confirme qu'il peut être atteint avec les informations d'identification actuelles. La connexion au noeud final est validée à partir d'un nœud sur chaque site.

Étapes

1. Sélectionnez l'extrémité.
2. Sur la page des détails du noeud final, sélectionnez **Configuration**.
3. Modifiez la configuration de point final selon vos besoins.
4. Sélectionnez **connexion > Tester la connexion**.

Identifiants de point de terminaison avec autorisations insuffisantes

Lorsque StorageGRID valide un terminal de services de plateforme, il confirme que les identifiants du terminal peuvent être utilisés pour contacter la ressource de destination et il vérifie les 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 lors de la tentative d'utilisation d'un service de plate-forme (par exemple « 403 interdit »), vérifiez les autorisations associées aux identifiants du noeud final.

Informations associées

- "[Administration de StorageGRID ; dépannage des services de plate-forme](#)"
- "[Créer un terminal de services de plate-forme](#)"
- "[Tester la connexion pour le point final des services de plate-forme](#)"
- "[Modifier le point final des services de plate-forme](#)"

Configurez la réPLICATION CloudMirror

Le "[Service de réPLICATION CloudMirror](#)" Est l'un des trois services de plateforme StorageGRID. Vous pouvez utiliser la réPLICATION CloudMirror pour répliquer automatiquement les objets dans un compartiment S3 externe.

Avant de commencer

- Les services de plateforme ont été activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous avez déjà créé un compartiment qui servira de source de réPLICATION.
- Le noeud final que vous prévoyez d'utiliser comme destination pour la réPLICATION CloudMirror existe déjà, et vous avez son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Gérez tous les compartiments ou l'autorisation d'accès racine](#)". Ces autorisations remplacent les paramètres d'autorisation des stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Gestionnaire de locataires.

Description de la tâche

La réPLICATION CloudMirror copie les objets à partir d'un compartiment source vers un compartiment de destination spécifié dans un terminal.



La réPLICATION CloudMirror présente des similarités et des différences importantes avec la fonction de réPLICATION multigrille. Pour en savoir plus, voir "[Comparez la réPLICATION entre les grilles et la réPLICATION CloudMirror](#)".

Pour activer la réPLICATION CloudMirror pour un COMPARTIMENT, vous devez créer et appliquer un FICHIER XML de configuration de réPLICATION de COMPARTIMENT valide. Le XML de configuration de réPLICATION doit utiliser l'URN d'un TERMINAL de COMPARTIMENT S3 pour chaque DESTINATION.



La réPLICATION n'est pas prise en charge pour les COMPARTIMENTS source ou de DESTINATION lorsque le verrouillage d'OBJET S3 est ACTIVÉ.

Pour obtenir des informations générales sur la réPLICATION de COMPARTIMENT et la configuration de celle-ci, reportez-vous à la section "[Documentation d'Amazon simple Storage Service \(S3\) : réPLICATION d'objETS](#)". Pour plus d'informations sur la manière dont StorageGRID implémente GetBucketReplication, DeleteBucketReplication et PutBucketReplication, reportez-vous au "[OpérATIONS sur les COMPARTIMENTS](#)".

Si vous activez la réPLICATION CloudMirror sur un COMPARTIMENT qui CONTIENT des OBJETS, les NOUVEAUX OBJETS ajoutés au COMPARTIMENT sont RÉPLIQUÉS, mais les OBJETS EXISTANTS du COMPARTIMENT ne sont PAS RÉPLIQUÉS. Vous devez mettre à jour des OBJETS EXISTANTS pour déclencher la réPLICATION.

Si vous spécifiez une CLASSE DE STOCKAGE dans le FICHIER XML de configuration de réPLICATION, StorageGRID utilise cette CLASSE lors des opérATIONS sur le TERMINAL S3 de DESTINATION. Le NOEUD FINAL de DESTINATION doit également prendre en charge la CLASSE DE STOCKAGE spécifiée. Veillez à suivre les recommandATIONS fournies par le FOURNISSEUR du système de DESTINATION.

Étapes

1. Activer la réPLICATION pour le COMPARTIMENT source :

Utilisez un éDITEUR DE TEXTE pour créer le FICHIER 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 le V1 de la configuration de la réPLICATION. Cela signifie que StorageGRID ne prend pas en charge l'utilisation de Filter Elément pour les règles, et suit les conventions V1 pour la suppression des versions d'OBJET. Pour plus d'informations, reportez-vous à la documentation Amazon sur la configuration de la réPLICATION.
- Utiliser l'URN d'un TERMINAL du COMPARTIMENT S3 comme DESTINATION.
- Vous pouvez éventuellement ajouter le <StorageClass> et spécifiez l'un des éléments suivants :
 - STANDARD: La CLASSE DE STOCKAGE par défaut. Si vous ne spécifiez pas de CLASSE DE STOCKAGE lors du TÉLÉCHARGEMENT d'un OBJET, le STANDARD CLASSE DE STOCKAGE est utilisée.
 - STANDARD_IA: (Standard - accès peu fréquent.) Utilisez cette CLASSE DE STOCKAGE pour les données auxquelles vous accédez moins fréquemment, mais qui exigent toujours un accès rapide lorsque cela est nécessaire.
 - REDUCED_REDUNDANCY: Utilisez cette CLASSE DE STOCKAGE pour les données non stratégiques reproductibles qui peuvent être stockées avec moins de redondance que le STANDARD CLASSE DE STOCKAGE.
- Si vous spécifiez un Role Dans le FICHIER XML de configuration, 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 compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.

3. Sélectionnez le nom du compartiment source.

La page des détails du compartiment s'affiche.

4. Sélectionnez **Platform Services > Replication**.

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**.

Bucket options **Bucket access** **Platform services**

Replication **Disabled** **^**

Enable the CloudMirror replication service to copy objects from a source bucket to a destination bucket that is specified in an endpoint.

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for each destination bucket.
- You must specify the URN of each endpoint in the replication configuration XML for the source bucket.

Enable replication

Clear

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
            <Bucket>urn:sgws:s3:::2017-records</Bucket>
            <StorageClass>STANDARD</StorageClass>
        </Destination>
    </Rule>
</ReplicationConfiguration>
```

Save changes



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 du grid. Contactez votre administrateur StorageGRID si une erreur se produit lors de l'enregistrement du XML de configuration.

7. Vérifiez que la réPLICATION est configurée correctement :

- Ajoutez un objet au compartiment source qui répond aux exigences de réPLICATION telles que spécifiées dans la configuration de la réPLICATION.

Dans l'exemple présenté précédemment, les objets qui correspondent au préfixe « 2020 » sont répliqués.

b. Confirmer que l'objet a été répliqué vers le compartiment de destination.

Pour les objets de petite taille, la réPLICATION s'effectue rapidement.

Informations associées

["Créer un terminal de services de plate-forme"](#)

Configurer les notifications d'événements

Le service de notifications est l'un des trois services de plate-forme StorageGRID. Vous pouvez activer les notifications d'un compartiment pour envoyer des informations sur les événements spécifiés vers un service de destination qui prend en charge le service SNS (simple notification Service™) d'AWS.

Avant de commencer

- Les services de plateforme ont été activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous avez déjà créé un compartiment qui sert de source de notifications.
- Le noeud final que vous avez l'intention d'utiliser comme destination pour les notifications d'événements existe déjà, et vous avez son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le "["Gérez tous les compartiments ou l'autorisation d'accès racine"](#)". Ces autorisations remplacent les paramètres d'autorisation des stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Gestionnaire de locataires.

Description de la tâche

Après avoir 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 SNS (simple notification Service) utilisée comme point final de destination. Pour activer les notifications pour un compartiment, vous devez créer et appliquer un XML de configuration de notification valide. Le XML de configuration de notification doit utiliser l'URN d'un terminal de notification d'événement pour chaque destination.

Pour obtenir des informations générales sur les notifications d'événements et leur configuration, consultez la documentation Amazon. Pour plus d'informations sur l'implémentation de l'API de configuration des notifications du compartiment S3 par StorageGRID, reportez-vous aux instructions d'implémentation des applications client S3.

Si vous activez les notifications d'événements pour un compartiment contenant des objets, les notifications sont envoyées uniquement pour les actions qui sont effectuées après l'enregistrement de la configuration de notification.

Étapes

1. Activer les notifications pour le compartiment source :

- Utilisez un éditeur de texte pour créer le XML de configuration de notification requis pour activer les notifications d'événement, comme spécifié dans l'API de notification S3.
- Lors de la configuration du XML, utilisez l'URN d'un terminal de notification d'événements comme sujet 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 **STORAGE (S3) > seaux**.

3. Sélectionnez le nom du compartiment source.

La page des détails du compartiment s'affiche.

4. Sélectionnez **Platform Services > Event Notifications**.

5. Cochez la case **Activer les notifications d'événements**.

6. Collez le XML de configuration de notification dans la zone de texte, puis sélectionnez **Enregistrer les modifications**.

Bucket options **Bucket access** **Platform services**

Replication Disabled ▼

Event notifications Disabled ▲

Enable the event notification service for an S3 bucket if you want StorageGRID to send notifications about specified events to a destination Amazon Simple Notification Service (SNS).

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for the destination of event notifications.
- You must specify the URN of that endpoint in the notification configuration XML for the source bucket.

Enable event notifications

Clear

```

<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>
  </TopicConfiguration>
</NotificationConfiguration>

```

Save changes



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 du grid. Contactez votre administrateur StorageGRID si une erreur se produit lors de l'enregistrement du XML de configuration.

7. Vérifiez que les notifications d'événements sont correctement configurées :

- Exécutez une action sur un objet du compartiment source qui répond aux exigences de déclenchement d'une notification telles qu'elles sont configurées dans le fichier 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 SNS de destination.

Par exemple, si le sujet de votre destination est hébergé sur le service SNS (simple notification Service) d'AWS, vous pouvez configurer le service pour vous envoyer un e-mail une fois la notification 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 dans la rubrique de destination, vous avez configuré votre compartiment source pour les notifications StorageGRID.

Informations associées

["Description des notifications pour les compartiments"](#)

["UTILISEZ L'API REST S3"](#)

["Créer un terminal de services de plate-forme"](#)

Utilisez le service d'intégration de la recherche

Le service d'intégration de la recherche est l'un des trois services de plate-forme StorageGRID. Vous pouvez activer ce service pour envoyer des métadonnées d'objet à un index de recherche de destination chaque fois qu'un objet est créé ou supprimé, ou que ses métadonnées ou balises sont mises à jour.

Vous pouvez configurer l'intégration de la recherche à l'aide du Gestionnaire de locataires pour appliquer un code XML de configuration StorageGRID personnalisé à un compartiment.



Comme le service d'intégration de recherche entraîne l'envoi des métadonnées d'objet vers une destination, son XML de configuration est appelé *metadata notification configuration XML*. Ce XML de configuration est différent de la configuration de *notification XML* utilisée pour activer les notifications d'événements.

Voir la ["Instructions d'implémentation des applications client S3"](#) Pour plus d'informations sur les opérations d'API REST personnalisées suivantes de StorageGRID S3 :

- SUPPRIMEZ la configuration de notification des métadonnées de compartiment
- CONFIGURATION DES notifications de métadonnées de compartiment
- CONFIGURATION de notification des métadonnées de compartiment

Informations associées

["XML de configuration pour l'intégration de la recherche"](#)

["Métadonnées d'objet incluses dans les notifications de métadonnées"](#)

["JSON généré par le service d'intégration de la recherche"](#)

["Configurez le service d'intégration de la recherche"](#)

["UTILISEZ L'API REST S3"](#)

XML de configuration pour l'intégration de la recherche

Le service d'intégration de recherche est configuré à l'aide d'un ensemble de règles contenues dans `<MetadataNotificationConfiguration>` et `</MetadataNotificationConfiguration>` balises. Chaque règle spécifie les objets auxquels la règle s'applique, et la destination vers laquelle StorageGRID doit envoyer les métadonnées de ces objets.

Les objets peuvent être filtrés sur le préfixe du nom de l'objet. Par exemple, vous pouvez envoyer les métadonnées pour les objets avec le préfixe `images` à une destination et aux métadonnées pour les objets avec le préfixe `videos` à un autre. Les configurations avec des préfixes qui 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 seconde règle pour les objets avec le préfixe `test2` n'est pas autorisé.

Les destinations doivent être spécifiées à l'aide de l'URN d'un terminal StorageGRID créé pour le service d'intégration de la recherche. Ces terminaux font référence à un index et à un type définis dans un cluster Elasticsearch.

```
<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 des métadonnées.

Nom	Description	Obligatoire
Configuration de la MetadaNotificationConfiguration	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 d'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.

Nom	Description	Obligatoire
ID	<p>Identifiant unique de la règle.</p> <p>Inclus dans l'élément règle.</p>	Non
État	<p>L'état peut être « activé » ou « désactivé ». Aucune action n'est prise 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 d'objet sont envoyées. Doit être l'URN d'un terminal 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 domain-name/myindex/mytype. <p>Les terminaux sont configurés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Ils se présentent sous la forme suivante :</p> <ul style="list-style-type: none"> • arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype <p>Le noeud final doit être configuré avant la soumission du XML de configuration, ou la configuration échouera avec une erreur 404.</p> <p>L'URNE est incluse dans l'élément destination.</p>	Oui.

Utilisez l'exemple de XML de configuration de notification de métadonnées pour apprendre à construire votre propre XML.

Configuration de notification des métadonnées qui s'applique à tous les objets

Dans cet exemple, les métadonnées d'objet de 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>
```

Configuration des notifications de métadonnées avec deux règles

Dans cet exemple, les métadonnées d'objet pour les objets qui correspondent au préfixe /images est envoyée à une destination, tandis que les métadonnées d'objet correspondent au préfixe /videos est envoyé à une seconde 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>
```

Informations associées

["UTILISEZ L'API REST S3"](#)

["Métadonnées d'objet incluses dans les notifications de métadonnées"](#)

"JSON généré par le service d'intégration de la recherche"

"Configurez le service d'intégration de la recherche"

Configurer le service d'intégration de la recherche

Le service d'intégration de recherche envoie des métadonnées d'objet à un index de recherche de destination chaque fois qu'un objet est créé ou supprimé, ou que ses métadonnées ou balises sont mises à jour.

Avant de commencer

- Les services de plateforme ont été activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous avez déjà créé un compartiment S3 dont vous souhaitez indexer le contenu.
- Le noeud final que vous avez l'intention d'utiliser comme destination pour le service d'intégration de recherche existe déjà, et vous avez son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Gérez tous les compartiments ou l'autorisation d'accès racine](#)". Ces autorisations remplacent les paramètres d'autorisation des stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Gestionnaire de locataires.

Description de la tâche

Une fois que vous avez configuré le service d'intégration de recherche pour un compartiment source, la création d'un objet ou la mise à jour des métadonnées ou des balises d'un objet déclenche l'envoi des métadonnées d'objet vers le terminal de destination. Si vous activez le service d'intégration de recherche pour un compartiment qui contient déjà des objets, les notifications de métadonnées ne sont pas automatiquement envoyées pour les objets existants. Vous devez mettre à jour ces objets existants pour vous assurer que leurs métadonnées sont ajoutées à l'index de recherche de destination.

Étapes

1. Utilisez un éditeur de texte pour créer le XML de notification de métadonnées requis pour activer l'intégration de la recherche.
 - Voir les informations sur le XML de configuration pour l'intégration de la recherche.
 - Lors de la configuration du XML, utilisez l'URN d'un noeud final d'intégration de recherche comme destination.

```
<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:111111111111:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

2. Dans le Gestionnaire de locataires, sélectionnez **STORAGE (S3) > seaux**.

3. Sélectionnez le nom du compartiment source.

La page des détails du compartiment s'affiche.

4. Sélectionnez **Platform Services > Search Integration**

5. Cochez la case **Activer l'intégration de la recherche**.

6. Collez la configuration de notification de métadonnées dans la zone de texte, puis sélectionnez **Enregistrer les modifications**.

The screenshot shows the 'Platform services' tab selected in the top navigation bar. Under the 'Search integration' section, the status is set to 'Disabled'. A note below explains that enabling search integration allows object metadata to be sent to a destination search index whenever an object is created, deleted, or its metadata or tags are updated. Three requirements are listed: Platform services must be enabled for your tenant account by a StorageGRID administrator, you must have already configured an endpoint for the search integration service, and you must specify the URN of that endpoint in the search integration configuration XML for the bucket you want to index. A checked checkbox labeled 'Enable search integration' is present. Below it is a 'Clear' button. A large text area contains the XML configuration for metadata notification:

```
<MetadataNotificationConfiguration>
    <Rule>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
            <Urn>arn:aws:es:us-east-1:111111111111:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

A blue 'Save changes' button is located at the bottom right of the configuration area.



Les services de plateforme doivent être activés pour chaque compte de locataire par un administrateur StorageGRID à l'aide de l'API Grid Manager ou de gestion. Contactez votre administrateur StorageGRID si une erreur se produit lors de l'enregistrement du XML de configuration.

7. Vérifiez que le service d'intégration de la recherche est configuré correctement :

- a. Ajoutez un objet au compartiment source qui répond aux exigences relatives au déclenchement d'une notification de métadonnées comme spécifié dans le XML de configuration.

Dans l'exemple présenté précédemment, tous les objets ajoutés au compartiment déclenchent une notification de métadonnées.

- b. Vérifiez qu'un document JSON contenant les métadonnées et les balises de l'objet a été ajouté à l'index de recherche spécifié dans le noeud final.

Une fois que vous avez terminé

Si nécessaire, vous pouvez désactiver l'intégration de la recherche pour un compartiment à l'aide de l'une des méthodes suivantes :

- Sélectionnez **STORAGE (S3) > Buckets** et décochez la case **Enable search Integration**.
- Si vous utilisez directement l'API S3, utilisez une demande de notification DE suppression des métadonnées du compartiment. Pour plus d'informations sur l'implémentation des applications client S3, reportez-vous aux instructions.

Informations associées

["Comprendre le service d'intégration de la recherche"](#)

["XML de configuration pour l'intégration de la recherche"](#)

["UTILISEZ L'API REST S3"](#)

["Créer un terminal de services de plate-forme"](#)

JSON généré par le service d'intégration de la recherche

Lorsque vous activez le service d'intégration de la recherche pour un compartiment, un document JSON est généré et envoyé au terminal de destination à chaque ajout, mise à jour ou suppression de métadonnées d'objet.

Cet exemple montre un exemple de fichier JSON qui peut être généré lorsqu'un objet doté de la clé est associé SGWS/Tagging.txt est créé dans un compartiment nommé test. Le test le compartiment n'est pas multiversion versionId l'étiquette 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 qui est envoyé au noeud final de destination lorsque l'intégration de la recherche est activée.

Le nom du document inclut le nom du compartiment, le nom de l'objet et l'ID de version, le cas échéant.

Type	Nom et description de l'élément
Informations sur les compartiments et les objets	bucket: Nom du compartiment
key: Nom de la clé d'objet	versionID: Version d'objet, pour les objets dans les compartiments multiversion
region: Région godet, par exemple us-east-1	Métadonnées de système
size: Taille de l'objet (en octets) visible par un client HTTP	md5: Hachage d'objet
Métadonnées d'utilisateur	metadata: Toutes les métadonnées utilisateur de l'objet, en tant que paires clé-valeur key:value
Étiquettes	tags: Toutes les balises d'objet définies pour l'objet, en tant que paires clé-valeur key:value



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

UTILISEZ 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 en tant que ensemble de services web REST (Representational State Transfer).

La prise en charge de l'API REST S3 vous permet de connecter les applications orientées services développées pour les services web S3 avec un stockage objet sur site qui utilise le système StorageGRID. L'utilisation actuelle des appels de l'API REST S3 par une application client requiert des modifications minimales.

Versions prises en charge

StorageGRID prend en charge les versions spécifiques suivantes de S3 et HTTP.

Élément	Version
Spécification S3	<i>Simple Storage Service API Reference</i> 2006-03-01
HTTP	1.1 Pour plus d'informations sur HTTP, consultez le document HTTP/1.1 (RFC 7230-35). Remarque: StorageGRID ne prend pas en charge HTTP/1.1 pipeline.

Informations associées

["IETF RFC 2616 : Protocole de transfert hypertexte \(HTTP/1.1\)"](#)

["Documentation Amazon Web Services \(AWS\) : référence de l'API Amazon simple Storage Service"](#)

Prise en charge des mises à jour de l'API REST S3

Relâchez	Commentaires
11.7	<ul style="list-style-type: none"> Ajouté "Référence rapide : demandes d'API S3 prises en charge". Ajout de la prise en charge du mode DE GOUVERNANCE avec S3 Object Lock. A ajouté la prise en charge des spécificités de StorageGRID x-ntap-sg-cgr-replication-status En-tête de réponse pour LES requêtes GET Object et HEAD Object. Cet en-tête fournit l'état de réPLICATION d'un objet pour la réPLICATION inter-grid. Les requêtes SelectObjectContent prennent désormais en charge les objets parquet.
11.6	<ul style="list-style-type: none"> Ajout de la prise en charge de l'utilisation du partNumber Paramètre de demande dans DEMANDES OBJET GET et objet TÊTE. Ajout de la prise en charge d'un mode de conservation par défaut et d'une période de conservation par défaut au niveau du compartiment pour le verrouillage d'objet S3. Prise en charge ajoutée de s3:object-lock-remaining-retention-days la touche condition de police permet de définir la plage de périodes de conservation autorisées pour vos objets. Modification de la taille recommandée maximale pour une opération objet PUT unique à 5 Gio (5,368,709,120 octets). Si vos objets sont supérieurs à 5 Gio, utilisez le téléchargement partitionné.
11.5	<ul style="list-style-type: none"> Ajout de la prise en charge de la gestion du chiffrement de compartiment. Ajout de la prise en charge des demandes de verrouillage d'objet S3 et des demandes de conformité héritées obsolètes. Ajout de la prise en charge de L'utilisation DE LA SUPPRESSION de plusieurs objets sur les compartiments multiversion. Le Content-MD5 l'en-tête de demande est désormais correctement pris en charge.
11.4	<ul style="list-style-type: none"> Prise en charge accrue du balisage de compartiment, DE L'étiquetage DES compartiments ET DU balisage de compartiment. Les étiquettes de répartition des coûts ne sont pas prises en charge. Pour les compartiments créés dans StorageGRID 11.4, il n'est plus nécessaire de limiter les noms de clés d'objet pour respecter les bonnes pratiques de performance. Ajout de la prise en charge des notifications de compartiment sur le s3:ObjectRestore:Post type d'événement. Les limites de taille d'AWS pour les pièces partitionnés sont maintenant appliquées. Chaque partie d'un téléchargement partitionné doit être comprise entre 5 MIB et 5 Gio. La dernière partie peut être plus petite que 5 MIB. Ajout de la prise en charge de TLS 1.3

Relâchez	Commentaires
11.3	<ul style="list-style-type: none"> • Ajout de la prise en charge du chiffrement côté serveur des données d'objet avec les clés fournies par le client (SSE-C). • Ajout de la prise en charge des opérations DE SUPPRESSION, D'OBTENTION et DE REMPLACEMENT du cycle de vie des compartiments (action d'expiration uniquement) et pour le <code>x-amz-expiration</code> en-tête de réponse. • PUT Object mis à jour, PUT Object - copie et Multipart Upload pour décrire l'impact des règles ILM utilisant un placement synchrone à l'entrée. • Les chiffrements TLS 1.1 ne sont plus pris en charge.
11.2	<p>Ajout de la prise en charge de la restauration POST-objet pour l'utilisation avec les pools de stockage cloud. Ajout de la prise en charge de l'utilisation de la syntaxe AWS pour ARN, des clés de condition de règle et des variables de règles de groupe et de compartiment Les règles de compartiment et de groupe qui utilisent la syntaxe StorageGRID restent prises en charge.</p> <p>Remarque : les utilisations de l'ARN/URN dans d'autres configurations JSON/XML, y compris celles utilisées dans les fonctions StorageGRID personnalisées, n'ont pas changé.</p>
11.1	<p>Ajout de la prise en charge du partage de ressources entre les sources (CORS), du protocole HTTP pour les connexions client S3 aux nœuds de grid et des paramètres de conformité dans les compartiments.</p>
11.0	<p>Ajout de la prise en charge de la configuration des services de plateforme (réplication CloudMirror, notifications et intégration de la recherche Elasticsearch) pour les compartiments Ajout également de la prise en charge des contraintes d'emplacement de balisage d'objets pour les compartiments, ainsi que du paramètre de contrôle de cohérence disponible.</p>
10.4	<p>Ajout de la prise en charge des modifications de l'analyse ILM sur la gestion des versions, mises à jour de la page noms de domaine de point final, conditions et variables dans les règles, exemples de règles et autorisation PutOverwriteObject.</p>
10.3	<p>Prise en charge ajoutée pour la gestion des versions.</p>
10.2	<p>Ajout de la prise en charge des règles d'accès de groupe et de compartiment, ainsi que de la copie multipart (Télécharger la pièce - copie).</p>
10.1	<p>Ajout de la prise en charge du téléchargement partitionné, des demandes de type hébergement virtuel et de l'authentification v4.</p>
10.0	<p>Prise en charge initiale de l'API REST S3 par le système StorageGRID.la version actuellement prise en charge de <i>simple Storage Service API Reference</i> est 2006-03-01.</p>

Référence rapide : demandes d'API S3 prises en charge

Cette page explique comment StorageGRID prend en charge les API Amazon simple Storage Service (S3).

Cette page inclut uniquement les opérations S3 prises en charge par StorageGRID.



Pour afficher la documentation AWS pour chaque opération, sélectionnez le lien dans l'en-tête.

Paramètres de requête URI courants et en-têtes de requête

Sauf mention contraire, les paramètres de requête URI courants suivants sont pris en charge :

- `versionId` (comme requis pour les opérations d'objet)

Sauf mention 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 associées

- "[Détails de l'implémentation de l'API REST S3](#)"
- "[Référence de l'API Amazon simple Storage Service : en-têtes de demande communs](#)"

["AbortMultipartUpload"](#)

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#). Pour cette demande, plus ce paramètre de requête URI supplémentaire :

- `uploadID`

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations pour les téléchargements partitionnés"](#)

"CompleteMultipartUpload"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) Pour cette demande, plus ce paramètre de requête URI supplémentaire :

- uploadId

Demander des balises XML de corps

StorageGRID prend en charge les balises XML de corps de requête suivantes :

- CompleteMultipartUpload
- Part
- ETag
- PartNumber

Documentation StorageGRID

"Chargement de pièces multiples complet"

"Objet de copie"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande, plus les en-têtes supplémentaires suivants :

- 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 demande

Aucune

Documentation StorageGRID

"[PLACER une copie d'objet](#)"

"CreateBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande, plus les en-têtes supplémentaires suivants :

- x-amz-bucket-object-lock-enabled

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

"[Opérations sur les compartiments](#)"

"CreateMultipartUpload"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande, plus les en-têtes supplémentaires suivants :

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- 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 demande

Aucune

Documentation StorageGRID

"[Lancer le téléchargement de pièces multiples](#)"

[**"DeleteBucket"**](#)

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Documentation StorageGRID

"[Opérations sur les compartiments](#)"

[**"DeleteBucketCors"**](#)

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 demande

Aucune

Documentation StorageGRID

"[Opérations sur les compartiments](#)"

[**"DeleteBucketEncryption"**](#)

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 demande

Aucune

Documentation StorageGRID

"[Opérations sur les compartiments](#)"

[**"DeleteBucketLifecycle"**](#)

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 demande

Aucune

Documentation StorageGRID

- "[Opérations sur les compartiments](#)"
- "[Création de la configuration du cycle de vie S3](#)"

"DeleteBucketPolicy"

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 demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"DeleteBucketReplication"

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 demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"DeleteBucketTagging"

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 demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"DeleteObject"

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 de demande supplémentaire :

- x-amz-bypass-governance-retention

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les objets"](#)

"DeleteObjects"

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 de demande supplémentaire :

- x-amz-bypass-governance-retention

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

"Opérations sur les objets" (SUPPRIMER plusieurs objets)

"DeleteObjectTagging"

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les objets"

"GetBucketAcl"

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 demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"GetBucketCors"

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 demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"GetBucketEncryption"

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 demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"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 demande

Aucune

Documentation StorageGRID

- "[Opérations sur les compartiments](#)" (GET Bucket Lifecycle)
- "[Création de la configuration du cycle de vie S3](#)"

"GetBuckeLocation"

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 demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"GetBucketNotificationConfiguration"

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 demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#) (GET Bucket notification)

"GetBucketPolicy"

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 demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"GetBuckeReplication"

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 demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"GetBucketTagging"

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 demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"GetBucketVersioning"

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 demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"GetObject"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) Pour cette demande, plus les paramètres de requête URI supplémentaires suivants :

- partNumber
- response-cache-control
- response-content-disposition
- response-content-encoding
- response-content-language
- response-content-type
- response-expires

Et ces en-têtes de demande 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 demande

Aucune

Documentation StorageGRID

["OBTENIR l'objet"](#)

[**"GetObjectAcl"**](#)

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 demande

Aucune

Documentation StorageGRID

["Opérations sur les objets"](#)

[**"GetObjectLegalHold"**](#)

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 demande

Aucune

Documentation StorageGRID

["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#)

[**"GetObjectLockConfiguration"**](#)

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 demande

Aucune

Documentation StorageGRID

["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#)

[**"GetObjectRetention"**](#)

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 demande

Aucune

Documentation StorageGRID

"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

"GetObjectTagging"

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 demande

Aucune

Documentation StorageGRID

"Opérations sur les objets"

"Godet principal"

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 demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"Objet principal"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande, plus les en-têtes supplémentaires suivants :

- 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 demande

Aucune

Documentation StorageGRID

"Objet TÊTE"

"Listseaux"

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 demande

Aucune

Documentation StorageGRID

["Opérations sur le service et gt ; OBTENIR le service"](#)

"ListMultipartUploads"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande, plus les paramètres supplémentaires suivants :

- delimiter
- encoding-type
- key-marker
- max-uploads
- prefix
- upload-id-marker

Corps de la demande

Aucune

Documentation StorageGRID

["Liste des téléchargements partitionnés"](#)

"ListObjects"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande, plus les paramètres supplémentaires suivants :

- delimiter
- encoding-type
- marker
- max-keys
- prefix

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#) (TÉLÉCHARGER le compartiment)

"ListentsV2"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande, plus les paramètres supplémentaires suivants :

- continuation-token
- delimiter
- encoding-type
- fetch-owner
- max-keys
- prefix
- start-after

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#) (TÉLÉCHARGER le compartiment)

"ListObjectVersions"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande, plus les paramètres supplémentaires suivants :

- delimiter
- encoding-type
- key-marker
- max-keys
- prefix
- version-id-marker

Corps de la demande

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#) (OBTENIR les versions d'objet compartiment)

"ListParts"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande, plus les paramètres supplémentaires suivants :

- max-parts

- part-number-marker
- uploadId

Corps de la demande

Aucune

Documentation StorageGRID

["Liste des téléchargements partitionnés"](#)

[**"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 demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

["Opérations sur les compartiments"](#)

[**"PutBucketEncryption"**](#)

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Demandeur des balises XML de corps

StorageGRID prend en charge les balises XML de corps de requête suivantes :

- ServerSideEncryptionConfiguration
- Rule
- ApplyServerSideEncryptionByDefault
- SSEAlgorithm

Documentation StorageGRID

["Opérations sur les compartiments"](#)

[**"PutBucketLifecycleConfiguration"**](#)

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Demandeur des balises XML de corps

StorageGRID prend en charge les balises XML de corps de requête suivantes :

- NewerNoncurrentVersions
- LifecycleConfiguration
- Rule

- Expiration
- Days
- Filter
- And
- Prefix
- Tag
- Key
- Value
- Prefix
- Tag
- Key
- Value
- ID
- NoncurrentVersionExpiration
- NoncurrentDays
- Prefix
- Status

Documentation StorageGRID

- "[Opérations sur les compartiments](#)" (Cycle de vie DU godet PUT)
- "[Création de la configuration du cycle de vie S3](#)"

"PutBucketNotificationConfiguration"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Demandeur des balises XML de corps

StorageGRID prend en charge les balises XML de corps de requête suivantes :

- Prefix
- Suffix
- NotificationConfiguration
- TopicConfiguration
- Event
- Filter
- S3Key
- FilterRule

- Name
- Value
- Id
- Topic

Documentation StorageGRID

["Opérations sur les compartiments"](#) (Notification PUT Bucket)

"PutBucketPolicy"

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 demande

Pour plus d'informations sur les champs de corps JSON pris en charge, reportez-vous à la section "[Utilisez les règles d'accès au compartiment et au groupe](#)".

"PutBucketReplication"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Demandeur des balises XML de corps

- ReplicationConfiguration
- Status
- Prefix
- Destination
- Bucket
- StorageClass
- Rule

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"Étiquetage PutBucketTagging"

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 demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"PutBucketVersioning"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Demander les paramètres du corps

StorageGRID prend en charge les paramètres de corps de demande suivants :

- VersioningConfiguration
- Status

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"PutObject"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande, plus les en-têtes supplémentaires suivants :

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- 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 demande

- Données binaires de l'objet

Documentation StorageGRID

["PLACER l'objet"](#)

"PutObjectLegalHold"

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 demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#)

"PutObjectLockConfiguration"

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 demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

["Utilisez l'API REST S3 pour configurer le verrouillage 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 demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#)

"Marquage PutObject"

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 demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

["Opérations sur les objets"](#)

"SelectObjectContent"

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 demande

Pour plus d'informations sur les champs de corps pris en charge, reportez-vous aux sections suivantes :

- ["Utiliser S3 Select"](#)
- ["Sélectionnez contenu de l'objet"](#)

"UploadPart"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) Pour cette demande, plus les paramètres de requête URI supplémentaires suivants :

- partNumber
- uploadId

Et ces en-têtes de demande supplémentaires :

- 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 demande

- Données binaires de la pièce

Documentation StorageGRID

"Télécharger la pièce"

"UploadPartCopy"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) Pour cette demande, plus les paramètres de requête URI supplémentaires suivants :

- partNumber
- uploadId

Et ces en-têtes de demande 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 demande

Aucune

Documentation StorageGRID

["Télécharger la pièce - Copier"](#)

Configurez les comptes et les connexions des locataires

Pour configurer StorageGRID pour accepter les connexions à partir des applications client, vous devez créer un ou plusieurs comptes de tenant et configurer les connexions.

Créez et configurez des comptes de locataire S3

Un compte de locataire S3 est requis avant que les clients d'API S3 ne puissent stocker et récupérer des objets sur StorageGRID. Chaque compte de locataire possède son propre ID de compte, ses propres groupes, utilisateurs, compartiments et objets.

