# Utilisez un compte locataire

StorageGRID software

NetApp
July 23, 2026

# Sommaire

# Utilisez un compte locataire

## Utilisez un compte locataire StorageGRID

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

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

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

Les comptes locataires permettent de segmenter les objets stockés par différentes entités. Par exemple, plusieurs comptes locataires peuvent être utilisés dans les deux cas suivants :

- **Cas d'utilisation en entreprise :** si le système StorageGRID est utilisé au sein d'une entreprise, le stockage d'objets de la grille peut être cloisonné par les différents départements de l'organisation. Par exemple, il peut y avoir des comptes locataires pour le département Marketing, le département Support client, le département Ressources humaines, etc.

> Si vous utilisez le protocole client S3, vous pouvez également utiliser les compartiments S3 et les stratégies de compartiment pour segmenter les objets entre les services d'une entreprise. Vous n'avez pas besoin de créer des comptes locataires distincts. Consultez les instructions de mise en œuvre "Compartiments S3 et politiques de compartiment" pour plus d'informations.

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

### ${post_edited_translations.segment}

Les comptes locataires sont créés par un "${post_edited_translations.segment}". Lors de la création d'un compte locataire, l'administrateur du grid spécifie les éléments suivants :

- Informations de base, notamment le nom du locataire, le type de client (S3) et le quota de stockage facultatif.
- Les autorisations du compte locataire, telles que la possibilité pour ce dernier d'utiliser les services de la plateforme S3, de configurer sa propre source d'identité, d'utiliser S3 Select ou d'utiliser une connexion de fédération de grille.
- L'accès racine initial du locataire, en fonction de la manière dont le système StorageGRID utilise les groupes et utilisateurs locaux, la fédération d'identités ou l'authentification unique (SSO).

De plus, les administrateurs de la grille peuvent activer le paramètre S3 Object Lock pour le système StorageGRID si les comptes locataires S3 doivent se conformer aux exigences réglementaires. Lorsque S3 Object Lock est activé, tous les comptes locataires S3 peuvent créer et gérer des compartiments conformes.

### Configurer les locataires S3

Après un "${post_edited_translations.segment}", vous pouvez accéder au Gestionnaire de locataires pour effectuer des tâches telles que les suivantes :

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

Bien que vous puissiez créer et gérer des compartiments S3 avec le Tenant Manager, vous devez utiliser un "Client S3" ou "Console S3" pour ingérer et gérer des objets.