Les comptes de locataires S3 sont créés par un administrateur grid StorageGRID à l'aide de Grid Manager ou de l'API de gestion du grid. Voir "[Gérer les locataires](#)" pour plus d'informations. Une fois le compte d'un locataire S3 créé, les utilisateurs peuvent accéder au gestionnaire des locataires pour gérer les groupes, les utilisateurs, les clés d'accès et les compartiments. Voir "[Utilisez un compte de locataire](#)" pour plus d'informations.

 Les locataires S3 peuvent créer et gérer des clés d'accès S3 et des compartiments avec le gestionnaire de locataires. Ils doivent utiliser une application client S3 pour ingérer et gérer les objets. Voir "[UTILISEZ L'API REST S3](#)" pour plus d'informations.

Comment configurer les connexions client

Un administrateur du grid fait des choix de configuration qui affectent la façon dont les clients S3 se connectent à StorageGRID pour stocker et récupérer les données. La connexion d'StorageGRID à une application S3 se fait en quatre étapes de base :

- Effectuez les tâches requises dans StorageGRID, en fonction de la façon dont l'application client se connecte à StorageGRID.
- Utilisez StorageGRID pour obtenir les valeurs dont l'application a besoin pour se connecter à la grille. Vous pouvez l'un ou l'autre "[Utilisez l'assistant d'installation S3](#)" Ou configurez chaque entité StorageGRID manuellement.
- Utilisez l'application S3 pour terminer la connexion à StorageGRID. Créez des entrées DNS pour associer des adresses IP à tous les noms de domaine que vous prévoyez d'utiliser.

- Effectuez des tâches continues dans l'application et dans StorageGRID afin de gérer et de surveiller le stockage objet au fil du temps.

Pour plus de détails sur ces étapes, reportez-vous à la section "["Configurer les connexions client"](#)".

Informations requises pour les connexions client

Pour stocker ou récupérer des objets, les applications client S3 se connectent au service Load Balancer, qui est inclus sur tous les nœuds d'administration et les nœuds de passerelle, ou au service LDR (local distribution Router), qui est inclus sur tous les nœuds de stockage.

Les applications client peuvent se connecter à StorageGRID en utilisant l'adresse IP d'un nœud grid et le numéro de port du service sur ce nœud. Vous pouvez également créer des groupes haute disponibilité de nœuds d'équilibrage de la charge pour fournir des connexions haute disponibilité utilisant des adresses IP virtuelles (VIP). Si vous souhaitez vous connecter à StorageGRID à l'aide d'un nom de domaine complet (FQDN) au lieu d'une adresse IP ou VIP, vous pouvez configurer des entrées DNS.

Voir "["Résumé : adresses IP et ports pour les connexions client"](#)" pour en savoir plus.

Choisissez d'utiliser des connexions HTTPS ou HTTP

Lorsque les connexions client sont effectuées à l'aide d'un noeud final Load Balancer, les connexions doivent être effectuées à l'aide du protocole (HTTP ou HTTPS) spécifié pour ce noeud final. Pour utiliser HTTP pour les connexions client aux nœuds de stockage, vous devez activer son utilisation.

Par défaut, lorsque les applications client se connectent aux nœuds de stockage, elles doivent utiliser le protocole HTTPS chiffré pour toutes les connexions. Vous pouvez également activer des connexions HTTP moins sécurisées en sélectionnant **CONFIGURATION > Paramètres de sécurité > réseau et objets > Activer HTTP pour les connexions de noeud de stockage** dans le gestionnaire de grille. Par exemple, une application client peut utiliser HTTP lors du test de la connexion à un noeud de stockage dans un environnement non-production.



Soyez prudent lorsque vous activez HTTP pour une grille de production car les requêtes et les réponses seront envoyées sans cryptage.

Informations associées

["Administrez StorageGRID"](#)

["Avantages des connexions HTTP actives, inactives et simultanées"](#)

Noms de domaine de terminaux S3 pour les requêtes S3

Avant d'utiliser les noms de domaine de terminaux S3 pour les demandes client, un administrateur StorageGRID doit configurer le système pour qu'il accepte les connexions qui utilisent les noms de domaine de terminaux S3 dans les demandes de type chemin d'accès S3 et de type hébergement virtuel S3.

Description de la tâche

Pour pouvoir utiliser des demandes de style hébergement virtuel S3, un administrateur grid doit effectuer les tâches suivantes :

- Utilisez le Gestionnaire de grille pour ajouter les noms de domaine de points de terminaison S3 au système StorageGRID.
- Vérifiez que le certificat utilisé par le client pour les connexions HTTPS à StorageGRID est signé pour tous les noms de domaine requis par le client.

Par exemple, si le terminal du domaine de terminal du service d'API S3 est s3.company.com, l'administrateur de la grille doit s'assurer que le certificat utilisé pour les connexions HTTPS a s3.company.com En tant que nom commun du sujet et dans les autres noms du sujet, et *.s3.company.com Dans les autres noms du sujet.

- ["Configurer le serveur DNS"](#) Utilisé par le client pour inclure des enregistrements DNS qui correspondent aux noms de domaine du noeud final S3, y compris tous les enregistrements génériques requis.

Si le client se connecte à l'aide du service Load Balancer, le certificat que l'administrateur de la grille configure est le certificat du noeud final de l'équilibrEUR de charge utilisé par le client.



Chaque terminal de l'équilibrEUR de charge possède son propre certificat, et chaque terminal peut être configuré pour reconnaître différents noms de domaine de terminal S3.

Si le client se connecte aux nœuds de stockage, le certificat que l'administrateur de la grille configure est le certificat de serveur personnalisé unique utilisé pour la grille.

Reportez-vous aux instructions pour ["Administration d'StorageGRID"](#) pour en savoir plus.

Une fois ces étapes terminées, vous pouvez utiliser des requêtes de type hébergement virtuel.

Testez la configuration de l'API REST S3

Vous pouvez utiliser l'interface de ligne de commande d'Amazon Web Services (AWS CLI) pour tester votre connexion au système et vérifier que vous pouvez lire et écrire des objets sur le système.

Avant de commencer

- Vous avez téléchargé et installé l'interface de ligne de commandes AWS depuis ["aws.amazon.com/cli"](#).
- Vous avez créé un compte de locataire S3 dans le système StorageGRID.
- Vous avez créé une clé d'accès dans le compte de locataire.

Étapes

1. Configurez les paramètres de l'interface de ligne de commande AWS pour utiliser le compte que vous avez créé dans le système StorageGRID :
 - a. Passer en mode configuration : aws configure
 - b. Entrez l'ID de clé d'accès du compte que vous avez créé.
 - c. Entrez la clé d'accès secrète pour le compte que vous avez créé.
 - d. Entrez la région par défaut à utiliser, par exemple US-East-1.
 - e. Entrez le format de sortie par défaut à utiliser ou appuyez sur **entrée** pour sélectionner JSON.
2. Créer un compartiment.

Cet exemple suppose que vous avez configuré un noeud final d'équilibrEUR 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 compartiment est créé avec succès, l'emplacement du compartiment est renvoyé, comme illustré

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. Répertorier le contenu du compartiment 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. Supprimez 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 compartiment.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl  
delete-bucket --bucket testbucket
```

La prise en charge des services de plateforme StorageGRID

La plateforme StorageGRID permet aux comptes locataires d'StorageGRID d'utiliser des services tels qu'un compartiment S3 distant, un point de terminaison SNS (simple notification Service) ou un cluster Elasticsearch afin d'élargir les services fournis par un grid.

Le tableau suivant récapitule les services de plateforme disponibles et les API S3 utilisés pour les configurer.

Service de plateforme	Objectif	API S3 utilisée pour configurer le service
RéPLICATION CloudMirror	Réplique les objets à partir d'un compartiment StorageGRID source vers le compartiment S3 distant configuré.	PUT Bucket Replication (réPLICATION de compartiment) (voir " Opérations sur les compartiments ")
Notifications	Envoie des notifications sur les événements d'un compartiment StorageGRID source vers un point de terminaison SNS (simple notification Service) configuré.	Notification PUT Bucket (PLACER le compartiment) (voir " Opérations sur les compartiments ")
Intégration de la recherche	Envoie les métadonnées d'objet des objets stockés dans un compartiment StorageGRID vers un index Elasticsearch configuré.	" CONFIGURATION de notification des métadonnées de compartiment " Remarque : il s'agit d'une API S3 personnalisée StorageGRID.

L'administrateur du grid doit activer les services de plateforme pour un compte de locataire avant de pouvoir les utiliser. Voir "[Administrer StorageGRID](#)". Ensuite, un administrateur de tenant doit créer un noeud final qui représente le service distant dans le compte de tenant. Cette étape est requise avant la configuration d'un service. Voir "[Utilisez un compte de locataire](#)".

Recommandations relatives à l'utilisation des services de plate-forme

Avant d'utiliser les services de plateforme, vous devez connaître les recommandations suivantes :

- NetApp recommande de ne pas autoriser plus de 100 locataires actifs avec les demandes S3 nécessitant la réPLICATION CloudMirror, les notifications et l'intégration de la recherche. Avec plus de 100 locataires actifs, les performances des clients S3 sont plus lentes.
- Si la gestion des versions et la réPLICATION CloudMirror sont activées pour un compartiment S3 dans le système StorageGRID, NetApp recommande que la gestion des versions du compartiment S3 soit également activée sur le terminal de destination. Cela permet à la réPLICATION CloudMirror de générer des versions d'objet similaires sur le noeud final.
- La réPLICATION CloudMirror n'est pas prise en charge si le compartiment source est activé pour le verrouillage objet S3.
- La réPLICATION CloudMirror échoue avec une erreur AccessDenied si la conformité héritée du compartiment de destination est activée.

Implémentation de l'API REST S3 par StorageGRID

Requêtes des clients en conflit

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ».

La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.

Contrôles de cohérence

Les contrôles de cohérence assurent un équilibre entre la disponibilité des objets et la cohérence de ces objets entre plusieurs nœuds et sites de stockage, selon les exigences de votre application.

Par défaut, StorageGRID garantit la cohérence de lecture après écriture pour les nouveaux objets. Tout GET suivant un PUT réussi sera en mesure de lire les données nouvellement écrites. Les écrasements d'objets existants, les mises à jour de métadonnées et les suppressions sont cohérents. La propagation des écrasements ne prend généralement que quelques secondes ou minutes, mais peut prendre jusqu'à 15 jours.

Pour effectuer des opérations d'objet à un niveau de cohérence différent, vous pouvez définir un contrôle de cohérence pour chaque compartiment ou pour chaque opération d'API.

Contrôles de cohérence

Le contrôle de cohérence affecte la façon dont les métadonnées utilisées par StorageGRID pour suivre les objets sont distribuées entre les nœuds, et donc la disponibilité des objets pour les requêtes client.

Vous pouvez définir le contrôle de cohérence pour une opération de compartiment ou API sur l'une des valeurs suivantes :

- **All** : tous les nœuds reçoivent immédiatement les données, sinon la demande échouera.
- **Forte-global**: Garantit la cohérence 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 de clients au sein d'un site.
- **Read-after-New-write**: (Par défaut) fournit la cohérence lecture-après-écriture pour les nouveaux objets et éventuellement la cohérence pour les mises à jour d'objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.
- **Disponible** : assure la cohérence finale pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.

Utilisez des contrôles de cohérence « en cas de nouvelle écriture » et « disponibles »

Lorsqu'une OPÉRATION EN TÊTE ou GET utilise le contrôle de cohérence « en cas de nouvelle écriture », StorageGRID effectue la recherche en plusieurs étapes, comme suit :

- Il recherche tout d'abord l'objet à partir d'une faible cohérence.
- Si cette recherche échoue, elle répète la recherche au niveau de cohérence suivant jusqu'à ce qu'elle atteigne un niveau de cohérence équivalent au comportement de Strong-global.

Si une opération HEAD ou GET utilise le contrôle de cohérence « read-after-New-write », mais que l'objet n'existe pas, la recherche d'objets atteindra toujours un niveau de cohérence équivalent au comportement pour les groupes globaux forts. Ce niveau de cohérence exigeant la disponibilité de plusieurs copies des métadonnées d'objet sur chaque site, vous pouvez recevoir un nombre élevé d'erreurs de serveur interne 500 si deux nœuds de stockage ou plus sur le même site sont indisponibles.

À moins que vous n'ayez besoin de garanties de cohérence similaires à Amazon S3, vous pouvez empêcher ces erreurs de TÊTE et D'OBTENIR des opérations en définissant le contrôle de cohérence sur « disponible ». Lorsqu'une OPÉRATION DE TÊTE OU D'OBTENTION utilise le contrôle de cohérence « disponible », StorageGRID n'offre qu'une cohérence éventuelle. Elle n'essaie pas d'effectuer une opération ayant échoué à des niveaux de cohérence toujours plus élevés. Il n'est donc pas nécessaire que plusieurs copies des métadonnées de l'objet soient disponibles.

Spécifiez le contrôle de cohérence pour les opérations d'API

Pour définir le contrôle de cohérence pour une opération API individuelle, les contrôles de cohérence doivent être pris en charge pour l'opération, et vous devez spécifier le contrôle de cohérence dans l'en-tête de la demande. Cet exemple définit le contrôle de cohérence sur "site de segmentation" pour une opération D'OBTENTION d'objet.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```



Vous devez utiliser le même contrôle de cohérence pour les opérations PLACER l'objet et OBtenir l'objet.

Contrôle de cohérence du compartiment

Pour définir le contrôle de cohérence du compartiment, vous pouvez utiliser la demande de cohérence StorageGRID PUT bucket et la demande DE cohérence GET bucket. Vous pouvez également utiliser le Gestionnaire de locataires ou l'API de gestion des locataires.

Lors du réglage des commandes de cohérence pour un godet, tenez compte des éléments suivants :

- La configuration du contrôle de cohérence d'un compartiment détermine quel contrôle de cohérence est utilisé pour les opérations S3 effectuées sur les objets dans le compartiment ou sur la configuration du compartiment. Cela n'affecte pas les opérations du compartiment lui-même.
- Le contrôle de cohérence d'une opération API individuelle remplace le contrôle de cohérence du compartiment.
- En général, les compartiments doivent utiliser le contrôle de cohérence par défaut, « read-after-New-write ». Si les demandes ne fonctionnent pas correctement, modifiez le comportement du client d'application si possible. Ou configurez le client afin de spécifier le contrôle de cohérence pour chaque requête d'API. Réglez le contrôle de cohérence au niveau du godet uniquement en dernier recours.

[[comment les contrôles-cohérence-et-règles-ILM-interagissent]]Comment les contrôles de cohérence et les règles ILM interagissent pour protéger les données

Le contrôle de cohérence et la règle ILM de votre choix affectent la protection des objets. Ces paramètres peuvent interagir.

Par exemple, le contrôle de cohérence utilisé lorsqu'un objet est stocké affecte le placement initial des métadonnées d'objet, tandis que le comportement d'ingestion sélectionné pour la règle ILM affecte le placement initial des copies d'objet. Étant donné que StorageGRID nécessite l'accès aux métadonnées d'un objet et à ses données pour répondre aux demandes client, la sélection de niveaux de protection

correspondant au niveau de cohérence et au comportement d'ingestion permet d'améliorer la protection des données initiale et de mieux prévoir les réponses du système.

Les comportements d'ingestion suivants sont disponibles pour les règles ILM :

- **Dual commit** : StorageGRID effectue immédiatement des copies intermédiaires de l'objet et renvoie le succès au client. Les copies spécifiées dans la règle ILM sont effectuées 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 faire toutes les copies spécifiées dans la règle ILM à l'entrée; si ce n'est pas possible, des copies intermédiaires sont faites et le succès est renvoyé au client. Les copies spécifiées dans la règle ILM sont effectuées lorsque cela est possible.



Avant de sélectionner le comportement d'entrée d'une règle ILM, lisez la description complète de ces paramètres dans les instructions de gestion des objets avec la gestion du cycle de vie des informations.

Exemple d'interaction du contrôle de cohérence et de la règle ILM

Supposons que vous disposez d'une grille à deux sites avec la règle ILM suivante et le paramètre de niveau de cohérence suivant :

- **Règle ILM** : créez deux copies d'objet, une sur le site local et une sur un site distant. Le comportement d'entrée strict est sélectionné.
- **Niveau de cohérence**: "Sept-global" (les métadonnées d'objet sont immédiatement distribuées à tous les sites).

Lorsqu'un client stocke un objet dans la grille, StorageGRID effectue à la fois des copies d'objet et distribue les métadonnées aux deux sites avant de rétablir la réussite du client.

L'objet est entièrement protégé contre la perte au moment du message d'ingestion. Par exemple, si le site local est perdu peu de temps après l'ingestion, des copies des données de l'objet et des métadonnées de l'objet existent toujours sur le site distant. L'objet est entièrement récupérable.

Si vous utilisez à la place la même règle ILM et le niveau de cohérence "sept-site", le client peut recevoir un message de réussite après la réplication des données d'objet vers le site distant, mais avant que les métadonnées d'objet ne soient distribuées sur ce site. Dans ce cas, le niveau de protection des métadonnées d'objet ne correspond pas au niveau de protection des données d'objet. Si le site local est perdu peu de temps après l'ingestion, les métadonnées d'objet sont perdues. Impossible de récupérer l'objet.

L'interdépendance entre les niveaux de cohérence et les règles ILM peut être complexe. Contactez NetApp si vous avez besoin d'aide.

Informations associées

["Gestion des objets avec ILM"](#)

["OPTIMISEZ la cohérence des compartiments"](#)

["PRÉSERVER la cohérence du godet"](#)

Gestion des objets par les règles StorageGRID ILM

L'administrateur du grid crée des règles de gestion du cycle de vie des informations pour

gérer les données d'objet ingérées sur le système StorageGRID à partir des applications client de l'API REST S3. Ces règles sont ensuite ajoutées à la règle ILM pour déterminer la façon dont et l'emplacement de stockage des données d'objet au fil du temps.

Les paramètres ILM déterminent les aspects suivants d'un objet :

- **Géographie**

L'emplacement des données d'un objet, dans le système StorageGRID (pool de stockage) ou dans un pool de stockage cloud.

- **Grade de stockage**

Type de stockage utilisé pour stocker les données d'objet : par exemple, Flash ou disque rotatif.

- * Protection contre les pertes*

Le nombre de copies effectuées et les types de copies créées : réplication, code d'effacement, ou les deux.

- * Rétention*

Évolution au fil du temps de la gestion des données d'un objet, de leur emplacement de stockage et de leur protection contre la perte.

- * Protection pendant l'ingestion*

Méthode de protection des données d'objet lors de l'ingestion : placement synchrone (avec options équilibrées ou strictes pour le comportement d'ingestion) ou copies intermédiaires (avec l'option de double validation).

Les règles ILM peuvent filtrer et sélectionner des objets. Pour les objets ingérées à l'aide du protocole S3, les règles ILM peuvent filtrer les objets en fonction des métadonnées suivantes :

- Compte locataire
- Nom du compartiment
- Temps d'ingestion
- Clé
- Heure du dernier accès



Par défaut, les mises à jour de l'heure du dernier accès sont désactivées pour tous les compartiments S3. Si votre système StorageGRID inclut une règle ILM utilisant l'option heure du dernier accès, vous devez activer les mises à jour à l'heure du dernier accès pour les compartiments S3 spécifiés dans cette règle. Utilisez la demande DE l'heure du dernier accès du compartiment PUT, le Gestionnaire de locataires (voir "[Activez ou désactivez les mises à jour de l'heure du dernier accès](#)") Ou l'API de gestion des locataires. Lors de l'activation des mises à jour du dernier accès, notez que les performances du StorageGRID peuvent être réduites, notamment dans les systèmes dotés d'objets de petite taille.

- Contrainte d'emplacement
- Taille de l'objet

- Métagdonnées d'utilisateur
- Balise d'objet

Informations associées

["Utilisez un compte de locataire"](#)

["Gestion des objets avec ILM"](#)

["METTRE l'heure du dernier accès au compartiment"](#)

Gestion des versions d'objet

Vous pouvez utiliser la gestion des versions pour conserver plusieurs versions d'un objet, ce qui vous protège contre la suppression accidentelle d'objets et vous permet d'extraire et de restaurer les versions antérieures d'un objet.

Le système StorageGRID implémente la gestion des versions avec prise en charge de la plupart des fonctionnalités et avec certaines limites. StorageGRID prend en charge jusqu'à 1,000 versions de chaque objet.

Le contrôle de version d'objets peut être associé à la gestion du cycle de vie des informations (ILM) d'StorageGRID ou à la configuration du cycle de vie des compartiments S3. Vous devez activer explicitement la gestion des versions pour chaque compartiment pour activer cette fonctionnalité. Chaque objet du compartiment est associé à un ID de version, généré par le système StorageGRID.

La suppression de l'authentification multifacteur (MFA) n'est pas prise en charge.



Le contrôle de version ne peut être activé que pour les compartiments créés avec StorageGRID version 10.3 ou ultérieure.

ILM et gestion des versions

Les règles ILM sont appliquées à chaque version d'un objet. Un processus d'analyse ILM analyse en continu tous les objets, puis les évalue à nouveau en fonction de la règle ILM actuelle. Toute modification apportée aux règles ILM est appliquée à tous les objets précédemment ingérées. Ceci inclut les versions préalablement ingérées si la gestion des versions est activée. L'analyse ILM applique les modifications de l'ILM aux objets précédemment ingérées.

Pour les objets S3 dans les compartiments avec gestion des versions, la prise en charge des versions vous permet de créer des règles ILM qui utilisent « Noncurrent Time » comme heure de référence (sélectionnez **Yes** pour la question, « Apply this rule to Older versions only? ») po ["Étape 1 de l'assistant de création de règles ILM"](#)). Lorsqu'un objet est mis à jour, ses versions précédentes deviennent non actuelles. L'utilisation d'un filtre « Noncurrent Time » vous permet de créer des règles qui réduisent l'impact sur le stockage des versions précédentes d'objets.



Lorsque vous téléchargez une nouvelle version d'un objet à l'aide d'une opération de téléchargement partitionné, l'heure qui n'est pas à jour pour la version d'origine de l'objet correspond à la création du téléchargement partitionné pour la nouvelle version, et non à la fin du téléchargement partitionné. Dans des cas limités, l'heure non actuelle de la version d'origine peut être des heures ou des jours plus tôt que l'heure de la version actuelle.

Voir ["Règles et règles ILM pour les objets avec version S3 \(exemple 4\)"](#).

Utilisez l'API REST S3 pour configurer le verrouillage objet S3

Si le paramètre global de verrouillage des objets S3 est activé pour votre système StorageGRID, vous pouvez créer des compartiments avec le verrouillage des objets S3 activé. Vous pouvez spécifier des paramètres de conservation par défaut pour chaque compartiment ou pour chaque version d'objet.

Activation du verrouillage objet S3 pour un compartiment

Si le paramètre global de verrouillage d'objet S3 est activé pour votre système StorageGRID, vous pouvez activer le verrouillage d'objet S3 lorsque vous créez chaque compartiment.

Le verrouillage objet S3 est un paramètre permanent qui ne peut être activé que lorsque vous créez un compartiment. Une fois un compartiment créé, vous ne pouvez ni ajouter ni désactiver le verrouillage objet S3.

Pour activer le verrouillage objet S3 pour un compartiment, utilisez l'une des méthodes suivantes :

- Créez le compartiment à l'aide du Gestionnaire des locataires. Voir "[Créer un compartiment S3](#)".
- Créer le compartiment à l'aide d'une demande PUT bucket avec le `x-amz-bucket-object-lock-enabled` en-tête de demande. Voir "[Opérations sur les compartiments](#)".

Le verrouillage objet S3 requiert la gestion des versions des compartiments, qui est automatiquement activée lors de la création du compartiment. Vous ne pouvez pas suspendre la gestion des versions pour le compartiment. Voir "[Gestion des versions d'objet](#)".

Paramètres de conservation par défaut d'un compartiment

Lorsque le verrouillage objet S3 est activé pour un compartiment, vous pouvez éventuellement activer la conservation par défaut du compartiment et spécifier un mode de conservation par défaut et une période de conservation par défaut.

Mode de rétention par défaut

- En mode CONFORMITÉ :
 - L'objet ne peut pas être supprimé tant que sa date de conservation jusqu'à n'est pas atteinte.
 - La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être réduite.
 - La date de conservation de l'objet jusqu'à ne peut pas être supprimée tant que cette date n'est pas atteinte.
- En mode GOUVERNANCE :
 - Utilisateurs avec le `s3:BypassGovernanceRetention` l'autorisation peut utiliser le `x-amz-bypass-governance-retention: true` demander à l'en-tête de contourner les paramètres de rétention.
 - Ces utilisateurs peuvent supprimer une version d'objet avant d'atteindre sa date de conservation jusqu'à.
 - Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

Période de conservation par défaut

Une période de conservation par défaut peut être spécifiée en années ou en jours pour chaque compartiment.

Comment définir la conservation par défaut d'un compartiment

Pour définir la rétention par défaut d'un compartiment, utilisez l'une des méthodes suivantes :

- Gérez les paramètres de compartiment depuis le gestionnaire de locataires. Voir "[Créer un compartiment S3](#)" et "[Mettre à jour la conservation par défaut du verrouillage d'objet S3](#)".
- Émettre une demande DE configuration DE verrouillage d'objet PUT pour le compartiment afin de spécifier le mode par défaut et le nombre de jours ou d'années par défaut.

CONFIGURATION du verrouillage de l'objet

La demande PUT Object Lock Configuration vous permet de définir et de modifier le mode de rétention par défaut et la période de rétention par défaut pour un compartiment pour lequel S3 Object Lock est activé. Vous pouvez également supprimer les paramètres de conservation par défaut configurés précédemment.

Lorsque de nouvelles versions d'objet sont ingérées sur le compartiment, le mode de conservation 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 rétention 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 conservation à la date de la version de l'objet reste la même et n'est pas recalculée en utilisant la nouvelle période de conservation par défaut.

Vous devez avoir le `s3:PutBucketObjectLockConfiguration` autorisation, ou être root de compte, pour terminer cette opération.

Le Content-MD5 L'en-tête de demande doit être spécifié dans la demande PUT.

Exemple de demande

Cet exemple active le verrouillage objet S3 pour un compartiment 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 conservation par défaut d'un compartiment

Pour déterminer si le verrouillage objet S3 est activé pour un compartiment et pour afficher le mode de conservation et la période de conservation par défaut, utilisez l'une des méthodes suivantes :

- Affichez le compartiment dans le gestionnaire de locataires. Voir "[Afficher les compartiments S3](#)".
- Émettre une demande OBTENIR la configuration de verrouillage d'objet.

OBTENIR la configuration de verrouillage d'objet

La demande OBTENIR la configuration du verrouillage d'objet vous permet de déterminer si le verrouillage d'objet S3 est activé pour un compartiment et, si ce dernier est activé, vérifiez si un mode de conservation et une période de conservation par défaut sont configurés pour ce compartiment.

Lorsque de nouvelles versions d'objet sont ingérées sur le compartiment, le mode de conservation par défaut est appliqué si `x-amz-object-lock-mode` n'est pas spécifié. La période de rétention 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 root de compte, 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:
iVmcB7OXXJRKH1Fivq1151/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 compartiment lorsque le verrouillage objet S3 est activé peut contenir une combinaison d'objets avec ou sans paramètres de conservation du verrouillage objet S3.

Les paramètres de conservation au niveau objet sont spécifiés à l'aide de l'API REST S3. Les paramètres de conservation d'un objet remplacent les paramètres de conservation par défaut du compartiment.

Vous pouvez spécifier les paramètres suivants pour chaque objet :

- **Mode de conservation** : CONFORMITÉ ou GOUVERNANCE.
- **Conserver-jusqu'à-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 jusqu'à est dans le futur, l'objet peut être récupéré, mais il ne peut pas être modifié ou supprimé. La date de conservation jusqu'à peut être augmentée,

mais cette date ne peut pas être réduite ou supprimée.

- En mode GOUVERNANCE, les utilisateurs disposant d'une autorisation spéciale peuvent contourner le paramètre conserver jusqu'à la date. Ils peuvent supprimer une version d'objet avant la fin de sa période de conservation. Ils peuvent également augmenter, diminuer ou même supprimer la date de conservation jusqu'à.
- **Mise en garde légale** : l'application d'une mise en garde légale à une version d'objet verrouille immédiatement cet objet. Par exemple, vous devrez peut-être mettre une obligation légale sur un objet lié à une enquête ou à un litige juridique. Une obligation 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 jusqu'à. Si une version d'objet est en attente 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 compartiment, émettez un "[PLACER l'objet](#)", "[PLACER l'objet - Copier](#)", ou "[Lancer le téléchargement de pièces multiples](#)" demande.

Vous pouvez utiliser les éléments suivants :

- `x-amz-object-lock-mode`, Qui peut être CONFORMITÉ ou GOUVERNANCE (sensible à la casse).



Si vous spécifiez `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 conserver jusqu'à la date doit être au format 2020-08-10T21:46:00Z. Les secondes fractionnaires sont autorisées, mais seuls 3 chiffres après la virgule sont conservés (précision des millisecondes). Les autres formats ISO 8601 ne sont pas autorisés.

- La date de conservation doit être ultérieure.

- `x-amz-object-lock-legal-hold`

Si la conservation légale est ACTIVÉE (sensible à la casse), l'objet est placé sous une obligation légale. Si la mise en attente légale est désactivée, aucune mise en attente légale n'est mise. Toute autre valeur entraîne une erreur 400 Bad Request (InvalidArgument).

Si vous utilisez l'un de ces en-têtes de demande, tenez compte des restrictions suivantes :

- Le Content-MD5 l'en-tête de demande est requis le cas échéant `x-amz-object-lock-*` L'en-tête de la demande est présent dans la demande D'objet PUT. Content-MD5 N'est pas nécessaire pour PLACER l'objet - Copier ou lancer le téléchargement de pièces multiples.
- Si le verrouillage d'objet S3 n'est pas activé dans le compartiment et qu'un `x-amz-object-lock-*` L'en-tête de la demande est présent, une erreur 400 Bad Request (InvalidRequest) est renvoyée.
- La requête PUT Object prend en charge l'utilisation de `x-amz-storage-class: REDUCED_REDUNDANCY` Pour correspondre au comportement AWS. Cependant, lors de l'ingestion d'un objet dans un compartiment lorsque le verrouillage objet S3 est activé, StorageGRID effectue toujours une entrée à double validation.
- Une réponse ultérieure DE la version D'objet GET ou HEAD 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 demande est correct s3:Get* autorisations.

Vous pouvez utiliser le s3:object-lock-remaining-retention-days clé de condition de règle pour limiter les périodes de conservation minimale et maximale autorisée 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 conservation d'une version d'objet existante, vous pouvez effectuer les opérations de sous-ressource d'objet suivantes :

- PUT Object legal-hold

Si la nouvelle valeur de conservation légale est ACTIVÉE, l'objet est placé sous une mise en attente légale. Si la valeur de retenue légale est OFF, la suspension légale est levée.

- PUT Object retention

- La valeur du mode peut être CONFORMITÉ ou GOUVERNANCE (sensible à la casse).
 - La valeur conserver jusqu'à la date doit être au format 2020-08-10T21:46:00Z. Les secondes fractionnaires sont autorisées, mais seuls 3 chiffres après la virgule sont conservés (précision des millisecondes). Les autres formats ISO 8601 ne sont pas autorisés.
 - Si une version d'objet possède une date de conservation existante, vous pouvez uniquement l'augmenter. La nouvelle valeur doit être future.

Comment utiliser le mode GOUVERNANCE

Les utilisateurs qui disposent de s3:BypassGovernanceRetention L'autorisation peut contourner les paramètres de rétention actifs d'un objet qui utilise le mode DE GOUVERNANCE. Toute opération DE SUPPRESSION ou DE CONSERVATION D'objet PUT doit inclure le x-amz-bypass-governance-retention:true en-tête de demande. Ces utilisateurs peuvent effectuer les opérations supplémentaires suivantes :

- Effectuez DES opérations DE SUPPRESSION d'objet ou DE SUPPRESSION de plusieurs objets pour supprimer une version d'objet avant la fin de sa période de conservation.

Impossible de supprimer les objets qui sont en attente légale. La mise en attente légale doit être désactivée.

- Exécutez des opérations PUT Object Retention qui font passer le mode d'une version d'objet DE GOUVERNANCE À LA CONFORMITÉ avant que la période de conservation de l'objet ne soit écoulée.

Le passage du mode DE CONFORMITÉ À LA GOUVERNANCE n'est jamais autorisé.

- Exécutez des opérations PUT Object Retention pour augmenter, diminuer ou supprimer la période de conservation d'une version d'objet.

Informations associées

- "[Gestion des objets avec le verrouillage d'objets S3](#)"
- "[Utilisez le verrouillage d'objet S3 pour conserver les objets](#)"
- "[Guide de l'utilisateur Amazon simple Storage Service : utilisation du verrouillage d'objets S3](#)"

Création de la configuration du cycle de vie S3

Vous pouvez créer une configuration de cycle de vie S3 afin de contrôler la suppression d'objets spécifiques du système StorageGRID.

L'exemple simple de cette section illustre la façon dont une configuration du cycle de vie S3 peut contrôler la suppression de certains objets (expirés) dans des compartiments S3 spécifiques. L'exemple de cette section est fourni à titre d'illustration uniquement. Pour plus d'informations sur la création de configurations de cycle de vie S3, reportez-vous à la section "[Amazon simple Storage Service Developer Guide : gestion du cycle de vie des objets](#)". Notez que StorageGRID prend uniquement en charge les actions d'expiration, mais pas les actions de transition.

La configuration du cycle de vie

La configuration du cycle de vie est un ensemble de règles appliquées aux objets dans des compartiments S3 spécifiques. Chaque règle indique quels objets sont affectés et quand ces objets vont expirer (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 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 partir de l'ingestion de l'objet.
- NonactuelVersionExpiration : supprimez un objet lorsque le nombre de jours spécifié est atteint, à partir de quand l'objet est devenu non courant.
- Filtre (préfixe, étiquette)
- État
- ID

Si vous appliquez une configuration de cycle de vie à un compartiment, les paramètres de cycle de vie du compartiment prévalent toujours sur les paramètres ILM de StorageGRID. StorageGRID utilise les paramètres d'expiration du compartiment et non ILM pour déterminer s'il faut supprimer ou conserver des objets spécifiques.

Par conséquent, il est possible de supprimer un objet de la grille, même si les instructions de placement d'une règle ILM s'appliquent toujours à l'objet. Il est également possible de conserver un objet dans la grille même après l'expiration des instructions de placement ILM de l'objet. Pour plus de détails, voir "[Fonctionnement de ILM tout au long de la vie d'un objet](#)".



La configuration du cycle de vie des compartiments avec des compartiments dont le verrouillage objet S3 est activé, mais la configuration du cycle de vie des compartiments n'est pas prise en charge pour les compartiments conformes.

StorageGRID prend en charge les opérations suivantes des compartiments pour gérer les configurations du cycle de vie :

- SUPPRIMER le cycle de vie du compartiment
- OPTIMISEZ le cycle de vie des compartiments
- CYCLE de vie des compartiments

Créer une configuration de cycle de vie

Comme première étape de la création de la configuration du cycle de vie, vous créez un fichier JSON qui inclut une ou plusieurs règles. Par exemple, ce fichier JSON contient 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` 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` paramètre indique que les objets correspondant au filtre expirent 100 jours après leur ingestion.



Les règles spécifiant un nombre de jours sont relatives à l'ingestion de l'objet. Si la date actuelle dépasse la date d'ingestion et le nombre de jours, certains objets peuvent être supprimés du compartiment dès que la configuration de cycle de vie est appliquée.

3. La règle 3 s'applique uniquement aux objets qui correspondent au préfixe `category3/`. Le `Expiration` paramètre spécifie que toute version non actuelle des objets de correspondance expirera 50 jours après leur non-mise à jour.