# Comment se connecter et se déconnecter

## Se connecter à StorageGRID Tenant Manager

Vous accédez au gestionnaire de locataires en saisissant 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 d'accès au Tenant Manager, fournie par votre administrateur de grid. L'URL ressemblera à l'un des exemples suivants :

  ```
  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 comprend toujours un nom de domaine complet (FQDN), l'adresse IP d'un Admin Node ou l'adresse IP virtuelle d'un groupe HA d'Admin Nodes. Elle peut également inclure un numéro de port, l'ID de compte locataire à 20 chiffres, ou les deux.

- Si l'URL n'inclut pas l'identifiant de compte à 20 chiffres du locataire, vous disposez de cet identifiant 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, saisissez l'URL pour accéder à Tenant Manager.
3. ${post_edited_translations.segment}
4. Connectez-vous au Tenant Manager.

   ${post_edited_translations.segment}

   **Ne pas utiliser l'authentification unique (SSO)**

   ${post_edited_translations.segment}

   - Page de connexion de Grid Manager. Sélectionnez le lien **Tenant sign-in**.
   - La page de connexion du Gestionnaire de locataires. Le champ **Compte** est peut-être déjà renseigné.
     i. Si l'identifiant de compte à 20 chiffres du locataire n'est pas affiché, sélectionnez le nom du compte du locataire s'il apparaît dans la liste des comptes récents ou saisissez l'identifiant du compte.
     ii. Saisissez votre nom d'utilisateur et votre mot de passe.
     iii. Sélectionnez **Se connecter**.

     Le tableau de bord du Tenant Manager s'affiche.

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

   **Utilisation de l'authentification unique (SSO)**

   Si StorageGRID utilise l'authentification unique (SSO), l'un des écrans suivants apparaît :

   - La page SSO de votre organisation.

     Saisissez vos identifiants SSO standard et sélectionnez **Se connecter**.

   - ${post_edited_translations.segment}
     i. Si l'identifiant de compte à 20 chiffres du locataire n'est pas affiché, sélectionnez le nom du compte du locataire s'il apparaît dans la liste des comptes récents ou saisissez l'identifiant du compte.
     ii. Sélectionnez **Se connecter**.
     iii. Connectez-vous avec vos identifiants SSO habituels sur la page de connexion SSO de votre organisation.

     Le tableau de bord du Tenant Manager s'affiche.

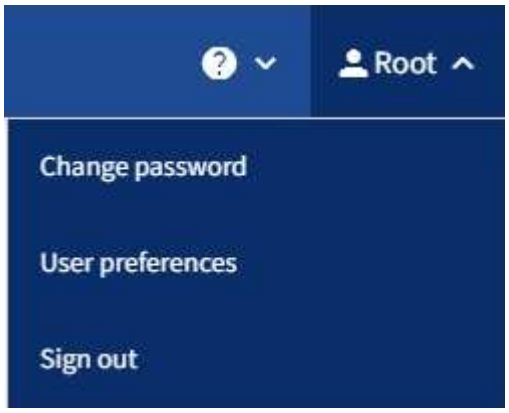
## Déconnexion de StorageGRID Tenant Manager

Lorsque vous avez fini d'utiliser le Tenant Manager, vous devez vous déconnecter pour garantir que des utilisateurs non autorisés ne puissent pas accéder au système

StorageGRID. La fermeture de votre navigateur peut ne pas vous déconnecter du système, selon les paramètres de cookies du navigateur.

**Étapes**

1. ${post_edited_translations.segment}




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

   - ${post_edited_translations.segment}

     Vous êtes déconnecté du nœud d'administration. La page de connexion du Tenant Manager s'affiche.

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

   - Si l'authentification unique (SSO) est activée :

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

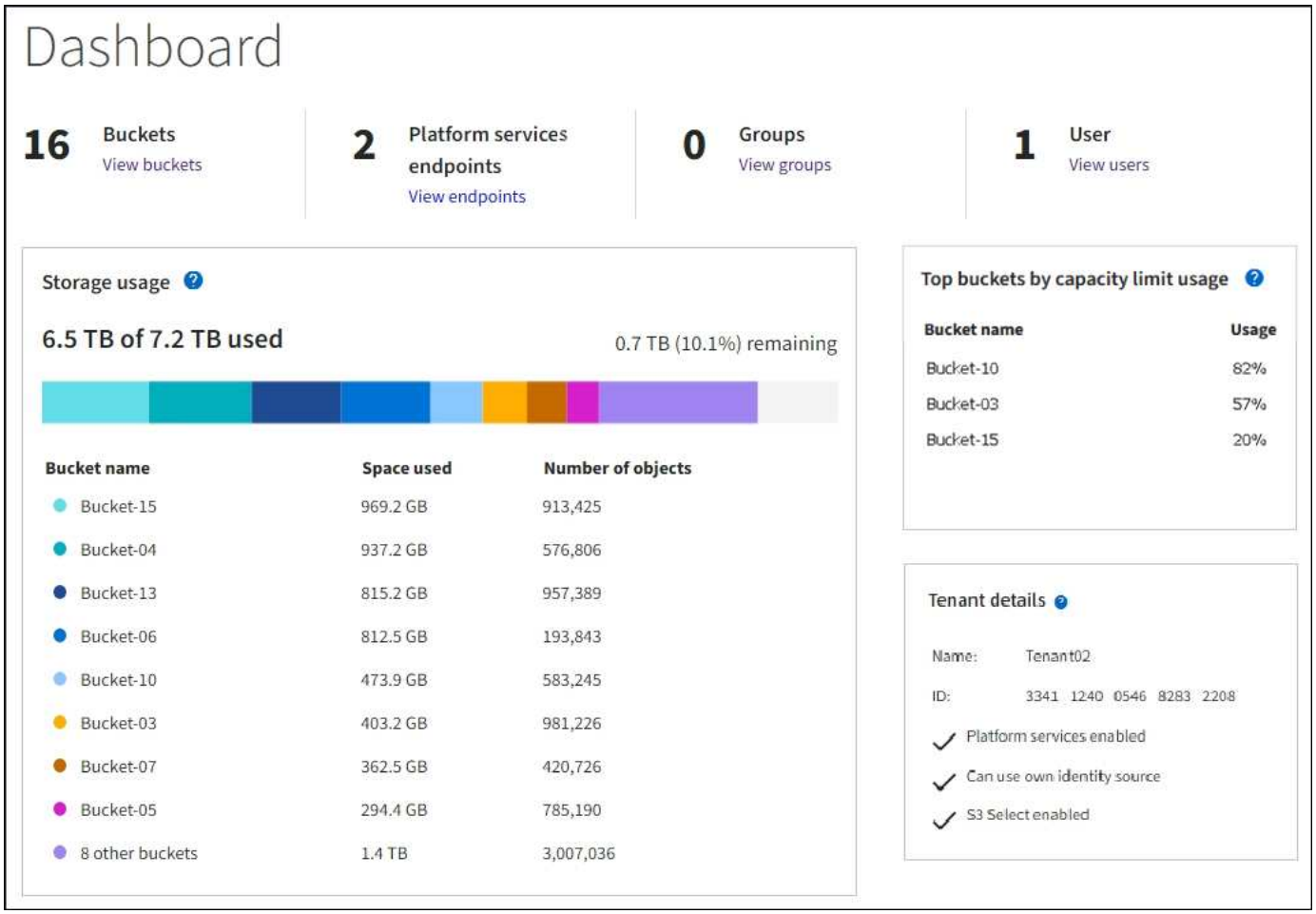
     ${post_edited_translations.segment}

# Tableau de bord Tenant Manager dans StorageGRID

Le tableau de bord du Tenant Manager fournit un aperçu de la configuration d'un compte de locataire et de l'espace utilisé par les objets dans les compartiments S3 du locataire. Si le locataire dispose d'un quota, le tableau de bord affiche la part du quota utilisée et la part restante. Si des erreurs sont liées au compte de locataire, elles s'affichent sur le tableau de bord.

La taille logique de tous les objets appartenant à ce locataire inclut les chargements multiparties incomplets et en cours. La taille n'inclut pas l'espace physique supplémentaire utilisé pour les politiques ILM. Les valeurs d'espace utilisé sont des estimations. Ces estimations sont influencées par le moment des ingestions, la connectivité réseau et l'état des nœuds.

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




## Informations sur le compte du locataire

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

Selon le "autorisations de gestion des locataires" dont vous disposez et les options que vous avez configurées, le reste du tableau de bord affiche différentes combinaisons de recommandations, d'utilisation du stockage, d'informations sur les objets et de détails sur les locataires.

## ${post_edited_translations.segment}

Le panneau d'utilisation du stockage contient les informations suivantes :

- ${post_edited_translations.segment}

  ${post_edited_translations.segment}

- Si un quota est défini, il indique 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 du quota est basée sur des estimations internes et peut être dépassée dans certains cas. Par exemple, StorageGRID vérifie le quota lorsqu'un client commence à charger des objets et refuse les nouvelles ingestions si le client a dépassé le quota. Cependant, StorageGRID ne prend pas en compte la taille du chargement en cours pour déterminer si le quota a été dépassé. Si des objets sont supprimés, un client peut être temporairement empêché de charger de nouveaux objets jusqu'à ce que l'utilisation du quota soit recalculée. Le calcul de l'utilisation du quota peut prendre 10 minutes ou plus.

- ${post_edited_translations.segment}

  Vous pouvez placer votre curseur sur n'importe quel segment du graphique pour afficher l'espace total consommé par ce compartiment ou conteneur.


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

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

  ${post_edited_translations.segment}

${post_edited_translations.segment}

## ${post_edited_translations.segment}

${post_edited_translations.segment}

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

${post_edited_translations.segment}

- ${post_edited_translations.segment}

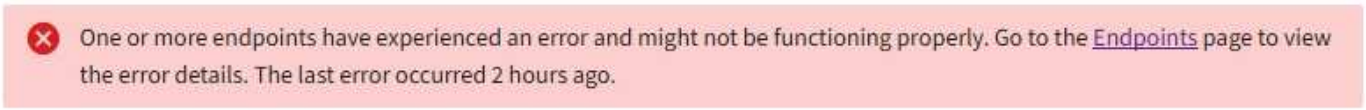
### ${post_edited_translations.segment}

${post_edited_translations.segment}

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

### ${post_edited_translations.segment}

${post_edited_translations.segment}




Pour afficher les détails concernant "${post_edited_translations.segment}", sélectionnez **Endpoints** pour afficher la page Endpoints.

# API de gestion des locataires

## Découvrez l’API de gestion des locataires StorageGRID

Vous pouvez effectuer des tâches de gestion système à l’aide de l’API REST Tenant Management plutôt qu’en utilisant l’interface utilisateur du Tenant Manager. Par exemple, vous pourriez vouloir utiliser l’API pour automatiser des opérations ou pour créer plusieurs entités, telles que des utilisateurs, plus rapidement.

${post_edited_translations.segment}

- Utilise la plateforme d’API open source Swagger. Swagger fournit une interface utilisateur intuitive qui permet aux développeurs et aux non-développeurs d’interagir avec l’API. L’interface utilisateur de Swagger fournit des détails complets et de la documentation pour chaque opération d’API.
- Utilise "${post_edited_translations.segment}".

${post_edited_translations.segment}

1. Connectez-vous au Tenant Manager.
2. En haut du Tenant Manager, sélectionnez l’icône d’aide et sélectionnez **API documentation**.

#### ${post_edited_translations.segment}

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- **auth** : Opérations permettant d’authentifier la session utilisateur.

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

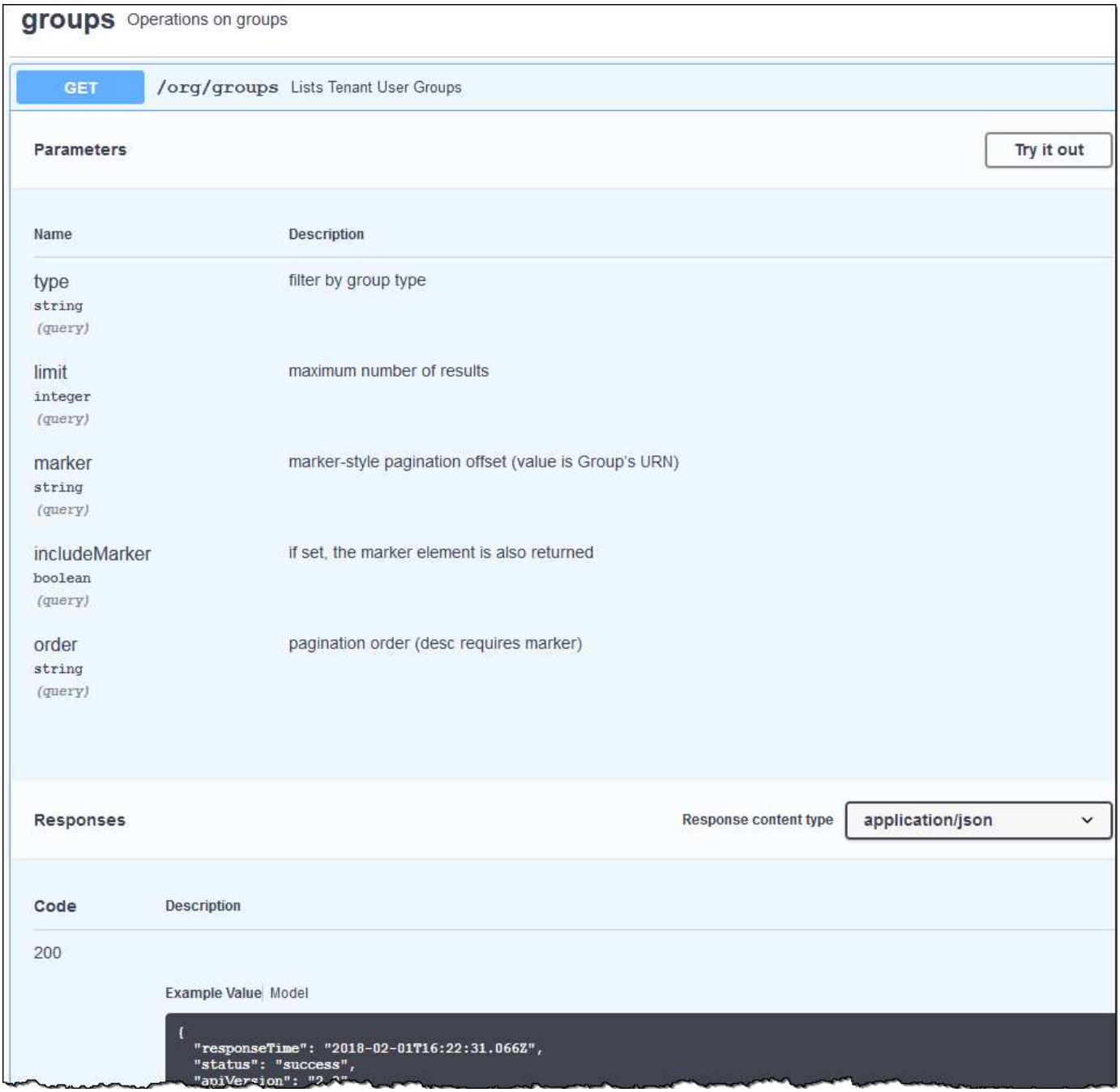
Pour obtenir des informations sur l'amélioration de la sécurité de l'authentification, consultez "Protégez-vous contre la falsification de requêtes intersites".

> Si l'authentification unique (SSO) est activée pour le système StorageGRID, vous devez effectuer des étapes différentes pour vous authentifier. Voir le "${post_edited_translations.segment}".

- **config** : opérations relatives à la version du produit et aux versions de l'API de gestion des locataires. Vous pouvez lister la version du produit et les versions majeures de l'API prises en charge par cette version.
- ${post_edited_translations.segment}
- **Fonctionnalités désactivées** : Opérations permettant d'afficher les fonctionnalités qui pourraient avoir été désactivées.
- **endpoints** : opérations de gestion d'un point de terminaison. Les points de terminaison permettent à un compartiment S3 d'utiliser un service externe pour la réplication CloudMirror de StorageGRID, les notifications ou l'intégration de la recherche.
- ${post_edited_translations.segment}
- **Groupes** : Opérations permettant de gérer les groupes de locataires locaux et de récupérer les groupes de locataires fédérés à partir d'une source d'identité externe.
- **identity-source** : Opérations permettant de configurer une source d'identité externe et de synchroniser manuellement les informations de groupe et d'utilisateur fédérés.
- **ilm** : Opérations sur les paramètres de gestion du cycle de vie de l'information (ILM).
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- **utilisateurs** : Opérations permettant de consulter et de gérer les utilisateurs locataires.

**${post_edited_translations.segment}**

${post_edited_translations.segment}




## Émettre des requêtes API

Toute opération API effectuée via la page de documentation API est une opération en direct. Veillez à ne pas créer, modifier ou supprimer par erreur des données de configuration ou autres.

### Étapes

1. Sélectionnez l'action HTTP pour afficher les détails de la requête.
2. Déterminez si la requête nécessite des paramètres supplémentaires, tels qu'un identifiant de groupe ou d'utilisateur. Ensuite, obtenez ces valeurs. Vous devrez peut-être d'abord effectuer une autre requête API pour obtenir les informations dont vous avez besoin.
3. Déterminez si vous devez modifier le corps de la requête d'exemple. Le cas échéant, vous pouvez sélectionner **Modèle** pour connaître les exigences relatives à chaque champ.

4. Sélectionnez **Try it out**.
5. Fournissez les paramètres requis ou modifiez le corps de la requête selon les besoins.
6. Sélectionnez **Exécuter**.
7. Examinez le code de réponse pour déterminer si la requête a réussi.

## Versionnage de l'API de gestion des locataires StorageGRID

L'API de gestion des locataires utilise le versionnage pour permettre des mises à niveau sans interruption de service.

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

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

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

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

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

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

> Vous pouvez configurer les versions prises en charge. Consultez la section **config** de la documentation de l'API Swagger pour "API de gestion de grille" plus d'informations. Vous devez désactiver la prise en charge de l'ancienne version après avoir mis à jour tous les clients API vers la nouvelle version.

Les requêtes obsolètes sont marquées comme dépréciées de la manière suivante :

- L'en-tête de réponse est « Deprecated: true »
- Le corps de la réponse JSON inclut "deprecated": true
- Un avertissement de dépréciation est ajouté au fichier nms.log. Par exemple :

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

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

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

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

#### Spécifiez une version d'API pour une requête

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

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

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

## Protégez-vous contre la falsification de requêtes intersites (CSRF) dans StorageGRID

Vous pouvez contribuer à protéger StorageGRID contre les attaques de type Cross-Site Request Forgery (CSRF) en utilisant des jetons CSRF pour renforcer l'authentification qui utilise des cookies. Le Grid Manager et le Tenant Manager activent automatiquement cette fonctionnalité de sécurité ; les autres clients API peuvent choisir de l'activer ou non lors de leur connexion.

Un attaquant capable de déclencher une requête vers un autre site (par exemple avec un formulaire HTTP POST) peut faire en sorte que certaines requêtes soient effectuées en utilisant les cookies de l'utilisateur connecté.

StorageGRID contribue à la protection contre les attaques CSRF grâce à l'utilisation de jetons CSRF. Lorsqu'elle est activée, le contenu d'un cookie spécifique doit correspondre à celui d'un en-tête spécifique ou d'un paramètre spécifique du corps de la requête POST.

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

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

Lorsque cette option est activée, un `GridCsrfToken` cookie est défini avec une valeur aléatoire pour les connexions au Grid Manager, et le `AccountCsrfToken` cookie est défini avec une valeur aléatoire pour les connexions au Tenant Manager.

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

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

Pour configurer la protection CSRF, utilisez le "API de gestion de grille" ou le "API de gestion des locataires".

> ⓘ Les requêtes comportant un cookie de jeton CSRF défini appliqueront également l'en-tête "Content-Type: application/json" à toute requête attendant un corps de requête JSON, comme protection supplémentaire contre les attaques CSRF.

# Utilisez les connexions de fédération de grille

## Cloner les groupes de locataires et les utilisateurs dans StorageGRID

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

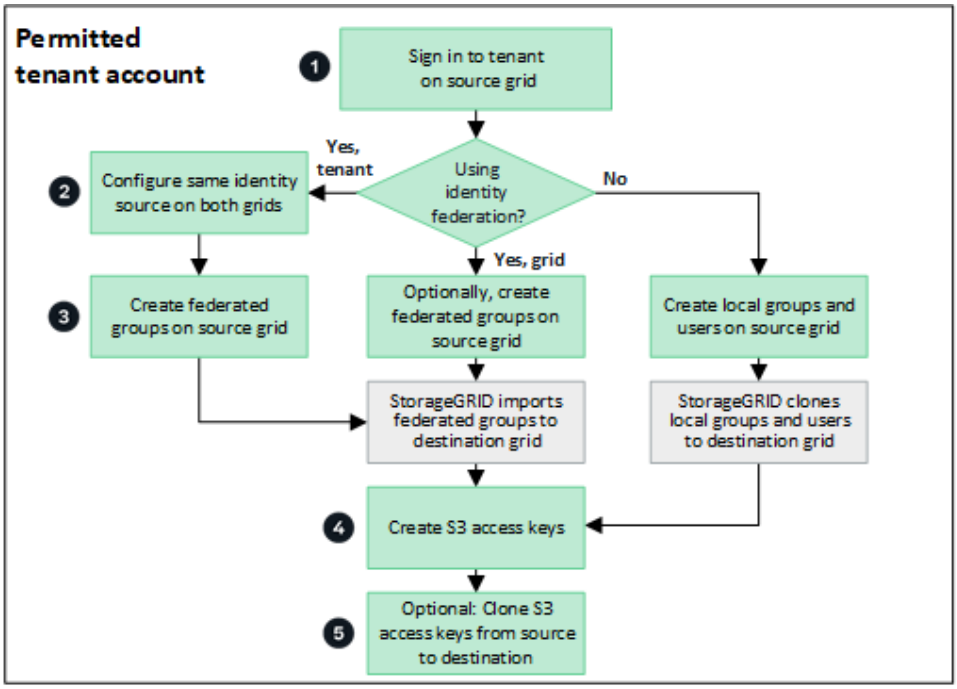
Le système StorageGRID dans lequel le locataire est initialement créé est la *grille source* du locataire. Le système StorageGRID dans lequel le locataire est répliqué est la *grille de destination* du locataire. Les deux comptes de locataire possèdent les mêmes ID de compte, nom, description, quota de stockage et autorisations attribuées, mais le locataire de destination ne dispose pas initialement d'un mot de passe d'utilisateur root. Pour plus de détails, consultez "Qu'est-ce qu'un clone de compte" et "Gérer les locataires autorisés".

Le clonage des informations de compte locataire est nécessaire pour "réplication inter-grilles" des objets de compartiment. Avoir les mêmes groupes de locataires et utilisateurs sur les deux grilles garantit que vous pouvez accéder aux compartiments et objets correspondants sur l'une ou l'autre grille.

**${post_edited_translations.segment}**

Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grille**, consultez le diagramme de flux de travail pour voir les étapes que vous effectuerez pour cloner les groupes, les utilisateurs

et les clés d'accès S3.




${post_edited_translations.segment}

### 1 Se connecter au locataire

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

### 2 Configurez éventuellement la fédération d'identité

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

### 3 Créer des groupes et des utilisateurs

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

- Si la fédération d'identité est configurée pour l'ensemble du système StorageGRID ou pour votre compte locataire, "créer de nouveaux groupes de locataires" en important des groupes fédérés depuis la source d'identité.
- Si vous n'utilisez pas la fédération d'identités, "${post_edited_translations.segment}" puis "${post_edited_translations.segment}".

### 4 Créer des clés d'accès S3

Vous pouvez "Créez vos propres clés d'accès" ou "créer les clés d'accès d'un autre utilisateur" sur la grille source ou la grille de destination pour accéder aux compartiments de cette grille.

### 5 En option, clonez les clés d'accès S3

Si vous devez 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 Tenant Manager pour les cloner manuellement sur la grille de destination. Pour obtenir des instructions, consultez "Cloner les clés d'accès S3 à l'aide de l'API".

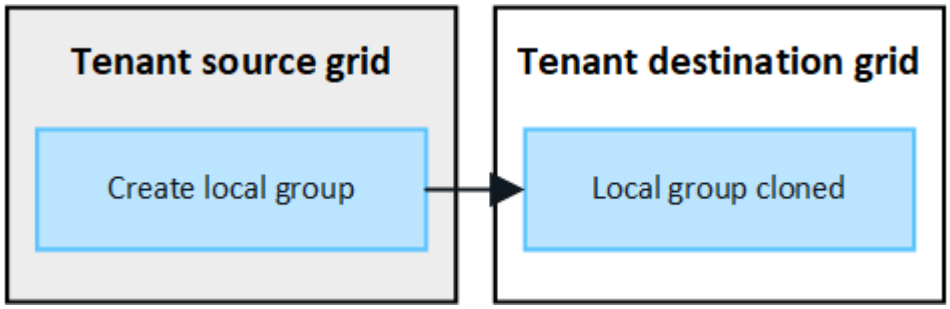
**${post_edited_translations.segment}**

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

#### Les groupes locaux créés sur la grille source sont clonés

${post_edited_translations.segment}

Le groupe d'origine et son clone possèdent le même mode d'accès, les mêmes autorisations de groupe et la même stratégie de groupe S3. Pour obtenir des instructions, consultez "Créer des groupes pour le locataire S3".

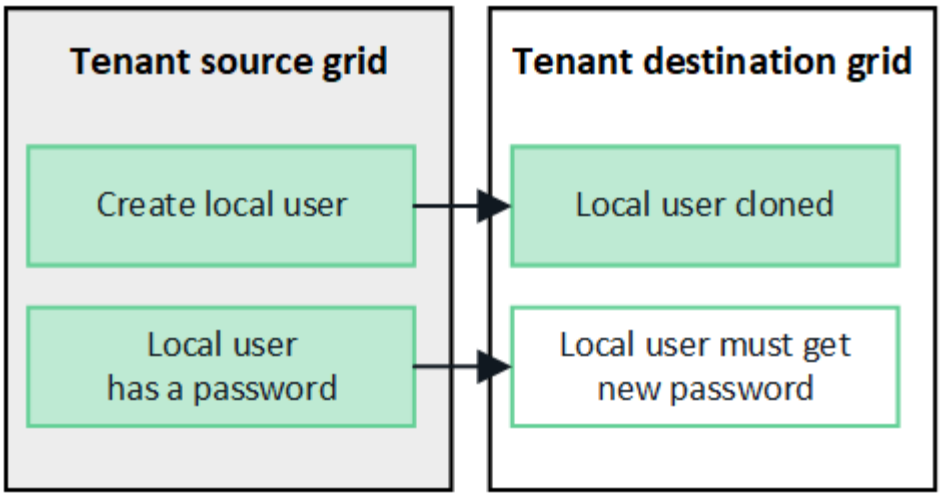



> Tous les utilisateurs que vous sélectionnez lorsque vous créez un groupe local sur la grille source ne sont pas inclus lorsque le groupe est cloné sur la grille de destination. Pour cette raison, ne sélectionnez pas d'utilisateurs lorsque vous créez le groupe. Sélectionnez plutôt le groupe lorsque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

#### ${post_edited_translations.segment}

Lorsque vous créez un nouvel utilisateur local sur la grille source, StorageGRID clone automatiquement cet utilisateur sur la grille de destination. L'utilisateur d'origine et son clone possèdent 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, consultez "Gérer les utilisateurs".

Pour des raisons de sécurité, les mots de passe des utilisateurs locaux ne sont pas dupliqués sur la grille de destination. Si un utilisateur local doit accéder à Tenant Manager sur la grille de destination, l'utilisateur root du compte locataire doit ajouter un mot de passe pour cet utilisateur sur la grille de destination. Pour obtenir des instructions, consultez "Gérer les utilisateurs".

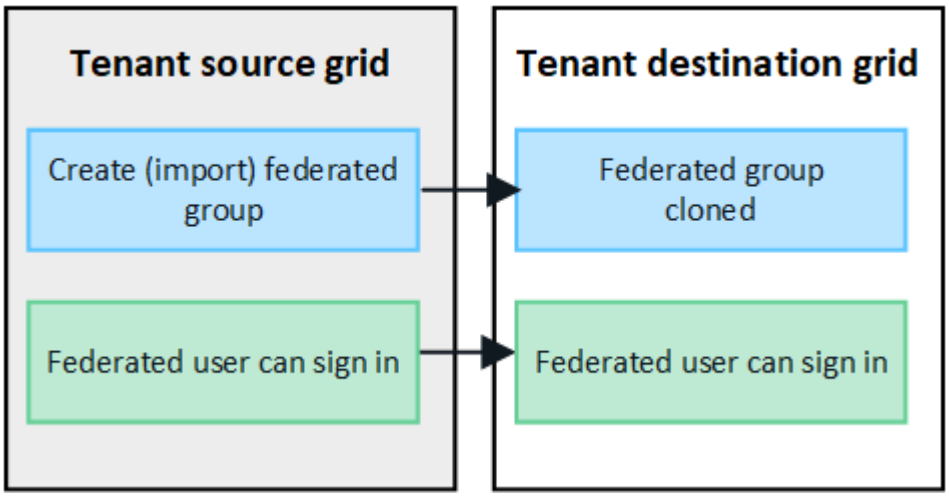



**${post_edited_translations.segment}**

Si les conditions requises pour utiliser le clonage de compte avec "authentification unique" et "fédération d'identité" sont remplies, les groupes fédérés que vous créez (importez) pour le locataire sur la grille source sont automatiquement clonés vers le locataire sur la grille de destination.

${post_edited_translations.segment}

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 sur l'une ou l'autre grille.

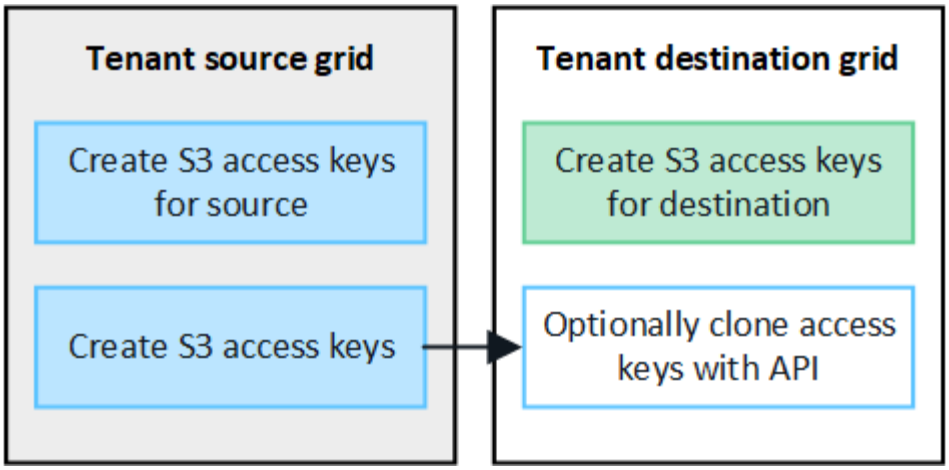



**Les clés d'accès S3 peuvent être clonées manuellement**

${post_edited_translations.segment}

${post_edited_translations.segment}

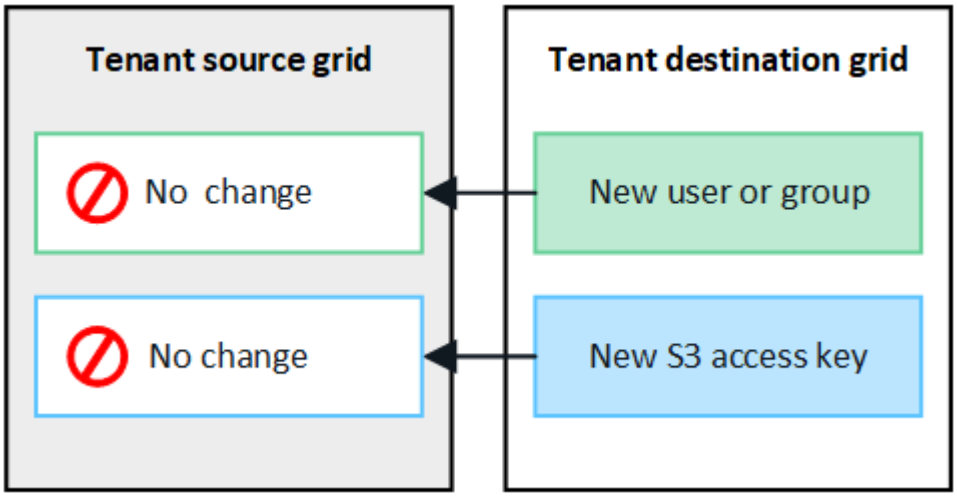
- Si vous n'avez pas besoin d'utiliser les mêmes clés pour chaque grille, vous pouvez "Créez vos propres clés d'accès" ou "créer les clés d'accès d'un autre utilisateur" sur chaque grille.
- Si vous devez utiliser les mêmes clés sur les deux grilles, vous pouvez créer des clés sur la grille source, puis utiliser l'API du Gestionnaire de locataires pour les "${post_edited_translations.segment}" manuellement vers la grille de destination.




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

**${post_edited_translations.segment}**

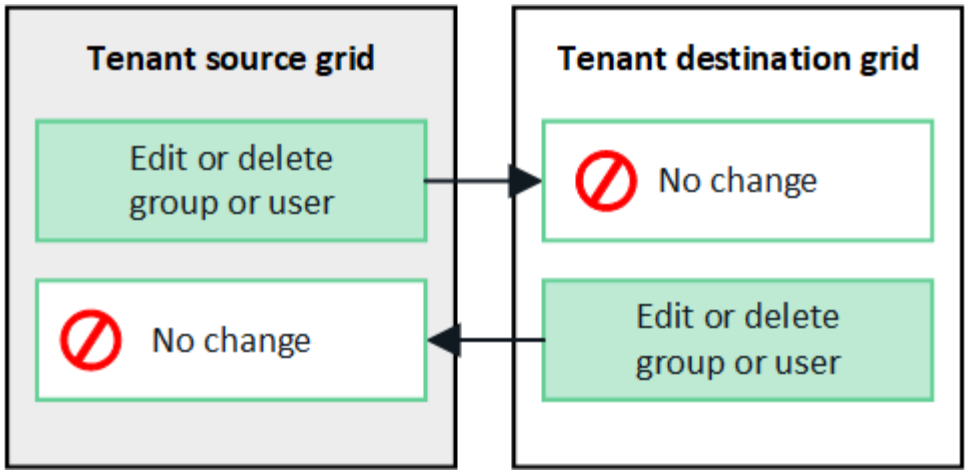
Le clonage s'effectue uniquement de la grille source du locataire vers la grille de destination du locataire. Si vous créez ou importez des groupes et des utilisateurs sur la grille de destination du locataire, StorageGRID ne clonera pas ces éléments en retour vers la grille source du locataire.




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

Le clonage n'a lieu que 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 entre les grilles StorageGRID à l'aide de l'API de gestion des locataires

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

**Avant de commencer**

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- Vous êtes connecté au Tenant Manager sur la grille source du locataire à l'aide d'un "navigateur Web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "${post_edited_translations.segment}".
- ${post_edited_translations.segment}

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

**${post_edited_translations.segment}**

${post_edited_translations.segment}

**Étapes**

1. Utilisez le Tenant Manager sur la grille source, "Créez vos propres clés d'accès" et téléchargez le `.csv` fichier.
2. En haut du Tenant Manager, sélectionnez l'icône d'aide et sélectionnez **API documentation**.
3. Dans la section **s3**, sélectionnez le point de terminaison suivant :

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

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

   Veillez à conserver les guillemets doubles autour de chaque chaîne de caractères.


6. Si la clé doit expirer, remplacez l'entrée d'exemple pour **expires** par la date et l'heure d'expiration sous la forme d'une chaîne au format de date et d'heure ISO 8601 (par exemple, `2024-02-28T22:46:33-08:00`). Si la clé ne doit pas expirer, saisissez **null** comme valeur pour l'entrée **expires** (ou supprimez la ligne **Expires** et la virgule qui la précède).
7. Sélectionnez **Exécuter**.
8. ${post_edited_translations.segment}

### Cloner les clés d'accès d'un autre utilisateur

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

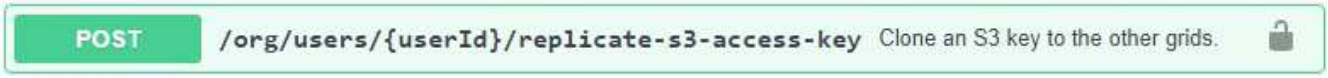
#### Étapes

1. À l'aide du Tenant Manager sur la grille source, "${post_edited_translations.segment}" et téléchargez le fichier `.csv`.
2. En haut du Tenant Manager, sélectionnez l'icône d'aide et sélectionnez **API documentation**.
3. Récupérez l'identifiant de l'utilisateur. Vous aurez besoin de cette valeur pour cloner les clés d'accès de l'autre utilisateur.
   a. ${post_edited_translations.segment}

      ```
      GET /org/users
      ```

   b. Sélectionnez **Try it out**.
   c. ${post_edited_translations.segment}
   d. Sélectionnez **Exécuter**.
   e. ${post_edited_translations.segment}
4. Dans la section **s3**, sélectionnez le point de terminaison suivant :

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



5. Sélectionnez **Try it out**.
6. Dans la zone de texte **userId**, collez l'identifiant utilisateur que vous avez copié.
7. Dans la zone de texte **corps**, remplacez les exemples d'entrées 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 de caractères.

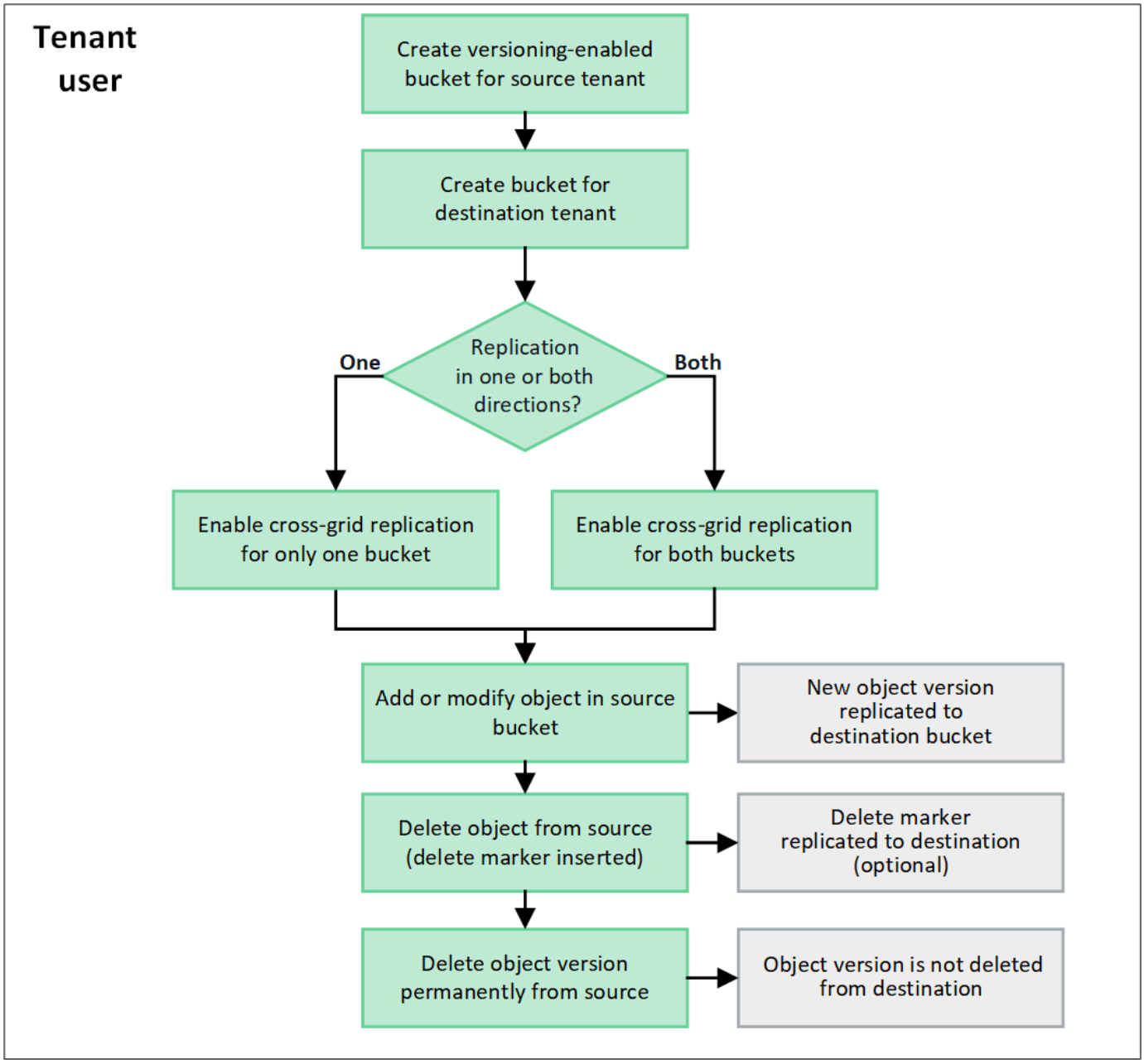
8. Si la clé doit expirer, remplacez l'exemple d'entrée pour **expires** par la date et l'heure d'expiration sous forme de chaîne au format date-heure ISO 8601 (par exemple, `2023-02-28T22:46:33-08:00`). Si la clé ne doit pas expirer, saisissez **null** comme valeur pour l'entrée **expires** (ou supprimez la ligne **Expires** et la virgule précédente).
9. Sélectionnez **Exécuter**.
10. ${post_edited_translations.segment}

## Gérer la réplication inter-grilles dans StorageGRID

Si l'autorisation **Utiliser la connexion de fédération de grilles** a été attribuée à votre compte locataire lors de sa création, vous pouvez utiliser la réplication inter-grilles 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-grilles peut s'effectuer dans un sens ou dans les deux.

#### Flux de travail pour la réplication inter-grilles

Le diagramme de flux de travail résume les étapes à suivre pour configurer la réplication inter-grilles entre les compartiments de deux grilles. Ces étapes sont décrites plus en détail ci-dessous.




### Configurer la réplication inter-grilles

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

#### Avant de commencer

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

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

#### Créez deux compartiments

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

**Étapes**

1. À partir de l'une ou l'autre des grilles de la connexion de fédération de grilles, créez un nouveau compartiment :
   a. Connectez-vous au compte locataire en utilisant les identifiants d'un utilisateur locataire qui existe sur les deux grilles.

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

   b. Suivez les instructions pour "créer un compartiment S3".

      Les noms des compartiments et les régions peuvent être différents sur chaque grille.

   c. Dans l'onglet **Gérer les paramètres de l'objet**, sélectionnez **Activer le versionnage des objets**.
   d. Si le verrouillage d'objet S3 est activé pour votre système StorageGRID, reportez-vous à "Réplication inter-grilles avec S3 Object Lock".
   e. Sélectionnez **Créer un compartiment**.
   f. Sélectionnez **Terminer**.
2. Répétez ces étapes pour créer un compartiment pour le même compte locataire sur l'autre grille dans la connexion de fédération de grilles.

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

#### Activer la réplication inter-grilles

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

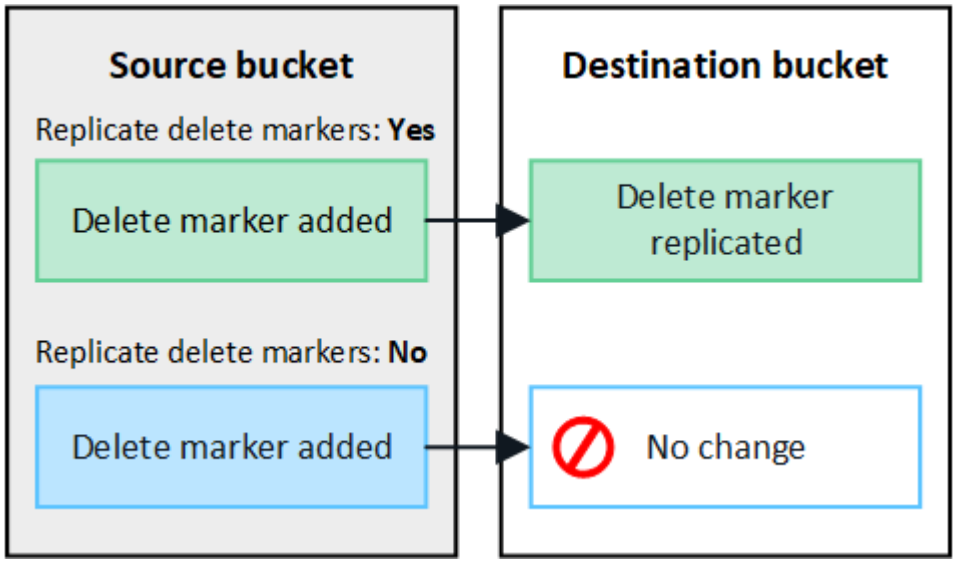
**Étapes**

1. À partir d'une grille dont vous souhaitez répliquer les objets, activez "réplication inter-grilles dans une direction" :
   a. Connectez-vous au compte locataire pour le compartiment.
   b. Sélectionnez **Afficher les compartiments** depuis 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 inter-grilles**.
   e. Sélectionnez **Activer** et consultez la liste des exigences.
   f. Si toutes les conditions requises sont remplies, sélectionnez la connexion de fédération de grille que

vous souhaitez utiliser.

g. Vous pouvez également modifier le paramètre **Répliquer les marqueurs de suppression** pour déterminer ce qui se passe sur la grille de destination si un client S3 envoie une requête de suppression à la grille source sans inclure d'ID de version :

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




> Si la requête de suppression inclut un ID de version, cette version de l'objet est définitivement supprimée du compartiment source. StorageGRID ne réplique pas les requêtes de suppression qui incluent un ID de version, donc la même version de l'objet n'est pas supprimée de la destination.

Consultez "Qu'est-ce que la réplication inter-grilles" pour plus de détails.

a. Vous pouvez également modifier le paramètre de la catégorie d'audit **Réplication inter-grilles** pour gérer le volume des messages d'audit :

   - **Erreur** (par défaut) : Seules les demandes de réplication inter-grilles ayant échoué sont incluses dans la sortie d'audit.
   - **Normal** : Toutes les demandes de réplication inter-grilles sont incluses, ce qui augmente considérablement le volume de la sortie d'audit.

b. Veuillez vérifier vos sélections. Vous ne pouvez pas modifier ces paramètres à moins que les deux compartiments ne soient vides.

c. Sélectionnez **Activer et tester**.

   Après quelques instants, un message de réussite s'affiche. Les objets ajoutés à ce compartiment sont désormais automatiquement répliqués sur l'autre grille. **La réplication inter-grilles** s'affiche en tant que fonctionnalité activée sur la page des détails du compartiment.

2. Vous pouvez également vous rendre dans le compartiment correspondant sur l'autre grille et "activer la réplication inter-grilles dans les deux sens".

### Tester la réplication entre les grilles

Si la réplication inter-grilles est activée pour un compartiment, vous devrez peut-être vérifier que la connexion et la réplication inter-grilles fonctionnent correctement et que les compartiments source et de destination répondent toujours à toutes les exigences (par exemple, le versionnage est toujours activé).

#### Avant de commencer

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

#### Étapes

1. Connectez-vous au compte locataire pour le compartiment.
2. Sélectionnez **Afficher les compartiments** depuis 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 inter-grilles**.
5. Sélectionnez **Test connection**.

   Si la connexion est saine, une bannière de réussite s'affiche. Dans le cas contraire, un message d'erreur apparaît, que vous et l'administrateur du grid pouvez utiliser pour résoudre le problème. Pour plus de détails, consultez "Dépanner les erreurs de fédération de grille".

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

### Désactiver la réplication inter-grilles

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

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

- La désactivation de la réplication inter-grilles ne supprime pas les objets déjà copiés entre les grilles. Par exemple, les objets dans `my-bucket` sur la grille 1 qui ont été copiés vers `my-bucket` sur la grille 2 ne sont pas supprimés si vous désactivez la réplication inter-grilles pour ce compartiment. Si vous souhaitez supprimer ces objets, vous devez les retirer manuellement.
- Si la réplication inter-grilles était activée pour chaque compartiment (c'est-à-dire si la réplication s'effectue dans les deux sens), vous pouvez désactiver la réplication inter-grilles pour l'un ou l'autre compartiment, voire pour les deux. Par exemple, vous pourriez vouloir désactiver la réplication des objets de `my-bucket` sur la grille 1 vers `my-bucket` sur la grille 2, tout en continuant à répliquer les objets de `my-bucket` sur la grille 2 vers `my-bucket` sur la grille 1.
- Vous devez désactiver la réplication inter-grilles avant de pouvoir supprimer l'autorisation d'un locataire à utiliser la connexion de fédération de grilles. Consultez "Gérer les locataires autorisés".
- Si vous désactivez la réplication inter-grilles pour un compartiment contenant des objets, vous ne pourrez pas réactiver la réplication inter-grilles à moins de supprimer tous les objets des compartiments source et de destination.

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

**Avant de commencer**

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

**Étapes**

1. À partir de la grille dont vous ne souhaitez plus répliquer les objets, arrêtez la réplication inter-grilles pour le compartiment :
   a. Connectez-vous au compte locataire pour le compartiment.
   b. Sélectionnez **Afficher les compartiments** depuis 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 inter-grilles**.
   e. Sélectionnez **Désactiver la réplication**.
   f. Si vous êtes sûr de vouloir désactiver la réplication inter-grilles 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 répliqués automatiquement sur l'autre grille. La **réplication inter-grilles** n'est plus affichée en tant que fonctionnalité activée sur la page Buckets.
2. Si la réplication inter-grilles a été configurée pour s'effectuer dans les deux sens, accédez au compartiment correspondant sur l'autre grille et arrêtez la réplication inter-grilles dans l'autre sens.

## Afficher les connexions de fédération de grilles dans StorageGRID

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

**Avant de commencer**

- ${post_edited_translations.segment}
- Vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès root".

**Étapes**

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

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

| Colonne | Description |
| --- | --- |
| Nom de la connexion | Les connexions de fédération de grid que ce locataire est autorisé à utiliser. |

| Colonne | Description |
| --- | --- |
| Buckets avec réplication inter-grille | Pour chaque connexion de fédération de grilles, les compartiments locataires pour lesquels la réplication inter-grilles 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 grilles, l'erreur la plus récente survenue, le cas échéant, lors de la réplication des données vers l'autre grille. Voir Effacez la dernière erreur. |

2. Vous pouvez également sélectionner un nom de compartiment à "${post_edited_translations.segment}".

### Effacer la dernière erreur

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

- La version de l'objet source est introuvable.
- Le compartiment source est introuvable.
- Le compartiment de destination a été supprimé.
- Le compartiment de destination a été recréé par un compte différent.
- Le versionnage du bucket de destination est suspendu.
- Le compartiment de destination a été recréé par le même compte, mais il n'est plus versionné.

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

**Étapes**

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

   Par exemple, cette erreur indique que le compartiment de destination pour la réplication inter-grilles était dans un état invalide, possiblement parce que le versionnage était suspendu ou que le S3 Object Lock était activé.


2. Effectuez les actions recommandées. Par exemple, si le versionnage a été suspendu sur le compartiment de destination pour la réplication inter-grilles, réactivez le versionnage pour ce compartiment.

3. Sélectionnez la connexion dans le tableau.
4. Sélectionnez **Effacer l'erreur**.
5. Sélectionnez **Oui** pour effacer le message et mettre à jour l'état du système.
6. Attendez 5 à 6 minutes, puis ajoutez un nouvel objet au bucket. Vérifiez que le message d'erreur ne réapparaît pas.

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

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

# Gérer les groupes et les utilisateurs

## Utilisez la fédération d'identité dans StorageGRID

${post_edited_translations.segment}

### Configurer la fédération d'identité pour Tenant Manager

Vous pouvez configurer la fédération d'identité pour le Tenant Manager si vous souhaitez que les groupes et utilisateurs de locataires soient gérés dans un autre système tel que Active Directory, Microsoft Entra ID, 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 root".
- Vous utilisez Active Directory, Microsoft Entra ID, OpenLDAP ou Oracle Directory Server comme fournisseur d'identité.

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

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

#### À propos de cette tâche

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

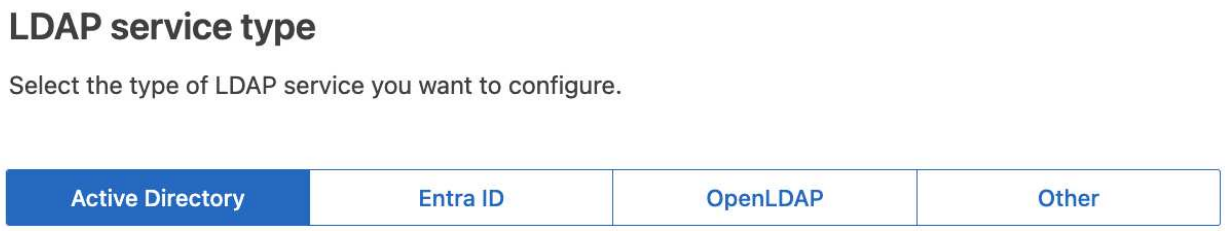
> This tenant account uses the LDAP server that is configured for the Grid Manager.
> Contact the grid administrator for information or to change this setting.

**${post_edited_translations.segment}**

${post_edited_translations.segment}

**Étapes**

1. Sélectionnez **Gestion des accès** > **Fédération d'identités**.
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.




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

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

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

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

  Pour Active Directory, vous pouvez également spécifier le nom d'ouverture de session de niveau inférieur ou le User Principal Name.

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

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

  > Si vous modifiez le mot de passe ultérieurement, vous devez le mettre à jour sur cette page.

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

  > Les valeurs du **nom unique du groupe** doivent être uniques au sein du **DN de base du groupe** auquel elles appartiennent.

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

  > Les valeurs du **nom unique de l'utilisateur** doivent être uniques au sein du **DN de base utilisateur** auquel elles appartiennent.

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

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

  Saisissez l'un de ces modèles :

  - **UserPrincipalName modèle (AD et Entra ID)**: `[USERNAME]@*example*.com`
  - **Modèle de nom d'ouverture de session de niveau inférieur (AD et Entra ID)** : `*example*\[USERNAME]`
  - **Modèle de nom unique** : `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

Incluez **[USERNAME]** exactement comme écrit.

6. Dans la section Transport Layer Security (TLS), sélectionnez un paramètre de sécurité.
   - **Utiliser STARTTLS** : Utilisez STARTTLS pour sécuriser les communications avec le serveur LDAP. Cette option est recommandée pour Active Directory, OpenLDAP ou Autre, mais cette option n'est pas prise en charge pour Microsoft Entra ID.
   - **Utiliser LDAPS** : L'option LDAPS (LDAP sur SSL) utilise TLS pour établir une connexion au serveur LDAP. Vous devez sélectionner cette option pour Microsoft Entra ID.
   - **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 Microsoft Entra ID.

   > ⓘ L'option « Ne pas utiliser TLS » n'est pas prise en charge si votre serveur Active Directory impose la signature LDAP. Vous devez utiliser STARTTLS ou LDAPS.

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

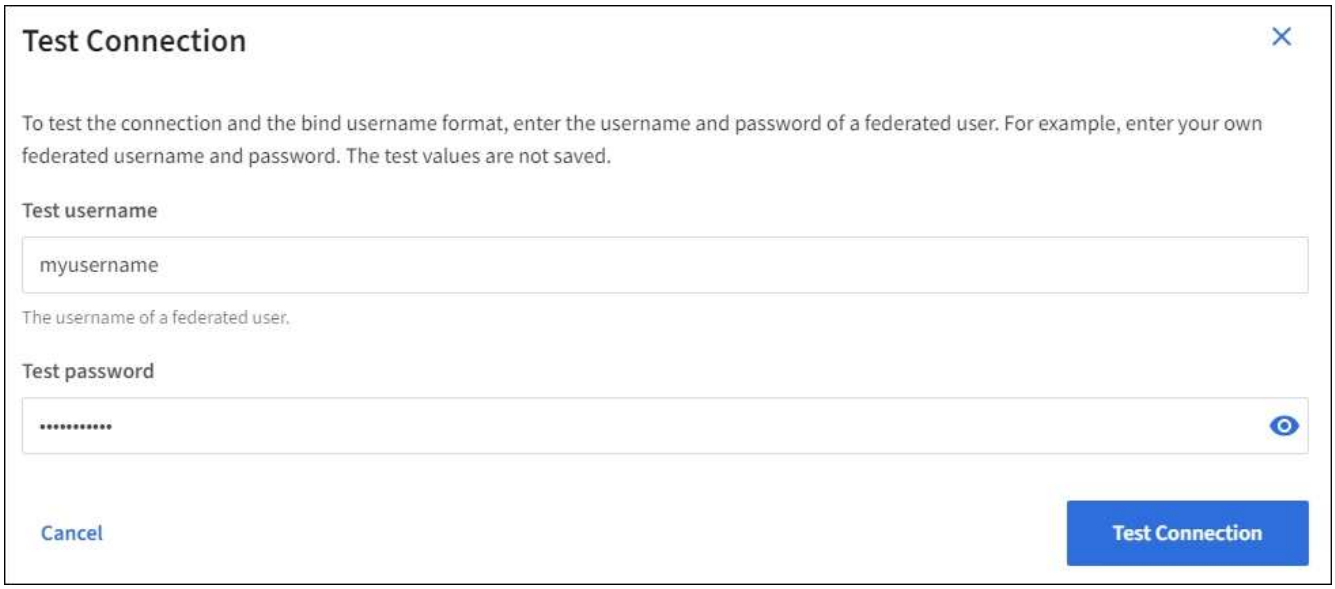
#### Testez la connexion et enregistrez la configuration

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

**Étapes**

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

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




- Un message « Test de connexion réussi » s'affiche si les paramètres de connexion sont valides. Sélectionnez **Enregistrer** pour enregistrer la configuration.
- Un message d'erreur s'affiche si les paramètres de connexion, le format du nom d'utilisateur de liaison ou le nom d'utilisateur et le mot de passe de test sont invalides. Résolvez les problèmes éventuels et testez à nouveau la connexion.

### Forcer la synchronisation avec la source d'identité

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

#### Étapes

1. Accédez à la page de fédération d'identités.
2. Sélectionnez **Sync server** en haut de la page.

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

L'alerte **Échec de la synchronisation de la fédération d'identités** est déclenchée en cas de problème lors de la synchronisation des groupes et utilisateurs fédérés à partir de la source d'identité.

### Désactivez la fédération d'identités

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

#### À propos de cette tâche

Avant de désactiver la fédération d'identités, vous devez prendre en compte les points suivants :

- Les utilisateurs fédérés ne pourront pas se connecter.
- Les utilisateurs fédérés actuellement connectés conserveront l'accès au système StorageGRID jusqu'à

l'expiration de leur session, mais ils ne pourront plus se connecter après l'expiration de celle-ci.

- La synchronisation entre le système StorageGRID et la source d'identité n'aura pas lieu et aucune alerte ne sera émise pour les comptes qui n'ont pas été synchronisés.
- La case à cocher **Activer la fédération d'identités** est désactivée si le statut de l'authentification unique (SSO) est **Activé** ou **Mode bac à sable**. Le statut SSO sur la page d'authentification unique doit être **Désactivé** avant que vous puissiez désactiver la fédération d'identités. Voir "Désactivez l'authentification unique".

**Étapes**

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

### Instructions pour la configuration du serveur OpenLDAP

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

> Pour les sources d'identité autres qu'Active Directory ou Microsoft Entra ID, StorageGRID ne bloque pas automatiquement l'accès S3 aux utilisateurs désactivés en externe. Pour bloquer l'accès S3, supprimez les clés S3 de l'utilisateur ou retirez l'utilisateur de tous les groupes.

#### Overlays Memberof et refint

Les superpositions memberof et refint doivent être activées. Pour plus d'informations, consultez les instructions relatives à la gestion des appartenances aux groupes inversées dans le "Documentation OpenLDAP : Guide de l'administrateur version 2.4".

#### Indexage

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

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

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

Consultez les informations relatives à la gestion des appartenances aux groupes inversés dans le "Documentation OpenLDAP : Guide de l'administrateur version 2.4".

## ${post_edited_translations.segment}

### Créez des groupes pour un locataire S3 dans StorageGRID

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

**Avant de commencer**

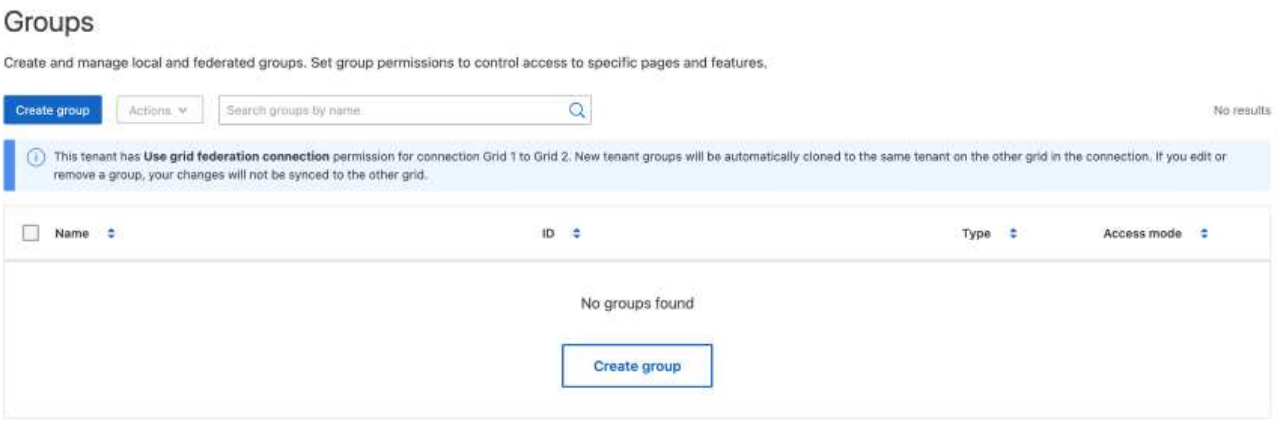
- Vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès root".
- Si vous prévoyez d'importer un groupe fédéré, vous avez "fédération d'identité configurée", et le groupe fédéré existe déjà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

#### ${post_edited_translations.segment}

Pour commencer, accédez à l'assistant de création de groupe.

### Étapes

1. Sélectionnez **Gestion des accès** > **Groupes**.
2. Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grilles**, vérifiez qu'une bannière bleue s'affiche, indiquant que les nouveaux groupes créés sur cette grille seront clonés sur le même locataire dans l'autre grille de la connexion. Si cette bannière n'apparaît pas, vous êtes peut-être connecté à la grille de destination du locataire.




3. Sélectionnez **Créer un groupe**.

#### Choisissez un type de groupe

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

### Étapes

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

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

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

- **Groupe fédéré** : saisissez le nom unique. Pour Active Directory, le nom unique est le nom associé à l'attribut `sAMAccountName`. Pour OpenLDAP, le nom unique est le nom associé à l'attribut `uid`.

3. Sélectionnez **Continue**.

#### 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 le **mode d'accès**, sélectionnez l'une des options suivantes :
   - **Lecture-écriture** (par défaut) : Les utilisateurs peuvent se connecter à Tenant Manager et gérer la configuration du locataire.
   - **Lecture seule** : Les utilisateurs peuvent uniquement consulter les paramètres et les fonctionnalités. Ils ne peuvent apporter aucune modification ni effectuer d'opérations dans le Tenant Manager ou l'API Tenant Management. Les utilisateurs locaux en lecture seule peuvent changer leur propre mot de passe.

   > Si un utilisateur appartient à plusieurs groupes et que l'un de ces groupes est configuré en lecture seule, l'utilisateur aura un accès en lecture seule à tous les paramètres et fonctionnalités sélectionnés.

2. Sélectionnez une ou plusieurs autorisations pour ce groupe.

   Voir "${post_edited_translations.segment}".

3. Sélectionnez **Continue**.

#### Définir la stratégie de groupe S3

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

**Étapes**

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

| stratégie de groupe | Description |
|---|---|
| Aucun accès S3 | Par défaut. Les utilisateurs de ce groupe n'ont pas accès aux ressources S3, à moins que l'accès ne soit accordé par une politique de compartiment. Si vous sélectionnez cette option, seul l'utilisateur root aura accès aux ressources S3 par défaut. |

| stratégie de groupe | Description |
| --- | --- |
| 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 lister les 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 apparaît dans la zone de texte. Vous ne pouvez pas modifier cette chaîne. |
| Accès complet | Les utilisateurs de ce groupe disposent d'un accès complet aux ressources S3, y compris les compartiments. Lorsque vous sélectionnez cette option, la chaîne JSON d'une stratégie de groupe d'accès complet s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne. |
| Atténuation des ransomwares | Cet exemple de politique s'applique à tous les compartiments de ce locataire. Les utilisateurs de ce groupe peuvent effectuer des actions courantes, mais ne peuvent pas supprimer définitivement des objets des compartiments pour lesquels le versionnement d'objets est activé.<br><br>Les utilisateurs Tenant Manager disposant de l'autorisation **Manage all buckets** peuvent ignorer cette stratégie de groupe. Limitez l'autorisation **Manage all buckets** aux utilisateurs de confiance et utilisez l'authentification multifacteur (MFA) lorsque disponible. |
| Personnalisé | ${post_edited_translations.segment} |

2. Si vous avez sélectionné **Custom**, saisissez la stratégie de groupe. Chaque stratégie de groupe est limitée à une taille de 5 120 octets. Vous devez saisir une chaîne au format JSON valide.

   Pour obtenir des informations détaillées sur les politiques de groupe, y compris la syntaxe du langage et des exemples, consultez "Exemples de stratégies de groupe".

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

#### Ajouter des utilisateurs (groupes locaux uniquement)

${post_edited_translations.segment}

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

**Étapes**

1. Facultativement, sélectionnez un ou plusieurs utilisateurs locaux pour ce groupe.
2. Sélectionnez **Créer un groupe** et **Terminer**.

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

Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grilles** et que vous êtes sur la grille source du locataire, le nouveau groupe est cloné vers la grille de destination du locataire. **Réussi** apparaît comme l'**état du clonage** dans la section Vue d'ensemble de la page de détails du groupe.

### Autorisations de gestion des locataires StorageGRID

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

Pour se connecter au Tenant Manager ou utiliser l'API Tenant Management, 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
- ${post_edited_translations.segment}

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

> Si un utilisateur appartient à plusieurs groupes et que l'un de ces groupes est configuré en lecture seule, l'utilisateur aura un accès en lecture seule à tous les paramètres et fonctionnalités sélectionnés.

${post_edited_translations.segment}

| Autorisation | Description | Détails |
|---|---|---|
| Accès root | Offre un accès complet au Tenant Manager et à l'API Tenant Management. | |
| Gérez vos propres identifiants S3 | ${post_edited_translations.segment} | Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu **STOCKAGE (S3)** > **Mes clés d'accès S3**. |
| ${post_edited_translations.segment} | ${post_edited_translations.segment} | ${post_edited_translations.segment}<br><br>Cette autorisation est remplacée par l'autorisation Gérer tous les compartiments. Elle n'affecte pas les politiques de groupe ou de compartiment S3 utilisées par les clients S3 ou la console S3. |

| Autorisation | Description | Détails |
| --- | --- | --- |
| ${post_edited_translations.segment} | Permet aux utilisateurs d'utiliser le Tenant Manager et l'API Tenant Management pour créer et supprimer des compartiments S3 et gérer les paramètres de tous les compartiments S3 du compte locataire, indépendamment des stratégies de compartiment S3 ou de groupe. | ${post_edited_translations.segment}<br><br>Cette autorisation remplace l'autorisation Afficher tous les compartiments. Elle n'affecte pas les politiques de compartiment ou de groupe S3 utilisées par les clients S3 ou la S3 Console. |
| Gérer les points de terminaison | Permet aux utilisateurs d'utiliser le Tenant Manager ou l'API de gestion des locataires pour créer ou modifier des points de terminaison de services de plateforme, qui sont utilisés comme destination pour les services de plateforme StorageGRID. | Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu **Points de terminaison des services de la plateforme**. |
| ${post_edited_translations.segment} | ${post_edited_translations.segment} | |

### Gérer les groupes de locataires StorageGRID

## ${post_edited_translations.segment}

**Avant de commencer**

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

#### ${post_edited_translations.segment}

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

**Étapes**

1. Sélectionnez **Gestion des accès** > **Groupes**.
2. ${post_edited_translations.segment}

   Si le compte du locataire dispose de l'autorisation **Utiliser la connexion de fédération de grille** et que vous consultez des groupes sur la grille source du locataire :

   - ${post_edited_translations.segment}
   - Au besoin, un message de bannière indique si des groupes n'ont pas été clonés sur le locataire de la grille de destination. Vous pouvez ${post_edited_translations.segment} qui ont échoué.
3. ${post_edited_translations.segment}
   a. Cochez la case correspondant au groupe.
   b. Sélectionnez **Actions** > **Modifier le nom du groupe**.
   c. Saisissez le nouveau nom.
   d. ${post_edited_translations.segment}

4. ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - Sélectionnez la case à cocher du groupe, puis sélectionnez **Actions** > **Afficher les détails du groupe**.
5. ${post_edited_translations.segment}
   - Nom d'affichage
   - Nom unique
   - Type
   - Mode d'accès
   - Autorisations
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
     - ${post_edited_translations.segment}
     - ${post_edited_translations.segment}
6. Modifiez les paramètres de groupe selon vos besoins. Reportez-vous à "Créer des groupes pour un locataire S3" pour obtenir des détails sur les informations à 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 du groupe**, mettez à jour les autorisations et sélectionnez **Enregistrer les modifications**.
   c. ${post_edited_translations.segment}

      ${post_edited_translations.segment}
7. Pour ajouter un ou plusieurs utilisateurs locaux existants au groupe :
   a. ${post_edited_translations.segment}


   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}

      Un message de confirmation apparaît en haut à droite.
8. ${post_edited_translations.segment}
   a. ${post_edited_translations.segment}

b. ${post_edited_translations.segment}

c. ${post_edited_translations.segment}

Un message de confirmation apparaît en haut à droite.

9. ${post_edited_translations.segment}

#### ${post_edited_translations.segment}

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

> Si votre compte 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 **Gestion des accès** > **Groupes**.
2. ${post_edited_translations.segment}
3. Sélectionnez **Actions** > **Dupliquer le groupe**.
4. Reportez-vous à "Créer des groupes pour un locataire S3" pour plus de détails sur les informations à saisir.
5. Sélectionnez **Créer un groupe**.

#### Réessayer le clonage du groupe

${post_edited_translations.segment}

1. Sélectionnez chaque groupe qui indique *(Échec du clonage)* sous le nom du groupe.
2. Sélectionnez **Actions** > **Clone groups**.
3. Consultez l'état de l'opération de clonage sur la page de détails de chaque groupe que vous clonez.

Pour plus d'informations, voir "Cloner les groupes de locataires et les utilisateurs".

#### Supprimer un ou plusieurs groupes

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

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

**Étapes**

1. Sélectionnez **Gestion des accès** > **Groupes**.
2. Cochez la case pour chaque groupe que vous souhaitez supprimer.
3. Sélectionnez **Actions** > **Supprimer le groupe** ou **Actions** > **Supprimer les groupes**.

Une boîte de dialogue de confirmation apparaît.

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

#### Configurez AssumeRole

**Avant de commencer**

Vous devez être administrateur pour configurer AssumeRole.

**À propos de cette tâche**

Pour configurer AssumeRole, créez le groupe cible à assumer, si le groupe n'existe pas déjà. Modifiez la politique S3 du groupe pour spécifier les actions autorisées pour assumer ce groupe. Modifiez la politique de confiance S3 du groupe pour spécifier les utilisateurs de confiance autorisés à assumer le groupe avec l'API AssumeRole.

Les informations d'identification de sécurité temporaires créées lors de l'adoption de ce groupe sont valides pour une durée limitée. La session dure entre 15 minutes et 12 heures, et la durée par défaut est d'une heure. Lorsque vous retirez l'utilisateur de la stratégie d'approbation S3 du groupe, l'utilisateur ne peut plus adopter ce groupe.

**Étapes**

1. Sélectionnez **Gestion des accès** > **Groupes**.
2. Cliquez sur le nom du groupe.
3. Sélectionnez l'onglet **Stratégie de confiance S3**.
4. Ajoutez votre politique de confiance S3, y compris une liste d'utilisateurs pouvant effectuer AssumeRole.
5. Sélectionnez **Save changes**.
6. Sélectionnez l'onglet **Stratégie de groupe S3**.
7. ${post_edited_translations.segment}
8. Sélectionnez **Save changes**.

**Exemple d'une AssumeRole politique de fiducie S3**

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Principal": {
                "AWS": [
                    "urn:sgws:identity::1234567890:user/user1",
                    "arn:aws:iam::1234567890:user/user2"
                ]
            }
        }
    ]
}
```