```
{
    "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"
        }
    ]
}
```

Appliquez la configuration du cycle de vie au compartiment

Une fois que vous avez créé le fichier de configuration du cycle de vie, vous l'appliquez à un compartiment en émettant une demande DE cycle de vie PUT bucket.

Cette demande applique la configuration du cycle de vie dans le fichier exemple aux objets d'un compartiment nommé testbucket.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-configuration  
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Pour vérifier qu'une configuration du cycle de vie a été appliquée avec succès au compartiment, émettez une demande GET Lifecycle. Par exemple :

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-configuration  
--bucket testbucket
```

Une réponse réussie répertorie la configuration de cycle de vie que vous venez d'appliquer.

Vérifiez que l'expiration du cycle de vie du compartiment s'applique à l'objet

Vous pouvez déterminer si une règle d'expiration dans la configuration de cycle de vie s'applique à un objet spécifique lors de l'émission d'une requête D'objet PUT, HEAD Object ou GET Object. Si une règle s'applique, la réponse comprend un `Expiration` paramètre qui indique quand l'objet expire et quelle règle d'expiration a été mise en correspondance.



Le cycle de vie des compartiments ignore ILM, le `expiry-date` l'illustration représente la date réelle à laquelle l'objet sera supprimé. Pour plus de détails, voir "["Méthode de détermination de la conservation des objets"](#)".

Par exemple, cette requête PUT Object a été émise le 22 juin 2020 et place un objet dans le testbucket godet.

```
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 (01 oct 2020) et qu'il correspond à la règle 2 de la configuration de cycle de vie.

```
{
    *"Expiration": "expiry-date=\\"Thu, 01 Oct 2020 09:07:49 GMT\\\"", rule-
    id=\"rule2\",
    "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

Par exemple, cette demande d'objet TÊTE a été utilisée pour obtenir les métadonnées du même objet dans le compartiment test.

```
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": {}
}
```

Recommandations pour l'implémentation de l'API REST S3

Suivez ces recommandations lors de l'implémentation de l'API REST S3 pour une utilisation avec StorageGRID.

Recommandations pour les têtes à des objets inexistant

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 le contrôle de cohérence « disponible ». Par exemple, vous devez utiliser le contrôle de cohérence « disponible » si votre application dirige un emplacement avant DE LE PLACER.

Sinon, si l'opération HEAD ne trouve pas l'objet, vous pouvez recevoir un nombre élevé de 500 erreurs de serveur interne si un ou plusieurs nœuds de stockage ne sont pas disponibles.

Vous pouvez définir le contrôle de cohérence « disponible » pour chaque compartiment à l'aide de la demande DE cohérence PUT bucket, ou spécifier le contrôle de 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 du compartiment.

Compartiments créés dans StorageGRID 11.4 ou version antérieure

- N'utilisez pas de valeurs aléatoires comme les quatre premiers caractères des clés d'objet. Cela contraste avec l'ancienne recommandation AWS pour les préfixes de clés. Utilisez plutôt des préfixes non aléatoires et non uniques, tels que `image`.
- Si vous suivez les recommandations d'AWS pour utiliser des caractères aléatoires et uniques dans les préfixes de clés, préfixez les clés d'objet à l'aide d'un nom de répertoire. C'est-à-dire, utilisez le format suivant :

`mybucket/mydir/f8e3-image3132.jpg`

Au lieu de ce format :

`mybucket/f8e3-image3132.jpg`

Compartiments créés dans StorageGRID 11.4 ou version ultérieure

Il n'est pas nécessaire de restreindre les noms de clés d'objet pour répondre aux bonnes pratiques de performances. Dans la plupart des cas, vous pouvez utiliser des valeurs aléatoires pour les quatre premiers caractères des noms de clé d'objet.

À cela s'exception près un workload 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, il est possible de faire varier la première partie du nom de clé tous les mille objets avec une date comme la date. Supposons par exemple qu'un client S3 écrit généralement 2,000 objets/seconde et que la règle de cycle de vie ILM ou compartiment supprime tous les objets au bout de trois jours. Pour réduire l'impact sur les performances, vous pouvez nommer les clés comme suit : `/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

Recommandations pour « plages de lectures »

Si le "option globale pour compresser les objets stockés" Est activé, les applications client S3 doivent éviter d'effectuer des opérations GET Object qui spécifient une plage d'octets à renvoyer. Ces opérations de « lecture à plage » sont inefficaces, car StorageGRID doit décompresser efficacement les objets pour accéder aux octets demandés. LES opérations GET Object qui demandent une petite plage d'octets provenant d'un objet très volumineux sont particulièrement inefficaces. Par exemple, il est inefficace de lire une plage de 10 Mo sur un objet compressé de 50 Go.

Si les plages sont lues à partir d'objets compressés, les demandes client peuvent être en attente.



Si vous devez compresser des objets et que votre application client doit utiliser des lectures de plage, augmentez le délai de lecture de l'application.

Informations associées

- "[Contrôles de cohérence](#)"
- "[PRÉSERVER la cohérence du godet](#)"
- "[Administre StorageGRID](#)"

Prise en charge de l'API REST Amazon S3

Détails de l'implémentation de l'API REST S3

Le système StorageGRID implémente l'API simple Storage Service (API version 2006-03-01) avec la prise en charge de la plupart des opérations et avec certaines limites. Vous devez connaître les détails d'implémentation lorsque vous intégrez des applications client de l'API REST S3.

Le système StorageGRID prend en charge les demandes de type hébergement virtuel et les demandes de type chemin d'accès.

Traitement de la date

L'implémentation StorageGRID de l'API REST S3 ne prend en charge que 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 heure de la date peut être spécifiée au format heure de Greenwich (GMT) ou au format heure coordonnée universelle (UTC) sans décalage de fuseau horaire (+0000 doit être spécifié). Si vous incluez le `x-amz-date` En-tête de votre demande, elle remplace toute valeur spécifiée dans l'en-tête de la demande de date. Lors de l'utilisation de la signature AWS 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 demande commune

Le système StorageGRID prend en charge les en-têtes de requête communs définis par "[Référence de l'API Amazon simple Storage Service : en-têtes de demande communs](#)", à une exception près.

En-tête de demande	Mise en place
Autorisation	Prise en charge complète de la signature AWS version 2 Prise en charge de la signature AWS version 4, à l'exception des cas suivants : <ul style="list-style-type: none">La valeur SHA256 n'est pas calculée pour le corps de la demande. La valeur soumise par l'utilisateur est acceptée sans validation, comme si la valeur UNSIGNED-PAYLOAD avait été prévu pour le <code>x-amz-content-sha256</code> en-tête.
jeton de sécurité x-amz	Non mis en œuvre. Retours <code>XNotImplemented</code> .

En-têtes de réponse commune

Le système StorageGRID prend en charge tous les en-têtes de réponse courants définis par l'*API simple Storage Service Reference*, à une exception près.

En-tête de réponse	Mise en place
<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 la version 2 de Signature et la version 4 de Signature pour authentifier les requêtes API S3.

Les demandes authentifiées doivent être signées à l'aide de votre ID de clé d'accès et de votre clé secrète d'accès.

Le système StorageGRID prend en charge deux méthodes d'authentification : le protocole HTTP Authorization en-tête et utilisation des paramètres de requête.

Utilisez l'en-tête HTTP Authorization

Le HTTP Authorization L'en-tête est utilisé par toutes les opérations de l'API S3 à l'exception des demandes anonymes lorsque la stratégie de compartiment l'autorise. Le Authorization en-tête contient toutes les informations de signature requises pour authentifier une demande.

Utiliser les paramètres de requête

Vous pouvez utiliser les paramètres de requête pour ajouter des informations d'authentification à une URL. Il s'agit de la présignature de l'URL, qui peut être utilisée pour accorder un accès temporaire à des ressources spécifiques. Les utilisateurs avec 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 limité tiers à une ressource.

Opérations sur le service

Le système StorageGRID prend en charge les opérations suivantes sur ce service.

Fonctionnement	Mise en place
ACCÉDER au service (ListBuckets)	Mise en œuvre avec tout le comportement de l'API REST Amazon S3. D'être modifiées sans préavis.
DÉCOUVREZ l'utilisation du stockage	La demande GET Storage usage 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 client peuvent émettre OPTIONS / Requêtes vers le port S3 d'un nœud de stockage, sans identifiants d'authentification S3, pour déterminer si le nœud de stockage est disponible. Vous pouvez utiliser cette requête pour la surveillance ou permettre aux équilibriseurs de charge externes d'identifier lorsqu'un nœud de stockage est arrêté.

Informations associées

["DÉCOUVREZ l'utilisation du stockage"](#)

Opérations sur les compartiments

Le système StorageGRID prend en charge un maximum de 1,000 compartiments pour chaque compte de locataire S3.

Les restrictions relatives aux noms de compartiment respectent les restrictions régionales standard AWS, mais vous devez les restreindre à une nomenclature DNS pour prendre en charge les demandes de type hébergement virtuel S3.

Pour plus d'informations, reportez-vous aux sections suivantes :

- "[Documentation Amazon Web Services \(AWS\) : restrictions et limites des compartiments](#)"
- "[Configuration des noms de domaine de terminaux S3](#)"

Les opérations GET Bucket (List Objects) et GET compartiment versions prennent en charge les contrôles de cohérence StorageGRID.

Vous pouvez vérifier si les mises à jour de l'heure du dernier accès sont activées ou désactivées pour les compartiments individuels.

Le tableau suivant décrit la façon dont StorageGRID implémente les opérations des compartiments de l'API REST S3. Pour effectuer l'une de ces opérations, les informations d'identification d'accès nécessaires doivent être fournies pour le compte.

Fonctionnement	Mise en place
SUPPRIMER le compartiment	Cette opération supprime le godet.
SUPPRIMER les godets	Cette opération supprime la configuration CORS pour le compartiment.
SUPPRIMER le chiffrement du compartiment	Cette opération supprime le chiffrement par défaut du compartiment. Les objets chiffrés existants restent chiffrés, mais aucun nouvel objet ajouté au compartiment n'est chiffré.
SUPPRIMER le cycle de vie du compartiment	Cette opération supprime la configuration du cycle de vie du compartiment. Voir " Création de la configuration du cycle de vie S3 ".
SUPPRIMER la règle de compartiment	Cette opération supprime la règle attachée au compartiment.
SUPPRIMER la réplication du compartiment	Cette opération supprime la configuration de réplication attachée au compartiment.
SUPPRIMER le balisage du compartiment	Cette opération utilise le tagging sous-ressource pour supprimer toutes les balises d'un compartiment.

Fonctionnement	Mise en place
RUBRIQUE GET (ListObjects) (ListObjectsV2)	<p>Cette opération renvoie une partie ou la totalité (jusqu'à 1,000) des objets dans un godet. La classe de stockage pour les objets peut avoir l'une ou l'autre des deux valeurs, même si l'objet a été ingéré avec le REDUCED_REDUNDANCY option de classe de stockage :</p> <ul style="list-style-type: none"> • STANDARD, Qui indique que l'objet est stocké dans un pool de stockage composé de nœuds de stockage. • GLACIER, Qui indique que l'objet a été déplacé vers le compartiment 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 une partie CommonPrefixes qui ne contiennent pas de clés.</p>
OBTENIR les versions d'objet de compartiment (ListObjectVersions)	Avec accès EN LECTURE sur un godet, cette opération avec le <code>versions</code> sous-ressource répertorie les métadonnées de toutes les versions des objets dans le compartiment.
OBTENIR l'acl du compartiment	Cette opération renvoie une réponse positive et l'ID, le DisplayName et l'autorisation du propriétaire du compartiment, indiquant que le propriétaire a un accès complet au compartiment.
OBTENIR les godets	Cette opération renvoie le <code>cors</code> configuration du compartiment.
CHIFFREMENT des compartiments	Cette opération renvoie la configuration de cryptage par défaut pour le compartiment.
OPTIMISEZ le cycle de vie des compartiments (GetBucketLifecycleConfiguration)	Cette opération retourne la configuration du cycle de vie du godet. Voir " Création de la configuration du cycle de vie S3 ".
ACCÉDER à l'emplacement du compartiment	Cette opération renvoie la région définie à l'aide de <code>LocationConstraint</code> Élément dans la demande PUT Bucket. Si la région du godet est de <code>us-east-1</code> , une chaîne vide est renvoyée pour la région.
GET Bucket notification (GetBucketNotificationConfiguration)	Cette opération renvoie la configuration de notification attachée au compartiment.
GET Bucket policy	Cette opération renvoie la politique attachée au godet.
RÉPLICATION des compartiments	Cette opération renvoie la configuration de réPLICATION attachée au compartiment.

Fonctionnement	Mise en place
GET Bucket tagging	Cette opération utilise le tagging sous-ressource pour renvoyer toutes les balises d'un compartiment.
GESTION des versions des compartiments	Cette implémentation utilise le <code>versioning</code> sous-ressource pour retourner l'état de gestion des versions d'un compartiment. <ul style="list-style-type: none"> • <i>Blank</i>: La gestion des versions n'a jamais été activée (le compartiment est « non versionné ») • Activé : la gestion des versions est activée • Suspendu : la gestion des versions a déjà été activée et est suspendue
OBTENIR la configuration de verrouillage d'objet	Cette opération renvoie le mode de rétention par défaut du compartiment et la période de conservation par défaut, si configuré. Voir " Utilisez l'API REST S3 pour configurer le verrouillage objet S3 ".
Godet DE TÊTE	Cette opération détermine si un compartiment existe et que vous êtes autorisé à y accéder. Cette opération renvoie : <ul style="list-style-type: none"> • <code>x-ntap-sg-bucket-id</code>: L'UUID du godet au format UUID. • <code>x-ntap-sg-trace-id</code>: ID de trace unique de la demande associée.

Fonctionnement	Mise en place
PLACER le godet	<p>Cette opération crée un nouveau godet. C'est en créant le compartiment que vous devenez le propriétaire.</p> <ul style="list-style-type: none"> Les noms de compartiment doivent être conformes aux règles suivantes : <ul style="list-style-type: none"> Il doit être unique sur chaque système StorageGRID (et pas seulement au sein du compte du locataire). Doit être conforme DNS. Doit contenir au moins 3 caractères 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 ou un chiffre en minuscules et ne peut utiliser que des lettres minuscules, des chiffres et des tirets. Ne doit pas ressembler à une adresse IP au format texte. Ne doit pas utiliser de périodes dans des demandes de type hébergement virtuel. Les périodes provoquera des problèmes avec la vérification du certificat générique du serveur. Par défaut, les compartiments sont créés dans le us-east-1 région ; cependant, vous pouvez utiliser le LocationConstraint élément de demande dans le corps de la demande pour spécifier une région différente. Lorsque vous utilisez le LocationConstraint Elément, 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 région que vous devez utiliser. <p>Remarque : une erreur se produit si votre demande PUT Bucket utilise une région qui n'a pas été définie dans StorageGRID.</p> <ul style="list-style-type: none"> Vous pouvez inclure le x-amz-bucket-object-lock-enabled Demander l'en-tête pour créer un compartiment avec le verrouillage objet S3 activé. Voir "Utilisez l'API REST S3 pour configurer le verrouillage objet S3". <p>Vous devez activer le verrouillage d'objet S3 lors de la création du compartiment. Une fois un compartiment créé, vous ne pouvez ni ajouter ni désactiver le verrouillage objet S3. Le verrouillage objet S3 requiert la gestion des versions de compartiment, qui est activée automatiquement lors de la création du compartiment.</p>
PLACEZ les godets	Cette opération définit la configuration du CORS pour un compartiment afin que le compartiment puisse traiter les demandes d'origine croisée. Le partage de ressources d'origine croisée (CORS) est un mécanisme de sécurité qui permet aux applications Web clientes d'un domaine d'accéder aux ressources d'un domaine différent. Supposons par exemple que vous utilisez un compartiment S3 nommé images pour stocker des graphiques. En définissant la configuration CORS pour le images le champ permet d'afficher les images de ce compartiment sur le site web http://www.example.com .

Fonctionnement	Mise en place
PUT Bucket Encryption	<p>Cette opération définit l'état de cryptage par défaut d'un compartiment existant. Lorsque le chiffrement au niveau du compartiment est activé, tout nouvel objet ajouté au compartiment est chiffré. StorageGRID prend en charge le chiffrement côté serveur avec des clés gérées par StorageGRID. Lorsque vous spécifiez la règle de configuration de cryptage côté serveur, définissez l' <code>SSEAlgorithm</code> paramètre à <code>AES256</code>, et n'utilisez pas le <code>KMSMasterKeyID</code> paramètre.</p> <p>La configuration de cryptage par défaut du compartiment est ignorée si la demande de téléchargement d'objet spécifie déjà le cryptage (c'est-à-dire, si la demande inclut le <code>x-amz-server-side-encryption-*</code> en-tête de demande).</p>
CYCLE de vie des compartiments (Configuration PutBucketLifecycleConfiguration)	<p>Cette opération crée une nouvelle configuration de cycle de vie pour le compartiment 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 cycle de vie. Chaque règle peut inclure les éléments XML suivants :</p> <ul style="list-style-type: none"> • Expiration (jours, date) • NonactuelVersionExp (Nontactut Days) • Filtre (préfixe, étiquette) • État • ID <p>StorageGRID ne prend pas en charge les actions suivantes :</p> <ul style="list-style-type: none"> • AbortIncompleteMultipartUpload • ExpiredObjectDeleteMarker • Transition <p>Voir "Création de la configuration du cycle de vie S3". Pour comprendre comment l'action d'expiration d'un cycle de vie de compartiment interagit avec les instructions de placement ILM, reportez-vous à la section "Fonctionnement de ILM tout au long de la vie d'un objet".</p> <p>Remarque : la configuration du cycle de vie des compartiments peut être utilisée avec des compartiments avec le verrouillage d'objet S3 activé, mais la configuration du cycle de vie des compartiments n'est pas prise en charge pour les compartiments conformes hérités.</p>

Fonctionnement	Mise en place
PUT Bucket notification (PutBucketNotificationConfiguration)	<p>Cette opération configure les notifications pour le compartiment à l'aide du XML de configuration de notification inclus dans le corps de la demande. Vous devez connaître les détails d'implémentation suivants :</p> <ul style="list-style-type: none"> StorageGRID prend en charge les rubriques SNS (simple notification Service) comme destinations. Les points finaux SQS (simple Queue Service) ou Lambda d'Amazon ne sont pas pris en charge. La destination des notifications doit être spécifiée comme URN d'un terminal StorageGRID. Les terminaux peuvent être créés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. <p>Le noeud final doit exister pour que la configuration des notifications réussisse. Si le noeud final 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 sont non pris en charge. <ul style="list-style-type: none"> ◦ s3:ReducedRedundancyLostObject ◦ s3:ObjectRestore:Completed Les notifications d'événements envoyées par StorageGRID utilisent le format JSON standard, sauf qu'elles n'incluent pas certaines clés et utilisent des valeurs spécifiques pour d'autres, comme illustré dans la liste suivante : <ul style="list-style-type: none"> ◦ EventSource sgws:s3 ◦ AwsRegion non inclus ◦ x-amz-id-2 non inclus ◦ arn urn:sgws:s3:::bucket_name
PUT Bucket policy	Cette opération définit la politique associée au compartiment.

Fonctionnement	Mise en place
RÉPLICATION des compartiments	<p>Cette opération est configurée "RéPLICATION StorageGRID CloudMirror" Pour le compartiment utilisant le XML de configuration de réPLICATION fourni dans le corps de la requête. Pour la réPLICATION CloudMirror, vous devez connaître les détails d'implémentation suivants :</p> <ul style="list-style-type: none"> • StorageGRID ne prend en charge que le V1 de la configuration de la réPLICATION. Cela signifie que StorageGRID ne prend pas en charge l'utilisation de Filter Elément pour les règles, et suit les conventions V1 pour la suppression des versions d'objet. Pour plus d'informations, reportez-vous à la "Documentation Amazon S3 sur la configuration de la réPLICATION". • La réPLICATION des compartiments peut être configurée sur les compartiments avec ou sans version. • Vous pouvez spécifier un compartiment de destination différent dans chaque règle du XML de configuration de réPLICATION. Un compartiment source peut être répliqué sur plusieurs compartiments de destination. • Les compartiments de destination doivent être spécifiés en tant que URN des terminaux StorageGRID, tel que spécifié dans le Gestionnaire de locataires ou l'API de gestion des locataires. Voir "Configurez la réPLICATION CloudMirror". <p>Le noeud final doit exister pour que la configuration de réPLICATION réussisse. Si le noeud final n'existe pas, la demande échoue en tant que 400 Bad Request. Le message d'erreur indique : <i>Unable to save the replication policy. The specified endpoint URN does not exist: URN.</i></p> <ul style="list-style-type: none"> • Vous n'avez pas besoin de spécifier un Role Dans le XML de configuration. Cette valeur n'est pas utilisée par StorageGRID et sera ignorée si elle a été soumise. • Si vous omettez la classe de stockage du XML de configuration, StorageGRID utilise le STANDARD classe de stockage par défaut. • Si vous supprimez un objet du compartiment source ou que vous supprimez le compartiment source lui-même, le comportement de réPLICATION inter-région est le suivant : <ul style="list-style-type: none"> ◦ Si vous supprimez l'objet ou le compartiment avant sa réPLICATION, l'objet/le compartiment n'est pas réplié et vous n'êtes pas averti. ◦ Si vous supprimez l'objet ou le compartiment après sa réPLICATION, StorageGRID suit le comportement de suppression Amazon S3 standard pour la version V1 de la réPLICATION multi-région.

Fonctionnement	Mise en place
PUT Bucket tagging	<p>Cette opération utilise le tagging sous-ressource pour ajouter ou mettre à jour un ensemble de balises pour un compartiment. Lors de l'ajout de balises de compartiment, tenez compte des limites suivantes :</p> <ul style="list-style-type: none"> StorageGRID et Amazon S3 prennent en charge jusqu'à 50 balises pour chaque compartiment. Les étiquettes associées à un compartiment doivent avoir des clés d'étiquette uniques. Une clé de balise peut comporter jusqu'à 128 caractères Unicode. Les valeurs de balise peuvent comporter jusqu'à 256 caractères Unicode. Les clés et les valeurs sont sensibles à la casse
GESTION des versions du compartiment	<p>Cette implémentation utilise le <i>versioning</i> sous-ressource pour définir l'état de gestion des versions d'un compartiment existant. Vous pouvez définir l'état de la gestion des versions à l'aide de l'une des valeurs suivantes :</p> <ul style="list-style-type: none"> Activé : permet la gestion des versions des objets dans le compartiment. Tous les objets ajoutés au compartiment reçoivent un ID de version unique. Suspendu : désactive la gestion des versions des objets dans le compartiment. Tous les objets ajoutés au compartiment reçoivent l'ID de version null.
CONFIGURATION du verrouillage de l'objet	<p>Cette opération configure ou supprime le mode de conservation par défaut du compartiment et la période de conservation par défaut.</p> <p>Si la période de conservation par défaut est modifiée, la conservation jusqu'à la date des versions d'objet existantes reste la même et n'est pas recalculée en utilisant la nouvelle période de conservation par défaut.</p> <p>Voir "Utilisez l'API REST S3 pour configurer le verrouillage objet S3" pour des informations détaillées.</p>

Informations associées

["Contrôles de cohérence"](#)

["HEURE du dernier accès au compartiment"](#)

["Utilisez les règles d'accès au compartiment et au groupe"](#)

["Opérations S3 suivies dans les journaux d'audit"](#)

Opérations personnalisées dans les compartiments

Le système StorageGRID prend en charge les opérations de compartiment personnalisées, ajoutées à l'API REST S3 et propres au système.

Le tableau suivant répertorie les opérations de compartiment personnalisées prises en charge par StorageGRID.

Fonctionnement	Description	Pour en savoir plus
OPTIMISEZ la cohérence des compartiments	Renvoie le niveau de cohérence appliqué à un compartiment spécifique.	" OPTIMISEZ la cohérence des compartiments "
PRÉSERVER la cohérence du godet	Définit le niveau de cohérence appliqué à un compartiment spécifique.	" PRÉSERVER la cohérence du godet "
HEURE du dernier accès au compartiment	Indique si les mises à jour de l'heure du dernier accès sont activées ou désactivées pour un compartiment spécifique.	" HEURE du dernier accès au compartiment "
METTRE l'heure du dernier accès au compartiment	Permet d'activer ou de désactiver les mises à jour de l'heure du dernier accès pour un compartiment spécifique.	" METTRE l'heure du dernier accès au compartiment "
SUPPRIMEZ la configuration de notification des métadonnées de compartiment	Supprime le XML de configuration de notification de métadonnées associé à un compartiment spécifique.	" SUPPRIMEZ la configuration de notification des métadonnées de compartiment "
CONFIGURATION DES notifications de métadonnées de compartiment	Renvoie le XML de configuration de notification de métadonnées associé à un compartiment spécifique.	" CONFIGURATION DES notifications de métadonnées de compartiment "
CONFIGURATION de notification des métadonnées de compartiment	Configure le service de notification des métadonnées pour un compartiment.	" CONFIGURATION de notification des métadonnées de compartiment "
PUT Bucket with Compliance settings	Obsolète et non pris en charge : vous ne pouvez plus créer de compartiments avec conformité activée.	" Obsolète : METTEZ le compartiment avec les paramètres de conformité "
ASSUREZ la conformité aux compartiments	Obsolète mais pris en charge : renvoie les paramètres de conformité actuellement en vigueur pour un compartiment compatible existant.	" Obsolète : CONFORMITÉ DES compartiments "
METTEZ le godet en conformité	Obsolète mais pris en charge : permet de modifier les paramètres de conformité d'un compartiment compatible existant.	" Obsolète : conformité DES compartiments PUT "

Informations associées

"Opérations S3 suivies dans les journaux d'audit"

Opérations sur les objets

Cette section décrit la manière dont le système StorageGRID implémente les opérations de l'API REST S3 pour les objets.

Les conditions suivantes s'appliquent à toutes les opérations d'objet :

- StorageGRID "[contrôles de cohérence](#)" sont prises en charge par toutes les opérations sur les objets, à l'exception de ce qui suit :
 - OBTENIR l'ACL d'objet
 - OPTIONS /
 - METTRE l'objet en attente légale
 - CONSERVATION des objets
 - SÉLECTIONNEZ contenu de l'objet
- Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». Le calendrier de l'évaluation « derniers-victoires » est basé sur le moment où le système StorageGRID remplit une demande donnée et non sur le moment où les clients S3 commencent une opération.
- Tous les objets d'un compartiment StorageGRID sont détenus par le propriétaire du compartiment, 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 ci-dessous décrit la manière dont StorageGRID implémente les opérations sur les objets de l'API REST S3.

Fonctionnement	Mise en place
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 requête DE SUPPRESSION d'objet, StorageGRID tente de supprimer immédiatement toutes les copies de l'objet des 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 et indique que le client a réussi.</p> <p>Gestion des versions</p> <p>Pour supprimer une version spécifique, le demandeur doit être le propriétaire du compartiment et utiliser la <code>versionId</code> sous-ressource. L'utilisation de cette sous-ressource supprime définitivement la version. Si la <code>versionId</code> correspond à un marqueur de suppression, l'en-tête de réponse <code>x-amz-delete-marker</code> est renvoyé à <code>true</code>.</p> <ul style="list-style-type: none"> Si un objet est supprimé sans la <code>versionId</code> sous-ressource sur un compartiment activé pour la version, il génère un marqueur de suppression. Le <code>versionId</code> pour le marqueur de suppression, est renvoyé à l'aide du <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 à <code>true</code>. Si un objet est supprimé sans la <code>versionId</code> sous-ressource sur un compartiment suspendu de version, elle entraîne la suppression permanente d'une version existante 'null' 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 à <code>true</code>. <p>Remarque : dans certains cas, plusieurs marqueurs de suppression peuvent exister pour un objet.</p> <p>Voir "Utilisez l'API REST S3 pour configurer le verrouillage objet S3" Pour apprendre à supprimer des versions d'objets en mode GOUVERNANCE.</p>
SUPPRIMER plusieurs objets (DeleteObjects)	<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 "Utilisez l'API REST S3 pour configurer le verrouillage objet S3" Pour apprendre à supprimer des versions d'objets en mode GOUVERNANCE.</p>

Fonctionnement	Mise en place
SUPPRIMER le balisage d'objets	<p>Utilise le tagging sous-ressource pour supprimer toutes les balises d'un objet.</p> <p>Gestion des versions</p> <p>Si le <code>versionId</code> le paramètre query n'est pas spécifié dans la demande, l'opération supprime toutes les balises de la version la plus récente de l'objet dans un compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, un état "methodNotAldue" est renvoyé avec l'<code>x-amz-delete-marker</code> réponse en-tête réglée sur <code>true</code>.</p>
OBTENIR l'objet	" OBTENIR l'objet "
OBTENIR l'ACL d'objet	Si les informations d'identification d'accès nécessaires sont fournies pour le compte, l'opération renvoie une réponse positive ainsi que l'ID, le DisplayName et l'autorisation du propriétaire de l'objet, ce qui indique que le propriétaire dispose d'un accès complet à l'objet.
OBTENIR la mise en attente légale de l'objet	" Utilisez l'API REST S3 pour configurer le verrouillage objet S3 "
OBTENIR la conservation des objets	" Utilisez l'API REST S3 pour configurer le verrouillage objet S3 "
OBTENIR le balisage d'objets	<p>Utilise le tagging sous-ressource pour renvoyer toutes les balises d'un objet.</p> <p>Gestion des versions</p> <p>Si le <code>versionId</code> le paramètre query n'est pas spécifié dans la demande, l'opération renvoie toutes les balises de la version la plus récente de l'objet dans un compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, un état "methodNotAldue" est renvoyé avec l'<code>x-amz-delete-marker</code> réponse en-tête réglée sur <code>true</code>.</p>
Objet TÊTE	" Objet TÊTE "
Restauration POST-objet	" Restauration POST-objet "
PLACER l'objet	" PLACER l'objet "
PLACER l'objet - Copier	" PLACER l'objet - Copier "
METTRE l'objet en attente légale	" Utilisez l'API REST S3 pour configurer le verrouillage objet S3 "
CONSERVATION des objets	" Utilisez l'API REST S3 pour configurer le verrouillage objet S3 "

Fonctionnement	Mise en place
PUT Object tagging	<p>Utilise le tagging 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 à de nouveaux objets lorsque vous les téléchargez ou les ajouter à des 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 comporter jusqu'à 128 caractères Unicode et les valeurs de balise peuvent comporter jusqu'à 256 caractères Unicode. Les clés et les valeurs sont sensibles à la casse</p> <p>Mises à jour des balises et comportement d'ingestion</p> <p>Lorsque vous utilisez PUT Object tagging pour mettre à jour les balises d'un objet, StorageGRID ne réingérer pas l'objet. Cela signifie que l'option de comportement d'ingestion spécifiée dans la règle ILM correspondante n'est pas utilisée. Tout changement au placement d'objet déclenché par la mise à jour est apporté lors de l'évaluation de ILM par des processus ILM en arrière-plan normaux.</p> <p>En d'autres termes, si la règle ILM utilise l'option strict pour le comportement d'ingestion, aucune action n'est entreprise si les placements d'objet requis ne peuvent pas être effectués (par exemple, parce qu'un nouvel emplacement n'est pas disponible). L'objet mis à jour conserve son emplacement actuel jusqu'à ce que le placement requis soit possible.</p> <p>Résolution des conflits</p> <p>Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur la base des « derniers-victoires ». Le calendrier de l'évaluation « derniers-victoires » est basé sur le moment où le système StorageGRID remplit 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 compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, un état "methodNotAldue" est renvoyé avec l'<code>x-amz-delete-marker</code> réponse en-tête réglée sur <code>true</code>.</p>
SelectObjectContent	" SelectObjectContent "

Informations associées

["Opérations S3 suivies dans les journaux d'audit"](#)

Utiliser S3 Select

StorageGRID prend en charge les clauses, types de données et opérateurs Amazon S3 Select suivants pour le "[Commande SelectObjectContent](#)".



Les éléments non répertoriés ne sont pas pris en charge.

Pour la syntaxe, voir "[SelectObjectContent](#)". Pour plus d'informations sur S3 Select, consultez le ["Documentation AWS pour S3 Select"](#).

Seuls les comptes de tenant dont S3 Select est activé peuvent émettre des requêtes SelectObjectContent. Voir la ["Considérations et configuration requise pour l'utilisation de S3 Select"](#).

Clauses

- SÉLECTIONNER la liste
- Clause FROM
- Clause WHERE
- Clause DE LIMITÉ

Types de données

- bool
- entier
- chaîne
- flottement
- décimale, numérique
- horodatage

Opérateurs

Opérateurs logiques

- ET
- PAS
- OU

Opérateurs de comparaison

- <
- >
- < ;=
- >=
- =
- =
- <>

- !=
- ENTRE
- DANS

Opérateurs de correspondance de répétition

- COMME
- _
- %

Opérateurs unitaires

- EST NULL
- N'EST PAS NULL

Opérateurs mathématiques

- +
- -
- *
- /
- %

StorageGRID suit la priorité de l'opérateur Amazon S3 Select.

Fonctions d'agrégation

- MOY()
- NOMBRE(*)
- MAX()
- MIN()
- SOMME()

Fonctions conditionnelles

- CASSE
- FUSIONNE
- NULLIF

Fonctions de conversion

- CAST (pour les types de données pris en charge)

Fonctions de date

- DATE_AJOUTER
- DATE_DIFF

- EXTRAIRE
- TO_STRING
- TO_TIMESTAMP
- CODE D'ARTICLE

Fonctions de chaîne

- CHAR_LENGTH, CARACTÈRE_LENGTH
- ABAISSEMENT
- SOUS-CHAÎNE
- GARNITURE
- SUPÉRIEUR

Utilisez le cryptage côté serveur

Le chiffrement côté serveur vous permet de protéger vos données au repos objet. StorageGRID crypte les données lors de leur écriture et décrypte 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 gestion des clés de cryptage :

- **SSE (chiffrement côté serveur avec clés gérées par StorageGRID)** : lorsque vous émettez une demande S3 pour stocker un objet, StorageGRID crypte l'objet avec une clé unique. Lorsque vous émettez une requête S3 pour récupérer l'objet, StorageGRID utilise la clé stockée pour décrypter 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 décrypté et vos données d'objet sont renvoyées.

StorageGRID gère toutes les opérations de cryptage et de décryptage des objets, mais vous devez gérer les clés de cryptage 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 godet ou de la grille sont ignorés.

Utiliser SSE

Pour chiffrer un objet avec une clé unique gérée par StorageGRID, utilisez l'en-tête de demande suivant :

`x-amz-server-side-encryption`

L'en-tête de demande SSE est pris en charge par les opérations d'objet suivantes :

- "PLACER l'objet"

- "["PLACER l'objet - Copier"](#)
- "["Lancer le téléchargement de pièces multiples"](#)

Utiliser SSE-C

Pour crypter un objet avec une clé unique que vous gérez, vous utilisez trois en-têtes de requête :

En-tête de demande	Description
x-amz-server-side -encryption-customer -algorithm	Spécifiez l'algorithme de cryptage. La valeur de la barre de coupe doit être de AES256.
x-amz-server-side -encryption-customer-key	Spécifiez la clé de cryptage qui sera utilisée pour crypter ou décrypter l'objet. La valeur de la clé doit être codée en 256 bits, en base64.
x-amz-server-side -encryption-customer-key -MD5	Spécifiez le résumé MD5 de la clé de chiffrement selon la RFC 1321, qui est utilisé pour garantir que la clé de chiffrement a été transmise sans erreur. La valeur du résumé MD5 doit être codée en base64 à 128 bits.

Les en-têtes de demande SSE-C sont pris en charge par les opérations objet suivantes :

- "["OBTENIR l'objet"](#)
- "["Objet TÊTE"](#)
- "["PLACER l'objet"](#)
- "["PLACER l'objet - Copier"](#)
- "["Lancer le téléchargement de pièces multiples"](#)
- "["Télécharger la pièce"](#)
- "["Télécharger la pièce - Copier"](#)

Considérations relatives au chiffrement côté serveur avec clés fournies par le client (SSE-C)

Avant d'utiliser SSE-C, tenez compte des points suivants :

- Vous devez utiliser https.
-  StorageGRID rejette toute demande effectuée sur http en utilisant SSE-C. Pour des considérations de sécurité, vous devez envisager toute clé que vous envoyez accidentellement en utilisant http pour être compromise. Mettez la clé au rebut et tournez-la selon les besoins.
- L'ETag dans la réponse n'est pas le MD5 des données objet.
 - Vous devez gérer le mappage des clés de chiffrement aux objets. StorageGRID ne stocke pas de clés de chiffrement. Vous êtes responsable du suivi de la clé de chiffrement que vous fournissez pour chaque objet.
 - Si le contrôle de version du compartiment est activé, chaque version d'objet doit disposer de sa propre clé de chiffrement. Vous êtes responsable du suivi de la clé de chiffrement utilisée pour chaque version d'objet.

- Comme vous gérez les clés de chiffrement côté client, vous devez également gérer d'autres dispositifs de protection, tels 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-grid ou CloudMirror est configurée pour le compartiment, vous ne pouvez pas acquérir d'objets SSE-C. L'opération d'acquisition échoue.

Informations associées

["Guide pour les développeurs Amazon S3 : protection des données à l'aide du chiffrement côté serveur avec clés de chiffrement fournies par le client \(SSE-C\)"](#)

OBTENIR l'objet

Vous pouvez utiliser la requête D'objet GET S3 pour récupérer un objet à partir d'un compartiment S3.

OBTENIR un objet et des objets partitionnés

Vous pouvez utiliser le `partNumber` paramètre de demande pour récupérer une partie spécifique d'un objet partitionné ou segmenté. Le `x-amz-mp-parts-count` l'élément de réponse indique le nombre de pièces dont dispose l'objet.

Vous pouvez définir `partNumber` à 1 pour les objets segmentés/multisegments et les objets non segmentés/non-partitionnés ; cependant, le `x-amz-mp-parts-count` l'élément de réponse n'est renvoyé que pour les objets segmentés ou partitionnés.

Caractères UTF-8 dans les métadonnées utilisateur

StorageGRID n'analyse ni n'interprète pas les caractères UTF-8 qui se sont 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 comporte des caractères non imprimables.

En-tête de demande non pris en charge

L'en-tête de demande 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 extrait la version la plus récente de l'objet dans un compartiment multiversion. Si la version actuelle de l'objet est un marqueur de suppression, un état « non trouvé » est renvoyé avec le `x-amz-delete-marker` réponse en-tête réglée sur `true`.

En-têtes de demande pour chiffrement côté serveur avec 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:** Spécifiez AES256.
- **x-amz-server-side-encryption-customer-key:** Spécifiez votre clé de cryptage pour l'objet.
- **x-amz-server-side-encryption-customer-key-MD5:** Spécifiez le résumé 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 des clés fournies par le client pour sécuriser les données d'objet, consultez les points à prendre en compte dans la section "[Utilisez le cryptage côté serveur](#)".

Comportement de L'objet GET pour les objets de pool de stockage cloud

Si un objet a été stocké dans un "[Pool de stockage cloud](#)", Le comportement d'une requête GET Object dépend de l'état de l'objet. Voir "[Objet TÊTE](#)" pour en savoir plus.



Si un objet est stocké dans un pool de stockage cloud et qu'une ou plusieurs copies de cet objet existent également dans la grille, L'OBTENTION des demandes d'objet tente d'extraire les données de la grille avant de les récupérer depuis le pool de stockage cloud.

État de l'objet	Comportement de L'objet GET
Les objets sont ingéré dans StorageGRID mais pas encore évalués par ILM, ou objet stocké dans un pool de stockage traditionnel ou au moyen d'un code d'effacement	200 OK Une copie de l'objet est récupérée.
Objet dans Cloud Storage Pool, mais pas encore migré vers un état non récupérable	200 OK Une copie de l'objet est récupérée.
L'objet a été transféré à un état non récupérable	403 Forbidden, InvalidObjectState Utiliser un " Restauration POST-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 DE restauration POST Object soit terminée.
Objet entièrement restauré dans le pool de stockage cloud	200 OK Une copie de l'objet est récupérée.

Objets partitionnés ou segmentés dans un pool de stockage cloud

Si vous avez téléchargé un objet partitionné ou si StorageGRID le divise en segments, StorageGRID détermine si l'objet est disponible dans le pool de stockage cloud en échantillonant un sous-ensemble de parties ou de segments de l'objet. Dans certains cas, une demande GET Object peut retourner de manière

incorrecte 200 OK lorsque certaines parties de l'objet ont déjà été migrées à un état non récupérable ou lorsque certaines parties de l'objet n'ont pas encore été restaurées.

Dans ces cas :

- La demande GET Object peut renvoyer certaines données mais s'arrête à mi-chemin du transfert.
- Une requête GET Object suivante peut revenir 403 Forbidden.

OBTENEZ la réPLICATION objET et inter-grid

Si vous utilisez "fédération des grilles" et "réPLICATION entre plusieurs grilles" Est activé pour un compartiment. Le client S3 peut vérifier l'état de réPLICATION d'un objet en envoyant une requête GET Object. La réponse inclut la réponse spécifique à StorageGRID x-ntap-sg-cgr-replication-status en-tête de réponse, qui aura l'une des valeurs suivantes :

Grille	État de la réPLICATION
Source	<ul style="list-style-type: none">• SUCCÈS : la réPLICATION a réussi.• EN ATTENTE : l'objet n'a pas encore été répliqué.• ÉCHEC : la réPLICATION a échoué avec une défaillance permanente. L'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.

Informations associées

["Opérations S3 suivies dans les journaux d'audit"](#)

Objet TÊTE

Vous pouvez utiliser la requête d'objet TÊTE S3 pour extraire les métadonnées à partir d'un objet sans y retourner. Si l'objet est stocké dans un pool de stockage cloud, vous pouvez utiliser HEAD Object pour déterminer l'état de transition de l'objet.

Objet TÊTE et objets multipart

Vous pouvez utiliser le partNumber paramètre de demande pour récupérer les métadonnées d'une partie spécifique d'un objet partitionné ou segmenté. Le x-amz-mp-parts-count l'élément de réponse indique le nombre de pièces dont dispose l'objet.

Vous pouvez définir partNumber à 1 pour les objets segmentés/multisegments et les objets non segmentés/non-partitionnés ; cependant, le x-amz-mp-parts-count l'élément de réponse n'est renvoyé que pour les objets segmentés ou partitionnés.

Caractères UTF-8 dans les métadonnées utilisateur

StorageGRID n'analyse ni n'interprète pas les caractères UTF-8 qui se sont échappés dans les métadonnées définies par l'utilisateur. Les demandes 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 comporte des caractères non imprimables.

En-tête de demande non pris en charge

L'en-tête de demande 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 extrait la version la plus récente de l'objet dans un compartiment multiversion. Si la version actuelle de l'objet est un marqueur de suppression, un état « non trouvé » est renvoyé avec le `x-amz-delete-marker` réponse en-tête réglée sur `true`.

En-têtes de demande pour chiffrement côté serveur avec 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`: Spécifiez AES256.
- `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de cryptage pour l'objet.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé 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 des clés fournies par le client pour sécuriser les données d'objet, consultez les points à prendre en compte dans la section "["Utilisez le cryptage côté serveur"](#)".

Réponses D'objet PRINCIPAL pour les objets de pool de stockage cloud

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 lors de son déplacement vers Cloud Storage Pool, qui peut être migré vers un état non récupérable et restauré.

État de l'objet	Réponse à l'objet TÊTE
Les objets sont ingéré dans StorageGRID mais pas encore évalués par ILM, ou objet stocké dans un pool de stockage traditionnel ou au moyen d'un code d'effacement	200 OK (Aucun en-tête à réponse spéciale n'est renvoyé.)

État de l'objet	Réponse à l'objet TÊTE
Objet dans Cloud Storage Pool, mais pas encore migré vers 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 à un état non récupérable, la valeur de expiry-date est sur le point de passer un moment lointain dans le futur. L'heure exacte de la transition n'est pas contrôlée par le système StorageGRID.</p>
L'objet est passé à l'état non récupérable, mais il existe au moins une copie 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 expiry-date est sur le point de passer un moment lointain 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 "Restauration POST-objet" Demande de restauration de la copie à partir du pool de stockage cloud avant que vous puissiez récupérer l'objet.</p>
L'objet a été transféré 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 l'objet TÊTE
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 20 2018 00:00:00 GMT"</p> <p>Le expiry-date Indique quand l'objet du pool de stockage cloud sera renvoyé à un état non récupérable.</p>

Objets partitionnés ou segmentés dans Cloud Storage Pool

Si vous avez téléchargé un objet partitionné ou si StorageGRID le divise en segments, StorageGRID détermine si l'objet est disponible dans le pool de stockage cloud en échantillonant un sous-ensemble de parties ou de segments de l'objet. Dans certains cas, une requête d'objet DE TÊTE peut revenir de manière incorrecte x-amz-restore: ongoing-request="false" lorsque certaines parties de l'objet ont déjà été migrées à un état non récupérable ou lorsque certaines parties de l'objet n'ont pas encore été restaurées.

HEAD réPLICATION d'objets et de cross-grid

Si vous utilisez "fédération des grilles" et "réPLICATION entre plusieurs grilles" Est activé pour un compartiment, le client S3 peut vérifier l'état de réPLICATION d'un objet en émettant une requête d'objet PRINCIPAL. La réponse inclut la réponse spécifique à StorageGRID x-ntap-sg-cgr-rePLICATION-status en-tête de réponse, qui aura l'une des valeurs suivantes :

Grille	État de la réPLICATION
Source	<ul style="list-style-type: none"> SUCCÈS : la réPLICATION a réussi. EN ATTENTE : l'objet n'a pas encore été répliqué. ÉCHEC : la réPLICATION a échoué avec une défaillance permanente. L'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.

Informations associées

["Opérations S3 suivies dans les journaux d'audit"](#)

Restauration POST-objet

Vous pouvez utiliser la demande de restauration POST-objet S3 pour restaurer un objet stocké dans un pool de stockage cloud.

Type de demande pris en charge

StorageGRID ne prend en charge que les demandes DE restauration POST-objet pour restaurer un objet. Elle ne prend pas en charge le SELECT type de restauration. Sélectionnez demandes de retour XNot Implemented.

Gestion des versions

Spécifiez éventuellement versionId pour restaurer une version spécifique d'un objet dans un compartiment multiversion. Si vous ne spécifiez pas versionId, la version la plus récente de l'objet est restaurée

Comportement de restauration POST-objet sur les objets de pool de stockage cloud

Si un objet a été stocké dans un pool de stockage cloud (voir les instructions de gestion des objets avec gestion du cycle de vie des informations), une demande de restauration POST-objet présente le comportement suivant, en fonction de l'état de l'objet. Voir « objet TÊTE » pour plus de détails.

 Si un objet est stocké dans un pool de stockage cloud et qu'une ou plusieurs copies de cet objet existent également dans la grille, il n'est pas nécessaire de le restaurer en émettant une demande de restauration POST-objet. En revanche, la copie locale peut être récupérée directement à l'aide d'une demande D'OBJET GET.

État de l'objet	Comportement de la restauration POST-objet
L'objet est 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 Cloud Storage Pool, mais pas encore migré vers un état non récupérable	200 OK Aucune modification n'est apportée. Remarque : avant qu'un objet ne soit transféré à un état non récupérable, vous ne pouvez pas le modifier expiry-date.
L'objet a été transféré à un état non récupérable	202 Accepted Restaure une copie récupérable de l'objet vers 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 renvoyé à un état non récupérable. Si vous le souhaitez, utilisez le Tier élément de demande pour déterminer la durée de la tâche de restauration (Expedited, Standard, ou Bulk). Si vous ne spécifiez pas Tier, le Standard le niveau est utilisé. 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 du Expedited niveau. L'erreur suivante est renvoyée 403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class.

État de l'objet	Comportement de la restauration POST-objet
Objet en cours de restauration à partir d'un état non récupérable	409 Conflict, RestoreAlreadyInProgress
Objet entièrement restauré dans le pool de stockage cloud	<p>200 OK</p> <p>Remarque : si un objet a été restauré à un état récupérable, vous pouvez le modifier expiry-date En réémettant la demande DE restauration POST Object avec une nouvelle valeur pour Days. La date de restauration est mise à jour par rapport à l'heure de la demande.</p>

Informations associées

["Gestion des objets avec ILM"](#)

["Objet TÊTE"](#)

["Opérations S3 suivies dans les journaux d'audit"](#)

PLACER l'objet

Vous pouvez utiliser la demande S3 PUT Object pour ajouter un objet à un compartiment.

Résoudre les conflits

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.

Taille de l'objet

La taille maximale recommandée pour une opération d'objet PUT unique est de 5 Gio (5,368,709,120 octets). Si vos objets sont supérieurs à 5 Gio, utilisez le téléchargement partitionné.

La taille supportée maximale pour une opération objet PUT unique est de 5 Tio (5,497,558,138,880 octets). Cependant, l'alerte **S3 PUT Object size trop importante** est déclenchée si vous tentez de télécharger un objet supérieur à 5 Gio.

Taille des métadonnées utilisateur

Amazon S3 limite la taille des métadonnées définies par l'utilisateur au sein de chaque en-tête de requête À 2 Ko. StorageGRID limite les métadonnées utilisateur à 24 Kio. La taille des métadonnées définies par l'utilisateur est mesurée en prenant la somme du nombre d'octets dans le codage UTF-8 de chaque clé et valeur.

Caractères UTF-8 dans les métadonnées utilisateur

Si une requête inclut (non échappé) les valeurs UTF-8 dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur, le comportement StorageGRID n'est pas défini.

StorageGRID n'analyse ni n'interprète pas les caractères UTF-8 qui se sont échappé 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 demandes PUT, PUT Object-Copy, GET et HEAD sont satisfaites 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 comprend des caractères non imprimables.

Limites des balises d'objet

Vous pouvez ajouter des balises à de nouveaux objets lorsque vous les téléchargez ou les ajouter à des 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 comporter jusqu'à 128 caractères Unicode et les valeurs de balise peuvent comporter jusqu'à 256 caractères Unicode. Les clés et les valeurs sont sensibles à la casse

Propriété de l'objet

Dans StorageGRID, tous les objets sont détenus par le compte du propriétaire de compartiment, y compris les objets créés par un compte autre que le propriétaire ou un utilisateur anonyme.

En-têtes de demande 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 de 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

Le codage du transfert haché est pris en charge si `aws-chunked` la signature de charge utile est également utilisée.

- `x-amz-meta-`, suivi d'une paire nom-valeur contenant des métadonnées définies par l'utilisateur.

Lorsque vous spécifiez la paire nom-valeur pour les métadonnées définies par l'utilisateur, utilisez le format général suivant :

```
x-amz-meta-name: value
```

Si vous souhaitez utiliser l'option **temps de création défini par l'utilisateur** comme heure de référence pour une règle ILM, vous devez utiliser `creation-time` nom des métadonnées enregistrées lors de la création de l'objet. Par exemple :

```
x-amz-meta-creation-time: 1443399726
```

La valeur pour `creation-time` Est évaluée 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 les options équilibrées ou strictes pour le comportement d'ingestion. Une erreur est renvoyée lors de la création de la règle ILM.

- `x-amz-tagging`
- En-têtes de requête 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 rétention par défaut du compartiment sont utilisés pour calculer le mode de version de l'objet et conserver jusqu'à la date. Voir "[Utilisez l'API REST S3 pour configurer le verrouillage objet S3](#)".

- En-têtes de demande 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 [Demander des en-têtes pour le cryptage côté serveur](#)

En-têtes de requête non pris en charge

Les en-têtes de demande suivants ne sont pas pris en charge :

- Le `x-amz-acl` l'en-tête de demande n'est pas pris en charge.
- Le `x-amz-website-redirect-location` l'en-tête de demande n'est pas pris en charge et renvoie `XNotImplemented`.

Options de classe de stockage

Le `x-amz-storage-class` l'en-tête de demande est pris en charge. Valeur soumise pour `x-amz-storage-class` StorageGRID protège les données d'objet lors de leur ingestion, mais pas le nombre de copies

persistentes de l'objet stockées dans le système StorageGRID (déterminé par ILM).

Si la règle ILM correspondant à un objet ingéré utilise l'option stricte pour le comportement d'ingestion, le `x-amz-storage-class` la barre de coupe n'a aucun effet.

Les valeurs suivantes peuvent être utilisées pour `x-amz-storage-class`:

- STANDARD (Valeur par défaut)
 - **Double commit** : si la règle ILM spécifie l'option de double validation pour le comportement d'ingestion, dès qu'un objet est ingéré, une seconde copie de cet objet est créée et distribuée à un autre nœud de stockage (double commit). Une fois la règle ILM évaluée, StorageGRID détermine si ces copies intermédiaires initiales répondent aux instructions de placement de la règle. Si ce n'est pas le cas, de nouvelles copies d'objet peuvent avoir besoin d'être effectuées à différents emplacements et les copies intermédiaires initiales peuvent avoir besoin d'être supprimées.
 - **Balanced** : si la règle ILM spécifie l'option équilibrée et que StorageGRID ne peut pas immédiatement effectuer toutes les copies spécifiées dans la règle, StorageGRID effectue deux copies intermédiaires sur différents nœuds de stockage.

Si StorageGRID peut immédiatement créer toutes les copies d'objet spécifiées dans la règle ILM (placement synchrone), l'`x-amz-storage-class` la barre de coupe n'a aucun effet.

- REDUCED_REDUNDANCY

- **Double commit** : si la règle ILM spécifie l'option de double validation pour le comportement d'ingestion, StorageGRID crée une copie intermédiaire unique lors de l'ingestion de l'objet (simple commit).
- **Équilibré** : si la règle ILM spécifie l'option équilibrée, StorageGRID effectue une seule copie intermédiaire uniquement si le système ne peut pas immédiatement effectuer toutes les copies spécifiées dans la règle. Si StorageGRID peut effectuer un placement synchrone, cet en-tête n'a aucun effet. La `REDUCED_REDUNDANCY` L'option est meilleure lorsque la règle ILM correspondant à l'objet crée une copie répliquée unique. Dans ce cas, utilisez `REDUCED_REDUNDANCY` élimine la création et la suppression inutiles d'une copie d'objet supplémentaire pour chaque opération d'ingestion.

À l'aide du `REDUCED_REDUNDANCY` cette option n'est pas recommandée dans d'autres cas.

`REDUCED_REDUNDANCY` augmente le risque de perte de données d'objet lors de l'ingestion. Vous risquez par exemple de perdre des données si une seule copie est initialement stockée sur un nœud de stockage qui échoue avant l'évaluation du ILM.

 Le fait d'avoir une seule copie répliquée pendant une période donnée présente un risque de perte permanente des données. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur importante d'un noeud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, l'accès à l'objet est temporairement perdu.

Spécification `REDUCED_REDUNDANCY` l'impact sur le nombre de copies créées uniquement lors de l'ingestion d'un objet. Elle n'affecte pas le nombre de copies de l'objet lorsque celui-ci est évalué par la règle ILM active ; le stockage des données ne se produit pas à des niveaux de redondance inférieurs dans le système StorageGRID.



Si vous ingez un objet dans un compartiment avec l'option de verrouillage objet S3 activée, la REDUCED_REDUNDANCY l'option est ignorée. Si vous ingez un objet dans un compartiment conforme d'ancienne génération, le REDUCED_REDUNDANCY option renvoie une erreur. StorageGRID procède toujours à une récupération à double engagement afin de satisfaire les exigences de conformité.

Demander des en-têtes pour le cryptage côté serveur

Vous pouvez utiliser les en-têtes de requête suivants pour crypter un objet avec un chiffrement côté serveur. Les options SSE et SSE-C sont mutuellement exclusives.

- **SSE:** Utilisez l'en-tête suivant si vous voulez chiffrer l'objet avec une clé unique gérée par StorageGRID.
 - x-amz-server-side-encryption
- **SSE-C:** Utilisez les trois en-têtes si vous voulez chiffrer l'objet avec une clé unique que vous fournissez et gérez.
 - x-amz-server-side-encryption-customer-algorithm: Spécifiez AES256.
 - x-amz-server-side-encryption-customer-key: Spécifiez votre clé de cryptage pour le nouvel objet.
 - x-amz-server-side-encryption-customer-key-MD5: Spécifiez le résumé 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 des clés fournies par le client pour sécuriser les données d'objet, consultez les points à prendre en compte à la section "[utilisation du chiffrement côté serveur](#)".



Si un objet est chiffré avec SSE ou SSE-C, tous les paramètres de chiffrement au niveau du godet ou de la grille sont ignorés.

Gestion des versions

Si le contrôle de version est activé pour un compartiment, un contrôle unique `versionId` est automatiquement généré pour la version de l'objet stocké. C'est ça `versionId` est également renvoyé dans la réponse en utilisant le `x-amz-version-id` en-tête de réponse.

Si la gestion des versions est suspendue, la version de l'objet est stockée avec un null `versionId` si une version nulle existe déjà, elle sera remplacée.

Calculs de signature pour l'en-tête autorisation

Lorsque vous utilisez le `Authorization` En-tête pour l'authentification des demandes, StorageGRID diffère d'AWS de la manière suivante :

- StorageGRID n'est pas nécessaire `host` en-têtes à inclure dans `CanonicalHeaders`.
- StorageGRID n'est pas nécessaire `Content-Type` à inclure dans `CanonicalHeaders`.
- StorageGRID n'est pas nécessaire `x-amz-*` en-têtes à inclure dans `CanonicalHeaders`.



En règle générale, incluez toujours ces en-têtes dans CanonicalHeaders Pour s'assurer 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 dans un seul bloc \(signature AWS version 4\)](#)".

Informations associées

["Gestion des objets avec ILM"](#)

["Opérations sur les compartiments"](#)

["Opérations S3 suivies dans les journaux d'audit"](#)

["Configuration des connexions client"](#)

PLACER l'objet - Copier

Vous pouvez utiliser la demande S3 PUT Object - copie pour créer une copie d'un objet déjà stocké dans S3. Une opération PUT Object - Copy est la même que l'exécution d'un GET puis D'un PUT.

Résoudre les conflits

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.

Taille de l'objet

La taille maximale recommandée pour une opération d'objet PUT unique est de 5 Gio (5,368,709,120 octets). Si vos objets sont supérieurs à 5 Gio, utilisez le téléchargement partitionné.

La taille supportée maximale pour une opération objet PUT unique est de 5 Tio (5,497,558,138,880 octets). Cependant, l'alerte **S3 PUT Object size trop importante** est déclenchée si vous tentez de télécharger un objet supérieur à 5 Gio.

Caractères UTF-8 dans les métadonnées utilisateur

Si une requête inclut (non échappé) les valeurs UTF-8 dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur, le comportement StorageGRID n'est pas défini.

StorageGRID n'analyse ni n'interprète pas les caractères UTF-8 qui se sont échappé 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 comprend des caractères non imprimables.

En-têtes de demande 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 permet de copier l'objet et les métadonnées associées.

Vous pouvez spécifier REPLACE pour remplacer les métadonnées existantes lors de la copie de l'objet ou pour la mise à jour des 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 remplacer 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 rétention par défaut du compartiment sont utilisés pour calculer le mode de version de l'objet et conserver jusqu'à la date. Voir "[Utilisez l'API REST S3 pour configurer le verrouillage objet S3](#)".

- En-têtes de demande 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 [Demander des en-têtes pour le cryptage côté serveur](#)

En-têtes de requête non pris en charge

Les en-têtes de demande suivants ne sont pas pris en charge :

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-website-redirect-location

Options de classe de stockage

Le x-amz-storage-class L'en-tête de demande est pris en charge et affecte le nombre de copies d'objet créé par StorageGRID si la règle ILM correspondante spécifie le comportement d'ingestion de la double validation ou de l'équilibrage.

- STANDARD

(Valeur par défaut) Spécifie une opération d'ingestion à double validation lorsque la règle ILM utilise l'option de validation double, ou lorsque l'option équilibrée revient à créer des copies intermédiaires.

- REDUCED_REDUNDANCY

Spécifie une opération d'entrée de validation unique lorsque la règle ILM utilise l'option Double allocation ou lorsque l'option équilibrée revient à créer des copies intermédiaires.



Si vous ingez un objet dans un compartiment avec l'option de verrouillage objet S3 activée, la REDUCED_REDUNDANCY l'option est ignorée. Si vous ingez un objet dans un compartiment conforme d'ancienne génération, le REDUCED_REDUNDANCY option renvoie une erreur. StorageGRID procède toujours à une récupération à double engagement afin de satisfaire les exigences de conformité.

Utilisation de x-amz-copy-source dans PUT Object - Copy

Si le godet source et la clé, spécifiés dans le x-amz-copy-source en-tête diffèrent du compartiment de destination et de la clé, une copie des données de l'objet source est écrite sur la destination.

Si la source et la destination correspondent, et 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. Ceci a deux conséquences importantes :

- Vous ne pouvez pas utiliser METTRE objet - Copier pour chiffrer un objet existant ou pour modifier le chiffrement d'un objet existant. 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 la requête XNotImplemented.
- L'option de comportement d'ingestion spécifiée dans la règle ILM correspondante n'est pas utilisée. Tout changement au placement d'objet déclenché par la mise à jour est apporté lors de l'évaluation de ILM par des processus ILM en arrière-plan normaux.

En d'autres termes, si la règle ILM utilise l'option strict pour le comportement d'ingestion, aucune action n'est entreprise si les placements d'objet requis ne peuvent pas être effectués (par exemple, parce qu'un nouvel emplacement n'est pas disponible). L'objet mis à jour conserve son emplacement actuel jusqu'à ce que le placement requis soit possible.

Demander des en-têtes pour le cryptage côté serveur

Si vous utilisez le chiffrement côté serveur, les en-têtes de requête que vous fournissez dépendent du chiffrement de l'objet source et de l'intention 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 PUT Object - Copy, afin que l'objet puisse être décrypté puis copié :
 - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Spécifiez AES256.
 - `x-amz-copy-source-server-side-encryption-customer-key`: Spécifiez la clé de cryptage que vous avez fournie lors de la création de l'objet source.
 - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 que vous avez fourni lors de la création de l'objet source.
- Si vous souhaitez chiffrer 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`: Spécifiez AES256.
 - `x-amz-server-side-encryption-customer-key`: Spécifiez une nouvelle clé de cryptage pour l'objet cible.
 - `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé 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 des clés fournies par le client pour sécuriser les données d'objet, consultez les points à prendre en compte à la section "[utilisation du chiffrement côté serveur](#)".

- Si vous souhaitez chiffrer l'objet cible (la copie) avec une clé unique gérée par StorageGRID (SSE), incluez cet en-tête dans la demande PUT Object - Copy :
 - `x-amz-server-side-encryption`



Le `server-side-encryption` impossible de mettre à jour la valeur de l'objet. Faites plutôt une copie avec un nouveau `server-side-encryption` valeur à l'aide de `x-amz-metadata-directive: REPLACE`.

Gestion des versions

Si le compartiment source est multiversion, 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 l'`versionId` sous-ressource. Si le compartiment de destination est multiversion, la version générée est renvoyée dans le `x-amz-version-id` en-tête de réponse. Si le contrôle de version est suspendu pour le compartiment cible, alors `x-amz-version-id` renvoie une valeur « nulle ».

Informations associées

"Gestion des objets avec ILM"

"Opérations S3 suivies dans les journaux d'audit"

"PLACER l'objet"

SelectObjectContent

Vous pouvez utiliser la requête S3 SelectObjectContent pour filtrer le contenu d'un objet S3 à partir d'une instruction SQL simple.

Pour plus d'informations, reportez-vous au "[Documentation AWS pour SelectObjectContent](#)".

Avant de commencer

- Le compte de tenant dispose de l'autorisation S3 Select.
- Vous avez s3:GetObject autorisation pour l'objet à interroger.
- L'objet que vous souhaitez interroger doit être dans l'un des formats suivants :
 - **CSV.** Peut être utilisé tel qu'il est ou compressé dans des archives GZIP ou BZIP2.
 - **Parquet.** Exigences supplémentaires pour les objets parquet :
 - S3 Select prend uniquement en charge la compression par colonne à l'aide de GZIP ou de 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 compressées est de 512 Mo.
 - Vous devez utiliser les types de données spécifiés dans le schéma de l'objet.
 - Vous ne pouvez pas utiliser de types logiques D'INTERVALLE, de JSON, DE LISTE, DE TEMPS ou d'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 MIB.



L'utilisation de ScanRange n'est pas prise en charge.

Exemple de syntaxe de demande 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, 2010 populations, environ 2015 populations et le pourcentage de changement des données de recensement des États-Unis. 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, regardez comme 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, regardez comme 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 de l'interface de ligne de commande AWS (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, change.csv, se 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 partitionnés

Cette section décrit comment StorageGRID prend en charge les opérations de téléchargement partitionné.

Les conditions et notes suivantes s'appliquent à toutes les opérations de téléchargement partitionné :

- Vous ne devez pas dépasser 1,000 téléchargements partitionnés simultanés dans un seul compartiment car les résultats des requêtes List Multipart Uploads pour ce compartiment pourraient renvoyer des résultats incomplets.
- StorageGRID fait respecter les limites de taille d'AWS pour les pièces en plusieurs parties. Les clients S3 doivent respecter les consignes suivantes :
 - Chaque partie d'un téléchargement partitionné 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, la taille des pièces doit être la plus grande possible. Par exemple, utilisez une taille de pièce de 5 Gio pour un objet de 100 Gio. Chaque pièce étant considérée comme un objet unique, l'utilisation de pièces de grande taille réduit la surcharge liée aux métadonnées StorageGRID.
 - Pour les objets de moins de 5 Gio, envisagez l'utilisation de téléchargement non partitionné.
- La gestion des règles ILM est évaluée pour chaque partie d'un objet en plusieurs parties lors de son ingestion et pour l'objet dans son ensemble lorsque le téléchargement partitionné est terminé, si la règle ILM utilise le comportement d'ingestion équilibré ou strict. Vous devez savoir comment cela affecte le positionnement de l'objet et de la pièce :
 - Si le téléchargement partitionné est en cours de modification du ILM, si le téléchargement partitionné et certaines parties de l'objet peuvent ne pas répondre aux exigences ILM actuelles. Toute pièce qui n'est pas placée correctement est mise en file d'attente pour la réévaluation ILM et est déplacée

ultérieurement au bon emplacement.

- Lors de l'évaluation d'ILM pour une pièce, StorageGRID filtre la taille de la pièce, et non la taille de l'objet. Ainsi, certaines parties d'un objet peuvent être stockées dans des emplacements qui ne respectent pas les exigences de la règle ILM pour l'ensemble de l'objet. Par exemple, si une règle indique que tous les objets de 10 Go ou plus sont stockés dans DC1 alors que tous les objets plus petits sont stockés dans DC2, à l'acquisition chaque partie de 1 Go d'un téléchargement partitionné en 10 parties est stockée dans DC2. Lorsque ILM est évaluée pour l'ensemble de l'objet, toutes les parties de l'objet sont déplacées vers DC1.
- Toutes les opérations de téléchargement partitionné prennent en charge les contrôles de cohérence StorageGRID.
- Si nécessaire, vous pouvez utiliser le cryptage côté serveur avec des téléchargements partitionnés. Pour utiliser SSE (chiffrement côté serveur avec clés gérées par StorageGRID), vous avez accès au `x-amz-server-side-encryption` En-tête de demande dans la demande de téléchargement de pièces multiples uniquement. Pour utiliser SSE-C (chiffrement côté serveur avec clés fournies par le client), vous devez spécifier les trois mêmes en-têtes de demande de clé de chiffrement dans la demande de lancement de Multipart Upload et dans chaque demande de chargement de pièce suivante.

Fonctionnement	Mise en place
Liste des téléchargements partitionnés	Voir " Liste des téléchargements partitionnés "
Lancer le téléchargement de pièces multiples	Voir " Lancer le téléchargement de pièces multiples "
Télécharger la pièce	Voir " Télécharger la pièce "
Télécharger la pièce - Copier	Voir " Télécharger la pièce - Copier "
Chargement de pièces multiples complet	Voir " Chargement de pièces multiples complet "
Abandonner le téléchargement de pièces multiples	Mise en œuvre avec tout le comportement de l'API REST Amazon S3. D'être modifiées sans préavis.
Répertorier les pièces	Mise en œuvre avec tout le comportement de l'API REST Amazon S3. D'être modifiées sans préavis.