Une fois la configuration terminée, les utilisateurs listés dans la stratégie d'approbation S3 peuvent effectuer

AssumeRole et recevoir des informations d'identification. Les autorisations finales sont déterminées par la stratégie de groupe, la stratégie de compartiment et la stratégie de session. Pour plus d'informations, consultez "Utilisez les politiques d'accès".

## Gérer les utilisateurs locataires de StorageGRID

Vous pouvez créer des utilisateurs locaux et les affecter à des groupes locaux afin de définir les fonctionnalités auxquelles ces utilisateurs peuvent accéder. Vous pouvez également importer des utilisateurs fédérés. Le Tenant Manager inclut un utilisateur local prédéfini, nommé « root ». Bien que vous puissiez ajouter et supprimer des utilisateurs locaux, vous ne pouvez pas supprimer l'utilisateur root.

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

**Avant de commencer**

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

**${post_edited_translations.segment}**

${post_edited_translations.segment}

Les utilisateurs S3 qui n'appartiennent à aucun groupe ne disposent pas d'autorisations de gestion et aucune politique de groupe S3 ne leur est appliquée. Ces utilisateurs peuvent disposer d'un accès aux compartiments S3 accordé via une politique de compartiment.

**Accédez à l'assistant de création d'utilisateur**

**Étapes**

1. ${post_edited_translations.segment}

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


2. Sélectionnez **Créer un utilisateur**.

#### Saisissez vos identifiants

### Étapes

1. ${post_edited_translations.segment}

| Champ | Description |
|---|---|
| ${post_edited_translations.segment} | 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 | ${post_edited_translations.segment}<br><br>${post_edited_translations.segment} |
| Mot de passe et confirmation du mot de passe | ${post_edited_translations.segment} |
| ${post_edited_translations.segment} | Sélectionnez **Oui** pour empêcher cet utilisateur de se connecter au compte locataire, même s'il peut encore appartenir à un ou plusieurs groupes.<br><br>${post_edited_translations.segment} |

2. Sélectionnez **Continue**.

#### Attribuer aux groupes

### Étapes

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

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

   Les utilisateurs qui n'appartiennent à aucun groupe ne disposeront d'aucune autorisation de gestion. Les autorisations sont cumulatives. Les utilisateurs disposeront de toutes les autorisations pour tous les groupes auxquels ils appartiennent. Voir "${post_edited_translations.segment}".

2. Sélectionnez **Créer un utilisateur**.

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

3. ${post_edited_translations.segment}

**${post_edited_translations.segment}**

**Étapes**

1. ${post_edited_translations.segment}
2. Consultez les informations fournies sur la page Utilisateurs, qui répertorie les informations de base pour tous les utilisateurs locaux et fédérés de ce compte locataire.

   ${post_edited_translations.segment}

   - ${post_edited_translations.segment}
   - Au besoin, un message de bannière indique si des utilisateurs n'ont pas été clonés vers le locataire sur la grille de destination. Vous pouvez ${post_edited_translations.segment}.
3. ${post_edited_translations.segment}
   a. Cochez la case pour l'utilisateur.
   b. Sélectionnez **Actions** > **Modifier le nom complet**.
   c. Saisissez le nouveau nom.
   d. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}
   - Sélectionnez le nom d'utilisateur.
   - ${post_edited_translations.segment}
5. ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - Nom d'utilisateur
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - Mode d'accès
   - Adhésion au groupe
   - ${post_edited_translations.segment}
     - ${post_edited_translations.segment}
     - Une bannière bleue indique que si vous modifiez cet utilisateur, vos modifications ne seront pas synchronisées avec l'autre grille.
6. Modifiez les paramètres utilisateur selon vos besoins. Consultez ${post_edited_translations.segment} pour obtenir des détails sur les informations à 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 changer le nom d'utilisateur.

b. ${post_edited_translations.segment}

c. Dans l'onglet **Accès**, sélectionnez **Non** pour autoriser l'utilisateur à se connecter ou **Oui** pour l'empêcher de se connecter. Ensuite, sélectionnez **Enregistrer les modifications**.

d. Dans l'onglet **Touches d'accès**, sélectionnez **Créer une clé** et suivez les instructions pour "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 le retirer de groupes. Ensuite, sélectionnez **Enregistrer les modifications**.

7. ${post_edited_translations.segment}

### Importer les utilisateurs fédérés

Vous pouvez importer un ou plusieurs utilisateurs fédérés, jusqu'à un maximum de 100 utilisateurs, directement dans la page Utilisateurs.

**Étapes**

1. ${post_edited_translations.segment}
2. Sélectionnez **Importer les utilisateurs fédérés**.
3. Saisissez l'UUID ou le nom d'utilisateur d'un ou de plusieurs utilisateurs fédérés.

   Pour plusieurs entrées, ajoutez chaque UUID ou nom d'utilisateur sur une nouvelle ligne.

4. Sélectionnez **Importer**.

   Si l'importation dans le champ Utilisateurs échoue pour un ou plusieurs utilisateurs, procédez comme suit :

   a. Développez **Utilisateurs non importés** et sélectionnez **Copier les utilisateurs**.

   b. Réessayez l'importation en sélectionnant **Précédent** et en collant les utilisateurs copiés dans la boîte de dialogue **Import federated users**.

   Après la fermeture de la boîte de dialogue **Importer les utilisateurs fédérés**, les informations des utilisateurs fédérés s'affichent sur la page Utilisateurs pour les utilisateurs importés avec succès.

### ${post_edited_translations.segment}

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

${post_edited_translations.segment}

**Étapes**

1. ${post_edited_translations.segment}
2. Cochez la case correspondant à l'utilisateur que vous souhaitez dupliquer.
3. ${post_edited_translations.segment}
4. Consultez ${post_edited_translations.segment} pour obtenir des détails sur les informations à saisir.
5. Sélectionnez **Créer un utilisateur**.

### ${post_edited_translations.segment}

${post_edited_translations.segment}

1. ${post_edited_translations.segment}
2. Sélectionnez **Actions** > **Cloner les utilisateurs**.
3. Consultez l'état de l'opération de clonage depuis la page de détails de chaque utilisateur que vous clonez.

Pour plus d'informations, voir "Cloner les groupes de locataires et les utilisateurs".

**${post_edited_translations.segment}**

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

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

> ${post_edited_translations.segment}

**Étapes**

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. Sélectionnez **Actions** > **Supprimer l'utilisateur** ou **Actions** > **Supprimer les utilisateurs**.

   Une boîte de dialogue de confirmation apparaît.

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

# Gérer les clés d'accès S3

## Gérer les clés d'accès S3 dans StorageGRID

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

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

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

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

## Créez vos propres clés d'accès S3 dans StorageGRID

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 Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "${post_edited_translations.segment}".

**À propos de cette tâche**

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

Chaque clé peut avoir une date d'expiration spécifique ou ne pas avoir d'expiration. Suivez ces directives concernant la durée d'expiration :

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

> Les compartiments et objets S3 appartenant à votre compte sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichés pour votre compte dans le Tenant Manager. Pour cette raison, protégez les clés d'accès comme vous le feriez pour un mot de passe. Effectuez une rotation régulière des clés d'accès, supprimez toutes les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

**Étapes**

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

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

2. Sélectionnez **Créer une clé**.
3. Effectuez l'une des opérations suivantes :
   - Sélectionnez **Ne pas définir de date d'expiration** pour créer une clé qui n'expirera pas. (Par défaut)
   - Sélectionnez **Définir une date d'expiration**, puis indiquez la date et l'heure d'expiration.

     > La date d'expiration peut être fixée à un maximum de cinq ans à compter de la date actuelle. L'heure d'expiration peut être fixée à un minimum d'une minute à compter de l'heure actuelle.

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

La boîte de dialogue « Download access key » s'affiche, indiquant votre access key ID et votre secret access key.

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

   > Ne fermez pas cette boîte de dialogue tant que vous n'avez pas copié ou téléchargé ces informations. Vous ne pouvez pas copier ou télécharger les clés après la fermeture de la boîte de dialogue.

6. Sélectionnez **Terminer**.

   La nouvelle clé est répertoriée sur la page My access keys.

7. Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grille**, vous pouvez éventuellement utiliser l'API Tenant Management 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".

## Consultez vos clés d'accès S3 dans StorageGRID

Si vous utilisez un locataire S3 et que vous disposez de "autorisation appropriée", vous pouvez afficher la liste de vos clés d'accès S3. Vous pouvez trier la liste par date d'expiration afin de déterminer quelles clés vont bientôt expirer. Au besoin, vous pouvez "${post_edited_translations.segment}" ou "${post_edited_translations.segment}" que vous n'utilisez plus.

> Les compartiments et objets S3 appartenant à votre compte sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichés pour votre compte dans le Tenant Manager. Pour cette raison, protégez les clés d'accès comme vous le feriez pour un mot de passe. Effectuez une rotation régulière des clés d'accès, supprimez toutes les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

**Avant de commencer**

- Vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède l'autorisation Gérer vos propres informations d'identification S3 "${post_edited_translations.segment}".

**Étapes**

1. Sélectionnez **STOCKAGE (S3)** > **Mes clés d'accès**.
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}

   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 dans StorageGRID

Si vous utilisez un tenant S3 et que vous disposez des autorisations nécessaires, vous pouvez supprimer vos propres clés d'accès S3. Après la suppression d'une clé d'accès, elle ne peut plus être utilisée pour accéder aux objets et aux compartiments du compte du tenant.

**Avant de commencer**

- Vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Vous avez le "Gérez vos propres autorisations d'identifiants S3".

> Les compartiments et objets S3 appartenant à votre compte sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichés pour votre compte dans le Tenant Manager. Pour cette raison, protégez les clés d'accès comme vous le feriez pour un mot de passe. Effectuez une rotation régulière des clés d'accès, supprimez toutes les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

**Étapes**

1. Sélectionnez **STOCKAGE (S3)** > **Mes clés d'accès**.
2. ${post_edited_translations.segment}
3. Sélectionnez la touche **Delete key**.
4. Dans la boîte de dialogue de confirmation, sélectionnez **Delete key**.

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

## Créez les clés d'accès S3 d'un autre utilisateur dans StorageGRID

Si vous utilisez un locataire S3 et que vous disposez des autorisations appropriées, vous pouvez créer des clés d'accès S3 pour d'autres utilisateurs, comme des applications qui ont besoin d'accéder aux compartiments et aux objets.

**Avant de commencer**

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

**À propos de cette tâche**

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

Chaque clé peut avoir une date d'expiration spécifique ou ne pas avoir d'expiration. Suivez ces directives concernant la durée d'expiration :

- Définissez une date d'expiration pour les clés afin de limiter l'accès de l'utilisateur à une période donnée. La définition d'une date d'expiration courte peut aider à réduire les risques si l'ID de clé d'accès et la clé d'accès secrète sont accidentellement exposés. Les clés expirées sont supprimées automatiquement.

- Si le risque de sécurité dans votre environnement est faible et que vous n'avez pas besoin de créer régulièrement de nouvelles clés, il n'est pas nécessaire de définir une date d'expiration pour les clés. Si vous décidez ultérieurement de créer de nouvelles clés, supprimez les anciennes clés manuellement.

> Les compartiments et objets S3 d'un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichés pour cet utilisateur dans le Tenant Manager. Pour cette raison, protégez les clés d'accès comme vous le feriez pour un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez toute clé inutilisée du compte et ne les partagez jamais avec d'autres utilisateurs.

**Étapes**

1. ${post_edited_translations.segment}
2. Sélectionnez l'utilisateur dont vous souhaitez gérer les clés d'accès S3.

   La page de détails de l'utilisateur s'affiche.

3. Sélectionnez **Access keys**, puis sélectionnez **Create key**.
4. Effectuez l'une des opérations suivantes :
   - Sélectionnez **Ne pas définir de date d'expiration** pour créer une clé qui n'expire pas. (Par défaut)
   - Sélectionnez **Définir une date d'expiration**, puis indiquez la date et l'heure d'expiration.

   > La date d'expiration peut être fixée à un maximum de cinq ans à compter de la date actuelle. L'heure d'expiration peut être fixée à un minimum d'une minute à compter de l'heure actuelle.

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

   ${post_edited_translations.segment}

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

   > Ne fermez pas cette boîte de dialogue tant que vous n'avez pas copié ou téléchargé ces informations. Vous ne pouvez pas copier ou télécharger les clés après la fermeture de la boîte de dialogue.

7. Sélectionnez **Terminer**.

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

8. Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grille**, vous pouvez éventuellement utiliser l'API Tenant Management 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 dans StorageGRID

Si vous utilisez un tenant S3 et que vous disposez des autorisations nécessaires, vous pouvez consulter les clés d'accès S3 d'un autre utilisateur. Vous pouvez trier la liste par

date d'expiration afin de déterminer quelles clés expireront bientôt. Au besoin, vous pouvez créer de nouvelles clés et supprimer les clés qui ne sont plus utilisées.

**Avant de commencer**

- Vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Vous disposez de "Autorisation d'accès root".

> Les compartiments et objets S3 d'un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichés pour cet utilisateur dans le Tenant Manager. Pour cette raison, protégez les clés d'accès comme vous le feriez pour un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez toute clé inutilisée du compte et ne les partagez jamais avec d'autres utilisateurs.

**Étapes**

1. ${post_edited_translations.segment}
2. Sur la page Utilisateurs, sélectionnez l'utilisateur dont vous souhaitez consulter les clés d'accès S3.
3. ${post_edited_translations.segment}
4. Triez les clés par **heure d'expiration** ou **ID de clé d'accès**.
5. ${post_edited_translations.segment}

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

   Les clés expirées sont supprimées automatiquement.

**Informations connexes**

- "Créer les clés d'accès S3 d'un autre utilisateur"
- "${post_edited_translations.segment}"

## Supprimer les clés d'accès S3 d'un autre utilisateur dans StorageGRID

Si vous utilisez un tenant S3 et que vous disposez des autorisations nécessaires, vous pouvez supprimer les clés d'accès S3 d'un autre utilisateur. Après la suppression d'une clé d'accès, elle ne peut plus être utilisée pour accéder aux objets et aux compartiments du compte du tenant.

**Avant de commencer**

- Vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Vous disposez de "Autorisation d'accès root".

> Les compartiments et objets S3 d'un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichés pour cet utilisateur dans le Tenant Manager. Pour cette raison, protégez les clés d'accès comme vous le feriez pour un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez toute clé inutilisée du compte et ne les partagez jamais avec d'autres utilisateurs.

**Étapes**

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. Sur la page Détails de l'utilisateur, sélectionnez **Clés d'accès**, puis cochez la case correspondant à chaque clé d'accès que vous souhaitez supprimer.
4. ${post_edited_translations.segment}
5. Dans la boîte de dialogue de confirmation, sélectionnez **Delete key**.

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

# ${post_edited_translations.segment}

## Créez un compartiment StorageGRID S3

${post_edited_translations.segment}

**Avant de commencer**

- Vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Vous appartenez à un groupe d'utilisateurs disposant des droits d'accès racine ou de gestion de tous les compartiments "${post_edited_translations.segment}". Ces autorisations prévalent sur les paramètres d'autorisation définis dans les stratégies de groupe ou de compartiment.

  Les autorisations permettant de définir ou de modifier les propriétés S3 Object Lock des compartiments ou des objets peuvent être accordées par "${post_edited_translations.segment}".

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

  Chaque grille peut comporter un maximum de 100 000 compartiments, y compris "seaux de branches".

**Accédez à l'assistant**

**Étapes**

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

**Saisissez les détails**

**Étapes**

1. ${post_edited_translations.segment}

| Champ | Description |
| --- | --- |
| Nom du compartiment | Un nom pour le seau qui respecte ces règles :<br>• Doit être unique dans chaque système StorageGRID (et pas seulement unique au sein du compte du locataire).<br>• Doit être conforme au DNS.<br>• Doit contenir au moins 3 et au plus 63 caractères.<br>• ${post_edited_translations.segment}<br>• Ne doit pas contenir de points dans les requêtes de type hébergement virtuel. Les points entraîneront des problèmes lors de la vérification du certificat générique du serveur.<br>Pour plus d'informations, consultez le "${post_edited_translations.segment}".<br>${post_edited_translations.segment} |
| Région | La région du compartiment.<br>Votre administrateur StorageGRID gère les régions disponibles. La région d'un compartiment peut affecter la politique de protection des données appliquée aux objets. Par défaut, tous les compartiments sont créés dans la région `us-east-1`. Si la région par défaut est configurée sur une région autre que `us-east-1`, cette autre région est initialement sélectionnée dans la liste déroulante.<br>${post_edited_translations.segment} |

2. Sélectionnez **Continue**.

### Gérer les paramètres

#### Étapes

1. ${post_edited_translations.segment}

   Activez le versionnement d'objets si vous souhaitez stocker chaque version de chaque objet dans ce compartiment. Vous pouvez ensuite récupérer les versions précédentes d'un objet selon vos besoins.

   Vous devez activer le versionnage des objets si :

   ◦ ${post_edited_translations.segment}
   ◦ Vous souhaitez créer un "bucket de branche" à partir de ce bucket.

2. ${post_edited_translations.segment}

   Activez S3 Object Lock pour un compartiment uniquement si vous devez conserver des objets pendant une période définie, par exemple pour répondre à certaines exigences réglementaires. S3 Object Lock est un paramètre permanent qui vous permet d'empêcher la suppression ou la réécriture d'objets pendant une période définie ou indéfiniment.

Une fois le paramètre S3 Object Lock activé pour un compartiment, il ne peut plus 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 d'objet S3 pour un compartiment, le versionnage du compartiment est activé automatiquement.

3. ${post_edited_translations.segment}

Votre administrateur de la grille doit vous donner l'autorisation de "${post_edited_translations.segment}".

Lorsque la **Rétention par défaut** est activée, les nouveaux objets ajoutés au compartiment seront automatiquement protégés contre la suppression ou la réécriture. Le paramètre **Rétention par défaut** ne s'applique pas aux objets qui possèdent leurs propres périodes de rétention.

a. ${post_edited_translations.segment}

| Mode de rétention par défaut | Description |
|---|---|
| Gouvernance | • Les utilisateurs disposant de l' `s3:BypassGovernanceRetention`autorisation peuvent utiliser l' `x-amz-bypass-governance-retention: true`en-tête de requête pour contourner les paramètres de rétention.<br>• Ces utilisateurs peuvent supprimer une version d'objet avant que sa date de conservation ne soit atteinte.<br>• Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet. |
| Conformité | • L'objet ne peut pas être supprimé tant que sa date de conservation n'est pas atteinte.<br>• La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être diminuée.<br>• La date de conservation de l'objet ne peut pas être supprimée avant que cette date ne soit atteinte.<br><br>**Remarque** : Votre administrateur de grille doit vous autoriser à utiliser le mode de conformité. |

b. Si la **rétention par défaut** est activée, spécifiez la **période de rétention par défaut** pour le compartiment.

   La **période de rétention par défaut** indique la durée pendant laquelle les nouveaux objets ajoutés à ce compartiment doivent être conservés, à compter de leur ingestion. Spécifiez une valeur inférieure ou égale à la période de rétention maximale pour le locataire, telle que définie par l'administrateur de la grille.

Une période de conservation *maximale*, qui peut être une valeur allant de 1 jour à 100 ans, est définie lorsque l'administrateur de la grille crée le locataire. Lorsque vous définissez une période de conservation *par défaut*, elle ne peut pas dépasser la valeur définie pour la période de conservation maximale. Si

nécessaire, demandez à votre administrateur de la grille d'augmenter ou de diminuer la période de conservation maximale.

4. ${post_edited_translations.segment}

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

   Si aucune limite n'est définie, la capacité de ce bucket est illimitée. Reportez-vous à "Utilisation de la limite de capacité" pour plus d'informations.

5. ${post_edited_translations.segment}

   La limite du nombre d'objets est le nombre maximal d'objets que ce compartiment peut contenir. Cette valeur représente une quantité logique (nombre d'objets). Si aucune limite n'est définie, le nombre d'objets est illimité.

6. Sélectionnez **Créer un compartiment**.

   Le compartiment est créé et ajouté au tableau de la page Buckets.

7. Vous pouvez également sélectionner **Accéder à la page de détails du compartiment** pour "${post_edited_translations.segment}" et effectuer une configuration supplémentaire.

Vous pouvez également "créer des compartiments de branche" au besoin.

## Afficher les détails du compartiment S3 dans StorageGRID

Vous pouvez consulter les compartiments dans votre compte locataire.

**Avant de commencer**

- Vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui dispose de "Autorisation d'accès root, de gestion de tous les compartiments ou d'affichage de tous les compartiments". Ces autorisations remplacent les paramètres d'autorisation dans les stratégies de groupe ou de compartiment.

**Étapes**

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

   ${post_edited_translations.segment}

2. ${post_edited_translations.segment}

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

   Les valeurs affichées pour le nombre d'objets, l'espace utilisé et l'utilisation sont des estimations. Ces estimations sont affectées par le moment des ingestions, la connectivité réseau et l'état des nœuds. Si les compartiments ont le versionnage activé, les versions d'objets supprimées sont incluses dans le nombre d'objets.

**Nom**

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

**${post_edited_translations.segment}**

La liste des fonctionnalités activées pour le compartiment.

**Verrouillage d'objet S3**

${post_edited_translations.segment}

Cette colonne s'affiche uniquement si le verrouillage des objets S3 est activé pour la grille. Cette colonne présente également des informations sur les anciens compartiments Compliant.

**Région**

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

**${post_edited_translations.segment}**

Le nombre d'objets dans ce compartiment. Si le versionnement est activé pour les compartiments, les versions d'objet non actuelles sont incluses dans cette valeur.

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

**Espace utilisé**

La taille logique de tous les objets du compartiment. La taille logique n'inclut pas l'espace réel requis pour les copies répliquées ou codées par effacement, ni pour les métadonnées d'objet.

${post_edited_translations.segment}

**${post_edited_translations.segment}**

${post_edited_translations.segment}

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

${post_edited_translations.segment}

**Capacité**

Si cette option est activée, la limite de capacité du compartiment.

**${post_edited_translations.segment}**

Date et heure de création du compartiment. Cette colonne est masquée par défaut.