Informations associées

- "[Contrôles de cohérence](#)"
- "[Utilisez le cryptage côté serveur](#)"

Liste des téléchargements partitionnés

L'opération List Multipart Uploads répertorie les téléchargements partitionnés en cours pour un compartiment.

Les paramètres de demande suivants sont pris en charge :

- `encoding-type`

- key-marker
- max-uploads
- prefix
- upload-id-marker
- Host
- Date
- Authorization

Gestion des versions

Le téléchargement partitionné est constitué de différentes opérations permettant de lancer le téléchargement, de répertorier les téléchargements, de télécharger des pièces, d'assembler les pièces téléchargées et de terminer le téléchargement. Lorsque l'opération de téléchargement multipart complète est exécutée, c'est-à-dire le point où les objets sont créés (et versionnés le cas échéant).

Lancer le téléchargement de pièces multiples

L'opération Initiate Multipart Upload (CreateMultipartUpload) lance un téléchargement partitionné pour un objet et renvoie un ID de téléchargement.

Le `x-amz-storage-class` l'en-tête de demande est pris en charge. Valeur soumise pour `x-amz-storage-class` StorageGRID protège les données d'objet lors de leur ingestion, mais pas le nombre de copies persistantes de l'objet stockées dans le système StorageGRID (déterminé par ILM).

Si la règle ILM correspondant à un objet ingéré utilise l'option stricte pour le comportement d'ingestion, le `x-amz-storage-class` la barre de coupe n'a aucun effet.

Les valeurs suivantes peuvent être utilisées pour `x-amz-storage-class`:

- STANDARD (Valeur par défaut)
 - **Double commit** : si la règle ILM spécifie l'option de double validation pour le comportement d'ingestion, dès qu'un objet est ingéré, une seconde copie de cet objet est créée et distribuée à un autre nœud de stockage (double commit). Une fois la règle ILM évaluée, StorageGRID détermine si ces copies intermédiaires initiales répondent aux instructions de placement de la règle. Si ce n'est pas le cas, de nouvelles copies d'objet peuvent avoir besoin d'être effectuées à différents emplacements et les copies intermédiaires initiales peuvent avoir besoin d'être supprimées.
 - **Balanced** : si la règle ILM spécifie l'option équilibrée et que StorageGRID ne peut pas immédiatement effectuer toutes les copies spécifiées dans la règle, StorageGRID effectue deux copies intermédiaires sur différents nœuds de stockage.

Si StorageGRID peut immédiatement créer toutes les copies d'objet spécifiées dans la règle ILM (placement synchrone), l'`x-amz-storage-class` la barre de coupe n'a aucun effet.

- REDUCED_REDUNDANCY
 - **Double commit** : si la règle ILM spécifie l'option de double validation pour le comportement d'ingestion, StorageGRID crée une copie intermédiaire unique lors de l'ingestion de l'objet (simple commit).

- **Équilibré** : si la règle ILM spécifie l'option équilibrée, StorageGRID effectue une seule copie intermédiaire uniquement si le système ne peut pas immédiatement effectuer toutes les copies spécifiées dans la règle. Si StorageGRID peut effectuer un placement synchrone, cet en-tête n'a aucun effet. La **REDUCED_REDUNDANCY** L'option est meilleure lorsque la règle ILM correspondant à l'objet crée une copie répliquée unique. Dans ce cas, utilisez **REDUCED_REDUNDANCY** élimine la création et la suppression inutiles d'une copie d'objet supplémentaire pour chaque opération d'ingestion.

À l'aide du **REDUCED_REDUNDANCY** cette option n'est pas recommandée dans d'autres cas.

REDUCED_REDUNDANCY augmente le risque de perte de données d'objet lors de l'ingestion. Vous risquez par exemple de perdre des données si une seule copie est initialement stockée sur un nœud de stockage qui échoue avant l'évaluation du ILM.

 Le fait d'avoir une seule copie répliquée pendant une période donnée présente un risque de perte permanente des données. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur importante d'un noeud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, l'accès à l'objet est temporairement perdu.

Spécification **REDUCED_REDUNDANCY** l'impact sur le nombre de copies créées uniquement lors de l'ingestion d'un objet. Elle n'affecte pas le nombre de copies de l'objet lorsque celui-ci est évalué par la règle ILM active ; le stockage des données ne se produit pas à des niveaux de redondance inférieurs dans le système StorageGRID.

 Si vous ingez un objet dans un compartiment avec l'option de verrouillage objet S3 activée, la **REDUCED_REDUNDANCY** l'option est ignorée. Si vous ingez un objet dans un compartiment conforme d'ancienne génération, le **REDUCED_REDUNDANCY** option renvoie une erreur. StorageGRID procède toujours à une récupération à double engagement afin de satisfaire les exigences de conformité.

Les en-têtes de requête suivants sont pris en charge :

- Content-Type
- x-amz-meta-, suivi d'une paire nom-valeur contenant des métadonnées définies par l'utilisateur

Lorsque vous spécifiez la paire nom-valeur pour les métadonnées définies par l'utilisateur, utilisez le format général suivant :

```
x-amz-meta-_name_: `value`
```

Si vous souhaitez utiliser l'option **temps de création défini par l'utilisateur** comme heure de référence pour une règle ILM, vous devez utiliser `creation-time` nom des métadonnées enregistrées lors de la création de l'objet. Par exemple :

```
x-amz-meta-creation-time: 1443399726
```

La valeur pour `creation-time` Est évaluée en secondes depuis le 1er janvier 1970.



Ajout `creation-time` Comme les métadonnées définies par l'utilisateur n'sont pas autorisées si vous ajoutez un objet à un compartiment 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 rétention par défaut du compartiment sont utilisés pour calculer la version de l'objet conserver jusqu'à la date.

["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#)

- En-têtes de demande 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`

[Demander des en-têtes pour le cryptage côté serveur](#)



Pour plus d'informations sur la façon dont StorageGRID traite les caractères UTF-8, reportez-vous à la documentation relative à L'objet PUT.

Demander des en-têtes pour le cryptage côté serveur

Vous pouvez utiliser les en-têtes de demande suivants pour crypter un objet partitionné avec un cryptage côté serveur. Les options SSE et SSE-C sont mutuellement exclusives.

- **SSE** : utilisez l'en-tête suivant dans la demande lancer le téléchargement multi-pièces si vous souhaitez crypter l'objet avec une clé unique gérée par StorageGRID. Ne spécifiez pas cet en-tête dans les demandes de chargement de pièce.
 - `x-amz-server-side-encryption`
- **SSE-C** : utilisez les trois en-têtes de la demande de téléchargement multi pièces (et dans chaque demande de chargement ultérieure de pièce) si vous souhaitez chiffrer l'objet avec une clé unique que vous fournissez et gérez.
 - `x-amz-server-side-encryption-customer-algorithm`: Spécifiez AES256.
 - `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de cryptage pour le nouvel objet.
 - `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé 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 des clés fournies par le client pour sécuriser les données d'objet, consultez les points à prendre en compte à la section "utilisation du chiffrement côté serveur".

En-têtes de requête non pris en charge

L'en-tête de demande suivant n'est pas pris en charge et renvoie XNotImplemented

- x-amz-website-redirect-location

Gestion des versions

Le téléchargement partitionné est constitué de différentes opérations permettant de lancer le téléchargement, de répertorier les téléchargements, de télécharger des pièces, d'assembler les pièces téléchargées et de terminer le téléchargement. Les objets sont créés (et versionnés le cas échéant) lorsque l'opération de chargement multipièce complète est exécutée.

Informations associées

["Gestion des objets avec ILM"](#)

["PLACER l'objet"](#)

Télécharger la pièce

L'opération de téléchargement de pièce télécharge une pièce dans un téléchargement partitionné pour un objet.

En-têtes de demande pris en charge

Les en-têtes de requête suivants sont pris en charge :

- Content-Length
- Content-MD5

Demander des en-têtes pour le cryptage côté serveur

Si vous avez spécifié le cryptage SSE-C pour lancer la demande de téléchargement multipièce, vous devez également inclure les en-têtes de requête suivants dans chaque demande de chargement de pièce :

- x-amz-server-side-encryption-customer-algorithm: Spécifiez AES256.
- x-amz-server-side-encryption-customer-key: Spécifiez la même clé de cryptage que celle que vous avez fournie dans la demande de lancement de Multipart Upload.
- x-amz-server-side-encryption-customer-key-MD5: Spécifiez le même résumé MD5 que vous avez fourni dans la demande de lancement de Multipart Upload.



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, consultez les considérations de la section « utilisation du cryptage côté serveur ».

Gestion des versions

Le téléchargement partitionné est constitué de différentes opérations permettant de lancer le téléchargement, de répertorier les téléchargements, de télécharger des pièces, d'assembler les pièces téléchargées et de terminer le téléchargement. Les objets sont créés (et versionnés le cas échéant) lorsque l'opération de chargement multipièce complète est exécutée.

Informations associées

["Utilisez le cryptage côté serveur"](#)

Télécharger la pièce - Copier

L'opération Télécharger la pièce - Copier télécharge une partie d'un objet en copiant les données d'un objet existant en tant que source de données.

L'opération Télécharger la pièce - copie est implémentée avec tout le comportement de l'API REST Amazon S3. D'être modifiées sans préavis.

Cette requête lit et écrit les données de l'objet spécifiées dans `x-amz-copy-source-range` Dans le 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`

Demander des en-têtes pour le cryptage côté serveur

Si vous avez spécifié le cryptage SSE-C pour lancer la demande de téléchargement multi-pièces, vous devez également inclure les en-têtes de requête suivants dans chaque pièce de téléchargement - demande de copie :

- `x-amz-server-side-encryption-customer-algorithm`: Spécifiez AES256.
- `x-amz-server-side-encryption-customer-key`: Spécifiez la même clé de cryptage que celle que vous avez fournie dans la demande de lancement de Multipart Upload.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le même résumé MD5 que vous avez fourni dans la demande de lancement de Multipart Upload.

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 de copie de pièce de téléchargement, afin que l'objet puisse être décrypté puis copié :

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Spécifiez AES256.
- `x-amz-copy-source-server-side-encryption-customer-key`: Spécifiez la clé de cryptage que vous avez fournie lors de la création de l'objet source.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Spécifiez le résumé 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, consultez les considérations de la section « utilisation du cryptage côté serveur ».

Gestion des versions

Le téléchargement partitionné est constitué de différentes opérations permettant de lancer le téléchargement, de répertorier les téléchargements, de télécharger des pièces, d'assembler les pièces téléchargées et de terminer le téléchargement. Les objets sont créés (et versionnés le cas échéant) lorsque l'opération de chargement multipièce complète est exécutée.

Chargement de pièces multiples complet

L'opération complète de téléchargement de pièces multiples termine un téléchargement partitionné d'un objet en assemblant les pièces précédemment téléchargées.

Résoudre les conflits

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.

En-têtes de demande

Le `x-amz-storage-class` L'en-tête de demande est pris en charge et affecte le nombre de copies d'objet créé par StorageGRID si la règle ILM correspondante spécifie le comportement d'ingestion de la double validation ou de l'équilibrage.

- STANDARD

(Valeur par défaut) Spécifie une opération d'ingestion à double validation lorsque la règle ILM utilise l'option de validation double, ou lorsque l'option équilibrée revient à créer des copies intermédiaires.

- REDUCED_REDUNDANCY

Spécifie une opération d'entrée de validation unique lorsque la règle ILM utilise l'option Double allocation ou lorsque l'option équilibrée revient à créer des copies intermédiaires.



Si vous ingez un objet dans un compartiment avec l'option de verrouillage objet S3 activée, la `REDUCED_REDUNDANCY` l'option est ignorée. Si vous ingez un objet dans un compartiment conforme d'ancienne génération, le `REDUCED_REDUNDANCY` option renvoie une erreur. StorageGRID procède toujours à une récupération à double engagement afin de satisfaire les exigences de conformité.



Si un téléchargement partitionné 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 du `ETag` valeur pour les objets en plusieurs parties.

Gestion des versions

Cette opération termine un téléchargement partitionné. Si la gestion des versions est activée pour un compartiment, la version de l'objet est créée une fois le téléchargement partitionné terminé.

Si le contrôle de version est activé pour un compartiment, un contrôle unique `versionId` est automatiquement généré pour la version de l'objet stocké. C'est ça `versionId` est également renvoyé dans la réponse en utilisant le `x-amz-version-id` en-tête de réponse.

Si la gestion des versions est suspendue, la version de l'objet est stockée avec un null `versionId` si une version nulle existe déjà, elle sera remplacée.

 Lorsque le contrôle de version est activé pour un compartiment, le fait de terminer un téléchargement partitionné crée toujours une nouvelle version, même si des téléchargements partitionnés simultanés sont terminés sur la même clé d'objet. Lorsque le contrôle de version n'est pas activé pour un compartiment, il est possible de lancer un téléchargement partitionné et de lancer un autre lancement de téléchargement partitionné et de le terminer d'abord sur la même clé d'objet. Pour les compartiments non versionnés, le téléchargement partitionné de la dernière version est prioritaire.

Échec de la réPLICATION, de la notification ou de la notification des métadonnées

Si le compartiment dans lequel le téléchargement partitionné est configuré pour un service de plateforme, le téléchargement partitionné réussit même si l'action de réPLICATION ou de notification associée échoue.

Dans ce cas, une alarme est déclenchée dans le gestionnaire de grille sur Total Events (SMTT). Le message « échec de publication des notifications pour la clé nom-zone » s'affiche pour le dernier objet dont la notification a échoué. (Pour afficher ce message, sélectionnez **NOEUDS > noeud de stockage > événements**. Afficher le dernier événement en haut du tableau.) Les messages d'événement sont également répertoriés dans le `/var/local/log/bycast-err.log`.

Un locataire peut déclencher la réPLICATION ou la notification d'échec en mettant à jour les métadonnées ou les balises de l'objet. Un locataire peut soumettre à nouveau les valeurs existantes afin d'éviter toute modification non souhaitée.

Informations associées

["Gestion des objets avec ILM"](#)

Réponses d'erreur

Le système StorageGRID prend en charge toutes les réponses d'erreur de l'API REST S3 standard qui s'appliquent. En outre, l'implémentation de StorageGRID ajoute plusieurs réponses personnalisées.

Codes d'erreur de l'API S3 pris en charge

Nom	Statut HTTP
AccessDenied	403 interdit
BadDigest	400 demande erronée

Nom	Statut HTTP
BucketAlreadyExists	409 conflit
BucketNotEmpty	409 conflit
Corps entier	400 demande erronée
Erreur interne	500 erreur interne du serveur
InvalidAccessKeyId	403 interdit
Invalides	400 demande erronée
InvalidBucketName	400 demande erronée
InvalidBucketState	409 conflit
InvalidDigest	400 demande erronée
InvalidEncryptionAlgorithmError	400 demande erronée
Invalidpart	400 demande erronée
Ordre de pièce InvalidPartOrder	400 demande erronée
InvalidRange	416 Plage demandée non satisfiable
InvalidRequest	400 demande erronée
InvalidStorageClass	400 demande erronée
InvalidTag	400 demande erronée
URI non valide	400 demande erronée
KeyToolong	400 demande erronée
MalformedXML	400 demande erronée
MetadaTooLarge	400 demande erronée
MethodNotAllowed	405 méthode non autorisée
MissingContentLength	411 longueur requise

Nom	Statut HTTP
Erreur MissingestBodyError	400 demande erronée
En-tête MissinécuritéSent	400 demande erronée
NoSuchBucket	404 introuvable
NoSuchKey	404 introuvable
NoSuchUpload	404 introuvable
Note d'implémentation	501 non mis en œuvre
NoSuchBucketPolicy	404 introuvable
ObjectLockNotConfigurationError	404 introuvable
Pré-conditionFailed	412 Echec de la condition préalable
RequestTimeTooSkewed	403 interdit
Disponibilité des services	503 Service indisponible
SignatureDoesNotMatch	403 interdit
TooManyseaux	400 demande erronée
UserKeyMustBeSpecified	400 demande erronée

Codes d'erreur personnalisés StorageGRID

Nom	Description	Statut HTTP
XBucketLifecycleNotAlldue	La configuration du cycle de vie des compartiments n'est pas autorisée dans un compartiment conforme aux anciennes	400 demande erronée
XBucketPolicyParseException	Impossible d'analyser la politique de compartiment JSON.	400 demande erronée
XComplianceConflitt	Opération refusée en raison des paramètres de conformité hérités.	403 interdit

Nom	Description	Statut HTTP
XComplianceReduceRAIDForbidden	La réduction de la redondance est interdite dans le compartiment conforme aux réglementations existantes	400 demande erronée
XMaxBucketPolicyLengthExcediédé	Votre politique dépasse la longueur maximale autorisée pour la règle de gestion des compartiments.	400 demande erronée
XMissingInternalRequestHeader	En-tête d'une demande interne manquant.	400 demande erronée
XNoSuchBucketCompliance	La conformité héritée n'est pas activée dans le compartiment spécifié.	404 introuvable
XNotAcceptable	La demande contient un ou plusieurs en-têtes Accept qui n'ont pas pu être satisfaits.	406 non acceptable
XNotImplementation	La demande que vous avez fournie implique une fonctionnalité qui n'est pas implémentée.	501 non mis en œuvre

Requêtes StorageGRID S3

OPTIMISEZ la cohérence des compartiments

La demande D'obtention de cohérence de godet vous permet de déterminer le niveau de cohérence appliqué à un compartiment particulier.

Les contrôles de cohérence par défaut garantissent la lecture après écriture des nouveaux objets.

Pour effectuer cette opération, vous disposez de l'autorisation s3:GetBucketConsistency, ou d'un compte root.

Exemple de demande

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1  
Date: date  
Authorization: authorization string  
Host: host
```

Réponse

Dans le XML de réponse, <Consistency> renvoie l'une des valeurs suivantes :

Contrôle de cohérence	Description
tous	Tous les nœuds reçoivent les données immédiatement, sinon la requête échoue.
forte croissance mondiale	Garantit une 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 dans un site.
lecture-après-nouvelle-écriture	(Valeur par défaut) assure la cohérence en lecture après écriture des nouveaux objets et la cohérence des mises à jour des objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.
disponibilité	Assure la cohérence pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.

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 associées

["Contrôles de cohérence"](#)

PRÉSERVER la cohérence du godet

La demande de cohérence PUT bucket permet de spécifier le niveau de cohérence à appliquer aux opérations effectuées dans un compartiment.

Les contrôles de cohérence par défaut garantissent la lecture après écriture des nouveaux objets.

Avant de commencer

Vous disposez de l'autorisation s3:PutBucketConsistency, ou soyez root de compte, pour effectuer cette opération.

Demande

Le x-ntap-sg-consistency le paramètre doit contenir l'une des valeurs suivantes :

Contrôle de cohérence	Description
tous	Tous les nœuds reçoivent les données immédiatement, sinon la requête échoue.
forte croissance mondiale	Garantit une 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 dans un site.
lecture-après-nouvelle-écriture	(Valeur par défaut) assure la cohérence en lecture après écriture des nouveaux objets et la cohérence des mises à jour des objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.
disponibilité	Assure la cohérence pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.

Remarque: en général, vous devez utiliser la valeur de contrôle de cohérence "entre les nouvelles écritures". Si les demandes ne fonctionnent pas correctement, modifiez le comportement du client d'application si possible. Ou configurez le client afin de spécifier le contrôle de cohérence pour chaque requête d'API. Réglez le contrôle de cohérence au niveau du godet 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 associées

["Contrôles de cohérence"](#)

HEURE du dernier accès au compartiment

La demande D'heure de dernier accès À GET Bucket vous permet de déterminer si les dernières mises à jour de temps d'accès sont activées ou désactivées pour les

compartiments individuels.

Vous disposez de l'autorisation s3:GetBucketLastAccessTime, ou d'un compte root, pour effectuer 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 du temps de dernier accès sont activées pour le compartiment.

```
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>
```

METTRE l'heure du dernier accès au compartiment

La demande d'heure de dernier accès AU compartiment PERMET d'activer ou de désactiver les mises à jour des temps de dernier accès pour chaque compartiment. La désactivation des mises à jour du temps d'accès précédent améliore les performances. Il s'agit du paramètre par défaut pour tous les compartiments créés avec la version 10.3.0, ou ultérieure.

Pour terminer cette opération, vous disposez de l'autorisation s3:PutBuckLastAccessTime pour un compartiment, ou etre root pour un compte.

À partir de StorageGRID version 10.3, les mises à jour de l'heure du dernier accès sont désactivées par défaut pour tous les nouveaux compartiments. Si des compartiments ont été créés à l'aide d'une version antérieure de StorageGRID et que vous souhaitez faire correspondre le nouveau comportement par défaut, vous devez désactiver explicitement les mises à jour de la dernière heure d'accès pour chacune de ces rubriques précédentes. Vous pouvez activer ou désactiver les mises à jour de l'heure du dernier accès à l'aide de la demande PUT Bucket Last Access Time, de la case **S3 > Bucket > change Last Access Setting** dans le gestionnaire de locataires ou de l'API de gestion des locataires.



Si les dernières mises à jour de temps d'accès sont désactivées pour un compartiment, les opérations suivantes sont appliquées sur le compartiment :

- LES requêtes GET Object, GET Object ACL, GET Object Tagging et HEAD Object 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).
- PUT Object : les demandes de copie et DE BALISAGE d'objets 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 compartiment source, PUT Object - Copy Requests ne mettent pas à jour l'heure du dernier accès pour le compartiment source. L'objet copié n'est pas ajouté aux files d'attente pour l'évaluation ILM du compartiment source. Cependant, pour la destination, PLACER l'objet - demandes de copie toujours mettre à jour l'heure du dernier accès. La copie de l'objet est ajoutée aux files d'attente pour l'évaluation ILM.
- Terminer les demandes de téléchargement de pièces multiples mises à jour de l'heure de dernier accès. L'objet terminé est ajouté aux files d'attente pour l'évaluation ILM.

Exemples de demandes

Cet exemple permet d'activer le temps du dernier accès pour un compartiment.

```
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 pour un compartiment.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Informations associées

["Utilisez un compte de locataire"](#)

SUPPRIMEZ la configuration de notification des métadonnées de compartiment

La demande de configuration DE notification DE métadonnées DELETE Bucket vous permet de désactiver le service d'intégration de recherche pour les compartiments individuels en supprimant le XML de configuration.

Pour effectuer cette opération, vous disposez de l'autorisation s3>DeleteBucketMetadanotification pour un compartiment, ou être un compte root.

Exemple de demande

Cet exemple montre la désactivation du service d'intégration de recherche pour un compartiment.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

CONFIGURATION DES notifications de métadonnées de compartiment

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 chaque compartiment.

Pour terminer cette opération, vous disposez de l'autorisation s3:GetBucketMetadataNotification, ou d'un compte root.

Exemple de demande

Cette demande récupère la configuration de notification des métadonnées pour le compartiment nommé bucket.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Réponse

L'organe de réponse inclut la configuration de notification des métadonnées pour le compartiment. La configuration de notification des métadonnées vous permet de déterminer la configuration du compartiment pour l'intégration de la recherche. En d'autres termes, il vous permet de déterminer les objets à indexer et à quels terminaux 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 indique les objets qu'elle s'applique ainsi que la destination à laquelle StorageGRID doit envoyer les métadonnées d'objet. Les destinations doivent être spécifiées à l'aide de l'URN d'un terminal StorageGRID.

Nom	Description	Obligatoire
Configuration de la MetadaNotificationConfiguration	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 d'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 MetadaNotificationConfiguration.	Oui.
ID	Identifiant unique de la règle. Inclus dans l'élément règle.	Non
État	L'état peut être « activé » ou « désactivé ». Aucune action n'est prise pour les règles désactivées. Inclus dans l'élément règle.	Oui.

Nom	Description	Obligatoire
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 d'objet sont envoyées. Doit être l'URN d'un terminal 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 domain-name/myindex/mytype. <p>Les terminaux sont configurés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Ils se présentent sous la forme suivante :</p> <ul style="list-style-type: none"> • arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype <p>Le noeud final doit être configuré avant la soumission du XML de configuration, ou la configuration échouera avec une erreur 404.</p> <p>L'urne est incluse dans l'élément destination.</p>	Oui.

Exemple de réponse

XML inclus entre le

<MetadataNotificationConfiguration></MetadataNotificationConfiguration> les balises indiquent comment l'intégration avec un terminal d'intégration de la recherche est configurée pour le compartiment. Dans cet exemple, les métadonnées d'objet sont envoyées à un index Elasticsearch nommé current et le type nommé 2017 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-
1:3333333:domain/records/current/2017</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Informations associées

["Utilisez un compte de locataire"](#)

CONFIGURATION de notification des métadonnées de compartiment

La demande de configuration DE notification DE métadonnées PUT compartiments vous permet d'activer le service d'intégration de la recherche pour chaque compartiment. Le XML de configuration de notification de métadonnées que vous fournissez dans le corps de la requête spécifie les objets dont les métadonnées sont envoyées à l'index de recherche de destination.

Pour effectuer cette opération, vous disposez de l'autorisation s3:PutBucketMetadataNotification pour un compartiment ou être un compte root.

Demande

La demande doit inclure la configuration de notification de métadonnées dans l'organisme de demande. Chaque configuration de notification de métadonnées comprend une ou plusieurs règles. Chaque règle spécifie les objets à lesquels elle s'applique, ainsi que la destination vers laquelle StorageGRID doit envoyer les métadonnées d'objet.

Les objets peuvent être filtrés sur le préfixe du nom de l'objet. Par exemple, vous pouvez envoyer les métadonnées pour les objets avec le préfixe /images à une destination et à des objets avec le préfixe /videos à un autre.

Les configurations avec des préfixes qui se chevauchent ne sont pas valides et sont rejetées lorsqu'elles sont soumises. Par exemple, une configuration comprenant une règle pour les objets avec le préfixe test et une seconde 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 terminal StorageGRID. Le noeud final doit exister lorsque la configuration de notification de métadonnées est soumise, ou que 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 des métadonnées.

Nom	Description	Obligatoire
Configuration de la MetadaNotificationConfig uration	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 d'une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié. Les règles avec des prefixes qui se chevauchent sont rejetées. Inclus dans l'élément MetadaNotificationConfiguration.	Oui.
ID	Identifiant unique de la règle. Inclus dans l'élément règle.	Non

Nom	Description	Obligatoire
État	<p>L'état peut être « activé » ou « désactivé ». Aucune action n'est prise 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 d'objet sont envoyées. Doit être l'URN d'un terminal 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 domain-name/myindex/mytype. <p>Les terminaux sont configurés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Ils se présentent sous la forme suivante :</p> <ul style="list-style-type: none"> • arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype <p>Le noeud final doit être configuré avant la soumission du XML de configuration, ou 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 compartiment. Dans cet exemple, les métadonnées d'objet de 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 envoyée à une destination, tandis que les métadonnées d'objet correspondent au préfixe /videos est envoyé à une seconde 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-1:3333333: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>

```

JSON généré par le service d'intégration de la recherche

Lorsque vous activez le service d'intégration de la recherche pour un compartiment, un document JSON est généré et envoyé au terminal de destination à chaque ajout, mise à jour ou suppression de métadonnées d'objet.

Cet exemple montre un exemple de fichier JSON qui peut être généré lorsqu'un objet doté de la clé est associé SGWS/Tagging.txt est créé dans un compartiment nommé test. Le test le compartiment n'est pas multiversion versionId l'étiquette 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 qui est envoyé au noeud final de destination lorsque l'intégration de la recherche est activée.

Le nom du document inclut le nom du compartiment, le nom de l'objet et l'ID de version, le cas échéant.

Type	Nom de l'élément	Description
Informations sur les compartiments et les objets	godet	Nom du compartiment
Informations sur les compartiments et les objets	clé	Nom de clé d'objet
Informations sur les compartiments et les objets	ID de version	Version d'objet, pour les objets dans les compartiments multiversion
Informations sur les compartiments et les objets	région	Zone de godet, par exemple us-east-1
Métadonnées de système	taille	Taille de l'objet (en octets) visible par un client HTTP
Métadonnées de système	md5	Hachage d'objets
Métadonnées d'utilisateur	les métadonnées <i>key:value</i>	Toutes les métadonnées utilisateur pour l'objet, comme paires de clé-valeur

Type	Nom de l'élément	Description
Étiquettes	balises <i>key:value</i>	Toutes les balises d'objet définies pour l'objet, en tant que paires clé-valeur



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

Informations associées

["Utilisez un compte de locataire"](#)

DEMANDE d'utilisation du stockage

La demande GET Storage usage vous indique la quantité totale de stockage utilisée par un compte et pour chaque compartiment associé au compte.

Le volume de stockage utilisé par un compte et ses compartiments peut être obtenu à l'aide d'une demande GET Service modifiée avec le `x-ntap-sg-usage` paramètre de requête. L'utilisation du stockage par compartiment est suivie séparément des demandes DE 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. S'il est impossible d'obtenir une cohérence globale élevée, StorageGRID tente de récupérer les informations relatives à l'utilisation de façon cohérente sur les sites.

Vous disposez de l'autorisation `s3>ListAllMyseaux`, ou soyez root de compte, pour effectuer 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 contient 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 associées

["Contrôles de cohérence"](#)

Demandes de compartiment obsolètes pour la conformité des anciennes

Vous devrez peut-être utiliser l'API REST StorageGRID S3 pour gérer les compartiments qui ont été créés à l'aide de la fonctionnalité de conformité héritée.

Fonction de conformité obsolète

La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3.

Si vous avez précédemment activé le paramètre de conformité globale, le paramètre de verrouillage d'objet S3 global est activé dans StorageGRID 11.6. Vous ne pouvez plus créer de compartiments avec la conformité

activée. Toutefois, si nécessaire, vous pouvez utiliser l'API REST StorageGRID S3 pour gérer tous les compartiments conformes existants.

- "[Utilisez l'API REST S3 pour configurer le verrouillage objet S3](#)"
- "[Gestion des objets avec ILM](#)"
- "[Base de connaissances NetApp : comment gérer des compartiments conformes aux anciennes générations dans StorageGRID 11.5](#)"

Demandes de conformité obsolètes :

- "[Obsolète - METTRE les modifications de la demande de godet à des fins de conformité](#)"

L'élément XML SGCompliance est obsolète. Auparavant, vous pouviez inclure cet élément personnalisé StorageGRID dans le corps de demande XML facultatif de requêtes Put Bucket pour créer un compartiment conforme.

- "[Obsolète : OBTENEZ la conformité des compartiments](#)"

La demande DE conformité DE GET Bucket est obsolète. Cependant, vous pouvez continuer à utiliser cette demande pour déterminer les paramètres de conformité actuellement en vigueur pour un compartiment compatible existant.

- "[Obsolète : conformité DES compartiments PUT](#)"

La demande de conformité PUT Bucket est obsolète. Cependant, vous pouvez continuer à utiliser cette demande pour modifier les paramètres de conformité d'un compartiment conforme existant. Par exemple, vous pouvez placer un compartiment existant en attente légale ou augmenter sa période de conservation.

Obsolète : METTEZ les modifications de la demande de compartiment à des fins de conformité

L'élément XML SGCompliance est obsolète. Auparavant, vous pouviez inclure cet élément personnalisé StorageGRID dans le corps de demande XML facultatif de requêtes Put Bucket pour créer un compartiment conforme.



La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3.

["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#)

["Gestion des objets avec ILM"](#)

["Base de connaissances NetApp : comment gérer des compartiments conformes aux anciennes générations dans StorageGRID 11.5"](#)

Vous ne pouvez plus créer de compartiments avec la fonctionnalité conformité activée. Le message d'erreur suivant s'affiche si vous tentez d'utiliser les modifications de demande DE MISE en godet pour la conformité afin de créer un nouveau compartiment conforme :

The Compliance feature is deprecated.

Contact your StorageGRID administrator if you need to create new Compliant buckets.

Obsolète : RÉCUPÉRER la demande de conformité du compartiment

La demande DE conformité DE GET Bucket est obsolète. Cependant, vous pouvez continuer à utiliser cette demande pour déterminer les paramètres de conformité actuellement en vigueur pour un compartiment compatible existant.



La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3.

["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#)

["Gestion des objets avec ILM"](#)

["Base de connaissances NetApp : comment gérer des compartiments conformes aux anciennes générations dans StorageGRID 11.5"](#)

Vous disposez de l'autorisation s3:GetBucketCompliance, ou d'un compte root, pour effectuer cette opération.

Exemple de demande

Cet exemple de demande vous permet de déterminer les paramètres de conformité pour le compartiment nommé mybucket.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemple de réponse

Dans le XML de réponse, <SGCompliance> répertorie les paramètres de conformité utilisés pour le compartiment. Cet exemple de réponse montre les paramètres de conformité d'un compartiment dans lequel chaque objet sera conservé pendant un an (525,600 minutes), à partir de l'ingestion de l'objet dans la grille. Il n'y a actuellement aucune retenue légale sur ce godet. 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
RetentionPeriodMinutes	Durée de conservation des objets ajoutés à ce compartiment, en minutes. La période de conservation commence lorsque l'objet est ingéré dans la grille.
LegalHold	<ul style="list-style-type: none"> Vrai : ce compartiment est actuellement en attente 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 godet n'est pas actuellement en attente légale. Les objets de ce compartiment peuvent être supprimés à la fin de leur période de conservation.
Suppression automatique	<ul style="list-style-type: none"> Vrai : les objets de ce compartiment sont automatiquement supprimés lors de leur expiration, à moins que le compartiment ne soit soumis à une obligation légale. FALSE : les objets de ce compartiment ne sont pas supprimés automatiquement lorsque la période de conservation expire. Vous devez supprimer ces objets manuellement si vous devez les supprimer.

Réponses d'erreur

Si le compartiment 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 : PUT Bucket Compliance request

La demande de conformité PUT Bucket est obsolète. Cependant, vous pouvez continuer à utiliser cette demande pour modifier les paramètres de conformité d'un compartiment conforme existant. Par exemple, vous pouvez placer un compartiment existant en attente légale ou augmenter sa période de conservation.



La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3.

"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

"Gestion des objets avec ILM"

"Base de connaissances NetApp : comment gérer des compartiments conformes aux anciennes générations dans StorageGRID 11.5"

Vous disposez de l'autorisation s3:PutBucketCompliance, ou d'un compte root, pour effectuer 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 demande modifie les paramètres de conformité du compartiment nommé mybucket. Dans cet exemple, objets dans mybucket sera maintenant conservé pendant deux ans (1,051,200 minutes) au lieu d'un an, à partir de l'ingestion de l'objet dans le grid. Il n'y a pas de retenue légale sur ce godet. 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
RetentionPeriodMinutes	Durée de conservation des objets ajoutés à ce compartiment, en minutes. La période de conservation commence lorsque l'objet est ingéré dans la grille. Important lorsque vous spécifiez une nouvelle valeur pour RetentionPeriodMinutes, vous devez spécifier une valeur égale ou supérieure à la période de rétention actuelle du compartiment. Une fois la période de rétention du compartiment définie, vous ne pouvez pas la réduire ; vous pouvez uniquement l'augmenter.

Nom	Description
LegalHold	<ul style="list-style-type: none"> Vrai : ce compartiment est actuellement en attente 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 godet n'est pas actuellement en attente légale. Les objets de ce compartiment peuvent être supprimés à la fin de leur période de conservation.
Suppression automatique	<ul style="list-style-type: none"> Vrai : les objets de ce compartiment sont automatiquement supprimés lors de leur expiration, à moins que le compartiment ne soit soumis à une obligation légale. FALSE : les objets de ce compartiment ne sont pas supprimés automatiquement lorsque la période de conservation expire. Vous devez supprimer ces objets manuellement si vous devez les supprimer.

Niveau de cohérence des paramètres de conformité

Lorsque vous mettez à jour les paramètres de conformité d'un compartiment S3 avec une demande DE conformité PUT bucket, StorageGRID tente de mettre à jour les métadonnées du compartiment dans la grille. Par défaut, StorageGRID utilise le niveau de cohérence **Strong-global** pour garantir que tous les sites de data Center et tous les nœuds de stockage contenant des métadonnées de compartiment sont cohérents en lecture après écriture pour les paramètres de conformité modifiés.

Si StorageGRID ne parvient pas à atteindre le niveau de cohérence **strong-global** car un site de data Center ou plusieurs nœuds de stockage sur un site sont indisponibles, le code d'état HTTP de la réponse est 503 Service Unavailable.

Si vous recevez cette réponse, vous devez contacter l'administrateur du grid pour vous assurer que les services de stockage requis sont disponibles dans les plus brefs délais. Si l'administrateur de la grille ne parvient pas à mettre suffisamment de nœuds de stockage sur chaque site, le support technique vous demandera peut-être de relancer la demande échouée en forçant le niveau de cohérence **site fort**.

 Ne forcez jamais le niveau de cohérence **site fort** pour la conformité DU godet DE MISE à moins que vous n'ayez été invité à le faire par le support technique et à moins que vous compreniez les conséquences possibles de l'utilisation de ce niveau.

Lorsque le niveau de cohérence est réduit à **strong-site**, StorageGRID garantit que les paramètres de conformité mis à jour auront une cohérence lecture-après-écriture uniquement pour les requêtes client au sein d'un site. Il est donc possible que le système StorageGRID dispose de plusieurs paramètres incohérents pour ce compartiment 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 compartiment sous une obligation légale et que vous forcez un niveau de cohérence inférieur, les paramètres de conformité précédents du compartiment (c'est-à-dire la conservation légale) peuvent continuer à être en vigueur sur certains sites de data Center. Par conséquent, les objets qui, selon vous, sont en attente légale peuvent être supprimés à l'expiration de leur période de conservation, soit par l'utilisateur, soit par AutoDelete, si cette option est activée.

Pour forcer l'utilisation du niveau de cohérence **site fort**, réémettez la demande de conformité Put 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 compartiment n'a pas été créé pour être conforme, le code d'état HTTP de la réponse est 404 Not Found.
- Si RetentionPeriodMinutes Dans la demande est inférieure à la période de conservation actuelle du compartiment, le code d'état HTTP est 400 Bad Request.

Informations associées

"Obsolète : METTEZ les modifications de la demande de compartiment à des fins de conformité"

Règles d'accès au compartiment et au groupe

Utilisez les règles d'accès au compartiment et au groupe

StorageGRID utilise le langage de règles Amazon Web Services (AWS) pour permettre aux locataires S3 de contrôler l'accès aux compartiments et aux objets dans ces compartiments. Le système StorageGRID implémente un sous-ensemble du langage de règles de l'API REST S3. Les règles d'accès de l'API S3 sont écrites au format JSON.

Présentation de la stratégie d'accès

Il existe deux types de politiques d'accès pris en charge par StorageGRID.

- **Les règles de compartiment**, qui sont configurées à l'aide de la stratégie DE compartiment, DE LA règle DE compartiment PUT et DES opérations de L'API S3 de la politique de compartiment. Les règles de compartiment sont liées aux compartiments. Elles sont donc configurées de façon à contrôler l'accès des utilisateurs du compte du propriétaire du compartiment ou d'autres comptes au compartiment et aux objets. Une politique de compartiment s'applique à un seul compartiment et peut-être à plusieurs groupes.
- **Stratégies de groupe**, qui sont configurées à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Les stratégies de groupe sont associées à un groupe du compte, de sorte qu'elles sont configurées de manière à 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 peut-être plusieurs compartiments.



La priorité est la même entre les politiques de groupe et de compartiment.

Les règles de compartiment et de groupe StorageGRID respectent une grammaire spécifique définie par Amazon. À l'intérieur de chaque règle se trouve un ensemble d'énoncés de politique, et chaque instruction contient les éléments suivants :

- ID de déclaration (ID) (facultatif)
- Effet
- Principal/notPrincipal
- Ressource/NotResource
- Action/NotAction

- Condition (en option)

Les instructions de règles sont créées à l'aide de cette structure pour spécifier les autorisations : accorder <effet> pour autoriser/refuser <principal> d'exécuter <action> sur <ressource> lorsque <condition> s'applique.

Chaque élément de règle est utilisé pour une fonction spécifique :

Elément	Description
SID	L'élément Sid est facultatif. Le SID n'est destiné qu'à la description de l'utilisateur. Il est stocké mais non interprété par le système StorageGRID.
Effet	Utilisez l'élément d'effet pour déterminer si les opérations spécifiées sont autorisées ou refusées. Vous devez identifier les opérations que vous autorisez (ou refusez) les compartiments ou les objets à l'aide des mots clés action Element pris en charge.
Principal/notPrincipal	<p>Vous pouvez autoriser les utilisateurs, groupes et 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 peut accéder aux ressources qui lui sont propres.</p> <p>Il vous suffit de spécifier l'élément principal dans une stratégie de rubrique. Pour les stratégies de groupe, le groupe auquel la stratégie est associée est l'élément principal implicite.</p>
Ressource/NotResource	L'élément ressource identifie les compartiments et les objets. Vous pouvez autoriser ou refuser des autorisations pour les compartiments et les objets en utilisant le nom de ressource Amazon (ARN) pour identifier la ressource.
Action/NotAction	Les éléments action et effet sont les deux composants des autorisations. Lorsqu'un groupe demande une ressource, l'accès à la ressource est accordé ou refusé. L'accès est refusé sauf si vous attribuez des autorisations spécifiques, mais vous pouvez utiliser le refus explicite pour remplacer une autorisation accordée par une autre stratégie.
Condition	L'élément condition est facultatif. Les conditions vous permettent de créer des expressions pour déterminer quand une stratégie 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 à des 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 caractères ou plus, le point d'interrogation (?) correspond à n'importe quel caractère.

Dans l'élément principal, les caractères génériques ne sont pas pris en charge, sauf pour définir l'accès anonyme, qui accorde l'autorisation à tout le monde. Par exemple, vous définissez le caractère générique (*) comme valeur principale.

```
"Principal": "*"
```

Dans l'exemple suivant, l'instruction utilise les éléments effet, principal, action et ressource. Cet exemple montre une instruction de stratégie de compartiment complète qui utilise l'effet « Autoriser » pour donner les responsables, le groupe admin federated-group/admin et le groupe financier federated-group/finance, Autorisations d'exécution de l'action s3>ListBucket sur le compartiment nommé mybucket Et l'action s3GetObject sur tous les objets à l'intérieur de ce godet.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ],
        "Action": [
          "s3>ListBucket",
          "s3GetObject"
        ],
        "Resource": [
          "arn:aws:iam:s3:::mybucket",
          "arn:aws:iam:s3:::mybucket/*"
        ]
      }
    }
  ]
}
```

La stratégie de compartiment a une taille limite de 20,480 octets et la stratégie de groupe a une taille limite de 5,120 octets.

Paramètres de contrôle de cohérence des règles

Par défaut, toutes les mises à jour apportées aux stratégies de groupe sont cohérentes. Une fois la stratégie de groupe cohérente, les modifications peuvent prendre 15 minutes supplémentaires à appliquer en raison de la mise en cache des règles. Par défaut, toutes les mises à jour effectuées sur les règles de compartiment sont également cohérentes en définitive.

Si nécessaire, vous pouvez modifier les garanties de cohérence pour les mises à jour des règles de

compartiment. Par exemple, il peut être intéressant de vouloir modifier cette règle afin qu'elle devienne effective dès que possible pour des raisons de sécurité.

Dans ce cas, vous pouvez définir le Consistency-Control L'en-tête de la demande de stratégie PUT Bucket ou vous pouvez utiliser la demande DE cohérence PUT Bucket. Lorsque vous modifiez le contrôle de cohérence pour cette demande, vous devez utiliser la valeur **All**, qui fournit la garantie la plus élevée de cohérence de lecture après écriture. Si vous spécifiez une autre valeur de contrôle de cohérence dans un en-tête pour la demande DE cohérence PUT Bucket, la demande sera rejetée. Si vous spécifiez une autre valeur pour une demande de stratégie PUT Bucket, la valeur sera ignorée. Une fois la règle de compartiment cohérente, les modifications peuvent prendre 8 secondes supplémentaires pour effet, grâce à la mise en cache des règles.



Si vous définissez le niveau de cohérence sur **All** pour forcer une nouvelle stratégie de godet à devenir efficace plus tôt, veillez à remettre le contrôle au niveau du godet à sa valeur d'origine lorsque vous avez terminé. Sinon, toutes les futures demandes de rubrique utiliseront le paramètre **tous**.

Utilisez ARN dans les énoncés de politique

Dans les instructions de politique, le ARN est utilisé dans les éléments principal et ressource.

- Utilisez cette syntaxe pour spécifier la ressource S3 ARN :

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

- Utilisez cette syntaxe pour spécifier la ressource d'identité ARN (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 correspondre à zéro ou plus de caractères dans 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 de séquences d'échappement JSON \u. Le codage pourcentage n'est pas pris en charge.

"Syntaxe RFC 2141 URN"

Le corps de requête HTTP pour l'opération de stratégie PUT Bucket doit être codé avec charset=UTF-8.

Spécifiez les ressources dans une stratégie

Dans les instructions de stratégie, vous pouvez utiliser l'élément ressource pour spécifier le compartiment ou l'objet pour lequel les autorisations sont autorisées ou refusées.

- Chaque instruction de stratégie nécessite un élément ressource. Dans une politique, les ressources sont signalées par l'élément Resource, ou alternativement, NotResource pour exclusion.
- Vous spécifiez des ressources avec une ressource S3 ARN. Par exemple :

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- Vous pouvez également utiliser des variables de règles à l'intérieur de la clé d'objet. Par exemple :

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- La valeur de ressource peut spécifier un compartiment qui n'existe pas encore lorsqu'une stratégie de groupe est créée.

Spécifiez les entités de gestion dans une stratégie

Utilisez l'élément principal pour identifier l'utilisateur, le groupe ou le compte locataire qui est autorisé/refusé l'accès à la ressource par l'instruction de stratégie.

- Chaque énoncé de politique dans une politique de rubrique doit inclure un élément principal. Les énoncés de politique dans une stratégie de groupe n'ont pas besoin de l'élément principal car le groupe est considéré comme le principal.
- Dans une politique, les principes sont indiqués par l'élément « principal » ou « notprincipal » pour exclusion.
- Les identités basées sur les comptes doivent être spécifiées à l'aide d'un ID ou d'un ARN :

```
"Principal": { "AWS": "account_id"}  
"Principal": { "AWS": "identity_arn" }
```

- Dans cet exemple, le compte locataire utilise l'ID 27233906934684427525, qui inclut le compte root 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 (« gestionnaires ») :

```
"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 que Alex quitte l'entreprise et le nom d'utilisateur Alex est supprimé. Si un nouveau Alex rejoint l'organisation et est affecté de la même façon 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.

Spécifiez les autorisations dans une stratégie

Dans une stratégie, 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 stratégie, qui sont désignées par l'élément « action » ou par « NotAction » pour exclusion. Chacun de ces éléments est associé à des opérations spécifiques d'API REST S3.

Le tableau répertorie les autorisations qui s'appliquent aux compartiments et aux autorisations qui s'appliquent aux objets.

- (i) Amazon S3 utilise désormais l'autorisation s3:PutReplicationConfiguration pour les opérations de réPLICATION de compartiments PUT et DELETE. StorageGRID utilise des autorisations distinctes pour chaque action, qui correspond à la spécification Amazon S3 d'origine.
- (i) Une SUPPRESSION est effectuée lorsqu'un PUT est utilisé pour remplacer une valeur existante.

Autorisations qui s'appliquent aux compartiments

AUTORISATIONS	OPÉRATIONS DES API REST S3	PERSONNALISÉE POUR STORAGEGRID
s3:CreateBucket	PLACER le godet	
s3:DeleteBucket	SUPPRIMER le compartiment	

AUTORISATIONS	OPÉRATIONS DES API REST S3	PERSONNALISÉE POUR STORAGEGRID
s3>DeleteBucketMetadataNotification	SUPPRIMEZ la configuration de notification des métadonnées de compartiment	Oui.
s3>DeleteBucketPolicy	SUPPRIMER la règle de compartiment	
s3>DeleteReplicationConfiguration	SUPPRIMER la réplication du compartiment	Oui, séparer les autorisations pour PUT et DELETE*
s3:GetBucketAcl	OBTENIR l'ACL du compartiment	
s3:GetBucketCompliance	GARANTIR la conformité des compartiments (obsolète)	Oui.
s3:persistence GetBucketConsistency	OPTIMISEZ la cohérence des compartiments	Oui.
s3:GetBucketCORS	OBTENIR les godets	
s3:GetEncryptionConfiguration	CHIFFREMENT des compartiments	
s3:GetBucketLastAccessTime	HEURE du dernier accès au compartiment	Oui.
s3:GetBucketLocation	ACCÉDER à l'emplacement du compartiment	
s3:GetBucketMetadataNotification	CONFIGURATION DES notifications de métadonnées de compartiment	Oui.
s3:GetBucketNotification	GET Bucket notification	
s3:GetBucketObjectLockConfiguration	OBTENIR la configuration de verrouillage d'objet	
s3:GetBucketPolicy	GET Bucket policy	
s3:GetBucketTagging	GET Bucket tagging	
s3:GetBucketVersioning	GESTION des versions des compartiments	
s3:GetLifecycleConfiguration	OPTIMISEZ le cycle de vie des compartiments	

AUTORISATIONS	OPÉRATIONS DES API REST S3	PERSONNALISÉE POUR STORAGEGRID
s3:GetReplicationTM	RÉPLICATION des compartiments	
s3>ListAllMyseaux	<ul style="list-style-type: none"> • ACCÉDER au service • DÉCOUVREZ l'utilisation du stockage 	Oui, pour BÉNÉFICIER DE l'utilisation DU stockage
s3>ListBucket	<ul style="list-style-type: none"> • OBTENIR le compartiment (liste d'objets) • Godet DE TÊTE • Restauration POST-objet 	
s3>ListBuckMultipartUploads	<ul style="list-style-type: none"> • Liste des téléchargements partitionnés • Restauration POST-objet 	
s3>ListBuckeVersions	OBTENIR les versions de compartiment	
s3:PutBuckeCompliance	MISE en conformité des compartiments (obsolète)	Oui.
s3:persistance de PutBuckeConsistency	PRÉSERVER la cohérence du godet	Oui.
s3:PutBuckeCORS	<ul style="list-style-type: none"> • SUPPRIMER les godets† • PLACEZ les godets 	
s3:PutEncryptionConfiguration	<ul style="list-style-type: none"> • SUPPRIMER le chiffrement du compartiment • PUT Bucket Encryption 	
s3:PutBuckeLastAccessTime	METTRE l'heure du dernier accès au compartiment	Oui.
s3:PutBuckeMetadanotification	CONFIGURATION de notification des métadonnées de compartiment	Oui.
s3:PutBuckenotification	PUT Bucket notification	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:PutBucketLockConfiguration	<ul style="list-style-type: none"> PLACEZ le godet avec le <code>x-amz-bucket-object-lock-enabled: true</code> En-tête de demande (nécessite également l'autorisation <code>s3:CreateBucket</code>) CONFIGURATION du verrouillage de l'objet 	
s3:PutBucketPolicy	PUT Bucket policy	
s3:PutBucketTagging	<ul style="list-style-type: none"> SUPPRIMER le marquage du compartiment† PUT Bucket tagging 	
s3:PutBucketVersioning	GESTION des versions du compartiment	
s3:PutLifecycleConfiguration	<ul style="list-style-type: none"> SUPPRIMER le cycle de vie du godet† CYCLE de vie des compartiments 	
s3:PutReplicationTM	RÉPLICATION des compartiments	Oui, séparer les autorisations pour PUT et DELETE*

Autorisations qui s'appliquent aux objets

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:AbortMultipartUpload	<ul style="list-style-type: none"> Abandonner le téléchargement de pièces multiples Restauration POST-objet 	
s3:BypassGovernanceRetention	<ul style="list-style-type: none"> SUPPRIMER l'objet SUPPRIMER plusieurs objets CONSERVATION des objets 	
s3>DeleteObject	<ul style="list-style-type: none"> SUPPRIMER l'objet SUPPRIMER plusieurs objets Restauration POST-objet 	
s3>DeleteObjectTagging	SUPPRIMER le balisage d'objets	

AUTORISATIONS	OPÉRATIONS DES API REST S3	PERSONNALISÉE POUR STORAGEGRID
s3:DeleteObjectVersionTagging	SUPPRIMER le balisage d'objets (une version spécifique de l'objet)	
s3:DeleteObjectVersion	SUPPRIMER l'objet (une version spécifique de l'objet)	
s3:GetObject	<ul style="list-style-type: none"> • OBTENIR l'objet • Objet TÊTE • Restauration POST-objet • SÉLECTIONNEZ contenu de l'objet 	
s3:GetObjectAcl	OBTENIR l'ACL d'objet	
s3:GetObjectLegalHold	OBTENIR la mise en attente légale de l'objet	
s3:GetObjectRetention	OBTENIR la conservation des objets	
s3:GetObjectTagging	OBTENIR le balisage d'objets	
s3:GetObjectVersionTagging	OBTENIR le balisage d'objets (une version spécifique de l'objet)	
s3:GetObjectVersion	OBTENIR objet (une version spécifique de l'objet)	
s3>ListMultipartUploadParts	Répertorier les pièces, POST-restauration d'objet	
s3:PutObject	<ul style="list-style-type: none"> • PLACER l'objet • PLACER l'objet - Copier • Restauration POST-objet • Lancer le téléchargement de pièces multiples • Chargement de pièces multiples complet • Télécharger la pièce • Télécharger la pièce - Copier 	
s3:PutObjectLegalHold	METTRE l'objet en attente légale	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:PutObjectRetention	CONSERVATION des objets	
s3:PutObjectTagging	PLACER le balisage d'objets	
s3:PutObjectVersionTagging	PUT Object Tagging (une version spécifique de l'objet)	
s3:PutOverwriteObject	<ul style="list-style-type: none"> • PLACER l'objet • PLACER l'objet - Copier • PUT Object tagging • SUPPRIMER le balisage d'objets • Chargement de pièces multiples complet 	Oui.
s3:RestoreObject	Restauration POST-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 remplacer les données d'un objet, les métadonnées définies par l'utilisateur ou le balisage d'objets S3.

Les paramètres possibles pour cette autorisation sont les suivants :

- **Autoriser** : le client peut écraser un objet. Il s'agit du paramètre par défaut.
- **Deny** : le client ne peut pas écraser un objet. Lorsque cette option est définie sur Deny, l'autorisation PutOverwriteObject fonctionne comme suit :
 - Si un objet existant se trouve sur le même chemin :
 - Les données de l'objet, les métadonnées définies par l'utilisateur ou le balisage d'objets S3 ne peuvent pas être remplacés.
 - Toutes les opérations d'entrée en cours sont annulées et une erreur est renvoyée.
 - Si la gestion des versions S3 est activée, le paramètre Deny empêche les opérations PUT Object tagging ou DELETE Object tagging 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 autorisation a été définie.

 Si la règle S3 actuelle autorise l'érasrement 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'objet. En outre, si la case **empêcher la modification du client** est cochée (**CONFIGURATION > Paramètres de sécurité > réseau et objets**), ce paramètre remplace le paramètre de l'autorisation PutOverwriteObject.

Spécifiez les conditions dans une stratégie

Les conditions définissent le moment où une police sera en vigueur. Les conditions sont constituées d'opérateurs et de paires de clé-valeur.

Les conditions utilisent des paires de clé-valeur pour l'évaluation. Un élément condition peut contenir plusieurs conditions, et chaque condition peut contenir plusieurs paires clé-valeur. Le bloc condition utilise le format suivant :

```
Condition: {  
    condition_type: {  
        condition_key: condition_values
```

Dans l'exemple suivant, la condition ipAddress utilise la clé 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
- Valeur numérique
- Booléen
- Adresse IP
- Vérification nulle

Opérateurs de condition	Description
Equals à jambes de chaîne	Compare une clé à une valeur de chaîne en fonction de la correspondance exacte (sensible à la casse).
Equals stringNotEquals	Compare une clé à une valeur de chaîne basée sur la correspondance niée (sensible à la casse).
StringEqualIgnoreCase	Compare une clé à une valeur de chaîne basée sur la correspondance exacte (ignore case).
StringNotEqualIgnoreCase	Compare une clé à une valeur de chaîne basée sur la correspondance nérée (ignore le cas).

Opérateurs de condition	Description
StringLike	Compare une clé à une valeur de chaîne en fonction de la correspondance exacte (sensible à la casse). Peut inclure * et ? caractères génériques.
StringNotLike	Compare une clé à une valeur de chaîne basée sur la correspondance niée (sensible à la casse). Peut inclure * et ? caractères génériques.
Valeurs numériques	Compare une touche à une valeur numérique en fonction de la correspondance exacte.
NumericNotEquals	Compare une touche à une valeur numérique basée sur la correspondance annulée.
NumericGreaterThan	Compare une clé à une valeur numérique basée sur la comparaison « supérieure à ».
NumericGreaterThanOrEqual	Compare une clé à une valeur numérique basée sur la comparaison « supérieure ou égale ».
NumericLessThan	Compare une clé à une valeur numérique basée sur la comparaison « moins que ».
NumericLessThanOrEqual	Compare une clé à une valeur numérique basée sur la comparaison « inférieure à ou égale ».
BOOL	Compare une clé à une valeur booléenne basée sur la correspondance « vrai ou faux ».
Adresse IP	Compare une clé à une adresse IP ou une plage d'adresses IP.
Adresse de la note	Compare une clé à une adresse IP ou une plage d'adresses IP basée sur la correspondance annulée.
Nul	Vérifie si une clé condition est présente dans le contexte de demande actuel.

Touches de condition prises en charge

Catégorie	Toches de condition applicables	Description
Opérateurs IP	aws:Sourcelp	<p>Compare à l'adresse IP à partir de laquelle la demande a été envoyée. Peuvent être utilisées pour les opérations de compartiment ou d'objet.</p> <p>Remarque : si la requête S3 a été envoyée via le service Load Balancer sur les nœuds Admin et les passerelles, cela se compare à l'adresse IP en amont du service Load Balancer.</p> <p>Remarque : si un équilibrer de charge tiers non transparent est utilisé, il sera comparé à l'adresse IP de cet équilibrer de charge. Toutes X-Forwarded-For l'en-tête sera ignoré car sa validité ne peut pas être établie.</p>
Ressource/identité	aws:nom d'utilisateur	Compare le nom d'utilisateur de l'expéditeur à partir duquel la demande a été envoyée. Peuvent être utilisées pour les opérations de compartiment ou d'objet.
s3>ListBucket et s3:permissions ListBuckeVersions	s3:délimiteur	Compare avec le paramètre de délimiteur spécifié dans une demande GET Bucket ou GET Bucket Object versions.
s3>ListBucket et s3:permissions ListBuckeVersions	s3:touches max	Compare au paramètre max-keys spécifié dans une demande GET Bucket ou GET Bucket Object versions.
s3>ListBucket et s3:permissions ListBuckeVersions	s3:préfixe	Compare au paramètre de préfixe spécifié dans une demande GET Bucket ou GET Bucket Object versions.
s3:PutObject	s3 :conservation des jours restants avec un verrouillage objet	<p>Compare à la date de conservation spécifiée dans le x-amz-object-lock-retain-until-date demander l'en-tête ou calculé à partir de la période de rétention par défaut du compartiment pour s'assurer que ces valeurs se situent dans la plage autorisée pour les demandes suivantes :</p> <ul style="list-style-type: none"> • PLACER l'objet • PLACER l'objet - Copier • Lancer le téléchargement de pièces multiples

Catégorie	Toches de condition applicables	Description
s3:PutObjectRetention	s3 :conservation des jours restants avec un verrouillage objet	Compare à la date de conservation spécifiée dans la demande DE conservation D'objet PUT pour s'assurer qu'elle se trouve dans la plage autorisée.

Spécifiez les variables d'une règle

Vous pouvez utiliser des variables dans les règles pour remplir les informations relatives aux règles lorsqu'elles sont disponibles. Vous pouvez utiliser des variables de règle dans le Resource comparaisons d'éléments et de chaînes dans 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 condition :

```
"Condition": {
    "StringLike": {
        "s3:prefix": "${aws:username}/*"
        ...
    },
    ...
}
```

Variable	Description
\${aws:SourceIp}	Utilise la touche SourceIp comme variable fournie.
\${aws:username}	Utilise la clé de nom d'utilisateur comme variable fournie.
\${s3:prefix}	Utilise la clé de préfixe spécifique au service comme variable fournie.
\${s3:max-keys}	Utilise la touche max-keys spécifique au service comme variable fournie.
\${*}	Caractère spécial. Utilise le caractère comme caractère littéral *.
\${?}	Caractère spécial. Utilise le caractère comme littéral ? caractère.
\${\$}	Caractère spécial. Utilise le caractère comme caractère littéral \$.

Créez des règles nécessitant une gestion spéciale

Parfois, une politique peut accorder des autorisations dangereuses pour la sécurité ou dangereuses pour les opérations continues, telles que le verrouillage de l'utilisateur racine du compte. L'implémentation de l'API REST StorageGRID S3 est moins restrictive lors de la validation des règles qu'Amazon, mais tout aussi stricte lors de l'évaluation des règles.

Description de la politique	Type de règle	Comportement Amazon	Comportement de StorageGRID
Refusez vous-même toutes les autorisations sur le compte racine	Godet	Valide et appliquée, mais le compte utilisateur root conserve les autorisations nécessaires pour toutes les opérations des règles de compartiment S3	Identique
Refusez vous-même les autorisations d'accès à l'utilisateur/au groupe	Groupe	Valide et appliquée	Identique
Autoriser un groupe de comptes étrangers toute autorisation	Godet	Principal non valide	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 méthode non autorisée lorsque cela est autorisé par une règle
Autoriser un utilisateur ou une racine de compte étranger à accorder toute autorisation	Godet	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 méthode non autorisée lorsque cela est autorisé par une règle	Identique
Autoriser tout le monde à autoriser toutes les actions	Godet	Valide, mais les autorisations pour toutes les opérations de politique de compartiment S3 renvoient une erreur 405 méthode non autorisée pour la racine du compte étranger et les utilisateurs	Identique
Refuser les autorisations de tous pour toutes les actions	Godet	Valide et appliquée, mais le compte utilisateur root conserve les autorisations nécessaires pour toutes les opérations des règles de compartiment S3	Identique

Description de la politique	Type de règle	Comportement Amazon	Comportement de StorageGRID
Le principal est un utilisateur ou un groupe inexistant	Godet	Principal non valide	Valide
La ressource est un compartiment S3 inexistant	Groupe	Valide	Identique
Principal est un groupe local	Godet	Principal non valide	Valide
La police accorde à un compte non propriétaire (y compris les comptes anonymes) des autorisations pour METTRE des objets	Godet	Valide. Les objets sont détenus par le compte de créateur et la stratégie 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 d'objet.	Valide. Les objets sont la propriété du compte du propriétaire du compartiment. La politique de compartiment s'applique.

Protection WORM (Write-once, Read-many)

Vous pouvez créer des compartiments WORM (Write-once, Read-many) pour protéger les données, les métadonnées d'objet définies par l'utilisateur et le balisage d'objets S3. Vous configurez les compartiments WORM pour permettre la création de nouveaux objets et empêcher les écrasements ou la suppression de contenu existant. Utilisez l'une des approches décrites ici.

Pour vous assurer que les écrasements sont toujours refusés, vous pouvez :

- Dans 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 suivantes et les règles S3 :
 - Ajoutez une opération DE REFUS PutOverwriteObject à la règle S3.
 - Ajoutez une opération DE REFUS DeleteObject à la règle S3.
 - Ajouter une opération D'AUTORISATION PLACER l'objet à la règle S3.



La définition de DeleteObject sur DENY dans une politique 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 contre)

```
/mybucket/important.doc  
PUT#1 ---> OK  
PUT#2 -----> OK
```

Situation B: Remplacements séquentiels terminés (protégés contre)

```
/mybucket/important.doc  
PUT#1 -----> PUT#2 ---X (denied)
```

Informations associées

- "[Gestion des objets par les règles StorageGRID ILM](#)"
- "[Exemples de politiques de compartiments](#)"
- "[Exemples de stratégies de groupe](#)"
- "[Gestion des objets avec ILM](#)"
- "[Utilisez un compte de locataire](#)"

Exemples de politiques de compartiments

Utilisez les exemples de cette section pour créer des règles d'accès StorageGRID pour les compartiments.

Les politiques de compartiment spécifient les autorisations d'accès pour le compartiment à lequel la politique est attachée. Les règles de compartiment sont configurées à l'aide de l'API S3 PutBuckPolicy. Voir "[Opérations sur les compartiments](#)".

Il est possible de configurer une politique de compartiment à l'aide de l'interface de ligne de commandes AWS, comme indiqué dans la commande suivante :

```
> aws s3api put-bucket-policy --bucket examplebucket --policy  
file://policy.json
```

Exemple : autoriser tout le monde à accéder en lecture seule à un compartiment

Dans cet exemple, tout le monde, y compris anonyme, est autorisé à lister les objets dans le compartiment et à effectuer des opérations get Object sur tous les objets du compartiment. 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, ne peut écrire dans le compartiment.

```
{  
  "Statement": [  
    {  
      "Sid": "AllowEveryoneReadOnlyAccess",  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": [ "s3:GetObject", "s3>ListBucket" ],  
      "Resource":  
        ["arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*"]  
    }  
  ]  
}
```

Exemple : autoriser l'accès complet de tous les utilisateurs d'un compte et permettre à chacun d'un autre compte d'accéder en lecture seule à un compartiment

Dans cet exemple, tout le monde d'un compte spécifié peut accéder intégralement à un compartiment, tandis que les utilisateurs d'un autre compte spécifié ne sont autorisés qu'à répertorier le compartiment et effectuer des opérations GetObject sur les objets du compartiment en commençant par le shared/ préfixe de clé d'objet.



Dans StorageGRID, les objets créés par un compte autre que le propriétaire (y compris les comptes anonymes) sont détenus par le compte du propriétaire du compartiment. La politique de compartiment 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 accéder entièrement au groupe spécifié

Dans cet exemple, tout le monde, y compris anonyme, est autorisé à répertorier le compartiment et à effectuer des opérations GET Object sur tous les objets du compartiment, tandis que seuls les utilisateurs appartenant au groupe Marketing le compte spécifié est autorisé à accéder pleinement.

```

{
  "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 lire et à écrire l'accès à un compartiment si le client se trouve dans la plage IP

Dans cet exemple, tout le monde, y compris anonyme, est autorisé à répertorier le compartiment et à effectuer toutes les opérations objet sur tous les objets du compartiment, à condition que les demandes proviennent d'une plage 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 un accès complet à un compartiment exclusivement par un utilisateur fédéré spécifié

Dans cet exemple, l'utilisateur fédéré Alex est autorisé à accéder pleinement au examplebucket le godet et ses objets. Tous les autres utilisateurs, y compris « root », sont explicitement refusés à toutes les opérations. Notez toutefois que « root » n'est jamais refusé les autorisations de mettre/obtenir/DeleteBuckePolicy.

```

{
  "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 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 d'objets 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 stratégies d'accès StorageGRID pour les groupes.

Les stratégies de groupe spécifient les autorisations d'accès pour le groupe auquel la stratégie est associée. Il n'y a pas de `Principal` élément de la règle car il est implicite. Les règles de groupe sont configurées à l'aide du Gestionnaire de locataires ou de l'API.

Exemple : définissez la stratégie de groupe à l'aide du Gestionnaire de locataires

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 les membres de ce groupe auront accès. Voir "[Créez 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 règle de compartiment. Si vous sélectionnez cette option, seul l'utilisateur root peut accéder aux ressources S3 par défaut.
- **Accès en lecture seule** : les utilisateurs de ce groupe ont accès en lecture seule aux ressources S3. Par exemple, les utilisateurs de ce groupe peuvent afficher la liste des objets et lire les données d'objet, les métadonnées et les balises. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe en lecture seule s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Accès complet** : les utilisateurs de ce groupe ont accès aux ressources S3, y compris aux compartiments. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe à accès complet s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Atténuation des ransomware** : cet exemple de politique s'applique à tous les compartiments pour ce locataire. Les utilisateurs de ce groupe peuvent effectuer des actions courantes, mais ne peuvent pas supprimer définitivement des objets des compartiments pour lesquels la gestion des versions d'objet est activée.
- **Custom** : les utilisateurs du groupe disposent des autorisations que vous spécifiez dans la zone de texte.

Exemple : autoriser l'accès complet du groupe à toutes les rubriques

Dans cet exemple, tous les membres du groupe sont autorisés à accéder à tous les compartiments appartenant au compte du locataire, sauf s'ils sont explicitement refusés 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, à moins qu'ils ne soient explicitement refusés par la règle de compartiment. Par exemple, les utilisateurs de ce groupe peuvent afficher la liste des objets et lire les données d'objet, les métadonnées et les balises.

```
{  
    "Statement": [  
        {  
            "Sid": "AllowGroupReadOnlyAccess",  
            "Effect": "Allow",  
            "Action": [  
                "s3>ListAllMyBuckets",  
                "s3>ListBucket",  
                "s3>ListBucketVersions",  
                "s3GetObject",  
                "s3GetObjectTagging",  
                "s3GetObjectVersion",  
                "s3GetObjectVersionTagging"  
            ],  
            "Resource": "arn:aws:s3:::*"  
        }  
    ]  
}
```

Exemple : permettre aux membres du groupe d'accéder pleinement à leur « dossier » uniquement dans un compartiment

Dans cet exemple, les membres du groupe ne sont autorisés qu'à répertorier et accéder à leur dossier spécifique (préfixe de clé) dans le compartiment spécifié. Notez que les autorisations d'accès à partir d'autres stratégies de groupes et de la règle 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}/*"
    }
  ]
}

```

Configuration de la sécurité pour l'API REST

Il est recommandé de passer en revue les mesures de sécurité mises en œuvre pour l'API REST et de comprendre comment sécuriser votre système.