3. Pour afficher les détails d'un compartiment spécifique, sélectionnez le nom du compartiment dans le tableau.
   a. Consultez les informations récapitulatives en haut de la page Web pour confirmer les détails du compartiment, tels que la région et le nombre d'objets.

b. Consultez les barres d'utilisation de la limite de capacité et d'utilisation de la limite du nombre d'objets. Si l'utilisation est de 100 % ou proche de 100 %, envisagez d'augmenter la limite ou de supprimer certains objets.

c. ${post_edited_translations.segment}

> Prêtez une attention particulière aux mises en garde qui s'affichent lorsque vous sélectionnez chacune de ces options. Pour plus d'informations, reportez-vous à :
>
> - "Supprimez tous les objets d'un compartiment"
> - "Supprimer un compartiment" (le seau doit être vide)

d. ${post_edited_translations.segment}

- **S3 Console** : affichez les objets du compartiment. Pour plus d'informations, reportez-vous à "Utilisez la console S3".
- **Options du compartiment** : Consultez ou modifiez les paramètres des options. Certains paramètres, comme S3 Object Lock, ne peuvent pas être modifiés après la création du compartiment.
  - "${post_edited_translations.segment}"
  - "${post_edited_translations.segment}"
  - "Limite de capacité"
  - "Limite du nombre d'objets"
  - "Versionnage d'objets"
  - "Verrouillage d'objet S3"
  - "${post_edited_translations.segment}"
  - "Gérer la réplication inter-grilles" (si autorisé pour le locataire)
- **Services de plateforme** : "Gérer les services de plateforme" (s'ils sont autorisés pour le locataire)
- **Accès au bucket** : afficher ou modifier les paramètres d'option. Vous devez disposer d'autorisations d'accès spécifiques.
  - Configurez "CORS pour les compartiments et les objets" pour que le compartiment et les objets du compartiment soient accessibles aux applications web d'autres domaines.
  - "${post_edited_translations.segment}" pour un compartiment S3 et les objets de ce compartiment.
- **Branches** : affichez la liste des compartiments de branche pour le compartiment. "Créer un nouveau compartiment de branche ou gérer les compartiments de branche".

## Découvrez les compartiments de branche StorageGRID

### ${post_edited_translations.segment}

Vous créez un compartiment de branche à partir d'un compartiment existant. Après avoir créé un compartiment de branche, le compartiment d'origine à partir duquel il a été créé est appelé le *compartiment de base*. De plus, vous pouvez créer un compartiment de branche à partir d'un autre compartiment de branche.

Un compartiment de branche fournit un accès aux données protégées, mais ne sert pas de sauvegarde. Pour continuer à protéger les données, utilisez ces fonctionnalités sur les compartiments de base :

- "Verrouillage d'objet S3"
- "Réplication inter-grilles" pour les compartiments de base
- "${post_edited_translations.segment}" pour les compartiments versionnés afin de nettoyer les anciennes versions d'objets

${post_edited_translations.segment}

- Vous pouvez accéder aux objets des compartiments de succursale en utilisant "Console S3 pour télécharger des objets".
- Lorsque les clients accèdent aux objets dans un bucket de branche, ce sont les "${post_edited_translations.segment}" du bucket de branche, plutôt que les politiques du bucket de base, qui déterminent si l'accès est accordé ou refusé.
- Les objets créés dans un compartiment de base sont évalués en fonction de la manière dont "Règles ILM" s'appliquent au compartiment de base. Les objets créés dans un compartiment de branche sont évalués en fonction de la manière dont les règles ILM s'appliquent au compartiment de branche.
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

**Exemples d'utilisation des compartiments de branche**

- ${post_edited_translations.segment}
- Vous enregistrez des données dans un compartiment versionné. Une vulnérabilité accidentelle a entraîné l'ingestion de nombreux objets indésirables après l'instant *T*. Vous pouvez créer un compartiment de branche pour la valeur temporelle Before, *T*, et rediriger les opérations des clients vers ce compartiment de branche. Ainsi, seuls les objets ingérés avant la valeur temporelle Before *T* sont exposés aux clients.

**Opérations sur les objets dans les compartiments de branche**

- Une opération PUT object sur un bucket de branche crée un objet dans la branche.
- Une opération GET sur un bucket de branche récupère un objet de la branche. Si l'objet n'existe pas dans le bucket de branche, il est récupéré depuis le bucket de base.
- La suppression d'objets dans les compartiments de branche s'effectue comme suit :

| Opération | Cible | Résultat | ${post_edited_translations.segment} | ${post_edited_translations.segment} |
|---|---|---|---|---|
| ${post_edited_translations.segment} | ${post_edited_translations.segment} | Le marqueur de suppression est créé uniquement pour le compartiment de base | ${post_edited_translations.segment} | HEAD/GET renvoie Objet existe, et des versions spécifiques restent accessibles<br><br>Le marqueur de suppression aurait été créé après le `beforeTime` du compartiment de branche. |

| Opération | Cible | Résultat | ${post_edited_translations.segment} | ${post_edited_translations.segment} |
|---|---|---|---|---|
| Supprimer avec l'ID de version | ${post_edited_translations.segment} | ${post_edited_translations.segment} | ${post_edited_translations.segment} | ${post_edited_translations.segment} |
| ${post_edited_translations.segment} | ${post_edited_translations.segment} | Le marqueur de suppression est créé uniquement pour le compartiment de branche | ${post_edited_translations.segment} | HEAD/GET renvoie Objet n'existe pas |
| Supprimer avec l'ID de version | ${post_edited_translations.segment} | La version spécifique de l'objet est supprimée uniquement pour le compartiment de branche | HEAD/GET renvoie une version spécifique de l'objet (l'objet de base du bucket n'est pas affecté) | ${post_edited_translations.segment} |

Voir aussi "${post_edited_translations.segment}".

## Gérer les compartiments de branche StorageGRID

### ${post_edited_translations.segment}

**Avant de commencer**

- Vous vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui dispose de l'accès Root ou "${post_edited_translations.segment}". Ces autorisations remplacent les paramètres d'autorisation dans les politiques de groupe ou de compartiment.
- Le bucket de base à partir duquel vous souhaitez créer une branche possède "versionnage activé".
- ${post_edited_translations.segment}

**À propos de cette tâche**

${post_edited_translations.segment}

- Les autorisations permettant de définir les propriétés de verrouillage d'objets S3 des compartiments ou des objets peuvent être accordées par "${post_edited_translations.segment}".
- Si vous suspendez le versionnage sur le compartiment principal, le contenu du compartiment principal ne sera plus visible dans ses compartiments secondaires.

${post_edited_translations.segment}

**Créer un bucket de branche**

**Étapes**

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

2. ${post_edited_translations.segment}
3. Sur la page de détails du compartiment, sélectionnez **Branches** > **Créer un compartiment de branche**.

   Le bouton **Créer un compartiment de branche** est désactivé si le compartiment de base n'a pas le versionnage activé.

### Saisissez les détails

#### Étapes

1. Saisissez les détails du compartiment de branche.

| Champ | Description |
|---|---|
| ${post_edited_translations.segment} | ${post_edited_translations.segment}<br>• Doit être unique dans chaque système StorageGRID (et pas seulement unique au sein du compte du locataire).<br>• Doit être conforme au DNS.<br>• Doit contenir au moins 3 et au plus 63 caractères.<br>• ${post_edited_translations.segment}<br>• Ne doit pas contenir de points dans les requêtes de type hébergement virtuel. Les points entraîneront des problèmes lors de la vérification du certificat générique du serveur.<br>Pour plus d'informations, consultez le "${post_edited_translations.segment}".<br>**Remarque** : Vous ne pouvez pas modifier le nom après avoir créé le compartiment de branche. |
| ${post_edited_translations.segment} | ${post_edited_translations.segment}<br>${post_edited_translations.segment} |
| Avant l'heure | L'heure limite pour que les versions d'objets créées dans le compartiment de base soient accessibles depuis le compartiment de branche. Le compartiment de branche permet d'accéder aux versions d'objets créées avant l'heure Before time.<br>La date et l'heure « Avant » doivent être une date et une heure passées. Il ne peut pas s'agir d'une date future. |
| Type de compartiment de branche | • ${post_edited_translations.segment}<br>• **Lecture seule** : Vous ne pouvez pas modifier les objets dans le compartiment de la branche.<br>**Remarque** : vous ne pouvez définir le type de bucket de branche sur lecture seule que si le bucket de branche est vide. Si le type d'un bucket de branche existant est défini sur lecture-écriture et que vous n'y avez pas écrit, vous pouvez modifier le type en lecture seule. |

2. Sélectionnez **Continue**.

**${post_edited_translations.segment}**

Les paramètres d'objet d'un compartiment de branche n'affectent pas les versions d'objet dans le compartiment de base.

**Étapes**

1. Si le paramètre global S3 Object Lock est activé, vous pouvez également activer S3 Object Lock pour le compartiment de branche. Pour activer S3 Object Lock, le compartiment de branche doit être un compartiment en lecture-écriture.

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

   > Une fois le paramètre de verrouillage des objets S3 activé pour un compartiment, il ne peut pas être désactivé. Toute personne disposant des autorisations appropriées peut ajouter des objets au compartiment de la branche qui ne peuvent pas être modifiés. Il se peut que vous ne puissiez pas supprimer ces objets ni le compartiment de la branche lui-même.

2. Si vous avez sélectionné **Activer le verrouillage des objets S3**, vous pouvez également activer **Rétention par défaut** pour le compartiment de branche.

   > Votre administrateur de la grille doit vous donner l'autorisation de "${post_edited_translations.segment}".

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

   a. Si la **rétention par défaut** est activée, spécifiez un **mode de rétention par défaut** pour le compartiment de branche.

| Mode de rétention par défaut | Description |
|---|---|
| Gouvernance | • Les utilisateurs disposant de l' `s3:BypassGovernanceRetention`autorisation peuvent utiliser l' `x-amz-bypass-governance-retention: true`en-tête de requête pour contourner les paramètres de rétention.<br>• Ces utilisateurs peuvent supprimer une version d'objet avant que sa date de conservation ne soit atteinte.<br>• Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet. |

| Mode de rétention par défaut | Description |
| --- | --- |
| Conformité | • L'objet ne peut pas être supprimé tant que sa date de conservation n'est pas atteinte.<br>• La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être diminuée.<br>• La date de conservation de l'objet ne peut pas être supprimée avant que cette date ne soit atteinte.<br><br>**Remarque** : Votre administrateur de grille doit vous autoriser à utiliser le mode de conformité. |

b. ${post_edited_translations.segment}

La **période de rétention par défaut** indique la durée pendant laquelle les nouveaux objets ajoutés au compartiment de succursale doivent être conservés, à compter de leur ingestion. Spécifiez une valeur inférieure ou égale à la période de rétention maximale pour le locataire, telle que définie par l'administrateur du grid.

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

3. ${post_edited_translations.segment}

La limite de capacité correspond à la capacité maximale disponible pour le compartiment de branche. Cette valeur représente une taille logique (taille de l'objet), et non une taille physique (taille sur le disque).

Si aucune limite n'est définie, la capacité du compartiment de branche est illimitée. Consultez "Utilisation de la limite de capacité" pour plus d'informations.

${post_edited_translations.segment}

4. Vous pouvez éventuellement sélectionner **Activer la limite du nombre d'objets**.

La limite du nombre d'objets est le nombre maximal d'objets que le compartiment de succursale peut contenir. Cette valeur représente une quantité logique (nombre d'objets). Si aucune limite n'est définie, le nombre d'objets est illimité.

${post_edited_translations.segment}

5. Sélectionnez **Créer un compartiment**.

${post_edited_translations.segment}

6. Vous pouvez également sélectionner **Accéder à la page de détails du compartiment** pour "${post_edited_translations.segment}" et effectuer une configuration supplémentaire.

Sur la page de détails du compartiment, certaines options de configuration relatives à la modification des objets sont désactivées pour les compartiments en lecture seule.

## Appliquer une étiquette de stratégie ILM à un compartiment StorageGRID

Choisissez une étiquette de stratégie ILM à appliquer à un compartiment en fonction de vos exigences de stockage d'objets.

La politique ILM contrôle l'emplacement de stockage des données d'objet et leur suppression après une certaine période. Votre administrateur de grille crée des politiques ILM et les assigne à des balises de politique ILM lorsqu'il utilise plusieurs politiques actives.

> Évitez de réattribuer fréquemment l'étiquette de stratégie d'un compartiment. Sinon, des problèmes de performance pourraient survenir.

**Avant de commencer**

- Vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui dispose de "Autorisation d'accès root, de gestion de tous les compartiments ou d'affichage de tous les compartiments". Ces autorisations remplacent les paramètres d'autorisation dans les stratégies de groupe ou de compartiment.

**Étapes**

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

   La page « Buckets » s'affiche. Selon vos besoins, vous pouvez trier les informations par n'importe quelle colonne ou avancer et reculer dans la liste page par page.

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

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

   > Les valeurs affichées pour le nombre d'objets et l'espace utilisé sont des estimations. Ces estimations sont affectées par le moment des ingestions, la connectivité réseau et l'état des nœuds. Si le versionnage est activé pour les compartiments, les versions d'objets supprimées sont incluses dans le nombre d'objets.

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

   > Modifier l'étiquette de stratégie ILM d'un compartiment entraînera une réévaluation ILM de tous les objets de ce compartiment. Si la nouvelle stratégie conserve les objets pendant une durée limitée, les objets les plus anciens seront supprimés.

5. ${post_edited_translations.segment}
6. Sélectionnez **Enregistrer les modifications**. Une nouvelle étiquette de compartiment S3 sera créée sur le compartiment avec la clé `NTAP-SG-ILM-BUCKET-TAG` et la valeur du nom de l'étiquette de stratégie ILM.

Veillez à ce que vos applications S3 ne remplacent ni ne suppriment accidentellement la nouvelle balise de compartiment. Si cette balise est omise lors de l'application d'un nouveau TagSet au compartiment, les objets du compartiment seront à nouveau évalués selon la stratégie ILM par défaut.

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

${post_edited_translations.segment}

## Gérer la politique du compartiment StorageGRID

${post_edited_translations.segment}

**Avant de commencer**

- Vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède les "Autorisation d'accès root". Les autorisations « View all buckets » et « Manage all buckets » permettent uniquement la consultation.
- Vous avez vérifié que le nombre requis de nœuds de stockage et de sites est disponible. Si deux nœuds de stockage ou plus ne sont pas disponibles dans un site, ou si un site n'est pas disponible, les modifications de ces paramètres peuvent ne pas être disponibles.

**Étapes**

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. Effectuez l'une des opérations suivantes :
   - Définissez une stratégie de compartiment en cochant la case **Activer la stratégie**. Saisissez ensuite une chaîne au format JSON valide.

     ${post_edited_translations.segment}

   - Modifiez une politique existante en modifiant la chaîne.
   - ${post_edited_translations.segment}

Pour obtenir des informations détaillées sur les politiques de compartiment, y compris la syntaxe du langage et des exemples, consultez "${post_edited_translations.segment}".

## Gérer la cohérence des buckets StorageGRID

Les valeurs de cohérence peuvent être utilisées pour spécifier la disponibilité des modifications des paramètres de compartiment, ainsi que pour assurer un équilibre entre la disponibilité des objets au sein d'un compartiment et la cohérence de ces objets sur différents Storage Nodes et sites. Vous pouvez modifier les valeurs de cohérence afin qu'elles diffèrent des valeurs par défaut pour permettre aux applications clientes de répondre à leurs besoins opérationnels.

**Avant de commencer**

- Vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui dispose de la "Gérer tous les compartiments ou autorisation d'accès Root". Ces autorisations remplacent les paramètres d'autorisation des politiques de groupe ou de compartiment.

**${post_edited_translations.segment}**

La cohérence du compartiment est utilisée pour déterminer la cohérence pour les applications clientes affectant les objets au sein de ce compartiment S3. En général, vous devriez utiliser la cohérence **Read-after-new-write** pour vos compartiments.

**${post_edited_translations.segment}**

Si la cohérence **Read-after-new-write** ne répond pas aux exigences de l'application cliente, vous pouvez la modifier en configurant la cohérence du compartiment ou en utilisant l' `Consistency-Control` header. L' `Consistency-Control` header remplace la cohérence du compartiment.

${post_edited_translations.segment}

**Étapes**

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

   ${post_edited_translations.segment}

3. Dans l'onglet **Options du seau**, sélectionnez l'** accordion.
4. ${post_edited_translations.segment}
   - **Tous** : Garantit le plus haut niveau de cohérence. Tous les nœuds reçoivent les données immédiatement, ou la requête échouera.
   - **Strong-global** : Garantit la cohérence de lecture après écriture pour toutes les requêtes client sur tous les sites.
   - **Site robuste** : Garantit la cohérence de lecture après écriture pour toutes les requêtes client au sein d'un site.
   - **Read-after-new-write** (par défaut) : assure la cohérence lecture-après-écriture pour les nouveaux objets et la cohérence à terme pour les mises à jour d'objets. Offre des garanties de haute disponibilité et de protection des données. Recommandé dans la plupart des cas.
   - **Disponible** : Garantit la cohérence éventuelle pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez cette fonctionnalité uniquement en cas de besoin (par exemple, pour un compartiment contenant des valeurs de journaux rarement lues, ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments S3 FabricPool.
5. Sélectionnez **Save changes**.

**${post_edited_translations.segment}**

${post_edited_translations.segment}

Les paramètres de compartiment suivants utilisent la cohérence **forte** par défaut. Si deux nœuds de stockage

ou plus ne sont pas disponibles sur un site, ou si un site n'est pas disponible, les modifications apportées à ces paramètres peuvent ne pas être disponibles.

- "Suppression en arrière-plan du compartiment vide"
- "${post_edited_translations.segment}"
- "Cycle de vie du bucket"
- "Politique de compartiment"
- "Étiquetage de compartiments"
- "${post_edited_translations.segment}"
- "Verrouillage d'objet S3"
- "Chiffrement du compartiment"

${post_edited_translations.segment}

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

- "Configuration des services de plateforme : notification, réplication ou intégration de recherche"
- "Configurer StorageGRID CORS pour les compartiments et les objets"
- Modifier la cohérence du compartiment

Si la cohérence par défaut utilisée lors de la modification des paramètres du bucket ne répond pas aux exigences de l'application cliente, vous pouvez modifier la cohérence en utilisant l'en-tête `Consistency-Control` pour "API REST S3" ou en utilisant les options `reducedConsistency` ou `force` dans "API de gestion des locataires".

## Activer ou désactiver les mises à jour du temps d'accès dans StorageGRID

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

Ces instructions s'appliquent uniquement aux systèmes StorageGRID qui incluent au moins une règle ILM utilisant l'option **Dernier temps d'accès** comme filtre avancé ou comme temps de référence. Vous pouvez ignorer ces instructions si votre système StorageGRID ne comporte pas de règle de ce type. Voir "Utilisez le temps d'accès dans les règles ILM" pour plus de détails.

**Avant de commencer**

- Vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui dispose de la "Gérer tous les compartiments ou autorisation d'accès Root". Ces autorisations remplacent les paramètres d'autorisation des politiques de groupe ou de compartiment.

**À propos de cette tâche**

Le **dernier temps d'accès** est l'une des options disponibles pour l'instruction de placement **Heure de référence** d'une règle ILM. Définir l'Heure de référence d'une règle sur Dernier temps d'accès permet aux administrateurs de la grille de spécifier que les objets soient placés dans certains emplacements de stockage en fonction du moment où ces objets ont été récupérés (lus ou consultés) pour la dernière fois.

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

- ${post_edited_translations.segment}
- Les objets qui n'ont pas été récupérés au cours du mois écoulé doivent être déplacés vers un site externe.

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

${post_edited_translations.segment}

${post_edited_translations.segment}

- Mettre à jour les objets avec de nouveaux horodatages
- ${post_edited_translations.segment}

Le tableau récapitule le comportement appliqué à tous les objets du compartiment lorsque le temps d'accès est désactivé ou activé.

| Type de demande | Comportement si le temps d'accès est désactivé (par défaut) | | ${post_edited_translations.segment} | |
|---|---|---|---|---|
| | ${post_edited_translations.segment} | Objet ajouté à la file d'attente d'évaluation ILM ? | ${post_edited_translations.segment} | Objet ajouté à la file d'attente d'évaluation ILM ? |
| ${post_edited_translations.segment} | Non | Non | Non | Non |
| Demande de récupération d'un objet, de sa liste de contrôle d'accès ou de ses métadonnées | Non | Non | Oui | Oui |
| Demande de mise à jour des métadonnées d'un objet | Oui | Oui | Oui | Oui |

| | | | | |
|---|---|---|---|---|
| Demande de liste d'objets ou de versions d'objets | Non | Non | Non | Non |
| Demande de copie d'un objet d'un bucket à un autre | • Non, pour la copie source<br>• Oui, pour la copie de destination | • Non, pour la copie source<br>• Oui, pour la copie de destination | • Oui, pour la copie source<br>• Oui, pour la copie de destination | • Oui, pour la copie source<br>• Oui, pour la copie de destination |
| Demande de finalisation d'un téléchargement en plusieurs parties | Oui, pour l'objet assemblé | Oui, pour l'objet assemblé | Oui, pour l'objet assemblé | Oui, pour l'objet assemblé |

**Étapes**

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

   ${post_edited_translations.segment}

3. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}
5. Sélectionnez **Save changes**.

## Modifier le versionnage des objets pour un compartiment S3 dans StorageGRID

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

**Avant de commencer**

- Vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui dispose de la "Gérer tous les compartiments ou autorisation d'accès Root". Ces autorisations remplacent les paramètres d'autorisation des politiques de groupe ou de compartiment.
- Vous avez vérifié que le nombre requis de nœuds de stockage et de sites est disponible. Si deux nœuds de stockage ou plus ne sont pas disponibles dans un site, ou si un site n'est pas disponible, les modifications de ces paramètres peuvent ne pas être disponibles.

**À propos de cette tâche**

Vous pouvez activer ou suspendre le versionnement d'objets pour un compartiment. Après avoir activé le versionnement pour un compartiment, celui-ci ne peut plus revenir à un état non versionné. Toutefois, vous pouvez suspendre le versionnement pour ce compartiment.

- ${post_edited_translations.segment}
- Activé : Le versionnage est activé

- Suspendu : le versionnage était précédemment activé et est suspendu

Pour plus d'informations, consultez les documents suivants :

- "Versionnage d'objets"
- "Règles et politiques ILM pour les objets versionnés S3 (Exemple 4)"
- "Comment les objets sont supprimés"

**Étapes**

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

   ${post_edited_translations.segment}

3. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}

   Le versionnage des objets doit rester activé pour un compartiment utilisé pour la réplication inter-grilles. Si S3 Object Lock ou la conformité héritée est activé, les options **Object versioning** sont désactivées.

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

5. Sélectionnez **Save changes**.

## Utilisez S3 Object Lock pour conserver les objets dans StorageGRID

Vous pouvez utiliser S3 Object Lock si les compartiments et les objets doivent se conformer aux exigences réglementaires en matière de conservation.

${post_edited_translations.segment}

**Qu'est-ce que le S3 Object Lock ?**

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

Lorsque le paramètre global de verrouillage des objets S3 est activé pour un système StorageGRID, un compte locataire S3 peut créer des compartiments avec ou sans verrouillage des objets S3 activé. Si un

compartiment a le verrouillage des objets S3 activé, le versionnage du compartiment est requis et est activé automatiquement.

**Un bucket sans S3 Object Lock** ne peut contenir que des objets sans paramètres de rétention spécifiés. Aucun objet ingéré ne disposera de paramètres de rétention.

**Un compartiment avec S3 Object Lock** peut contenir des objets avec ou sans paramètres de rétention définis par les applications clientes S3. Certains objets ingérés auront des paramètres de rétention.

Un compartiment avec S3 Object Lock et une rétention par défaut configurée peut contenir des objets chargés avec des paramètres de rétention spécifiés et de nouveaux objets sans paramètres de rétention. Les nouveaux objets utilisent le paramètre par défaut, car la rétention n'a pas été configurée au niveau de l'objet.

En pratique, tous les nouveaux objets ingérés se voient attribuer des paramètres de rétention lorsque la rétention par défaut est configurée. Les objets existants sans paramètres de rétention d'objet restent inchangés.

#### Modes de rétention

La fonctionnalité StorageGRID S3 Object Lock prend en charge deux modes de rétention pour appliquer différents niveaux de protection aux objets. Ces modes sont équivalents aux modes de rétention Amazon S3.

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

#### Paramètres de conservation des versions d'objets

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

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

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

Pour plus de détails sur les paramètres de l'objet, voir "Utilisez l'API REST S3 pour configurer S3 Object Lock".

#### Paramètre de rétention par défaut pour les compartiments

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

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

Les paramètres par défaut des compartiments s'appliquent uniquement aux nouveaux objets qui ne possèdent pas leurs propres paramètres de rétention. Les objets existants dans les compartiments ne sont pas affectés lorsque vous ajoutez ou modifiez ces paramètres par défaut.