Comment StorageGRID assure la sécurité pour l'API REST

Vous devez comprendre comment le système StorageGRID implémente la sécurité, l'authentification et l'autorisation pour l'API REST.

StorageGRID utilise les mesures de sécurité suivantes.

- Les communications client avec le service Load Balancer utilisent HTTPS si HTTPS est configuré pour le noeud final Load Balancer.

Lorsque vous configurez un point final d'équilibrage de charge, HTTP peut éventuellement être activé. Par exemple, vous pouvez utiliser HTTP à des fins de test ou autres que la production. Pour plus d'informations, reportez-vous aux instructions d'administration de StorageGRID.

- Par défaut, StorageGRID utilise HTTPS pour les communications client avec les nœuds de stockage.

HTTP peut éventuellement être activé pour ces connexions. Par exemple, vous pouvez utiliser HTTP à des fins de test ou autres que la production. Pour plus d'informations, reportez-vous aux instructions d'administration de StorageGRID.

- Les communications entre StorageGRID et le client sont chiffrées à l'aide de TLS.

- Les communications entre le service Load Balancer et les nœuds de stockage dans la grille sont cryptées que le terminal de l'équilibrer de charge soit configuré pour accepter les connexions HTTP ou HTTPS.
- Les clients doivent fournir des en-têtes d'authentification HTTP à StorageGRID pour effectuer des opérations d'API REST.

Certificats de sécurité et applications client

Les clients peuvent se connecter au service Load Balancer sur les nœuds de passerelle ou les nœuds d'administration, directement aux nœuds de stockage.

Dans tous les cas, les applications client peuvent établir des connexions TLS à l'aide d'un certificat de serveur personnalisé chargé par l'administrateur de la grille ou d'un certificat généré par le système StorageGRID :

- Lorsque les applications client se connectent au service Load Balancer, elles le font à l'aide du certificat configuré pour le noeud final de l'équilibrer de charge spécifique utilisé pour établir la connexion. Chaque noeud final possède son propre certificat, qui est soit un certificat de serveur personnalisé chargé par l'administrateur de la grille, soit un certificat que l'administrateur de la grille a généré dans StorageGRID lors de la configuration du noeud final.
- Lorsque les applications client se connectent directement à un nœud de stockage, elles utilisent les certificats de serveur générés par le système qui ont été générés pour les nœuds de stockage lors de l'installation du système StorageGRID (qui sont signés par l'autorité de certification du système), ou un seul certificat de serveur personnalisé fourni pour la grille par un administrateur de grille.

Les clients doivent être configurés pour approuver l'autorité de certification qui a signé le certificat qu'ils utilisent pour établir des connexions TLS.

Pour plus d'informations sur la configuration des terminaux d'équilibrage de charge et sur l'ajout d'un certificat de serveur personnalisé unique pour les connexions TLS directement aux nœuds de stockage, reportez-vous aux instructions relatives à l'administration de StorageGRID.

Récapitulatif

Le tableau suivant montre comment les problèmes de sécurité sont implémentés dans les API REST S3 et Swift :

Problème de sécurité	Implémentation pour l'API REST
Sécurité de la connexion	TLS
Authentification du serveur	Certificat de serveur X.509 signé par l'autorité de certification du système ou certificat de serveur personnalisé fourni par l'administrateur
Authentification client	<ul style="list-style-type: none"> • S3 : compte S3 (ID de clé d'accès et clé d'accès secrète) • SWIFT : compte Swift (nom d'utilisateur et mot de passe)
Autorisation du client	<ul style="list-style-type: none"> • S3 : propriété des compartiments et toutes les règles de contrôle d'accès applicables • SWIFT : accès aux rôles d'administrateur

Informations associées

Algorithmes de hachage et de cryptage pris en charge pour les bibliothèques TLS

Le système StorageGRID prend en charge un ensemble limité de suites de chiffrement que les applications clientes peuvent utiliser lors de l'établissement d'une session TLS (transport Layer Security). Pour configurer les chiffrements, accédez à **CONFIGURATION > sécurité > Paramètres de sécurité** et sélectionnez **règles TLS et SSH**.

Versions supportées de TLS

StorageGRID supporte TLS 1.2 et TLS 1.3.



SSLv3 et TLS 1.1 (ou versions antérieures) ne sont plus pris en charge.

Informations associées

["Configurez les comptes et les connexions des locataires"](#)

Surveiller et auditer les opérations

Contrôler les taux d'entrée et de récupération des objets

Vous pouvez surveiller les taux d'entrée et de récupération des objets, ainsi que les mesures relatives au nombre d'objets, aux requêtes et à la vérification. Vous pouvez afficher le nombre de tentatives de lecture, d'écriture et de modification d'objets du système StorageGRID ayant échoué et réussies par les applications client.

Étapes

1. Connectez-vous au Grid Manager à l'aide d'un "[navigateur web pris en charge](#)".
2. Sur le tableau de bord, sélectionnez **Performance > S3 Operations** ou **Performance > Swift Operations**.

Cette section récapitule le nombre d'opérations client effectuées par votre système StorageGRID. La moyenne des débits de protocole est calculée au cours des deux dernières minutes.

3. Sélectionnez **NOEUDS**.
4. Dans la page d'accueil noeuds (niveau de déploiement), cliquez sur l'onglet **Load Balancer**.

Les graphiques présentent les tendances de tout le trafic client dirigé vers les terminaux d'équilibrage de charge dans la grille. Vous pouvez sélectionner un intervalle de temps en heures, jours, semaines, mois ou années, vous pouvez également appliquer un intervalle personnalisé.

5. Dans la page d'accueil noeuds (niveau de déploiement), cliquez sur l'onglet **objets**.

Le graphique montre les taux d'entrée et de récupération de l'intégralité de votre système StorageGRID en octets par seconde et en octets totaux. Vous pouvez sélectionner un intervalle de temps en heures, jours, semaines, mois ou années, vous pouvez également appliquer un intervalle personnalisé.

6. Pour afficher les informations relatives à un noeud de stockage particulier, sélectionnez-le dans la liste de gauche, puis cliquez sur l'onglet **objets**.

Le tableau affiche les taux d'entrée et de récupération de l'objet pour ce noeud de stockage. L'onglet inclut également des mesures pour le nombre d'objets, les requêtes et la vérification. Vous pouvez cliquer sur les

étiquettes pour afficher les définitions de ces mesures.



7. Si vous voulez encore plus de détails :

- Sélectionnez **SUPPORT > Outils > topologie de grille**.
- Sélectionnez **site > Présentation > main**.

La section opérations d'API affiche un récapitulatif des informations sur l'ensemble de la grille.

- Sélectionnez **Storage Node > LDR > client application > Présentation > main**

La section opérations affiche un récapitulatif des informations sur le nœud de stockage sélectionné.

Examiner les journaux d'audit

Les messages d'audit sont générés par les services StorageGRID et stockés dans des fichiers journaux texte. Des messages d'audit spécifiques aux API dans les journaux d'audit fournissent des données stratégiques de sécurité, d'exploitation et de surveillance des performances qui vous aideront à évaluer l'état de votre système.

Avant de commencer

- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez le `Passwords.txt` fichier.
- Vous connaissez l'adresse IP d'un nœud d'administration.

Description de la tâche

Le fichier journal d'audit actif est nommé `audit.log`, Et il est stocké sur des nœuds d'administration.

Une fois par jour, le fichier `audit.log` actif est enregistré, et un nouveau `audit.log` le fichier est démarré. Le nom du fichier enregistré indique quand il a été enregistré, au format `yyyy-mm-dd.txt`.

Après un jour, le fichier enregistré est compressé et renommé, au format `yyyy-mm-dd.txt.gz`, qui conserve la date originale.

Cet exemple montre l'actif `audit.log` fichier du jour précédent (`2018-04-15.txt`), et le fichier compressé pour la veille (`2018-04-14.txt.gz`).

```
audit.log  
2018-04-15.txt  
2018-04-14.txt.gz
```

Étapes

1. Connectez-vous à un nœud d'administration :
 - a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour passer à la racine : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Accédez au répertoire contenant les fichiers journaux d'audit :

```
cd /var/local/audit/export
```

3. Afficher le fichier journal d'audit actuel ou enregistré, selon les besoins.

Opérations S3 suivies dans les journaux d'audit

Plusieurs opérations de compartiment et les opérations d'objets sont suivies dans les journaux d'audit de StorageGRID.

Les opérations des compartiments sont suivies dans les journaux d'audit

- SUPPRIMER le compartiment
- SUPPRIMER le balisage du compartiment
- SUPPRIMER plusieurs objets
- OBTENIR le compartiment (liste d'objets)
- OBTENIR les versions d'objet de compartiment
- GET Bucket tagging
- Godet DE TÊTE
- PLACER le godet
- METTEZ le godet en conformité
- PUT Bucket tagging
- GESTION des versions du compartiment

Opérations d'objet suivies dans les journaux d'audit

- Chargement de pièces multiples complet
- Télécharger la pièce (lorsque la règle ILM utilise les comportements d'ingestion équilibrés ou stricts)
- Télécharger la pièce - Copier (lorsque la règle ILM utilise les comportements d'ingestion équilibrés ou stricts)
- SUPPRIMER l'objet
- OBTENIR l'objet
- Objet TÊTE
- Restauration POST-objet
- PLACER l'objet
- PLACER l'objet - Copier

Informations associées

["Opérations sur les compartiments"](#)

["Opérations sur les objets"](#)

Avantages des connexions HTTP actives, inactives et simultanées

La configuration des connexions HTTP peut avoir un impact sur les performances du système StorageGRID. Les configurations varient selon que la connexion HTTP est active ou inactive ou si vous avez simultanément plusieurs connexions.

Vous pouvez identifier les avantages en termes de performances pour les types de connexions HTTP suivants :

- Connexions HTTP inactives
- Connexions HTTP actives
- Connexions HTTP simultanées

Avantages de maintenir les connexions HTTP inactives ouvertes

Vous devez maintenir les connexions HTTP ouvertes même lorsque les applications client sont inactives pour permettre aux applications client d'effectuer les transactions suivantes sur la connexion ouverte. En fonction des mesures du système et de l'expérience d'intégration, vous devez garder une connexion HTTP inactive ouverte pendant 10 minutes maximum. StorageGRID peut fermer automatiquement une connexion HTTP qui reste ouverte et inactive pendant plus de 10 minutes.

Les connexions HTTP ouvertes et inactives offrent les avantages suivants :

- Réduction de la latence entre le moment où le système StorageGRID détermine qu'il doit effectuer une transaction HTTP et le moment où le système StorageGRID peut effectuer la transaction

La réduction de la latence constitue l'avantage principal, notamment pour la durée nécessaire à l'établissement des connexions TCP/IP et TLS.

- Augmentation de la vitesse de transfert des données en amorçant l'algorithme TCP/IP à démarrage lent avec des transferts effectués précédemment
- Notification instantanée de plusieurs classes de conditions de défaillance qui interrompent la connectivité entre l'application cliente et le système StorageGRID

Déterminer la durée d'ouverture d'une connexion inactive est un compromis entre les avantages du démarrage lent associés à la connexion existante et l'affectation idéale de la connexion aux ressources système internes.

Avantages des connexions HTTP actives

Pour les connexions directes aux nœuds de stockage, vous devez limiter la durée d'une connexion HTTP active à un maximum de 10 minutes, même si la connexion HTTP effectue des transactions en continu.

La détermination de la durée maximale pendant laquelle une connexion doit être maintenue ouverte est un compromis entre les avantages de la persistance de connexion et l'allocation idéale de la connexion aux ressources système internes.

Pour les connexions client aux nœuds de stockage, la limitation des connexions HTTP actives offre les avantages suivants :

- Équilibrage optimal de la charge sur l'ensemble du système StorageGRID.

Avec le temps, une connexion HTTP pourrait ne plus être optimale au fur et à mesure que les besoins en équilibrage de la charge évoluent. Le système réalise son meilleur équilibrage de charge lorsque les applications client établissent une connexion HTTP distincte pour chaque transaction, mais cela annule les gains les plus importants associés aux connexions persistantes.

- Permet aux applications clientes de diriger des transactions HTTP vers des services LDR qui ont de l'espace disponible.
- Permet de démarrer les procédures de maintenance.

Certaines procédures de maintenance ne démarrent qu'une fois toutes les connexions HTTP en cours terminées.

Pour les connexions client au service Load Balancer, limiter la durée des connexions ouvertes peut être utile pour permettre le démarrage rapide de certaines procédures de maintenance. Si la durée des connexions client n'est pas limitée, l'arrêt automatique des connexions actives peut prendre plusieurs minutes.

Avantages des connexions HTTP simultanées

Vous devez maintenir plusieurs connexions TCP/IP ouvertes au système StorageGRID pour permettre le parallélisme, ce qui augmente les performances. Le nombre optimal de connexions parallèles dépend de divers facteurs.

Les connexions HTTP simultanées offrent les avantages suivants :

- Latence réduite

Les transactions peuvent commencer immédiatement au lieu d'attendre que d'autres transactions soient effectuées.

- Rendement accru

Le système StorageGRID peut effectuer des transactions parallèles et augmenter le débit des transactions globales.

Les applications client doivent établir plusieurs connexions HTTP. Lorsqu'une application client doit effectuer une transaction, elle peut sélectionner et utiliser immédiatement toute connexion établie qui ne traite pas actuellement une transaction.

Le débit maximal de chaque topologie de chaque système StorageGRID est différent pour les transactions et les connexions simultanées, avant que les performances ne commencent à se dégrader. Le pic de débit dépend de facteurs tels que les ressources informatiques, les ressources réseau, les ressources de stockage et les liaisons WAN. Des facteurs sont également pris en charge par le nombre de serveurs et de services, ainsi que par le nombre d'applications prises en charge par le système StorageGRID.

Les systèmes StorageGRID prennent souvent en charge plusieurs applications client. Vous devez garder cela à l'esprit lorsque vous déterminez le nombre maximal de connexions simultanées utilisées par une application client. Si l'application client se compose de plusieurs entités logicielles qui établissent chacune des connexions avec le système StorageGRID, vous devez ajouter toutes les connexions entre les entités. Vous devrez peut-être régler le nombre maximal de connexions simultanées dans les situations suivantes :

- La topologie du système StorageGRID affecte le nombre maximal de transactions et de connexions simultanées pris en charge par le système.
- Les applications client qui interagissent avec le système StorageGRID sur un réseau avec une bande passante limitée peuvent être contraintes de réduire le niveau de simultanéité pour s'assurer que les transactions individuelles sont effectuées dans un délai raisonnable.
- Lorsque de nombreuses applications client partagent le système StorageGRID, il peut être nécessaire de réduire le degré de simultanéité pour ne pas dépasser les limites du système.

Séparation des pools de connexions HTTP pour les opérations de lecture et d'écriture

Vous pouvez utiliser des pools séparés de connexions HTTP pour les opérations en lecture et écriture, et contrôler la proportion que vous souhaitez utiliser pour chacun d'eux. Le recours à des pools séparés de connexions HTTP vous permet de contrôler les transactions et d'équilibrer la charge plus efficacement.

Les applications client peuvent créer des chargements qui sont dominants par la récupération (lecture) ou dominants par le stockage (écriture). Grâce à des pools séparés de connexions HTTP pour les transactions en lecture et écriture, vous pouvez ajuster la quantité de chaque pool à dédier pour les transactions en lecture ou en écriture.

Utiliser l'API REST de Swift (obsolète)

Utilisez l'API REST de Swift : présentation

Les applications client peuvent utiliser l'API OpenStack Swift pour interagir avec le système StorageGRID.



La prise en charge des applications du client Swift a été obsolète et sera supprimée dans une prochaine version.

StorageGRID prend en charge les versions spécifiques suivantes de Swift et HTTP.

Élément	Version
Spécification SWIFT	OpenStack Swift Object Storage API v1 depuis novembre 2015
HTTP	1.1 pour plus d'informations sur HTTP, consultez le document HTTP/1.1 (RFC 7230-35). Remarque: StorageGRID ne prend pas en charge HTTP/1.1 pipeline.

Informations associées

["OpenStack : API de stockage objet"](#)

Historique de la prise en charge de l'API Swift dans StorageGRID

Notez que des modifications ont été apportées à la prise en charge du système StorageGRID pour l'API REST Swift.

Relâchez	Commentaires
11.7	La prise en charge des applications du client Swift a été obsolète et sera supprimée dans une prochaine version.
11.6	Modifications éditoriales mineures.
11.5	Suppression du contrôle de cohérence faible Le niveau de cohérence disponible sera utilisé à la place.
11.4	Ajout de la prise en charge de TLS 1.3. Ajout d'une description de l'interrelation entre ILM et paramètre de cohérence.

Relâchez	Commentaires
11.3	Les opérations PUT mises à jour décrivent l'impact des règles ILM qui utilisent le placement synchrone à l'ingestion (options équilibrées et strictes pour le comportement d'ingestion). Ajout d'une description des connexions client qui utilisent des noeuds finaux d'équilibrage de charge ou des groupes de haute disponibilité. Les chiffrements TLS 1.1 ne sont plus pris en charge.
11.2	Modifications rédactionnelles mineures apportées au document
11.1	Ajout de la prise en charge de l'utilisation des connexions client HTTP pour Swift aux noeuds de la grille. Mise à jour des définitions des contrôles de cohérence.
11.0	Ajout de la prise en charge de 1,000 conteneurs pour chaque compte locataire.
10.3	Mises à jour administratives et corrections du document. Suppression des sections pour la configuration des certificats de serveur personnalisés.
10.2	Prise en charge initiale de l'API Swift par le système StorageGRID. La version actuellement prise en charge est l'API de stockage objet OpenStack Swift v1.

Comment StorageGRID implémente l'API REST Swift

Une application client peut utiliser les appels de l'API REST Swift pour se connecter aux nœuds de stockage et aux nœuds de passerelle afin de créer des conteneurs et de stocker et récupérer des objets. Les applications orientées services développées pour OpenStack Swift peuvent ainsi se connecter au stockage objet sur site fourni par le système StorageGRID.

Gestion des objets Swift

À l'entrée des objets Swift dans le système StorageGRID, ils sont gérés par les règles de gestion du cycle de vie des informations de la politique ILM active du système. Le "[Règles ILM](#)" et "[Politique ILM](#)" Créeation et distribution de copies des données d'objet par StorageGRID et gestion de ces copies au fil du temps Par exemple, une règle ILM peut s'appliquer aux objets de conteneurs Swift spécifiques et peut spécifier que plusieurs copies d'objets seront enregistrées dans plusieurs data centers pendant un certain nombre d'années.

Contactez votre consultant en services professionnels NetApp ou votre administrateur StorageGRID si vous avez besoin de comprendre en quoi les règles et règles ILM de la grille affecteront les objets de votre compte de locataire Swift.

Requêtes des clients en conflit

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». Le moment auquel l'évaluation « derniers-victoires » est basé sur la date à laquelle le système StorageGRID remplit une demande donnée et non sur la date à laquelle les clients Swift entament une opération.

Garanties et contrôles de cohérence

Par défaut, StorageGRID fournit une cohérence de lecture après écriture pour les objets nouvellement créés et une cohérence éventuelle pour les mises à jour et les OPÉRATIONS HEAD d'objet. Toutes "OBTENEZ" suite à une exécution réussie "EN" pourra lire les données nouvellement écrites. Les écrasements d'objets existants, les mises à jour de métadonnées et les suppressions sont cohérents. La propagation des écrasements ne prend généralement que quelques secondes ou minutes, mais peut prendre jusqu'à 15 jours.

StorageGRID vous permet également de contrôler la cohérence par conteneur. Les contrôles de cohérence assurent un équilibre entre la disponibilité des objets et la cohérence de ces objets entre plusieurs nœuds et sites de stockage, selon les exigences de votre application.

Recommandations pour l'implémentation de l'API REST Swift

Suivez ces recommandations lors de la mise en œuvre de l'API REST Swift pour une utilisation avec StorageGRID.

Recommandations pour les têtes à des objets inexistantes

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 le contrôle de cohérence « disponible ». Par exemple, vous devez utiliser le contrôle de cohérence « disponible » si votre application effectue une opération DE TÊTE à un emplacement avant d'effectuer une opération DE MISE à cet emplacement.

Sinon, si l'opération HEAD ne trouve pas l'objet, vous pouvez recevoir un nombre élevé de 500 erreurs de serveur interne si un ou plusieurs nœuds de stockage ne sont pas disponibles.

Vous pouvez définir le contrôle de cohérence « disponible » pour chaque conteneur à l'aide du "[REQUÊTE de cohérence du conteneur](#)". Le contrôle de cohérence « disponible » est défini pour chaque conteneur utilisant le "[DEMANDE DE cohérence du conteneur](#)".

Recommandations pour les noms d'objet

Pour les conteneurs créés dans StorageGRID 11.4 ou version ultérieure, il n'est plus nécessaire de limiter les noms d'objet afin de respecter les bonnes pratiques de performance. Par exemple, vous pouvez maintenant utiliser des valeurs aléatoires pour les quatre premiers caractères des noms d'objets.

Pour les conteneurs créés dans des versions antérieures à StorageGRID 11.4, suivez ces recommandations pour les noms d'objet :

- Vous ne devez pas utiliser de valeurs aléatoires comme les quatre premiers caractères des noms d'objets. Cela contraste avec l'ancienne recommandation AWS pour les préfixes de noms. Au lieu de cela, vous devez utiliser des préfixes non aléatoires et non uniques, tels que `image`.
- Si vous suivez l'ancienne recommandation AWS pour utiliser des caractères aléatoires et uniques dans les préfixes de noms, vous devez préfixer les noms d'objets avec un nom de répertoire. C'est-à-dire, utilisez le format suivant :

```
mycontainer/mydir/f8e3-image3132.jpg
```

Au lieu de ce format :

Recommandations pour « plages de lectures »

Si le "option globale pour compresser les objets stockés" Est activé, les applications clientes Swift doivent éviter d'effectuer des opérations GET Object qui spécifient une plage d'octets à renvoyer. Ces opérations de « lecture à plage » sont inefficaces, car StorageGRID doit décompresser efficacement les objets pour accéder aux octets demandés. LES opérations GET Object qui demandent une petite plage d'octets provenant d'un objet très volumineux sont particulièrement inefficaces. Par exemple, il est très 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 client peuvent être en attente.



Si vous devez compresser des objets et que votre application client doit utiliser des lectures de plage, augmentez le délai de lecture de l'application.

Configurez les comptes et les connexions des locataires

Pour configurer StorageGRID pour accepter les connexions à partir des applications client, vous devez créer un ou plusieurs comptes de tenant et configurer les connexions.

Créez et configurez des comptes de locataire Swift

Un compte de locataire Swift est requis pour que les clients de l'API Swift puissent stocker et récupérer des objets sur StorageGRID. Chaque compte de locataire possède son propre ID de compte, groupes et utilisateurs, ainsi que des conteneurs et des objets.

Les comptes de locataires Swift sont créés par un administrateur StorageGRID GRID à l'aide de Grid Manager ou de l'API de gestion du grid.

Quand "Création d'un compte de locataire Swift", l'administrateur de la grille spécifie les informations suivantes :

- "Nom d'affichage du locataire" (L'ID de compte du locataire est attribué automatiquement et ne peut pas être modifié)
- En option, un "quota de stockage pour le compte locataire" — le nombre maximal de gigaoctets, de téraoctets ou de pétaoctets disponibles pour les objets du locataire. Le quota de stockage d'un locataire représente une quantité logique (taille d'objet), et non une quantité physique (taille sur disque).
- Si "Authentification unique (SSO)" N'est pas utilisé pour le système StorageGRID, que le compte de locataire utilise son propre référentiel d'identité ou partage le référentiel d'identité de la grille, ainsi que le mot de passe initial pour l'utilisateur root local du locataire.
- Si SSO est activé, quel groupe fédéré dispose de l'autorisation d'accès racine pour configurer le compte de locataire.

Après la création d'un compte de locataire Swift, les utilisateurs disposant de l'autorisation d'accès racine peuvent accéder au gestionnaire de locataires pour effectuer des tâches telles que :

- Configuration de la fédération des identités (sauf si le référentiel d'identité est partagé avec la grille) et création de groupes et d'utilisateurs locaux

- Contrôle de l'utilisation du stockage



Les utilisateurs Swift doivent disposer de l'autorisation d'accès racine à "[Accédez au gestionnaire de locataires](#)". Toutefois, l'autorisation d'accès racine ne permet pas aux utilisateurs de s'authentifier auprès de l'API REST Swift pour créer des conteneurs et ingérer des objets. Les utilisateurs doivent disposer de l'autorisation Administrateur Swift pour s'authentifier dans l'API REST de Swift.

Configuration des connexions client

Un administrateur du grid fait des choix de configuration qui affectent la manière dont les clients Swift se connectent à StorageGRID pour stocker et récupérer les données. Les informations spécifiques dont vous avez besoin pour établir une connexion dépendent de la configuration choisie.

Les applications client peuvent stocker ou récupérer des objets en se connectant au service Load Balancer sur des nœuds d'administration ou des nœuds de passerelle, ou éventuellement l'adresse IP virtuelle d'un groupe haute disponibilité de nœuds d'administration ou de nœuds de passerelle.



Toutes les applications qui dépendent de StorageGRID pour l'équilibrage de la charge doivent se connecter à l'aide du service Load Balancer.

- Des nœuds de stockage, avec ou sans équilibrEUR de charge externe

Lors de la configuration de StorageGRID, un administrateur de la grille peut utiliser le gestionnaire de grille ou l'API de gestion de grille pour effectuer les étapes suivantes, qui sont toutes facultatives :

1. Configurez les noeuds finaux pour le service Load Balancer.

Vous devez configurer les noeuds finaux pour utiliser le service Load Balancer. Le service Load Balancer sur les nœuds d'administration ou de passerelle distribue les connexions réseau entrantes des applications client aux nœuds de stockage. Lors de la création d'un terminal d'équilibrage de charge, l'administrateur StorageGRID spécifie un numéro de port, si le terminal accepte les connexions HTTP ou HTTPS, le type de client (S3 ou Swift) qui utilisera le terminal ainsi que le certificat à utiliser pour les connexions HTTPS (le cas échéant). SWIFT les prend en charge "[types de points finaux](#)".

2. Configurer des réseaux clients non fiables.

Si un administrateur StorageGRID configure le réseau client d'un nœud pour qu'il ne soit pas fiable, le nœud accepte uniquement les connexions entrantes sur le réseau client sur les ports explicitement configurés en tant que noeuds finaux d'équilibrEUR de charge.

3. Configurez les groupes haute disponibilité.

Si l'administrateur crée un groupe haute disponibilité, les interfaces réseau de plusieurs nœuds d'administration ou nœuds de passerelle sont placées dans une configuration de sauvegarde active/active. Les connexions client sont établies à l'aide de l'adresse IP virtuelle du groupe haute disponibilité.

Voir "[Options de configuration pour les groupes haute disponibilité](#)" pour en savoir plus.

Résumé : adresses IP et ports pour les connexions client

Les applications client se connectent à StorageGRID en utilisant l'adresse IP d'un nœud de grid et le numéro de port d'un service sur ce nœud. Si des groupes de haute disponibilité sont configurés, les applications client peuvent se connecter en utilisant l'adresse IP virtuelle du groupe de haute disponibilité.

Informations requises pour établir des connexions client

Le tableau récapitule les différentes façons dont les clients peuvent se connecter à StorageGRID ainsi que les adresses IP et les ports utilisés pour chaque type de connexion. Voir "[Adresses IP et ports pour les connexions client](#)" Ou contactez votre administrateur StorageGRID pour plus d'informations.

Là où la connexion est établie	Service auquel le client se connecte	Adresse IP	Port
Groupe HAUTE DISPONIBILITÉ	Équilibrer de charge	Adresse IP virtuelle d'un groupe haute disponibilité	<ul style="list-style-type: none">• Port du terminal de l'équilibrer de charge
Nœud d'administration	Équilibrer de charge	Adresse IP du nœud d'administration	<ul style="list-style-type: none">• Port du terminal de l'équilibrer de charge
Nœud de passerelle	Équilibrer de charge	Adresse IP du nœud de passerelle	<ul style="list-style-type: none">• Port du terminal de l'équilibrer de charge
Nœud de stockage	LDR	Adresse IP du nœud de stockage	Ports Swift par défaut : <ul style="list-style-type: none">• HTTPS: 18083• HTTP : 18085

Exemple

Pour connecter un client Swift au point de terminaison Load Balancer d'un groupe HA de nœuds de passerelle, utilisez une URL structurée comme indiqué ci-dessous :

- `https://VIP-of-HA-group:LB-endpoint-port`

Par exemple, si l'adresse IP virtuelle du groupe HA est 192.0.2.6 et que le numéro de port d'un noeud final Swift Load Balancer est 10444, un client Swift peut utiliser l'URL suivante pour se connecter à StorageGRID :

- `https://192.0.2.6:10444`

Il est possible de configurer un nom DNS pour l'adresse IP que les clients utilisent pour se connecter à StorageGRID. Contactez votre administrateur réseau local.

Choisissez d'utiliser des connexions HTTPS ou HTTP

Lorsque les connexions client sont effectuées à l'aide d'un noeud final Load Balancer, les connexions doivent être effectuées à l'aide du protocole (HTTP ou HTTPS) spécifié pour ce noeud final. Pour utiliser HTTP pour les connexions client aux nœuds de stockage, vous devez activer son utilisation.

Par défaut, lorsque les applications client se connectent aux nœuds de stockage, elles doivent utiliser le protocole HTTPS chiffré pour toutes les connexions. Vous pouvez éventuellement activer des connexions HTTP moins sécurisées en sélectionnant le "["Activez HTTP pour les connexions de nœud de stockage"](#)" Dans Grid Manager. Par exemple, une application client peut utiliser HTTP lors du test de la connexion à un noeud de stockage dans un environnement non-production.



Soyez prudent lorsque vous activez HTTP pour une grille de production car les requêtes et les réponses seront envoyées sans cryptage.

Si l'option **Activer HTTP pour les connexions de nœud de stockage** est sélectionnée, les clients doivent utiliser des ports HTTP différents de ceux utilisés pour HTTPS.

Testez votre connexion dans la configuration de l'API Swift

Vous pouvez utiliser l'interface de ligne de commandes Swift pour tester votre connexion au système StorageGRID et vérifier que vous pouvez lire et écrire des objets sur le système.

Avant de commencer

- Vous devez avoir téléchargé et installé python-swaftclient, le client de ligne de commande Swift.

"SwiftStack: python-swftclient"

- Vous devez disposer d'un compte de locataire Swift dans le système StorageGRID.

Description de la tâche

Si vous n'avez pas configuré la sécurité, vous devez ajouter le `--insecure` marquer pour chacune de ces commandes.