Voir "Créez un compartiment S3" et "Mettre à jour la rétention par défaut de S3 Object Lock".

### ${post_edited_translations.segment}

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

**Administrateur de grille**

- Activez le paramètre de verrouillage global des objets S3 pour l'ensemble du système StorageGRID.
- Assurez-vous que les politiques de gestion du cycle de vie de l'information (ILM) sont *conformes*; c'est-à-dire qu'elles répondent aux "exigences relatives aux compartiments avec S3 Object Lock activé".
- Au besoin, autorisez un locataire à utiliser le mode Conformité comme mode de conservation. Sinon, seul le mode Gouvernance est autorisé.
- Au besoin, définissez une période de rétention maximale pour un locataire.

**Utilisateur locataire**

- Examinez les points à prendre en compte pour les compartiments et les objets avec S3 Object Lock.
- Au besoin, contactez l'administrateur de la grille pour activer le paramètre de verrouillage global S3 Object Lock et définir les autorisations.
- Créez des compartiments avec la fonctionnalité S3 Object Lock activée.
- Vous pouvez également configurer les paramètres de rétention par défaut d'un compartiment :
  - Mode de rétention par défaut : Gouvernance ou Conformité, si autorisé par l'administrateur du grid.
  - Durée de conservation par défaut : doit être inférieure ou égale à la durée de conservation maximale définie par l'administrateur du grid.
- Utilisez l'application cliente S3 pour ajouter des objets et, éventuellement, définir une durée de conservation spécifique à chaque objet :
  - Mode de conservation. Gouvernance ou conformité, si autorisé par l'administrateur du grid.
  - À conserver jusqu'à cette date : doit être inférieure ou égale à la durée de conservation maximale autorisée par l'administrateur du grid.

### Exigences pour les compartiments avec S3 Object Lock activé

- Si le paramètre global S3 Object Lock est activé pour le système StorageGRID, vous pouvez utiliser le Tenant Manager, l'API de gestion des locataires ou l'API REST S3 pour créer des compartiments avec S3 Object Lock activé.
- Si vous prévoyez d'utiliser S3 Object Lock, vous devez activer S3 Object Lock lors de la création du compartiment. Vous ne pouvez pas activer S3 Object Lock pour un compartiment existant.
- Lorsque le verrouillage d'objets S3 est activé pour un compartiment, StorageGRID active automatiquement le versionnage pour ce compartiment. Vous ne pouvez pas désactiver le verrouillage d'objets S3 ni suspendre le versionnage pour ce compartiment.
- Vous pouvez, si vous le souhaitez, spécifier un mode de conservation par défaut et une période de conservation pour chaque compartiment à l'aide du Tenant Manager, 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 n'ont pas 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 de son chargement.
- La configuration du cycle de vie des compartiments est prise en charge pour les compartiments avec S3 Object Lock activé.
- La réplication CloudMirror n'est pas prise en charge pour les compartiments avec le verrouillage d'objet S3 activé.

### Exigences relatives aux objets dans les compartiments avec S3 Object Lock activé

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

### Cycle de vie des objets dans les compartiments avec le S3 Object Lock activé

Chaque objet enregistré dans un compartiment avec le verrouillage d'objet S3 activé passe par les étapes suivantes :

1. **Ingestion d'objet**

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

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

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

2. **Conservation et suppression des objets**

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

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

#### Puis-je encore gérer les anciens compartiments conformes ?

La fonctionnalité S3 Object Lock remplace la fonctionnalité de conformité qui était disponible dans les versions précédentes de StorageGRID. 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 nouveaux compartiments conformes. Pour obtenir des instructions, consultez "Base de connaissances NetApp : Comment gérer les compartiments conformes hérités dans StorageGRID 11.5".

## Mettre à jour la rétention par défaut du verrouillage d'objet S3 dans StorageGRID

Si vous avez activé S3 Object Lock lors de la création du compartiment, vous pouvez modifier le compartiment pour changer les paramètres de rétention par défaut. Vous pouvez activer (ou désactiver) la rétention par défaut et définir un mode de rétention par défaut ainsi qu'une période de rétention.

#### Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui dispose de la "Gérer tous les compartiments ou autorisation d'accès Root". Ces autorisations remplacent les paramètres d'autorisation des politiques de groupe ou de compartiment.
- Le verrouillage d'objets S3 est activé globalement pour votre système StorageGRID, et vous avez activé le verrouillage d'objets S3 lors de la création du compartiment. Voir "${post_edited_translations.segment}".

#### Étapes

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

   ${post_edited_translations.segment}

3. ${post_edited_translations.segment}
4. Vous pouvez activer ou désactiver la **conservation par défaut** pour ce compartiment.

   ${post_edited_translations.segment}

5. ${post_edited_translations.segment}

| Mode de rétention par défaut | Description |
| --- | --- |
| Gouvernance | • Les utilisateurs disposant de l' `s3:BypassGovernanceRetention`autorisation peuvent utiliser l' `x-amz-bypass-governance-retention: true`en-tête de requête pour contourner les paramètres de rétention.<br>• Ces utilisateurs peuvent supprimer une version d'objet avant que sa date de conservation ne soit atteinte.<br>• Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet. |
| Conformité | • L'objet ne peut pas être supprimé tant que sa date de conservation n'est pas atteinte.<br>• La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être diminuée.<br>• La date de conservation de l'objet ne peut pas être supprimée avant que cette date ne soit atteinte.<br>**Remarque** : Votre administrateur de grille doit vous autoriser à utiliser le mode de conformité. |

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

   La **période de rétention par défaut** indique la durée pendant laquelle les nouveaux objets ajoutés à ce compartiment doivent être conservés, à compter de leur ingestion. Spécifiez une valeur inférieure ou égale à la période de rétention maximale pour le locataire, telle que définie par l'administrateur de la grille.

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

7. Sélectionnez **Save changes**.

## Configurer CORS pour les compartiments S3 dans StorageGRID

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

**Avant de commencer**

- Vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Pour les requêtes de configuration GET CORS, vous appartenez à un groupe d'utilisateurs qui possède la "Autorisation de gérer tous les compartiments ou d'afficher tous les compartiments". Ces autorisations prévalent sur les paramètres d'autorisation dans les politiques de groupe ou de compartiment.
- Pour les requêtes de configuration PUT CORS, vous appartenez à un groupe d'utilisateurs disposant de l'"${post_edited_translations.segment}". Cette autorisation remplace les paramètres d'autorisation définis dans les stratégies de groupe ou de compartiment.

- Le "Autorisation d'accès root" permet d'accéder à toutes les requêtes de configuration CORS.

**À propos de cette tâche**

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

### Activer CORS pour un bucket

**Étapes**

1. Utilisez un éditeur de texte pour créer le XML requis. Cet exemple montre le XML utilisé pour activer le CORS pour un compartiment S3. Plus précisément :
   - Autorise tout domaine à envoyer des requêtes GET au compartiment
   - Autorise uniquement le `http://www.example.com` domaine à envoyer des requêtes GET, POST et DELETE
   - Tous les en-têtes de requête sont autorisés

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

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

2. Sélectionnez **Afficher les compartiments** depuis le tableau de bord, ou sélectionnez **STOCKAGE (S3)** > **Compartiments**.
3. Sélectionnez le nom du compartiment dans le tableau.

   ${post_edited_translations.segment}

4. Dans l'onglet **Accès au compartiment**, sélectionnez l'accordéon **Partage de ressources entre origines (CORS)**.
5. Sélectionnez la case à cocher **Activer CORS**.

6. Collez le code XML de configuration CORS dans la zone de texte.
7. Sélectionnez **Save changes**.

#### Modifier les paramètres CORS

#### Étapes

1. Mettez à jour le fichier XML de configuration CORS dans la zone de texte, ou sélectionnez **Clear** pour recommencer.
2. Sélectionnez **Save changes**.

#### Désactiver le paramètre CORS

#### Étapes

1. Décochez la case **Enable CORS**.
2. Sélectionnez **Save changes**.

#### Informations connexes

"Configurer StorageGRID CORS pour une interface de gestion"

## Supprimer des objets d'un compartiment StorageGRID S3

${post_edited_translations.segment}

#### ${post_edited_translations.segment}

${post_edited_translations.segment}

- Lorsque vous supprimez des objets dans un bucket, StorageGRID supprime définitivement tous les objets et toutes les versions d'objet dans chaque bucket sélectionné, de tous les nœuds et sites de votre système StorageGRID. StorageGRID supprime également toutes les métadonnées associées à ces objets. Vous ne pourrez pas récupérer ces informations.
- ${post_edited_translations.segment}
- Si un compartiment comporte "Verrouillage d'objet S3 activé", il peut rester dans l'état **Deleting objects: read-only** pendant des *années*.

  ${post_edited_translations.segment}

- Pendant la suppression d'objets, l'état du compartiment est **Suppression d'objets : lecture seule**. Dans cet état, vous ne pouvez pas ajouter de nouveaux objets au compartiment.
- Lorsque tous les objets ont été supprimés, le compartiment reste à l'état de lecture seule. Vous pouvez effectuer l'une des actions suivantes :
  - Remettez le bucket en mode écriture et réutilisez-le pour de nouveaux objets
  - Supprimez le compartiment
  - Conservez le bucket en mode lecture seule pour réserver son nom pour une utilisation ultérieure
- Si le versionnage des objets est activé pour un compartiment, les marqueurs de suppression créés dans StorageGRID 11.8 ou une version ultérieure peuvent être supprimés à l'aide des opérations Delete objects in bucket.
- Si le versionnement d'objets est activé sur un compartiment, l'opération de suppression d'objets ne retirera

pas les marqueurs de suppression créés dans StorageGRID 11.7 ou version antérieure. Consultez les informations relatives à la suppression d'objets dans un compartiment dans "${post_edited_translations.segment}".

- Si vous utilisez "réplication inter-grilles", veuillez noter ce qui suit :
  - ${post_edited_translations.segment}
  - Si vous sélectionnez cette option pour le compartiment source, l'alerte **Échec de la réplication inter-grilles** sera 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 sur l'autre grille, "désactiver la réplication inter-grilles" pour ce compartiment avant de supprimer tous les objets du compartiment.

**Avant de commencer**

- Vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui dispose de "Autorisation d'accès root". Cette autorisation remplace les paramètres d'autorisation définis dans les stratégies de groupe ou de compartiment.

**Étapes**

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

   La page « Buckets » s'affiche et présente tous les buckets S3 existants.

2. ${post_edited_translations.segment}

   **Menu Actions**

   a. Cochez la case correspondant à chaque compartiment dont vous souhaitez supprimer des objets.

   b. ${post_edited_translations.segment}

   **Page de détails**

   a. Sélectionnez un nom de compartiment pour afficher ses détails.

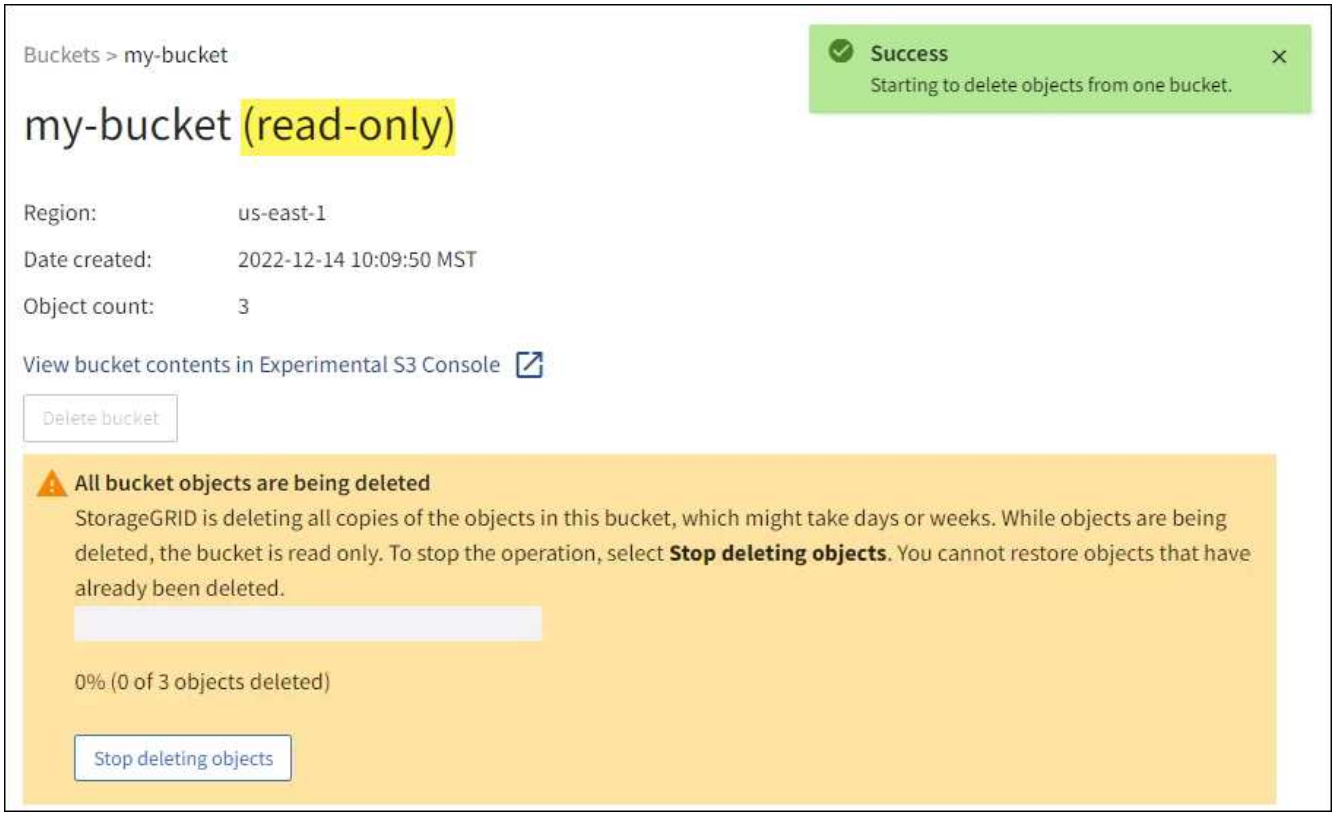
   b. Sélectionnez **Supprimer les objets du compartiment**.

3. Lorsque la boîte de dialogue de confirmation apparaît, vérifiez les détails, saisissez **Yes** et sélectionnez **OK**.

4. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

   - Une bannière jaune s'affiche sur la page de détails du compartiment. La barre de progression indique le pourcentage d'objets supprimés.
   - **(lecture seule)** apparaît après le nom du compartiment sur la page de détails du compartiment.
   - ${post_edited_translations.segment}

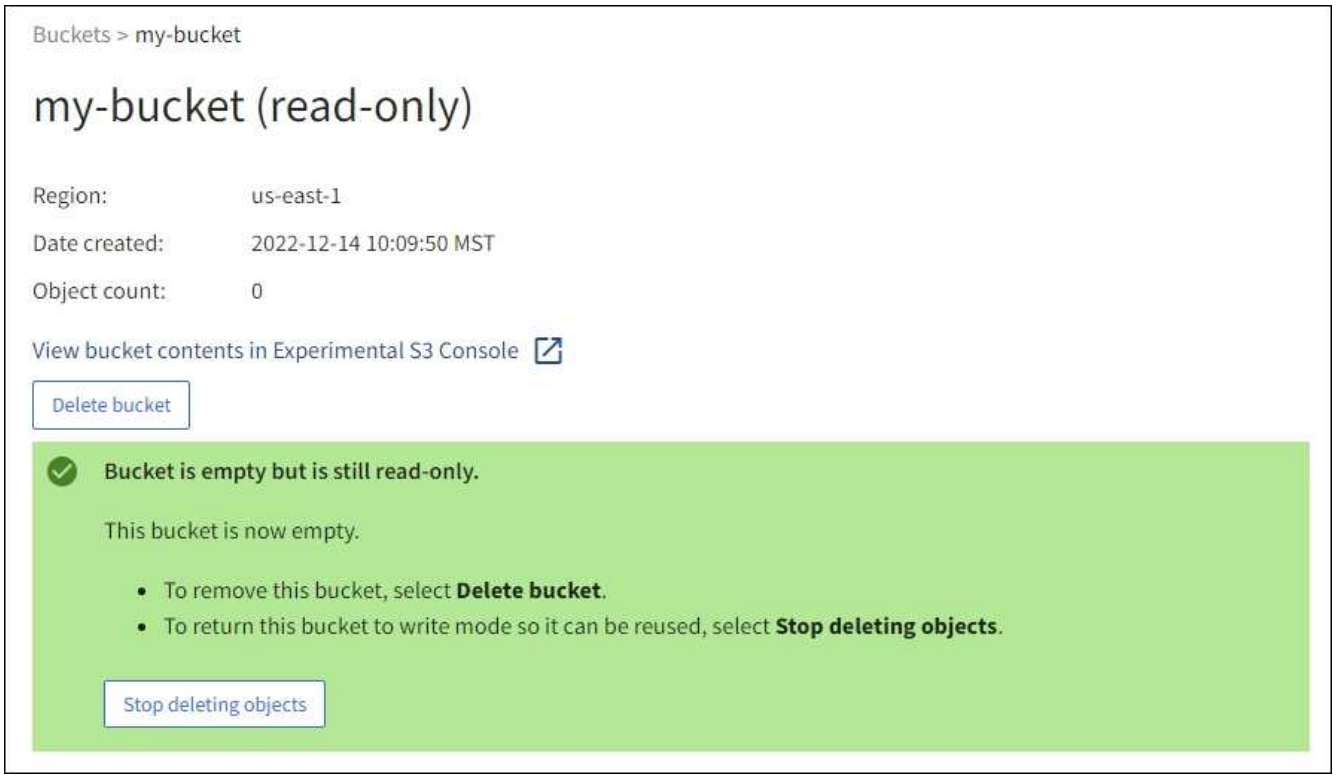



5. Au besoin, pendant que l'opération est en cours, sélectionnez **Arrêter la suppression d'objets** pour interrompre le processus. Ensuite, si vous le souhaitez, sélectionnez **Supprimer les objets du compartiment** pour reprendre le processus.

   ${post_edited_translations.segment}

6. Attendez que l'opération soit terminée.

   ${post_edited_translations.segment}




7. Effectuez l'une des opérations suivantes :
   - Quittez la page pour conserver le compartiment en mode lecture seule. Par exemple, vous pouvez conserver un compartiment vide en mode lecture seule pour réserver le nom du compartiment pour une utilisation ultérieure.
   - Supprimer le compartiment. Vous pouvez sélectionner **Supprimer le compartiment** pour supprimer un seul compartiment ou revenir à la page Compartiments et sélectionner **Actions** > **Supprimer les compartiments** pour en supprimer plusieurs.

     Si vous ne parvenez pas à supprimer un compartiment versionné après la suppression de tous les objets, il est possible que des marqueurs de suppression subsistent. Pour supprimer le compartiment, vous devez supprimer tous les marqueurs de suppression restants.

   - Remettez le compartiment en mode écriture et, si vous le souhaitez, réutilisez-le 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.

## Supprimer un compartiment StorageGRID S3

Vous pouvez utiliser le Tenant Manager pour supprimer un ou plusieurs compartiments S3 vides.

**Avant de commencer**

- Vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui dispose de la "Gérer tous les compartiments ou autorisation d'accès Root". Ces autorisations remplacent les paramètres d'autorisation des politiques de groupe ou de compartiment.

- Les compartiments que vous souhaitez supprimer sont vides. Si les compartiments que vous souhaitez supprimer ne sont *pas* vides, "supprimer des objets du compartiment".

**À propos de cette tâche**

Ces instructions décrivent comment supprimer un compartiment S3 à l'aide du Gestionnaire de locataires. Vous pouvez également supprimer des compartiments S3 à l'aide de "API de gestion des locataires" ou de "API REST S3".

Vous ne pouvez pas supprimer un compartiment S3 s'il contient des objets, des versions d'objets obsolètes ou des marqueurs de suppression. Pour plus d'informations sur la suppression des objets versionnés S3, consultez "Comment les objets sont supprimés".

**Étapes**

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

   La page « Buckets » s'affiche et présente tous les buckets S3 existants.

2. ${post_edited_translations.segment}

   **Menu Actions**

   a. Cochez la case correspondant à chaque compartiment que vous souhaitez supprimer.

   b. ${post_edited_translations.segment}

   **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 apparaît, sélectionnez **Oui**.

   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 "${post_edited_translations.segment}" avant de pouvoir supprimer le compartiment.

## Utilisez la console S3 dans StorageGRID

### ${post_edited_translations.segment}

${post_edited_translations.segment}

- Téléverser, télécharger, renommer, copier, déplacer et supprimer des objets
- Afficher, restaurer, télécharger et supprimer les versions d'objets
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

La console S3 offre une expérience utilisateur améliorée dans la plupart des cas. Elle n'est pas conçue pour remplacer les opérations de ligne de commande ou d'API dans toutes les situations.

Si l'utilisation de la console S3 entraîne des opérations trop longues (par exemple, minutes ou heures), envisagez :

- Réduction du nombre d'objets sélectionnés
- ${post_edited_translations.segment}

**Avant de commencer**

- Vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Si vous souhaitez gérer des objets, vous devez appartenir à un groupe d'utilisateurs disposant de l'autorisation d'accès Root. Alternativement, vous devez appartenir à un groupe d'utilisateurs disposant de l'autorisation Utiliser l'onglet Console S3 et soit de l'autorisation Afficher tous les compartiments, soit de l'autorisation Gérer tous les compartiments. Voir "${post_edited_translations.segment}".
- Une stratégie de groupe ou de compartiment S3 a été configurée pour l'utilisateur. Voir "Utilisez les stratégies d'accès aux compartiments et aux groupes".
- Vous connaissez l'identifiant de clé d'accès et la clé d'accès secrète de l'utilisateur. Vous disposez éventuellement d'un fichier `.csv` contenant ces informations. Voir le "${post_edited_translations.segment}".

**Étapes**

1. Sélectionnez **Storage** > **Buckets** > ***bucket name***.
2. Sélectionnez l'onglet Console S3.
3. Collez l'ID de la clé d'accès et la clé d'accès secrète dans les champs. Sinon, sélectionnez **Importer les clés d'accès** et sélectionnez votre fichier `.csv`.
4. Sélectionnez **Se connecter**.
5. Le tableau des objets du compartiment s'affiche. Vous pouvez gérer les objets selon vos besoins.

**Informations complémentaires**

- **Recherche par préfixe** : la fonction de recherche par préfixe recherche uniquement les objets qui commencent par un mot spécifique par rapport au dossier actuel. La recherche n'inclut pas les objets qui contiennent le mot ailleurs. Cette règle s'applique également aux objets situés dans des dossiers. Par exemple, une recherche de `folder1/folder2/somefile-` renverrait les objets qui se trouvent dans le dossier `folder1/folder2/` et commencent par le mot `somefile-`.
- **Glisser-déposer** : vous pouvez glisser-déposer des fichiers depuis le gestionnaire de fichiers de votre ordinateur vers S3 Console. Toutefois, vous ne pouvez pas importer de dossiers.
- ${post_edited_translations.segment}
- **Suppression définitive lorsque le versionnage du compartiment est désactivé** : Lorsque vous écrasez ou supprimez un objet dans un compartiment dont le versionnage est désactivé, l'opération est définitive. Voir "${post_edited_translations.segment}".

# ${post_edited_translations.segment}

# Services de la plateforme S3

## Découvrez les services de plateforme pour StorageGRID

Avant de mettre en œuvre les services de la plateforme, consultez la présentation et les points à prendre en compte pour utiliser ces services.

Pour plus d'informations sur S3, voir "Utilisez l'API REST S3".

### Aperçu des services de la plateforme

${post_edited_translations.segment}

Étant donné que l'emplacement cible des services de plateforme est généralement externe à votre déploiement StorageGRID, ces services vous offrent la puissance et la flexibilité liées à 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 à la fois la "Service CloudMirror" et la "notifications" sur un compartiment StorageGRID S3 afin de mettre en miroir des objets spécifiques vers Amazon Simple Storage Service (S3), tout en envoyant une notification pour chaque objet à une application de surveillance tierce afin de vous aider à suivre vos dépenses AWS.

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

### Comment les services de la plateforme sont configurés

Les services de la plateforme communiquent avec des points de terminaison externes que vous configurez à l'aide de l'"Gestionnaire de locataires" ou de l'"API de gestion des locataires". Chaque point de terminaison représente une destination externe, telle qu'un compartiment StorageGRID S3, un compartiment Amazon Web Services, un sujet Amazon SNS, un point de terminaison webhook ou un cluster Elasticsearch hébergé localement, sur AWS ou ailleurs.

Après avoir créé un point de terminaison externe, vous pouvez activer un service de plateforme pour un 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 plateforme que vous souhaitez configurer. Par exemple :

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

${post_edited_translations.segment}

| Service de plateforme | API REST S3 | Consultez |
| --- | --- | --- |
| Réplication CloudMirror | • GetBucketReplication<br>• PutBucketReplication | • "Réplication CloudMirror"<br>• "Opérations sur les compartiments" |
| Notifications | • GetBucketNotificationConfiguration<br>• PutBucketNotificationConfiguration | • "Notifications"<br>• "Opérations sur les compartiments" |
| Intégration de la recherche | • Obtenir la configuration de notification des métadonnées du bucket<br>• Configuration de notification des métadonnées du compartiment PUT | • "Intégration de la recherche"<br>• "Opérations personnalisées StorageGRID" |

**Considérations relatives à l'utilisation des services de plateforme**

| ${post_edited_translations.segment} | Détails |
| --- | --- |
| Surveillance du point de terminaison de destination | Vous devez surveiller la disponibilité de chaque point de terminaison de destination. Si la connectivité au point de terminaison de destination est perdue pendant une période prolongée et qu'un important arriéré de requêtes existe, les requêtes client supplémentaires (telles que les requêtes PUT) adressées à StorageGRID échoueront. Vous devez réessayer ces requêtes ayant échoué lorsque le point de terminaison devient accessible. |
| Limitation du débit du point de terminaison de destination | Le logiciel StorageGRID peut limiter le nombre de requêtes S3 entrantes pour un compartiment si le débit d'envoi des requêtes dépasse le débit auquel le point de terminaison de destination peut les recevoir. La limitation ne se produit que lorsqu'il y a un retard d'envoi des requêtes en attente vers le point de terminaison de destination.<br><br>Le seul effet visible est un allongement du temps d'exécution des requêtes S3 entrantes. Si vous constatez un ralentissement significatif des performances, vous devez réduire le débit d'ingestion ou utiliser un point de terminaison offrant une capacité supérieure. Si le nombre de requêtes en attente continue d'augmenter, les opérations S3 côté client (telles que les requêtes PUT) finiront par échouer.<br><br>CloudMirror Les requêtes sont plus susceptibles d'être affectées par les performances du point de terminaison de destination, car elles impliquent généralement plus de transfert de données que les requêtes d'intégration de recherche ou de notification d'événements. |

| ${post_edited_translations.segment} | Détails |
| --- | --- |
| Garanties de commande | StorageGRID garantit l'ordre des opérations sur un objet au sein d'un site. Tant que toutes les opérations sur un objet sont effectuées au sein du même site, l'état final de l'objet (pour la réplication) sera toujours égal à l'état dans StorageGRID.<br><br>StorageGRID s'efforce d'ordonner les requêtes lors d'opérations effectuées sur plusieurs sites StorageGRID. Par exemple, si vous écrivez initialement un objet sur le site A, puis que vous écrasez ultérieurement le même objet sur le site B, l'objet final répliqué par CloudMirror dans le compartiment de destination n'est pas garanti d'être la version la plus récente. |
| Suppressions d'objets pilotées par ILM | Pour correspondre au comportement de suppression d'AWS CRR et d'Amazon Simple Notification Service, 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 requête CloudMirror ou de notification d'événement n'est envoyée si une règle ILM supprime un objet après 14 jours.<br><br>En revanche, les demandes d'intégration de recherche sont envoyées lorsque des objets sont supprimés en raison de l'ILM. |
| Utilisation des points de terminaison Kafka | Pour les points de terminaison Kafka, le protocole Mutual TLS n'est pas pris en charge. Par conséquent, si vous avez `ssl.client.auth` défini sur `required` dans la configuration de votre broker Kafka, cela peut entraîner des problèmes de configuration des points de terminaison Kafka.<br><br>L'authentification des points de terminaison Kafka utilise les types d'authentification suivants. Ces types diffèrent de ceux utilisés pour l'authentification d'autres points de terminaison, tels que Amazon SNS, et nécessitent des identifiants de nom d'utilisateur et de mot de passe.<br><br>• SASL/PLAIN<br>• SASL/SCRAM-SHA-256<br>• ${post_edited_translations.segment}<br><br>${post_edited_translations.segment} |

**Considérations relatives à l'utilisation du service de réplication CloudMirror**

| ${post_edited_translations.segment} | Détails |
| --- | --- |
| État de la réplication | StorageGRID ne prend pas en charge l' `x-amz-replication-status`en-tête. |

| ${post_edited_translations.segment} | Détails |
| --- | --- |
| Taille de l'objet | La taille maximale des objets pouvant être répliqués dans un compartiment de destination par le service de réplication CloudMirror est de 5 Tio, ce qui correspond à la taille maximale des objets *pris en charge*.<br><br>**Note** : la taille maximale *recommandée* pour une opération PutObject unique est de 5 Gio (5 368 709 120 octets). Si vous avez des objets d'une taille supérieure à 5 Gio, utilisez plutôt le chargement partitionné. |
| Gestion des versions de compartiments et identifiants de version | ${post_edited_translations.segment}<br><br>Lors de l'utilisation du versionnage, veuillez noter que l'ordre des versions d'objets dans le compartiment de destination est déterminé au mieux et n'est pas garanti par le CloudMirror service, en raison des limitations du protocole S3.<br><br>${post_edited_translations.segment} |
| ${post_edited_translations.segment} | Le service CloudMirror ne réplique pas les requêtes PutObjectTagging ou DeleteObjectTagging qui fournissent un ID de version, en raison des limites du protocole S3. Les ID de version de la source et de la destination n'étant pas liés, il est impossible de garantir qu'une mise à jour de balise pour un ID de version spécifique sera répliquée.<br><br>En revanche, le service CloudMirror réplique les requêtes PutObjectTagging ou DeleteObjectTagging qui ne spécifient pas d'identifiant de version. Ces requêtes mettent à jour les balises pour la clé la plus récente (ou la version la plus récente si le compartiment est versionné). Les ingestions normales avec balises (et non des mises à jour de balises) sont également répliquées. |
| Téléversements en plusieurs parties et `ETag` valeurs | Lors de la duplication d'objets téléchargés en plusieurs parties, le CloudMirror service ne conserve pas les différentes parties. Par conséquent, la valeur `ETag` de l'objet dupliqué sera différente de la valeur `ETag` de l'objet original. |
| Objets chiffrés 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 requête inclut les en-têtes SSE-C, l'opération échoue. |
| Compartiment avec S3 Object Lock activé | ${post_edited_translations.segment} |

#### Découvrez le service de réplication CloudMirror StorageGRID

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

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

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

#### CloudMirror et ILM

CloudMirror replication fonctionne indépendamment des politiques ILM actives de la grille. Le service CloudMirror réplique les objets dès qu'ils sont stockés dans le compartiment source et les transfère vers le compartiment de destination dès que possible. La livraison des objets répliqués est déclenchée lorsque l'ingestion de l'objet réussit.

#### CloudMirror et réplication inter-grilles

La réplication CloudMirror présente des similitudes et des différences importantes avec la fonctionnalité de réplication inter-grilles. Consultez "Comparez la réplication inter-grilles et la réplication CloudMirror".

#### CloudMirror et les compartiments S3

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

### Buckets existants

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

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

### ${post_edited_translations.segment}

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

### ${post_edited_translations.segment}

Vous pouvez configurer la réplication CloudMirror sur des compartiments versionnés ou non versionnés. Les compartiments de destination peuvent être versionnés ou non versionnés. Vous pouvez utiliser n'importe quelle combinaison de compartiments versionnés et non versionnés. Par exemple, vous pouvez spécifier un compartiment versionné comme destination pour un compartiment source non versionné, ou inversement. Vous pouvez également répliquer entre des compartiments non versionnés.

#### ${post_edited_translations.segment}

### Comportement de suppression

Est identique au comportement de suppression du service Amazon S3, Cross-Region Replication (CRR). La suppression d'un objet dans un compartiment source ne supprime jamais un objet répliqué dans la destination. Si les compartiments source et de destination sont tous deux versionnés, le marqueur de suppression est répliqué. Si le compartiment de destination n'est pas versionné, la suppression d'un objet dans le compartiment source ne réplique pas le marqueur de suppression dans le compartiment de destination et ne supprime pas l'objet de destination.

**${post_edited_translations.segment}**

Lors de la réplication des objets vers le compartiment de destination, StorageGRID les marque comme « répliques ». Un compartiment StorageGRID de destination ne répliquera pas à nouveau les objets marqués comme répliques, vous protégeant ainsi des boucles de réplication accidentelles. Ce marquage des répliques est interne à StorageGRID et ne vous empêche pas de tirer parti d'AWS CRR lorsque vous utilisez un compartiment Amazon S3 comme destination.

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

**Événements dans le compartiment de destination**

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 suite aux opérations effectuées pour garantir la réussite de la livraison. Dans de rares cas, lorsqu'un même objet est mis à jour simultanément depuis deux sites StorageGRID ou plus, l'ordre des opérations sur le compartiment de destination peut ne pas correspondre à l'ordre des événements sur le compartiment source.

### Découvrez les notifications d'événements StorageGRID pour les compartiments S3

Vous pouvez activer la notification d'événements pour un compartiment S3 si vous souhaitez que StorageGRID envoie des notifications concernant des événements spécifiques à un cluster Kafka de destination, un point de terminaison webhook ou Amazon Simple Notification Service.

Par exemple, vous pouvez configurer des alertes pour qu'elles soient envoyées aux administrateurs concernant chaque objet ajouté à un compartiment, où les objets représentent des fichiers journaux associés à un événement système critique.

Les notifications d'événements sont créées dans le compartiment source, conformément à la configuration des notifications, et sont transmises à la destination. Si un événement associé à un objet réussit, une notification concernant cet événement est créée et mise en file d'attente pour la livraison.

L'unicité et l'ordre des notifications ne sont pas garantis. Plusieurs notifications d'un même événement peuvent être envoyées à destination suite aux opérations mises en œuvre pour assurer la réussite de la livraison. De plus, la livraison étant asynchrone, l'ordre temporel des notifications à destination n'est pas garanti pour correspondre à l'ordre des événements sur le compartiment source, en particulier pour les opérations provenant de différents sites StorageGRID. Vous pouvez utiliser la clé `sequencer` dans le message d'événement pour déterminer l'ordre des événements pour un objet particulier, comme décrit dans la documentation Amazon S3.

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

- ${post_edited_translations.segment}
  - s3:ObjectCreated:
  - s3:ObjectCreated:Put
  - s3:ObjectCreated:Post
  - s3:ObjectCreated:Copie
  - s3:ObjectCreated:CompleteMultipartUpload
  - s3:ObjectRemoved:

- s3:ObjectRemoved:Supprimer
- s3:ObjectRemoved:DeleteMarkerCreated
- s3:ObjectRestore:Post

- Les notifications d'événements envoyées depuis StorageGRID utilisent le format JSON standard, mais n'incluent pas certaines clés et utilisent des valeurs spécifiques pour d'autres, comme indiqué dans le tableau :

| Nom de la clé | Valeur StorageGRID |
|---|---|
| eventSource | `sgws:s3` |
| awsRegion | *non inclus* |
| ${post_edited_translations.segment} | *non inclus* |
| arn | `urn:sgws:s3:::bucket_name` |

**Découvrez le service d'intégration de recherche StorageGRID**

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

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

Par exemple, vous pouvez configurer vos compartiments pour envoyer les métadonnées des objets S3 à un service Elasticsearch distant. Vous pouvez ensuite utiliser Elasticsearch pour effectuer des recherches dans vos compartiments et réaliser des analyses sophistiquées des tendances présentes dans les métadonnées de vos objets.

${post_edited_translations.segment}

> Étant donné que le service d'intégration de recherche entraîne l'envoi des métadonnées des objets vers une destination, son fichier XML de configuration est appelé « *metadata* notification configuration XML ». Ce fichier XML de configuration est différent du « notification configuration XML » utilisé pour activer les notifications *event*.

**${post_edited_translations.segment}**

Vous pouvez activer le service d'intégration de recherche pour tout compartiment, versionné ou non. L'intégration de recherche est configurée en associant une configuration XML de notification des métadonnées au compartiment, qui spécifie les objets concernés et la destination des métadonnées des objets.

Les notifications de métadonnées sont générées sous la forme d'un document JSON nommé avec le nom du

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 et métadonnées utilisateur de l'objet.

> Pour les balises et les métadonnées utilisateur, StorageGRID transmet les dates et les nombres à Elasticsearch sous forme de chaînes de caractères ou de notifications d'événements S3. Pour configurer Elasticsearch afin qu'il interprète ces chaînes comme des dates ou des nombres, suivez les instructions Elasticsearch pour le mappage dynamique des champs et le mappage des formats de date. Vous devez activer le mappage dynamique des champs sur l'index avant de configurer le service d'intégration de recherche. Après l'indexation d'un document, vous ne pouvez plus modifier les types de champs du document dans l'index.

**${post_edited_translations.segment}**

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

- Un objet est créé.
- ${post_edited_translations.segment}
- Les métadonnées ou étiquettes des objets sont ajoutées, mises à jour ou supprimées. L'ensemble complet des métadonnées et des étiquettes est toujours envoyé lors d'une mise à jour, pas seulement les valeurs modifiées.

Après avoir ajouté un fichier 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, ses métadonnées utilisateur ou ses balises. Cependant, aucune notification n'est envoyée pour les objets qui étaient déjà présents dans le compartiment. Pour garantir que les métadonnées des objets pour tous les objets du compartiment sont envoyées à la destination, vous devez effectuer l'une des actions suivantes :

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

**${post_edited_translations.segment}**

Le service d'intégration de recherche StorageGRID prend en charge un cluster Elasticsearch comme destination. Comme pour les autres services de plateforme, la destination est spécifiée dans le point de terminaison dont l'URN est utilisé dans le XML de configuration du service. Utilisez le "Outil NetApp Interoperability Matrix Tool" pour déterminer les versions d'Elasticsearch prises en charge.

## Gérer les points de terminaison des services de plateforme

### Configurez les points de terminaison des services de plateforme dans StorageGRID

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

L'accès aux services de la plateforme est activé pour chaque locataire par un administrateur StorageGRID. Pour créer ou utiliser un point de terminaison de services de plateforme, vous devez être un utilisateur locataire disposant de l'autorisation Gérer les points de terminaison ou d'un accès Root, dans une grille dont le réseau a été configuré pour permettre aux nœuds de stockage d'accéder aux ressources de points de

terminaison externes. Pour un seul locataire, vous pouvez configurer un maximum de 500 points de terminaison de services de plateforme. Contactez votre administrateur StorageGRID pour plus d'informations.

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

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

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

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

Vous pouvez utiliser le même point de terminaison comme destination pour plusieurs compartiments sources. Par exemple, vous pouvez configurer plusieurs compartiments sources pour envoyer les métadonnées des objets au même point de terminaison d'intégration de recherche afin de pouvoir effectuer des recherches sur plusieurs compartiments. Vous pouvez également configurer un compartiment source pour utiliser plusieurs points de terminaison comme cibles, ce qui vous permet, par exemple, d'envoyer des notifications concernant la création d'objets à une rubrique Amazon Simple Notification Service (Amazon SNS) et des notifications concernant la suppression d'objets à une seconde rubrique Amazon SNS.

#### Points d'extrémité pour la réplication CloudMirror

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

#### Points de terminaison pour les notifications

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

Pour les points de terminaison Kafka, l'authentification TLS mutuelle n'est pas prise en charge. Par conséquent, si vous avez `ssl.client.auth` défini sur `required` dans la configuration de votre broker Kafka, cela peut entraîner des problèmes de configuration des points de terminaison Kafka.

#### Points de terminaison pour le service d'intégration de recherche

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

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

**Informations connexes**

"Administrer StorageGRID"

#### Spécifiez un URN pour un point de terminaison des services de plateforme StorageGRID

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

StorageGRID valide les points de terminaison des services de plateforme lors de leur création. Avant de créer un point de terminaison des services de plateforme, vérifiez que la ressource spécifiée dans le point de terminaison existe et qu'elle est accessible.

##### ${post_edited_translations.segment}

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

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

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

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

| Service | Type |
|---|---|
| Réplication CloudMirror | `s3` |
| Notifications | `sns`, `kafka`, ou `webhook` |
| Intégration de la recherche | `es` |

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

Pour la plupart des points de terminaison, l'élément final de l'URN identifie la ressource cible spécifique à l'URI de destination, par exemple, `sns-topic-name`.

Pour les points de terminaison webhook, la ressource cible est l'URI de destination elle-même.

| Service | ${post_edited_translations.segment} |
|---|---|
| Réplication CloudMirror | `bucket-name` |
| Notifications | `sns-topic-name` ou `kafka-topic-name`<br><br>${post_edited_translations.segment} |

| Service | ${post_edited_translations.segment} |
| --- | --- |
| Intégration de la recherche | `domain-name/index-name/type-name`<br><br>**Remarque :** Si le cluster Elasticsearch n'est **pas** configuré pour créer automatiquement les index, vous devez créer l'index manuellement avant de créer le point de terminaison. |

#### URNs pour les services hébergés sur AWS et GCP

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

- Réplication CloudMirror :

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

- ${post_edited_translations.segment}

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

- Intégration de la recherche :

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

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

#### URN pour les services hébergés localement

Lorsque vous utilisez des services hébergés localement plutôt que des services cloud, vous pouvez spécifier l'URN de toute manière qui crée une URN valide et unique, à condition que l'URN inclue les éléments requis en troisième et dernière position. Vous pouvez laisser les éléments indiqués comme optionnels vides, ou les spécifier de toute manière qui vous aide à identifier la ressource et à rendre l'URN unique. Par exemple :

- Réplication CloudMirror :

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

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

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

- ${post_edited_translations.segment}

  Spécifiez un point de terminaison Amazon Simple Notification Service :

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

  Spécifiez un point de terminaison Kafka :

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

  ${post_edited_translations.segment}

  ```
  urn:mysite:webhook:optional:optional:webhook-name
  ```

- Intégration de la recherche :

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

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

**Créer un point de terminaison de services de plateforme StorageGRID**

## ${post_edited_translations.segment}

**Avant de commencer**

- Vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- ${post_edited_translations.segment}
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérer les autorisations d'accès aux points de terminaison ou à l'accès root".
- La ressource référencée par le point de terminaison des services de plateforme a été créée :
  - CloudMirror replication : compartiment S3
  - ${post_edited_translations.segment}
  - ${post_edited_translations.segment}
- Vous disposez des informations concernant la ressource de destination :
  - ${post_edited_translations.segment}

> 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 que vous devez saisir.

◦ ${post_edited_translations.segment}

"Spécifiez l'URN du point de terminaison des services de plateforme"

◦ Informations d'authentification (si nécessaire) :

**${post_edited_translations.segment}**

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

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

**CloudMirror endpoints de réplication**

Pour les points de terminaison de réplication CloudMirror, vous pouvez utiliser les identifiants suivants :

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

**${post_edited_translations.segment}**

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

- ${post_edited_translations.segment}

**${post_edited_translations.segment}**

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

◦ Certificat de sécurité (si une vérification du certificat est requise)

- ${post_edited_translations.segment}

**Étapes**

1. Sélectionnez **STOCKAGE (S3)** > **Points de terminaison des services de plateforme**. La page Points de terminaison des services de plateforme s'affiche.
2. Sélectionnez **Créer un point de terminaison**.
3. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

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

   Utilisez l'un des formats suivants :

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

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

- Port 443 pour les URI HTTPS et port 80 pour les URI HTTP (la plupart des points de terminaison)
- ${post_edited_translations.segment}