Étapes

1. Interrogez l'URL d'information pour votre déploiement StorageGRID Swift :

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/info
capabilities
```

Cela suffit pour tester le fonctionnement de votre déploiement Swift. Pour tester davantage la configuration des comptes en stockant un objet, passez aux étapes supplémentaires.

2. Placer un objet dans le conteneur :

```
touch test_object
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
upload test_container test_object
--object-name test_object
```

3. Procurez-vous le conteneur pour vérifier l'objet :

```
swift  
-U <Tenant_Account_ID:Account_User_Name>  
-K <User_Password>  
-A https://<FQDN | IP>:<Port>/auth/v1.0  
list test_container
```

4. Supprimez l'objet :

```
swift  
-U <Tenant_Account_ID:Account_User_Name>  
-K <User_Password>  
-A https://<FQDN | IP>:<Port>/auth/v1.0  
delete test_container test_object
```

5. Supprimez le conteneur :

```
swift  
-U `<_Tenant_Account_ID:Account_User_Name_>`  
-K `<_User_Password_>`  
-A `'\https://<_FQDN_ | _IP_>:<_Port_>/auth/v1.0'  
delete test_container
```

Informations associées

["Créez et configurez des comptes de locataire Swift"](#)

["Configuration de la sécurité pour l'API REST"](#)

Opérations prises en charge par l'API REST Swift

Le système StorageGRID prend en charge la plupart des opérations dans l'API OpenStack Swift. Avant d'intégrer des clients de l'API REST Swift avec StorageGRID, consultez les informations d'implémentation pour les opérations des comptes, des conteneurs et des objets.

Opérations prises en charge par StorageGRID

Les opérations de l'API Swift suivantes sont prises en charge :

- ["Opérations sur le compte"](#)
- ["Opérations sur les conteneurs"](#)
- ["Opérations sur l'objet"](#)

En-têtes de réponse courants pour toutes les opérations

Le système StorageGRID implémente toutes les en-têtes courants pour les opérations prises en charge, comme défini par l'API de stockage objet OpenStack Swift v1.

Informations associées

["OpenStack : API de stockage objet"](#)

Terminaux API Swift pris en charge

StorageGRID prend en charge les points de terminaison de l'API Swift suivants : l'URL info, l'URL d'authentification et l'URL de stockage.

URL info

Vous pouvez déterminer les capacités et les limites de l'implémentation de StorageGRID Swift en émettant une demande GET à l'URL de base Swift avec le chemin /info.

`https://FQDN | Node IP:Swift Port/info/`

Dans la demande :

- *FQDN* est le nom de domaine complet.
- *Node IP* Est l'adresse IP du nœud de stockage ou du nœud de passerelle sur le réseau StorageGRID.
- *Swift Port* Est le numéro de port utilisé pour les connexions API Swift sur le nœud de stockage ou le nœud de passerelle.

Par exemple, l'URL d'information suivante demande des informations à un noeud de stockage avec l'adresse IP 10.99.106.103 et le port 18083.

`https://10.99.106.103:18083/info/`

La réponse inclut les fonctionnalités de l'implémentation Swift sous forme de dictionnaire JSON. Un outil client peut analyser la réponse JSON pour déterminer les fonctionnalités de l'implémentation et les utiliser comme contraintes pour les opérations de stockage ultérieures.

La mise en œuvre de StorageGRID de Swift permet un accès non authentifié à l'URL info.

URL d'authentification

Un client peut utiliser l'URL d'authentification Swift pour s'authentifier en tant qu'utilisateur de compte de locataire.

`https://FQDN | Node IP:Swift Port/auth/v1.0/`

Vous devez fournir l'ID de compte de tenant, le nom d'utilisateur et le mot de passe comme paramètres dans le X-Auth-User et X-Auth-Key en-têtes de demande, comme suit :

X-Auth-User: *Tenant_Account_ID:Username*

X-Auth-Key: *Password*

Dans les en-têtes de demande :

- *Tenant_Account_ID* Est l'ID de compte attribué par StorageGRID lors de la création du locataire Swift. Il s'agit du même ID de compte de locataire que celui utilisé sur la page de connexion du Gestionnaire de locataires.
- *Username* Est le nom d'un utilisateur locataire qui a été créé dans le Gestionnaire de tenant. Cet utilisateur doit appartenir à un groupe disposant de l'autorisation Administrateur Swift. L'utilisateur root du locataire ne peut pas être configuré pour utiliser l'API REST Swift.

Si la fédération des identités est activée pour le compte de tenant, indiquez le nom d'utilisateur et le mot de passe de l'utilisateur fédéré à partir du serveur LDAP. Vous pouvez également indiquer le nom de domaine de l'utilisateur LDAP. Par exemple :

`X-Auth-User: Tenant_Account_ID:Username@Domain_Name`

- *Password* est le mot de passe de l'utilisateur tenant. Les mots de passe utilisateurs sont créés et gérés dans le Gestionnaire de locataires.

La réponse à une demande d'authentification réussie renvoie une URL de stockage et un jeton d'authentification, comme suit :

`X-Storage-Url: https://FQDN | IP:Swift_Port/v1/Tenant_Account_ID`

`X-Auth-Token: token`

`X-Storage-Token: token`

Par défaut, le jeton est valide pendant 24 heures à compter de l'heure de génération.

Des jetons sont générés pour un compte de locataire spécifique. Un jeton valide pour un compte n'autorise pas un utilisateur à accéder à un autre compte.

URL du stockage

Une application client peut émettre des appels de l'API REST Swift pour exécuter des opérations de compte, conteneur et objet prises en charge sur un nœud de passerelle ou un nœud de stockage. Les demandes de stockage sont adressées à l'URL de stockage renvoyée dans la réponse d'authentification. La demande doit également inclure l'en-tête X-Auth-Token et la valeur renvoyée par la demande d'autorisation.

`https://FQDN | IP:Swift_Port/v1/Tenant_Account_ID`

`[/container] [/object]`

`X-Auth-Token: token`

Certains en-têtes de réponse de stockage contenant des statistiques d'utilisation peuvent ne pas refléter les chiffres précis des objets récemment modifiés. L'affichage des nombres précis dans ces en-têtes peut prendre quelques minutes.

Les en-têtes de réponse suivants pour les opérations de compte et de conteneur sont des exemples de ceux qui contiennent des statistiques d'utilisation :

- `X-Account-Bytes-Used`
- `X-Account-Object-Count`

- X-Container-Bytes-Used
- X-Container-Object-Count

Informations associées

["Configurez les comptes et les connexions des locataires"](#)

["Opérations sur le compte"](#)

["Opérations sur les conteneurs"](#)

["Opérations sur l'objet"](#)

Opérations sur le compte

Les opérations de l'API Swift suivantes sont effectuées sur les comptes.

OBTENIR un compte

Cette opération récupère la liste de conteneurs associée aux statistiques d'utilisation du compte et du compte.

Le paramètre de demande suivant est requis :

- Account

L'en-tête de demande suivant est requis :

- X-Auth-Token

Les paramètres de requête pris en charge suivants sont facultatifs :

- Delimiter
- End_marker
- Format
- Limit
- Marker
- Prefix

Une exécution réussie renvoie les en-têtes suivants avec une réponse « HTTP/1.1 204 aucun contenu » si le compte est trouvé et qu'aucun conteneur n'est vide, ou une réponse « HTTP/1.1 200 OK » si le compte est trouvé et que la liste de conteneurs n'est pas vide :

- Accept-Ranges
- Content-Length
- Content-Type
- Date
- X-Account-Bytes-Used
- X-Account-Container-Count

- X-Account-Object-Count
- X-Timestamp
- X-Trans-Id

Compte PRINCIPAL

Cette opération récupère les informations et les statistiques du compte à partir d'un compte Swift.

Le paramètre de demande suivant est requis :

- Account

L'en-tête de demande suivant est requis :

- X-Auth-Token

Une exécution réussie renvoie les en-têtes suivants avec une réponse « HTTP/1.1 204 No Content » :

- Accept-Ranges
- Content-Length
- Date
- X-Account-Bytes-Used
- X-Account-Container-Count
- X-Account-Object-Count
- X-Timestamp
- X-Trans-Id

Informations associées

["Surveiller et auditer les opérations"](#)

Opérations sur les conteneurs

StorageGRID prend en charge un maximum de 1,000 conteneurs par compte Swift. Les opérations d'API Swift suivantes sont effectuées sur les conteneurs.

SUPPRIMER le conteneur

Cette opération supprime un conteneur vide d'un compte Swift dans un système StorageGRID.

Les paramètres de demande suivants sont requis :

- Account
- Container

L'en-tête de demande suivant est requis :

- X-Auth-Token

Une exécution réussie renvoie les en-têtes suivants avec une réponse "HTTP/1.1 204 No Content" :

- Content-Length
- Content-Type
- Date
- X-Trans-Id

CONTENEUR

Cette opération récupère la liste d'objets associée au conteneur, ainsi que les statistiques et métadonnées de conteneur dans un système StorageGRID.

Les paramètres de demande suivants sont requis :

- Account
- Container

L'en-tête de demande suivant est requis :

- X-Auth-Token

Les paramètres de requête pris en charge suivants sont facultatifs :

- Delimiter
- End_marker
- Format
- Limit
- Marker
- Path
- Prefix

Une exécution réussie renvoie les en-têtes suivants avec une réponse « HTTP/1.1 200 Success » ou « HTTP/1.1 204 No Content » :

- Accept-Ranges
- Content-Length
- Content-Type
- Date
- X-Container-Bytes-Used
- X-Container-Object-Count
- X-Timestamp
- X-Trans-Id

Conteneur DE TÊTE

Cette opération récupère les statistiques du conteneur et les métadonnées d'un système StorageGRID.

Les paramètres de demande suivants sont requis :

- Account
- Container

L'en-tête de demande suivant est requis :

- X-Auth-Token

Une exécution réussie renvoie les en-têtes suivants avec une réponse "HTTP/1.1 204 No Content" :

- Accept-Ranges
- Content-Length
- Date
- X-Container-Bytes-Used
- X-Container-Object-Count
- X-Timestamp
- X-Trans-Id

PLACER le conteneur

Cette opération crée un conteneur pour un compte dans un système StorageGRID.

Les paramètres de demande suivants sont requis :

- Account
- Container

L'en-tête de demande suivant est requis :

- X-Auth-Token

Une exécution réussie renvoie les en-têtes suivants avec une réponse « HTTP/1.1 201 created » ou « HTTP/1.1 202 Accepted » (si le conteneur existe déjà sous ce compte) :

- Content-Length
- Date
- X-Timestamp
- X-Trans-Id

Un nom de conteneur doit être unique dans le namespace StorageGRID. Si le conteneur existe sous un autre compte, l'en-tête suivant est renvoyé : « HTTP/1.1 409 Conflict ».

Informations associées

"Surveiller et auditer les opérations"

Opérations sur l'objet

Les opérations suivantes de l'API Swift sont effectuées sur des objets. Ces opérations peuvent être suivies dans "[Journal d'audit StorageGRID](#)".

SUPPRIMER l'objet

Cette opération supprime le contenu et les métadonnées d'un objet du système StorageGRID.

Les paramètres de demande suivants sont requis :

- Account
- Container
- Object

L'en-tête de demande suivant est requis :

- X-Auth-Token

Une exécution réussie renvoie les en-têtes de réponse suivants avec un HTTP/1.1 204 No Content réponse :

- Content-Length
- Content-Type
- Date
- X-Trans-Id

Lors du traitement d'une requête DE SUPPRESSION d'objet, StorageGRID tente de supprimer immédiatement toutes les copies de l'objet des 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 et indique que le client a réussi.

Pour plus d'informations, voir "[Comment supprimer les objets](#)".

OBJET GET

Cette opération récupère le contenu de l'objet et obtient ses métadonnées depuis un système StorageGRID.

Les paramètres de demande suivants sont requis :

- Account
- Container
- Object

L'en-tête de demande suivant est requis :

- X-Auth-Token

Les en-têtes de demande suivants sont facultatifs :

- Accept-Encoding
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since
- Range

Une exécution réussie renvoie les en-têtes suivants avec un HTTP/1.1 200 OK réponse :

- Accept-Ranges
- Content-Disposition, retourné seulement si Content-Disposition les métadonnées ont été définies
- Content-Encoding, retourné seulement si Content-Encoding les métadonnées ont été définies
- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Timestamp
- X-Trans-Id

Objet TÊTE

Cette opération récupère les métadonnées et les propriétés d'un objet ingéré à partir d'un système StorageGRID.

Les paramètres de demande suivants sont requis :

- Account
- Container
- Object

L'en-tête de demande suivant est requis :

- X-Auth-Token

Une exécution réussie renvoie les en-têtes suivants avec une réponse "HTTP/1.1 200 OK" :

- Accept-Ranges
- Content-Disposition, retourné seulement si Content-Disposition les métadonnées ont été définies

- Content-Encoding, retourné seulement si Content-Encoding les métadonnées ont été définies
- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Timestamp
- X-Trans-Id

PLACER l'objet

Cette opération crée un nouvel objet avec des données et des métadonnées, ou remplace un objet existant par des données et des métadonnées dans un système StorageGRID.

StorageGRID prend en charge les objets jusqu'à 5 Tio (5,497,558,138,880 octets).

 Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». Le moment auquel l'évaluation « derniers-victoires » est basé sur la date à laquelle le système StorageGRID remplit une demande donnée et non sur la date à laquelle les clients Swift entament une opération.

Les paramètres de demande suivants sont requis :

- Account
- Container
- Object

L'en-tête de demande suivant est requis :

- X-Auth-Token

Les en-têtes de demande suivants sont facultatifs :

- Content-Disposition
- Content-Encoding

Ne pas utiliser de moucheté Content-Encoding Si la règle ILM appliquée à un objet filtre les objets en fonction de leur taille et utilise le placement synchrone à l'ingestion (options équilibrées ou strictes pour le comportement d'ingestion).

- Transfer-Encoding

N'utilisez pas de compression ou de déboucheté Transfer-Encoding Si la règle ILM appliquée à un objet filtre les objets en fonction de leur taille et utilise le placement synchrone à l'ingestion (options équilibrées ou strictes pour le comportement d'ingestion).

- Content-Length

Si une règle ILM filtre les objets par taille et utilise le placement synchrone lors de l'ingestion, vous devez spécifier Content-Length.



Si vous ne suivez pas ces directives pour Content-Encoding, Transfer-Encoding, et Content-Length, StorageGRID doit enregistrer l'objet avant de déterminer la taille de l'objet et d'appliquer la règle ILM. En d'autres termes, StorageGRID doit créer par défaut des copies intermédiaires d'un objet à l'entrée. C'est-à-dire que StorageGRID doit utiliser l'option de double validation pour le comportement d'ingestion.

Pour plus d'informations sur le placement synchrone et les règles ILM, voir "[Options de protection des données pour l'ingestion](#)".

- Content-Type
- ETag
- X-Object-Meta-<name\> (métadonnées liées aux objets)

Si vous souhaitez utiliser l'option **temps de création défini par l'utilisateur** comme heure de référence pour une règle ILM, vous devez stocker la valeur dans un en-tête défini par l'utilisateur nommé X-Object-Meta-Creation-Time. Par exemple :

```
X-Object-Meta-Creation-Time: 1443399726
```

Ce champ est évalué en secondes depuis le 1er janvier 1970.

- X-Storage-Class: reduced_redundancy

Cet en-tête affecte le nombre de copies d'objet créées par StorageGRID si la règle ILM correspondant à l'objet ingéré spécifie le comportement d'ingestion de la double validation ou de l'équilibrage.

- **Double commit** : si la règle ILM spécifie l'option de double validation pour le comportement d'ingestion, StorageGRID crée une copie intermédiaire unique lors de l'ingestion de l'objet (simple commit).
- **Équilibré** : si la règle ILM spécifie l'option équilibrée, StorageGRID effectue une seule copie intermédiaire uniquement si le système ne peut pas immédiatement effectuer 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'en-tête est le plus utilisé lorsque la règle ILM correspondant à l'objet crée une copie répliquée unique. Dans ce cas, utilisez `reduced_redundancy` élimine la création et la suppression inutiles d'une copie d'objet supplémentaire pour chaque opération d'ingestion.

À l'aide du `reduced_redundancy` l'en-tête n'est pas recommandé dans d'autres cas, car il augmente le risque de perte de données d'objet lors de l'ingestion. Vous risquez par exemple de perdre des données si une seule copie est initialement stockée sur un nœud de stockage qui échoue avant l'évaluation du ILM.



Le fait d'avoir une seule copie répliquée pendant une période donnée présente un risque de perte permanente des données. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur importante d'un noeud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, l'accès à l'objet est temporairement perdu.

Notez que la spécification `reduced_redundancy` l'impact sur le nombre de copies créées uniquement lors de l'ingestion d'un objet. Elle n'affecte pas le nombre de copies de l'objet lorsque celui-ci est évalué par la règle ILM active et n'entraîne pas le stockage des données avec des niveaux de redondance inférieurs dans le système StorageGRID.

Une exécution réussie renvoie les en-têtes suivants avec une réponse "HTTP/1.1 201 created" :

- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Trans-Id

Demande D'OPTIONS

La demande D'OPTIONS vérifie la disponibilité d'un service Swift individuel. La demande D'OPTIONS est traitée par le noeud de stockage ou le noeud passerelle spécifié dans l'URL.

Méthode DES OPTIONS

Par exemple, les applications client peuvent émettre une demande D'OPTIONS vers le port Swift sur un noeud de stockage, sans fournir d'informations d'authentification Swift, pour déterminer si le noeud de stockage est disponible. Vous pouvez utiliser cette requête pour la surveillance ou permettre aux équilibreurs de charge externes d'identifier lorsqu'un noeud de stockage est arrêté.

Lorsqu'elle est utilisée avec l'URL info ou l'URL de stockage, la méthode OPTIONS renvoie une liste de verbes pris en charge pour l'URL donnée (par exemple, HEAD, GET, OPTIONS et PUT). La méthode D'OPTIONS ne peut pas être utilisée avec l'URL d'authentification.

Le paramètre de demande suivant est requis :

- Account

Les paramètres de demande suivants sont facultatifs :

- Container
- Object

Une exécution réussie renvoie les en-têtes suivants avec une réponse « HTTP/1.1 204 No Content ». La demande D'OPTIONS à l'URL de stockage ne nécessite pas que la cible existe.

- Allow (Une liste de verbes pris en charge pour l'URL donnée, par exemple, HEAD, GET, OPTIONS, Et PUT)
- Content-Length
- Content-Type
- Date
- X-Trans-Id

Informations associées

["Terminaux API Swift pris en charge"](#)

Réponse aux erreurs des opérations de l'API Swift

La compréhension des réponses d'erreur possibles peut vous aider à résoudre les problèmes.

Les codes d'état HTTP suivants peuvent être renvoyés lorsque des erreurs se produisent au cours d'une opération :

Nom de l'erreur Swift	Statut HTTP
AccountNameToolong, ContainerNameToolong, HeaderTooBig, InvalidContainerName, InvalidRequest, InvalidURI, MetadaNameToolong, MetadaValueTooBig, MissingSecurityHeader, ObjectNameToolong, TooManyContainers, TooManyMetadalItems, TotalMetadaTooLarge	400 demande erronée
AccessDenied	403 interdit
ContainerNotEmpty, ContainerAlreadyExists	409 conflit
Erreur interne	500 erreur interne du serveur
InvalidRange	416 Plage demandée non satisfiable
MethodNotAllowed	405 méthode non autorisée
MissingContentLength	411 longueur requise
NOTFOUND	404 introuvable
Note d'implémentation	501 non mis en œuvre
Pré-conditionFailed	412 Echec de la condition préalable
ResourceNotFound	404 introuvable

Nom de l'erreur Swift	Statut HTTP
Non autorisé	401 non autorisé
Entité intraitableEntity	422 entité impossible à traiter

Opérations de l'API REST StorageGRID Swift

Des opérations sont ajoutées à l'API REST Swift qui sont spécifiques au système StorageGRID.

DEMANDE DE cohérence du conteneur

"[Contrôles de cohérence](#)" Équilibre entre disponibilité des objets et cohérence entre ces objets sur différents nœuds et sites de stockage. La demande DE cohérence DU conteneur GET vous permet de déterminer le niveau de cohérence appliqué à un conteneur particulier.

Demande

En-tête HTTP de demande	Description
X-Auth-Token	Spécifie le jeton d'authentification Swift pour le compte à utiliser pour la demande.
x-ntap-sg-cohérence	Spécifie le type de demande, où true = COHÉRENCE GARANTIE entre les conteneurs, et false = CONTENEUR GET.
Hôte	Nom d'hôte auquel la demande est dirigée.

Exemple de demande

```
GET /v1/28544923908243208806/Swift container
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: true
Host: test.com
```

Réponse

En-tête HTTP de réponse	Description
Date	La date et l'heure de la réponse.
Connexion	Indique si la connexion au serveur est ouverte ou fermée.
X-Trans-ID	Identifiant de transaction unique pour la demande.

En-tête HTTP de réponse	Description
Longueur-contenu	Longueur du corps de réponse.
x-ntap-sg-cohérence	<p>Niveau de contrôle de cohérence appliqué au conteneur. Les valeurs suivantes sont prises en charge :</p> <p>Tous : tous les noeuds reçoivent les données immédiatement ou la demande échouera.</p> <p>Forte-global: Garantit la cohérence lecture-après-écriture pour toutes les demandes client sur tous les sites.</p> <p>Site fort : garantit la cohérence de lecture après écriture pour toutes les demandes de clients au sein d'un site.</p> <p>Read-after-New-write: (Par défaut) fournit la cohérence lecture-après-écriture pour les nouveaux objets et éventuellement la cohérence pour les mises à jour d'objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.</p> <p>Disponible : assure la cohérence finale pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.</p>

Exemple de réponse

```

HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
x-ntap-sg-consistency: strong-site

```

REQUÊTE de cohérence du conteneur

La demande DE cohérence PUT dans le conteneur vous permet de spécifier le niveau de cohérence à appliquer aux opérations effectuées dans un conteneur. Par défaut, les nouveaux conteneurs sont créés à l'aide du niveau de cohérence « read-after-New-write ».

Demande

En-tête HTTP de demande	Description
X-Auth-Token	Jeton d'authentification Swift pour le compte à utiliser pour la demande.

En-tête HTTP de demande	Description
x-ntap-sg-cohérence	<p>Niveau de contrôle de cohérence à appliquer aux opérations sur le conteneur. Les valeurs suivantes sont prises en charge :</p> <p>Tous : tous les nœuds reçoivent les données immédiatement ou la demande échouera.</p> <p>Forte-global: Garantit la cohérence lecture-après-écriture pour toutes les demandes client sur tous les sites.</p> <p>Site fort : garantit la cohérence de lecture après écriture pour toutes les demandes de clients au sein d'un site.</p> <p>Read-after-New-write: (Par défaut) fournit la cohérence lecture-après-écriture pour les nouveaux objets et éventuellement la cohérence pour les mises à jour d'objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.</p> <p>Disponible : assure la cohérence finale pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.</p>
Host	Nom d'hôte auquel la demande est dirigée.

Interaction des contrôles de cohérence et des règles ILM pour la protection des données

À la fois de votre choix "[contrôle de la cohérence](#)" De plus, votre règle ILM affecte la façon dont les objets sont protégés. Ces paramètres peuvent interagir.

Par exemple, le contrôle de cohérence utilisé lorsqu'un objet est stocké affecte le placement initial des métadonnées d'objet, tandis que l' "[comportement d'ingestion](#)" Cette case à cocher affecte le placement initial des copies d'objet. Étant donné que StorageGRID nécessite l'accès aux métadonnées d'un objet et à ses données pour répondre aux demandes client, la sélection de niveaux de protection correspondant au niveau de cohérence et au comportement d'ingestion permet d'améliorer la protection des données initiale et de mieux prévoir les réponses du système.

Exemple d'interaction du contrôle de cohérence et de la règle ILM

Supposons que vous disposez d'une grille à deux sites avec la règle ILM suivante et le paramètre de niveau de cohérence suivant :

- **Règle ILM** : créez deux copies d'objet, une sur le site local et une sur un site distant. Le comportement d'entrée strict est sélectionné.
- **Niveau de cohérence**: "Sept-global" (les métadonnées d'objet sont immédiatement distribuées à tous les sites).

Lorsqu'un client stocke un objet dans la grille, StorageGRID effectue à la fois des copies d'objet et distribue les métadonnées aux deux sites avant de rétablir la réussite du client.

L'objet est entièrement protégé contre la perte au moment du message d'ingestion. Par exemple, si le site local est perdu peu de temps après l'ingestion, des copies des données de l'objet et des métadonnées de l'objet existent toujours sur le site distant. L'objet est entièrement récupérable.

Si vous utilisez à la place la même règle ILM et le niveau de cohérence "sept-site", le client peut recevoir un message de réussite après la réPLICATION des données d'objet vers le site distant, mais avant que les métadonnées d'objet ne soient distribuées sur ce site. Dans ce cas, le niveau de protection des métadonnées d'objet ne correspond pas au niveau de protection des données d'objet. Si le site local est perdu peu de temps après l'ingestion, les métadonnées d'objet sont perdues. Impossible de récupérer l'objet.

L'interdépendance entre les niveaux de cohérence et les règles ILM peut être complexe. Contactez NetApp si vous avez besoin d'aide.

Exemple de demande

```
PUT /v1/28544923908243208806/_Swift_container_
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: strong-site
Host: test.com
```

Réponse

En-tête HTTP de réponse	Description
Date	La date et l'heure de la réponse.
Connection	Indique si la connexion au serveur est ouverte ou fermée.
X-Trans-Id	Identifiant de transaction unique pour la demande.
Content-Length	Longueur du corps de réponse.

Exemple de réponse

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
```

Configuration de la sécurité pour l'API REST

Il est recommandé de passer en revue les mesures de sécurité mises en œuvre pour l'API REST et de comprendre comment sécuriser votre système.

Comment StorageGRID assure la sécurité pour l'API REST

Vous devez comprendre comment le système StorageGRID implémente la sécurité, l'authentification et l'autorisation pour l'API REST.

StorageGRID utilise les mesures de sécurité suivantes.

- Les communications client avec le service Load Balancer utilisent HTTPS si HTTPS est configuré pour le noeud final Load Balancer.

Lorsque vous "[configuez un terminal d'équilibrage de charge](#)", HTTP peut être activé en option. Par exemple, vous pouvez utiliser HTTP à des fins de test ou autres que la production.

- Par défaut, StorageGRID utilise HTTPS pour les communications client avec les nœuds de stockage.

En option, "[Activez HTTP pour ces connexions](#)". Par exemple, vous pouvez utiliser HTTP à des fins de test ou autres que la production.

- Les communications entre StorageGRID et le client sont chiffrées à l'aide de TLS.
- Les communications entre le service Load Balancer et les nœuds de stockage dans la grille sont cryptées que le terminal de l'équilibrage de charge soit configuré pour accepter les connexions HTTP ou HTTPS.
- Les clients doivent fournir des en-têtes d'authentification HTTP à StorageGRID pour effectuer des opérations d'API REST.

Certificats de sécurité et applications client

Les clients peuvent se connecter au service Load Balancer sur les nœuds de passerelle ou les nœuds d'administration, directement aux nœuds de stockage.

Dans tous les cas, les applications client peuvent établir des connexions TLS à l'aide d'un certificat de serveur personnalisé chargé par l'administrateur de la grille ou d'un certificat généré par le système StorageGRID :

- Lorsque les applications client se connectent au service Load Balancer, elles le font à l'aide du certificat configuré pour le noeud final de l'équilibrage de charge spécifique utilisé pour établir la connexion. Chaque noeud final possède son propre certificat, qui est soit un certificat de serveur personnalisé chargé par l'administrateur de la grille, soit un certificat que l'administrateur de la grille a généré dans StorageGRID lors de la configuration du noeud final.
- Lorsque les applications client se connectent directement à un nœud de stockage, elles utilisent les certificats de serveur générés par le système qui ont été générés pour les nœuds de stockage lors de l'installation du système StorageGRID (qui sont signés par l'autorité de certification du système), ou un seul certificat de serveur personnalisé fourni pour la grille par un administrateur de grille.

Les clients doivent être configurés pour approuver l'autorité de certification qui a signé le certificat qu'ils utilisent pour établir des connexions TLS.

Voir "[configuration des terminaux d'équilibrage de charge](#)" et "[ajout d'un seul certificat de serveur personnalisé](#)" Pour les connexions TLS directement aux nœuds de stockage.

Récapitulatif

Le tableau suivant montre comment les problèmes de sécurité sont implémentés dans les API REST S3 et Swift :

Problème de sécurité	Implémentation pour l'API REST
Sécurité de la connexion	TLS
Authentification du serveur	Certificat de serveur X.509 signé par l'autorité de certification du système ou certificat de serveur personnalisé fourni par l'administrateur
Authentification client	<ul style="list-style-type: none"> S3 : compte S3 (ID de clé d'accès et clé d'accès secrète) SWIFT : compte Swift (nom d'utilisateur et mot de passe)
Autorisation du client	<ul style="list-style-type: none"> S3 : propriété des compartiments et toutes les règles de contrôle d'accès applicables SWIFT : accès aux rôles d'administrateur

Algorithmes de hachage et de cryptage pris en charge pour les bibliothèques TLS

Le système StorageGRID prend en charge un ensemble limité de suites de chiffrement que les applications clientes peuvent utiliser lors de l'établissement d'une session TLS (transport Layer Security). Pour configurer les chiffrements, accédez à **CONFIGURATION > sécurité > Paramètres de sécurité** et sélectionnez **règles TLS et SSH**.

Versions supportées de TLS

StorageGRID supporte TLS 1.2 et TLS 1.3.



SSLv3 et TLS 1.1 (ou versions antérieures) ne sont plus pris en charge.

Informations associées

["Configurez les comptes et les connexions des locataires"](#)

Surveiller et auditer les opérations

Vous pouvez surveiller les charges de travail et l'efficacité des opérations client en visualisant les tendances de transaction pour l'ensemble du grid ou pour des nœuds spécifiques. Vous pouvez utiliser des messages d'audit pour surveiller les opérations et les transactions des clients.

Contrôler les taux d'entrée et de récupération des objets

Vous pouvez surveiller les taux d'entrée et de récupération des objets, ainsi que les mesures relatives au nombre d'objets, aux requêtes et à la vérification. Vous pouvez afficher le nombre de tentatives de lecture, d'écriture et de modification d'objets du système StorageGRID ayant échoué et réussies par les applications client.

Étapes

1. Connectez-vous au Grid Manager à l'aide d'un "[navigateur web pris en charge](#)".

2. Sur le tableau de bord, sélectionnez **Performance > S3 Operations** ou **Performance > Swift Operations**.

Cette section récapitule le nombre d'opérations client effectuées par votre système StorageGRID. La moyenne des débits de protocole est calculée au cours des deux dernières minutes.

3. Sélectionnez **NOEUDS**.

4. Dans la page d'accueil noeuds (niveau de déploiement), cliquez sur l'onglet **Load Balancer**.

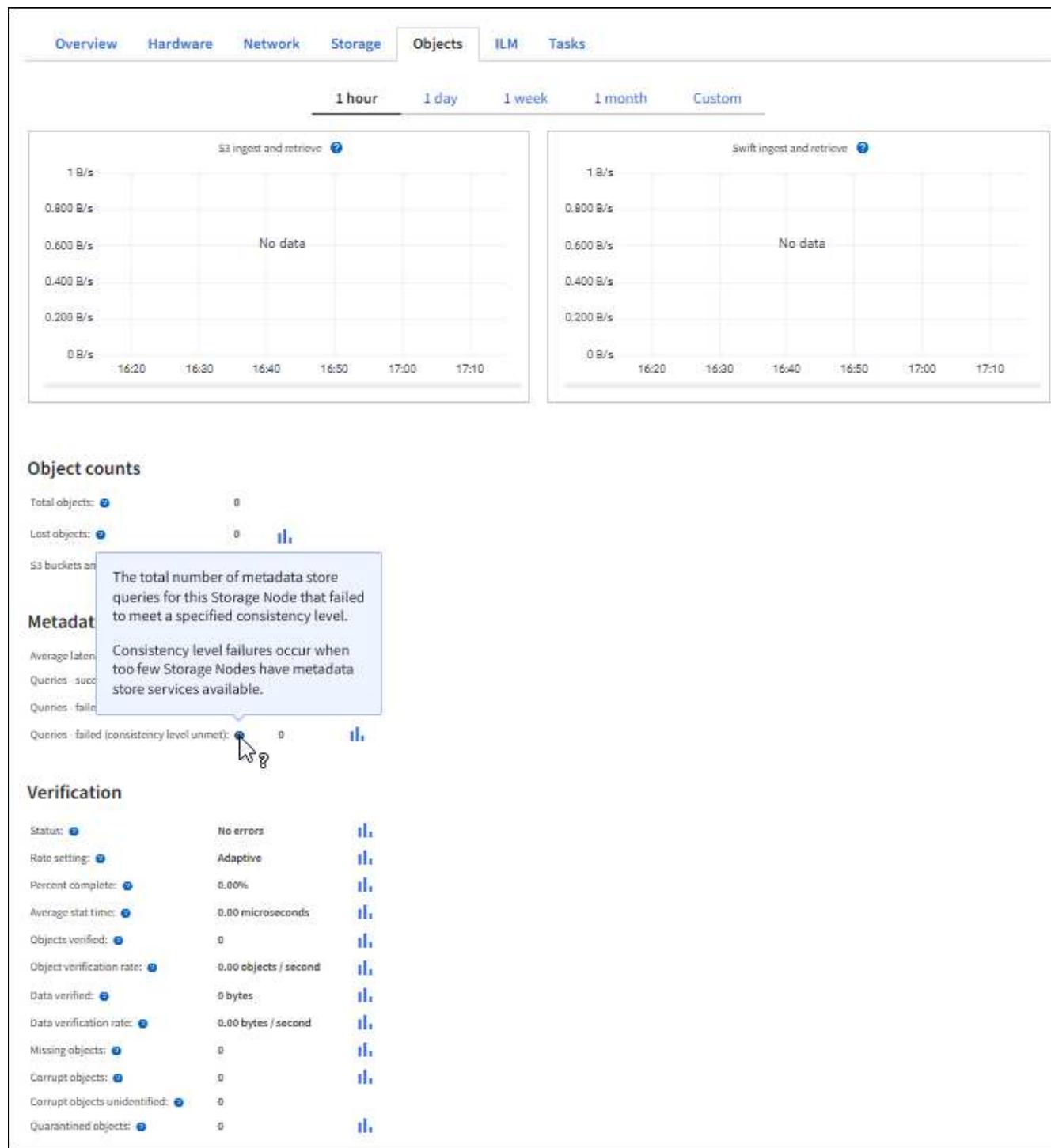
Les graphiques présentent les tendances de tout le trafic client dirigé vers les terminaux d'équilibrage de charge dans la grille. Vous pouvez sélectionner un intervalle de temps en heures, jours, semaines, mois ou années, vous pouvez également appliquer un intervalle personnalisé.

5. Dans la page d'accueil noeuds (niveau de déploiement), cliquez sur l'onglet **objets**.

Le graphique montre les taux d'entrée et de récupération de l'intégralité de votre système StorageGRID en octets par seconde et en octets totaux. Vous pouvez sélectionner un intervalle de temps en heures, jours, semaines, mois ou années, vous pouvez également appliquer un intervalle personnalisé.

6. Pour afficher les informations relatives à un noeud de stockage particulier, sélectionnez-le dans la liste de gauche, puis cliquez sur l'onglet **objets**.

Le tableau affiche les taux d'entrée et de récupération de l'objet pour ce nœud de stockage. L'onglet inclut également des mesures pour le nombre d'objets, les requêtes et la vérification. Vous pouvez cliquer sur les étiquettes pour afficher les définitions de ces mesures.



7. Si vous voulez encore plus de détails :

- Sélectionnez **SUPPORT > Outils > topologie de grille**.
- Sélectionnez **site > Présentation > main**.

La section opérations d'API affiche un récapitulatif des informations sur l'ensemble de la grille.

- Sélectionnez **Storage Node > LDR > *client application* > Présentation > main**

La section opérations affiche un récapitulatif des informations sur le nœud de stockage sélectionné.

Examiner les journaux d'audit

Les messages d'audit sont générés par les services StorageGRID et stockés dans des fichiers journaux texte. Des messages d'audit spécifiques aux API dans les journaux d'audit fournissent des données stratégiques de sécurité, d'exploitation et de surveillance des performances qui vous aideront à évaluer l'état de votre système.

Avant de commencer

- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir le `Passwords.txt` fichier.
- Vous devez connaître l'adresse IP d'un nœud d'administration.

Description de la tâche

Le "[fichier journal d'audit actif](#)" est nommé `audit.log`, Et il est stocké sur des nœuds d'administration.

Une fois par jour, le fichier `audit.log` actif est enregistré et un nouveau fichier `audit.log` est lancé. Le nom du fichier enregistré indique quand il a été enregistré, au format `yyyy-mm-dd.txt`.

Après un jour, le fichier enregistré est compressé et renommé, au format `yyyy-mm-dd.txt.gz`, qui conserve la date originale.

Cet exemple montre le fichier `audit.log` actif, le fichier de la veille (`2018-04-15.txt`) et le fichier compressé de la veille (`2018-04-14.txt.gz`).

```
audit.log  
2018-04-15.txt  
2018-04-14.txt.gz
```

Étapes

1. Connectez-vous à un nœud d'administration :
 - a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour passer à la racine : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
2. Accédez au répertoire contenant les fichiers journaux d'audit :`cd /var/local/audit/export`
3. Afficher le fichier journal d'audit actuel ou enregistré, selon les besoins.

Les opérations Swift sont suivies dans les journaux d'audit

Toutes les opérations de SUPPRESSION de stockage, D'OBTENTION, DE TÊTE, DE POST et DE PUT réussies sont suivies dans le "[Journal d'audit StorageGRID](#)". Les échecs ne sont pas consignés, ni les demandes d'informations, d'authentification ou D'OPTIONS.

Les informations sont suivies pour les opérations Swift suivantes.

Opérations sur le compte

- "OBTENIR un compte"
- "Compte PRINCIPAL"

Opérations sur les conteneurs

- "SUPPRIMER le conteneur"
- "CONTENEUR"
- "Conteneur DE TÊTE"
- "PLACER le conteneur"

Opérations sur l'objet

- "SUPPRIMER l'objet"
- "OBJET GET"
- "Objet TÊTE"
- "PLACER l'objet"

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 JOUSSANCE, 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 DÉLICTUELLE (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.