${post_edited_translations.segment}

```
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 (HA) StorageGRID, et `10443` représente le port défini dans le point de terminaison de l'équilibreur de charge.

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

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

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

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

5. ${post_edited_translations.segment}

> Vous ne pouvez pas modifier l'URN d'un point de terminaison après sa création.

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

> Si vous souhaitez une authentification pour les points de terminaison de webhook, configurez Mutual Transport Layer Security (mTLS) dans Étape 9.

**${post_edited_translations.segment}**

${post_edited_translations.segment}

${post_edited_translations.segment}

| Type d'authentification | Description | Informations d'identification |
|---|---|---|
| Anonyme | Fournit un accès anonyme à la destination. Fonctionne uniquement pour les endpoints dont la sécurité est désactivée. | ${post_edited_translations.segment} |
| ${post_edited_translations.segment} | ${post_edited_translations.segment} | • ID de la clé d'accès<br>• ${post_edited_translations.segment} |
| ${post_edited_translations.segment} | Utilise un nom d'utilisateur et un mot de passe pour authentifier les connexions à la destination. | • Nom d'utilisateur<br>• Mot de passe |

**CloudMirror endpoints de réplication**

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

${post_edited_translations.segment}

| Type d'authentification | Description | Informations d'identification |
|---|---|---|
| Anonyme | Fournit un accès anonyme à la destination. Fonctionne uniquement pour les endpoints dont la sécurité est désactivée. | ${post_edited_translations.segment} |
| ${post_edited_translations.segment} | ${post_edited_translations.segment} | • ID de la clé d'accès<br>• ${post_edited_translations.segment} |

| Type d'authentification | Description | Informations d'identification |
| --- | --- | --- |
| ${post_edited_translations.segment} | Utilise des certificats et des clés pour authentifier les connexions à la destination. | • ${post_edited_translations.segment}<br>• Certificat CA du serveur (téléversement de fichier PEM)<br>• ${post_edited_translations.segment}<br>• ${post_edited_translations.segment}<br>• Phrase secrète de la clé privée du client (facultatif) |

**${post_edited_translations.segment}**

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

${post_edited_translations.segment}

| Type d'authentification | Description | Informations d'identification |
| --- | --- | --- |
| Anonyme | Fournit un accès anonyme à la destination. Fonctionne uniquement pour les endpoints dont la sécurité est désactivée. | ${post_edited_translations.segment} |
| ${post_edited_translations.segment} | ${post_edited_translations.segment} | • ID de la clé d'accès<br>• ${post_edited_translations.segment} |

**${post_edited_translations.segment}**

Saisissez ou téléchargez les identifiants pour un point de terminaison Kafka.

${post_edited_translations.segment}

| Type d'authentification | Description | Informations d'identification |
| --- | --- | --- |
| Anonyme | Fournit un accès anonyme à la destination. Fonctionne uniquement pour les endpoints dont la sécurité est désactivée. | ${post_edited_translations.segment} |

| Type d'authentification | Description | Informations d'identification |
| --- | --- | --- |
| SASL/PLAIN | Utilise un nom d'utilisateur et un mot de passe en clair pour authentifier les connexions à la destination. | • Nom d'utilisateur<br>• Mot de passe |
| SASL/SCRAM-SHA-256 | Utilise un nom d'utilisateur et un mot de passe avec un protocole de défi-réponse et le hachage SHA-256 pour authentifier les connexions à la destination. | • Nom d'utilisateur<br>• Mot de passe |
| ${post_edited_translations.segment} | ${post_edited_translations.segment} | • Nom d'utilisateur<br>• Mot de passe |

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

8. Sélectionnez **Continue**.
9. Sélectionnez un bouton radio pour **Vérifier les certificats** afin de choisir comment la connexion TLS au point de terminaison est vérifiée.

**${post_edited_translations.segment}**

Vérifiez la connexion TLS pour l'intégration Search, la réplication CloudMirror, Amazon SNS ou les points de terminaison Kafka.

| Type de vérification de certificat | Description |
|---|---|
| TLS | ${post_edited_translations.segment} |
| Désactivées | La vérification du certificat est désactivée. Cette option n'est pas sécurisée. |
| Utilisez un certificat d'autorité de certification personnalisé | Le certificat d'autorité de certification personnalisé est utilisé pour vérifier l'identité du serveur lors de la connexion au point de terminaison. |
| ${post_edited_translations.segment} | Utilisez le certificat d'autorité de certification Grid par défaut installé sur le système d'exploitation pour sécuriser les connexions. |

**Points de terminaison Webhook uniquement**

Vérifiez la connexion TLS pour les points de terminaison webhook.

| Type de vérification de certificat | Description |
|---|---|
| TLS | ${post_edited_translations.segment} |
| mTLS | ${post_edited_translations.segment} |
| Désactivées | La vérification du certificat est désactivée. Cette option n'est pas sécurisée. |
| Utilisez un certificat d'autorité de certification personnalisé | Le certificat d'autorité de certification personnalisé est utilisé pour vérifier l'identité du serveur lors de la connexion au point de terminaison. |

${post_edited_translations.segment}

| Type de vérification de certificat | Description |
|---|---|
| ${post_edited_translations.segment} | Désactive la vérification du certificat du serveur, ce qui signifie que l'identité du serveur n'est pas vérifiée. Cette option n'est pas sécurisée. |
| Certificat client | ${post_edited_translations.segment} |

| Type de vérification de certificat | Description |
| --- | --- |
| Clé privée du client | La clé privée du certificat client. Si elle est chiffrée, elle doit utiliser le format traditionnel PKCS #1 (le format PKCS #8 n'est pas pris en charge). |
| Phrase secrète de la clé privée du client | La phrase de passe pour déchiffrer la clé privée du client. Si la clé privée n'est pas chiffrée, laissez ce champ vide. |

10. Sélectionnez **Tester et créer un point de terminaison**.
    - Un message de confirmation s'affiche si le point de terminaison est accessible avec les informations d'identification spécifiées. La connexion au point de terminaison est validée depuis un nœud sur chaque site.
    - Un message d'erreur s'affiche si la validation du point de terminaison échoue. Si vous devez modifier le point de terminaison pour corriger l'erreur, sélectionnez **Retourner aux détails du point de terminaison** et mettez à jour les informations. Ensuite, sélectionnez **Tester et créer le point de terminaison**.

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

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

**Informations connexes**

- "Spécifiez l'URN du point de terminaison des services de plateforme"
- "Configurer la réplication CloudMirror"
- "Configurer les notifications d'événements"
- "${post_edited_translations.segment}"

### Tester la connexion pour un point de terminaison des services de plateforme StorageGRID

${post_edited_translations.segment}

**Avant de commencer**

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

**À propos de cette tâche**

StorageGRID ne vérifie pas que les identifiants disposent des autorisations appropriées.

**Étapes**

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

   La page des points de terminaison des services de la plateforme s'affiche et présente la liste des points de

terminaison des services de la plateforme déjà configurés.

2. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

3. Sélectionnez **Test connection**.
   - Un message de confirmation s'affiche si le point de terminaison est accessible avec les informations d'identification spécifiées. La connexion au point de terminaison est validée depuis un nœud sur chaque site.
   - Un message d'erreur s'affiche si la validation du point de terminaison échoue. Si vous devez modifier le point de terminaison pour corriger l'erreur, sélectionnez **Configuration** et mettez à jour les informations. Ensuite, sélectionnez **Tester et enregistrer les modifications**.

#### Modifier un point de terminaison de services de plateforme dans StorageGRID

Vous pouvez modifier la configuration d'un point de terminaison de services de plateforme pour en changer le nom, l'URI ou d'autres détails. Par exemple, vous pourriez avoir besoin de mettre à jour des informations d'identification expirées ou de modifier l'URI pour qu'elle pointe vers un index Elasticsearch de secours en cas de basculement. Vous ne pouvez pas modifier l'URN d'un point de terminaison de services de plateforme.

**Avant de commencer**

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

**Étapes**

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

   La page des points de terminaison des services de la plateforme s'affiche et présente la liste des points de terminaison des services de la plateforme déjà configurés.

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

   ${post_edited_translations.segment}

3. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}

   > Vous ne pouvez pas modifier l'URN d'un point de terminaison après sa création.

   a. Pour modifier le nom d'affichage du point de terminaison, sélectionnez l'icône de modification .
   b. ${post_edited_translations.segment}
   c. Modifiez le type d'authentification si nécessaire.
      - Pour l'authentification par clé d'accès, modifiez la clé si nécessaire en sélectionnant **Modifier la clé S3** et en collant un nouvel ID de clé d'accès et une nouvelle clé d'accès secrète. Si vous devez annuler vos modifications, sélectionnez **Annuler la modification de la clé S3**.
      - Pour l'authentification CAP (C2S Access Portal), modifiez l'URL des informations d'identification

temporaires ou la phrase secrète facultative de la clé privée du client et téléchargez de nouveaux fichiers de certificat et de clé selon les besoins.

> La clé privée du client doit être au format chiffré OpenSSL ou au format de clé privée non chiffrée.

d. ${post_edited_translations.segment}

5. Sélectionnez **Tester et enregistrer les modifications**.
   - Un message de réussite s'affiche si le point de terminaison peut être atteint à l'aide des identifiants spécifiés. La connexion au point de terminaison est vérifiée depuis un nœud sur chaque site.
   - Un message d'erreur s'affiche si la validation du point de terminaison échoue. Modifiez le point de terminaison pour corriger l'erreur, puis sélectionnez **Tester et enregistrer les modifications**.

#### Supprimer un point de terminaison des services de plateforme StorageGRID

${post_edited_translations.segment}

**Avant de commencer**

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

**Étapes**

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

   La page des points de terminaison des services de la plateforme s'affiche et présente la liste des points de terminaison des services de la plateforme déjà configurés.

2. Cochez la case correspondant à chaque point de terminaison que vous souhaitez supprimer.

   > Si vous supprimez un point de terminaison de services de plateforme en cours d'utilisation, le service de plateforme associé sera désactivé pour tous les compartiments qui utilisent ce point de terminaison. Toutes les requêtes qui n'ont pas encore été terminées seront abandonnées. Les nouvelles requêtes continueront d'être générées jusqu'à ce que vous modifiez la configuration de votre compartiment pour ne plus faire référence à l'URN supprimé. StorageGRID signalera ces requêtes comme des erreurs irrécupérables.

3. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

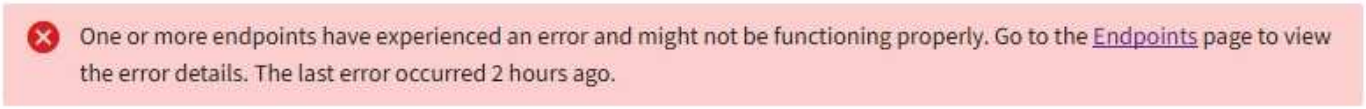
4. ${post_edited_translations.segment}

#### Dépanner les erreurs de point de terminaison des services de plateforme StorageGRID

Si une erreur se produit lorsque StorageGRID tente de communiquer avec un point de terminaison des services de plateforme, un message s'affiche sur le tableau de bord. Sur la page Points de terminaison des services de plateforme, la colonne Dernière erreur indique depuis combien de temps l'erreur s'est produite. Aucune erreur ne s'affiche si les autorisations associées aux identifiants d'un point de terminaison sont incorrectes.

#### ${post_edited_translations.segment}

Si des erreurs de point de terminaison des services de plateforme se sont produites au cours des 7 derniers jours, le tableau de bord du Gestionnaire de locataires affiche un message d'alerte. Vous pouvez accéder à la page Points de terminaison des services de plateforme pour obtenir plus de détails sur l'erreur.




La même erreur que celle qui s'affiche sur le tableau de bord apparaît également en haut de la page des points de terminaison des services de plateforme. Pour afficher un message d'erreur plus détaillé :

**Étapes**

1. ${post_edited_translations.segment}
2. Sur la page de détails du point de terminaison, sélectionnez **Connection**. Cet onglet affiche uniquement l'erreur la plus récente pour un point de terminaison et indique depuis combien de temps elle s'est produite. Les erreurs comportant l'icône X rouge ⊗ se sont produites au cours des 7 derniers jours.

#### ${post_edited_translations.segment}

Certaines erreurs peuvent continuer à apparaître dans la colonne **Dernière erreur** même après leur résolution. Pour vérifier si une erreur est toujours d'actualité ou pour forcer la suppression d'une erreur résolue du tableau :

**Étapes**

1. Sélectionnez le point de terminaison.

   ${post_edited_translations.segment}

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

La sélection de **Tester la connexion** permet à StorageGRID de valider que le point de terminaison des services de plateforme existe et qu'il est accessible avec les identifiants actuels. La connexion au point de terminaison est validée depuis un nœud sur chaque site.

#### Résoudre les erreurs de point de terminaison

Vous pouvez utiliser le message **Dernière erreur** sur la page de détails du point de terminaison pour vous aider à déterminer la cause de l'erreur. Certaines erreurs peuvent nécessiter que vous modifiiez le point de terminaison pour résoudre le problème. Par exemple, une erreur CloudMirroring peut se produire si StorageGRID ne parvient pas à accéder au compartiment S3 de destination parce qu'il ne dispose pas des autorisations d'accès appropriées ou que la clé d'accès a expiré. Le message est « Either the endpoint credentials or the destination access needs to be updated, » et les détails sont « AccessDenied » ou « InvalidAccessKeyId. »

Si vous devez modifier le point de terminaison pour résoudre une erreur, la sélection de **Tester et enregistrer les modifications** amène StorageGRID à valider le point de terminaison mis à jour et à confirmer qu'il est accessible avec les informations d'identification actuelles. La connexion au point de terminaison est validée depuis un nœud sur chaque site.

**Étapes**

1. Sélectionnez le point de terminaison.

2. Sur la page de détails du point de terminaison, sélectionnez **Configuration**.
3. Modifiez la configuration du point de terminaison selon vos besoins.
4. Sélectionnez **Connexion** > **Tester la connexion**.

#### Informations d'identification du point de terminaison avec des autorisations insuffisantes

Lorsque StorageGRID valide un point de terminaison de service de plateforme, il vérifie que les informations d'identification de ce point de terminaison permettent de contacter la ressource de destination et effectue un contrôle d'autorisations de base. Toutefois, StorageGRID ne valide pas toutes les autorisations requises pour certaines opérations des services de plateforme. Par conséquent, si vous recevez une erreur lors de la tentative d'utilisation d'un service de plateforme (par exemple, "403 Forbidden"), vérifiez les autorisations associées aux informations d'identification du point de terminaison.

#### Informations connexes

- **Administrer StorageGRID › Dépanner les services de plateforme**
- "Créer un point de terminaison de services de plateforme"
- "${post_edited_translations.segment}"
- "Modifier le point de terminaison des services de plateforme"

## Configurez la réplication CloudMirror dans StorageGRID

Pour activer la réplication CloudMirror pour un compartiment, vous créez et appliquez une configuration XML de réplication de compartiment valide.

#### Avant de commencer

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- Le point de terminaison que vous prévoyez d'utiliser comme destination pour la réplication CloudMirror existe déjà, et vous disposez de son URN.
- Vous appartenez à un groupe d'utilisateurs qui dispose de la "Gérer tous les compartiments ou autorisation d'accès Root". Ces autorisations prévalent sur les paramètres d'autorisation des politiques de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Tenant Manager.

#### À propos de cette tâche

CloudMirror réplique des copies d'objets d'un compartiment source vers un compartiment de destination spécifié dans un point de terminaison.

Pour obtenir des informations générales sur la réplication de compartiment et sa configuration, consultez "${post_edited_translations.segment}". Pour en savoir plus sur la façon dont StorageGRID implémente GetBucketReplication, DeleteBucketReplication et PutBucketReplication, consultez le "Opérations sur les compartiments".

> La réplication CloudMirror présente d'importantes similitudes et différences avec la fonctionnalité de réplication inter-grille. Pour en savoir plus, consultez "Comparez la réplication inter-grilles et la réplication CloudMirror".

Notez les exigences et caractéristiques suivantes lors de la configuration de la réplication CloudMirror :

- Lorsque vous créez et appliquez un fichier XML de configuration de réplication de compartiment valide, il

doit utiliser l'URN d'un point de terminaison de compartiment S3 pour chaque destination.

- ${post_edited_translations.segment}
- 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 dans le compartiment ne sont pas répliqués. Vous devez mettre à jour les objets existants pour déclencher la réplication.
- Si vous spécifiez une classe de stockage dans le fichier XML de configuration de réplication, StorageGRID utilise cette classe lors des opérations sur le point de terminaison S3 de destination. Le point de terminaison de destination doit également prendre en charge la classe de stockage spécifiée. Veillez à suivre toutes les recommandations fournies par le fournisseur du système de destination.

**Étapes**

1. ${post_edited_translations.segment}
   - 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.
   - ${post_edited_translations.segment}
     - Notez que StorageGRID ne prend en charge que la version 1 de la configuration de réplication. Cela signifie que StorageGRID ne prend pas en charge l'utilisation de l' `Filter`élément pour les règles et suit les conventions de la version 1 pour la suppression des versions d'objets. Consultez la documentation Amazon relative à la configuration de réplication pour plus de détails.
     - ${post_edited_translations.segment}
     - Ajoutez éventuellement l' `<StorageClass>`élément et spécifiez l'un des éléments suivants :
       - `STANDARD` : la classe de stockage par défaut. Si vous ne spécifiez pas de classe de stockage lorsque vous transférez un objet, la classe de stockage `STANDARD` est utilisée.
       - `STANDARD_IA` : (Standard - accès peu fréquent.) Utilisez cette classe de stockage pour les données consultées moins fréquemment, mais qui nécessitent tout de même un accès rapide en cas de besoin.
       - `REDUCED_REDUNDANCY` : Utilisez cette classe de stockage pour les données non critiques et reproductibles qui peuvent être stockées avec moins de redondance que la classe de stockage `STANDARD`.
     - Si vous spécifiez un `Role` dans le 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** depuis le tableau de bord, ou sélectionnez **STOCKAGE (S3)** > **Compartiments**.
3. Sélectionnez le nom du compartiment source.

   ${post_edited_translations.segment}

4. ${post_edited_translations.segment}
5. ${post_edited_translations.segment}
6. ${post_edited_translations.segment}

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

7. ${post_edited_translations.segment}
   a. ${post_edited_translations.segment}

      ${post_edited_translations.segment}

   b. Confirmez que l'objet a été répliqué dans le compartiment de destination.

      Pour les petits objets, la réplication se fait rapidement.

**Informations connexes**

"Créer un point de terminaison de services de plateforme"

## Configurez les notifications d'événements dans StorageGRID

Vous activez les notifications pour un compartiment en créant un fichier XML de configuration de notification et en utilisant le Tenant Manager pour appliquer le fichier XML à un compartiment.

**Avant de commencer**

- ${post_edited_translations.segment}
- Vous avez déjà créé un compartiment qui servira de source de notifications.
- Le point de terminaison que vous souhaitez utiliser comme destination pour les notifications d'événements existe déjà, et vous disposez de son URN.
- Vous appartenez à un groupe d'utilisateurs qui dispose de la "Gérer tous les compartiments ou autorisation d'accès Root". Ces autorisations prévalent sur les paramètres d'autorisation des politiques de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Tenant Manager.

**À propos de cette tâche**

Vous configurez les notifications d'événements en associant un fichier XML de configuration de notification à un compartiment source. Le fichier XML de configuration de notification suit les conventions S3 pour la configuration des notifications de compartiment, avec la destination (rubrique Amazon SNS, rubrique Kafka ou point de terminaison webhook) spécifiée comme l'URN d'un point de terminaison.

Pour obtenir des informations générales sur les notifications d'événements et leur configuration, consultez la

"Documentation Amazon". Pour des informations sur la manière dont StorageGRID implémente l'API de configuration des notifications de compartiment S3, consultez la "Instructions pour la mise en œuvre des applications clientes S3".

Notez les exigences et caractéristiques suivantes lors de la configuration des notifications d'événements pour un compartiment :

- Lorsque vous créez et appliquez un fichier XML de configuration de notification valide, celui-ci doit utiliser l'URN d'un point de terminaison de notification d'événement pour chaque destination.
- Bien que la notification d'événements puisse être configurée sur un compartiment avec S3 Object Lock activé, les métadonnées S3 Object Lock (y compris Retain Until Date et Legal Hold status) des objets ne seront pas incluses dans les messages de notification.
- Une fois les notifications d'événements configurées, lorsqu'un événement spécifié se produit pour un objet dans le compartiment source, une notification est générée et envoyée au sujet Amazon SNS, au sujet Kafka ou au point de terminaison webhook utilisé comme destination.
- Si vous activez les notifications d'événements pour un compartiment contenant des objets, les notifications ne sont envoyées que pour les actions effectuées après l'enregistrement de la configuration des notifications.

**Étapes**

1. Activez les notifications pour votre compartiment source :
   - Utilisez un éditeur de texte pour créer le fichier XML de configuration des notifications requis pour activer les notifications d'événements, comme spécifié dans l'API de notification S3.
   - Lors de la configuration du fichier XML, utilisez l'URN d'un point de terminaison de notifications 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 Tenant Manager, sélectionnez **STORAGE (S3)** > **Buckets**.
3. Sélectionnez le nom du compartiment source.

${post_edited_translations.segment}

4. Sélectionnez **Services de la plateforme** > **Notifications d'événements**.
5. Cochez la case **Activer les notifications d'événements**.
6. Collez le code XML de configuration des notifications dans la zone de texte, puis sélectionnez **Enregistrer les modifications**.

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

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

   a. Effectuez une action sur un objet dans le compartiment source qui répond aux exigences pour déclencher une notification, comme configuré dans le fichier XML de configuration.

      Dans cet 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 remise au sujet Amazon SNS, au sujet Kafka ou au point de terminaison webhook de destination.

      Par exemple, si votre sujet de destination est hébergé sur Amazon SNS, vous pouvez configurer le service pour qu'il vous envoie un e-mail lorsque la notification est livrée.

```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```

+ Si la notification est reçue sur le sujet de destination, vous avez correctement configuré votre compartiment source pour les notifications StorageGRID.

**Informations connexes**

- "Comprendre les notifications pour les compartiments"
- "Utilisez l'API REST S3"
- "Créer un point de terminaison de services de plateforme"

## Configurez le service d'intégration de recherche dans StorageGRID

Vous activez l'intégration de la recherche pour un compartiment en créant un fichier XML d'intégration de recherche et en utilisant le Tenant Manager pour appliquer le fichier XML au compartiment.

**Avant de commencer**

- ${post_edited_translations.segment}
- Vous avez déjà créé un compartiment S3 dont vous souhaitez indexer le contenu.
- Le point de terminaison que vous souhaitez utiliser comme destination pour le service d'intégration de recherche existe déjà, et vous disposez de son URN.
- Vous appartenez à un groupe d'utilisateurs qui dispose de la "Gérer tous les compartiments ou autorisation d'accès Root". Ces autorisations prévalent sur les paramètres d'autorisation des politiques de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Tenant Manager.

**À propos de cette tâche**

Une fois le service d'intégration de recherche configuré 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 de l'objet au point de terminaison de destination.

Si vous activez le service d'intégration de recherche pour un compartiment contenant déjà des objets, les notifications de métadonnées ne sont pas automatiquement envoyées pour les objets existants. Mettez à jour ces objets existants pour garantir que leurs métadonnées sont ajoutées à l'index de recherche de destination.

**Étapes**

1. Activer l'intégration de la recherche pour un compartiment :
    - Utilisez un éditeur de texte pour créer le fichier XML de notification des métadonnées requis pour activer l'intégration de la recherche.
    - Lors de la configuration du fichier XML, utilisez l'URN d'un point de terminaison d'intégration de recherche comme destination.

      Les objets peuvent être filtrés sur le préfixe du nom de l'objet. Par exemple, vous pouvez envoyer les métadonnées des objets avec le préfixe `images` à une destination, et les métadonnées des objets avec le préfixe `videos` à une autre. Les configurations comportant des préfixes qui se chevauchent ne sont pas valides et sont rejetées lors de leur soumission. 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 autorisée.

      Au besoin, reportez-vous au Exemples pour la configuration des métadonnées XML.

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>/Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

Éléments du fichier XML de configuration des notifications de métadonnées :

| Nom | Description | Obligatoire |
|---|---|---|
| MetadataNotificationConfiguration | Balise conteneur pour les règles utilisées pour spécifier les objets et la destination des notifications de métadonnées.<br><br>Contient un ou plusieurs éléments de règle. | Oui |
| Règle | Balise conteneur pour une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié.<br><br>Les règles comportant des préfixes qui se chevauchent sont rejetées.<br><br>Inclus dans l'élément MetadataNotificationConfiguration. | Oui |
| ID | Identifiant unique de la règle.<br><br>Inclus dans l'élément Rule. | Non |
| Statut | Le statut peut être « Activé » ou « Désactivé ». Aucune action n'est entreprise pour les règles désactivées.<br><br>Inclus dans l'élément Rule. | Oui |
| Préfixe | Les objets correspondant au préfixe sont concernés par la règle et leurs métadonnées sont envoyées à la destination spécifiée.<br><br>Pour faire correspondre tous les objets, spécifiez un préfixe vide.<br><br>Inclus dans l'élément Rule. | Oui |
| Destination | Étiquette conteneur pour la destination d'une règle.<br><br>Inclus dans l'élément Rule. | Oui |

| Nom | Description | Obligatoire |
| --- | --- | --- |
| Urn | URN de la destination où les métadonnées de l'objet sont envoyées. Doit être l'URN d'un point de terminaison StorageGRID possédant les propriétés suivantes :<br>• `es` doit être le troisième élément.<br>• L'URN doit se terminer par l'index et le type où les métadonnées sont stockées, sous la forme `domain-name/myindex/mytype`.<br>Les points de terminaison sont configurés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Ils se présentent sous la forme suivante :<br>• `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype`<br>• `urn:mysite:es:::mydomain/myindex/mytype`<br>Le point de terminaison doit être configuré avant la soumission du fichier XML de configuration, sinon la configuration échouera avec une erreur 404.<br>L'URN est inclus dans l'élément Destination. | Oui |

2. Dans le Tenant Manager, sélectionnez **STORAGE (S3)** > **Buckets**.
3. Sélectionnez le nom du compartiment source.

   ${post_edited_translations.segment}

4. Sélectionnez **Services de plateforme** > **Intégration de recherche**
5. Cochez la case **Activer l'intégration de la recherche**.
6. Collez la configuration de notification des métadonnées dans la zone de texte, puis sélectionnez **Enregistrer les modifications**.

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

7. Vérifiez que le service d'intégration de recherche est correctement configuré :
   a. Ajoutez un objet au compartiment source qui répond aux exigences de déclenchement d'une notification de métadonnées, comme spécifié dans le fichier XML de configuration.

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

   b. Confirmez qu'un document JSON contenant les métadonnées et les balises de l'objet a été ajouté à l'index de recherche spécifié dans le point de terminaison.

**Après avoir terminé**

Si nécessaire, vous pouvez désactiver l'intégration de recherche pour un compartiment en utilisant l'une des méthodes suivantes :

- Sélectionnez **STOCKAGE (S3)** > **Buckets** et décochez la case **Activer l'intégration de recherche**.
- Si vous utilisez directement l'API S3, utilisez une requête de notification de métadonnées DELETE Bucket. Consultez les instructions pour la mise en œuvre des applications clientes S3.

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

Dans cet exemple, les métadonnées de tous les objets sont envoyées à la même destination.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

**Exemple : Configuration des notifications de métadonnées avec deux règles**

Dans cet exemple, les métadonnées d'objet pour les objets qui correspondent au préfixe `/images` sont envoyées à une destination, tandis que les métadonnées d'objet pour les objets qui correspondent au préfixe `/videos` sont envoyées 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-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

**Format de notification des métadonnées**

${post_edited_translations.segment}

Cet exemple montre un exemple du JSON qui pourrait être généré lorsqu'un objet avec la clé `SGWS/Tagging.txt` est créé dans un compartiment nommé `test`. Le compartiment `test` n'est pas versionné, la balise `versionId` est donc vide.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

#### Champs inclus dans le document JSON

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

**Informations sur le bucket et l'objet**

`bucket` : Nom du compartiment

`key`: Nom de la clé de l'objet

`versionID`: Version de l'objet, pour les objets dans des compartiments versionnés

`region`: Région du compartiment, par exemple `us-east-1`

**Métadonnées système**

`size`: Taille de l'objet (en octets) telle qu'elle est visible pour un client HTTP

`md5`: Hachage d'objet

**Métadonnées utilisateur**

`metadata`: Toutes les métadonnées utilisateur de l'objet, sous forme de paires clé-valeur

`key:value`

**Étiquettes**

`tags`: Toutes les étiquettes d'objet définies pour l'objet, sous forme de paires clé-valeur

`key:value`

#### Comment afficher les résultats dans Elasticsearch

Pour les balises et les métadonnées utilisateur, StorageGRID transmet les dates et les nombres à Elasticsearch sous forme de chaînes ou de notifications d'événements S3. Pour configurer Elasticsearch afin qu'il interprète ces chaînes comme des dates ou des nombres, suivez les instructions Elasticsearch concernant le mappage dynamique des champs et le mappage des formats de date. Activez le mappage dynamique des champs sur l'index avant de configurer le service d'intégration de recherche. Après l'indexation d'un document, vous ne pouvez plus modifier les types de champs du document dans l'index.

## Informations sur le copyright



## Informations sur les marques commerciales