Utilisez un compte de locataire

StorageGRID software

NetApp
February 12, 2026

Sommaire

Utilisez un compte de locataire

Utilisez un compte de locataire

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

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

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

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

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

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

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

Comment créer un compte de locataire

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

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

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

Configurez les locataires S3

Après un "Le compte de locataire S3 est créé", vous pouvez accéder au gestionnaire de locataires pour effectuer des tâches telles que :

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

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

Comment se connecter et se déconnecter

Connectez-vous au Gestionnaire de locataires

Vous accédez au gestionnaire de locataires en entrant l'URL du locataire dans la barre d'adresse d'un "navigateur web pris en charge".

Avant de commencer

- Vous disposez de vos identifiants de connexion.
- Vous disposez d'une URL permettant d'accéder au gestionnaire de locataires, fournie par votre administrateur de grille. L'URL se présente comme l'un de ces exemples :

  ```
  https://FQDN_or_Admin_Node_IP/

  https://FQDN_or_Admin_Node_IP:port/

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

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

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

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

Étapes

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

4. Connectez-vous au Gestionnaire de locataires.

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

   Pas d'utilisation de SSO

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

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

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

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

   Utilisation de SSO

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

   - La page SSO de votre organisation.

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

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

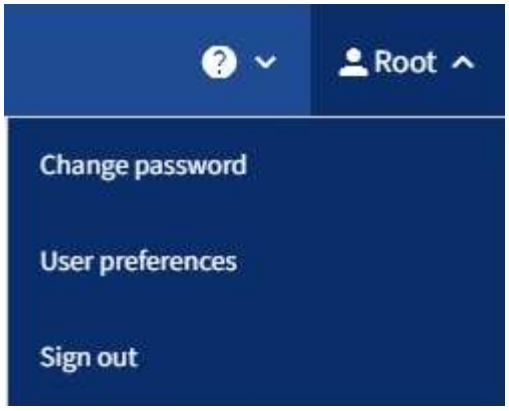
     Le tableau de bord du gestionnaire de locataires s'affiche.

Déconnectez-vous du Gestionnaire de locataires

Lorsque vous avez terminé de travailler avec le Gestionnaire de locataires, vous devez vous déconnecter pour vous assurer que les utilisateurs non autorisés ne peuvent pas accéder au système StorageGRID. La fermeture de votre navigateur risque de ne pas vous déconnecter du système, en fonction des paramètres des cookies du navigateur.

Étapes

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



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

   - Si SSO n'est pas utilisé :

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

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

   - Si SSO est activé :

     Vous êtes déconnecté de tous les nœuds d'administration auxquels vous accédiez. La page de connexion StorageGRID s'affiche. Le nom du compte de locataire que vous venez d'accéder est indiqué par défaut dans la liste déroulante **comptes récents** et le **ID de compte** du locataire s'affiche.

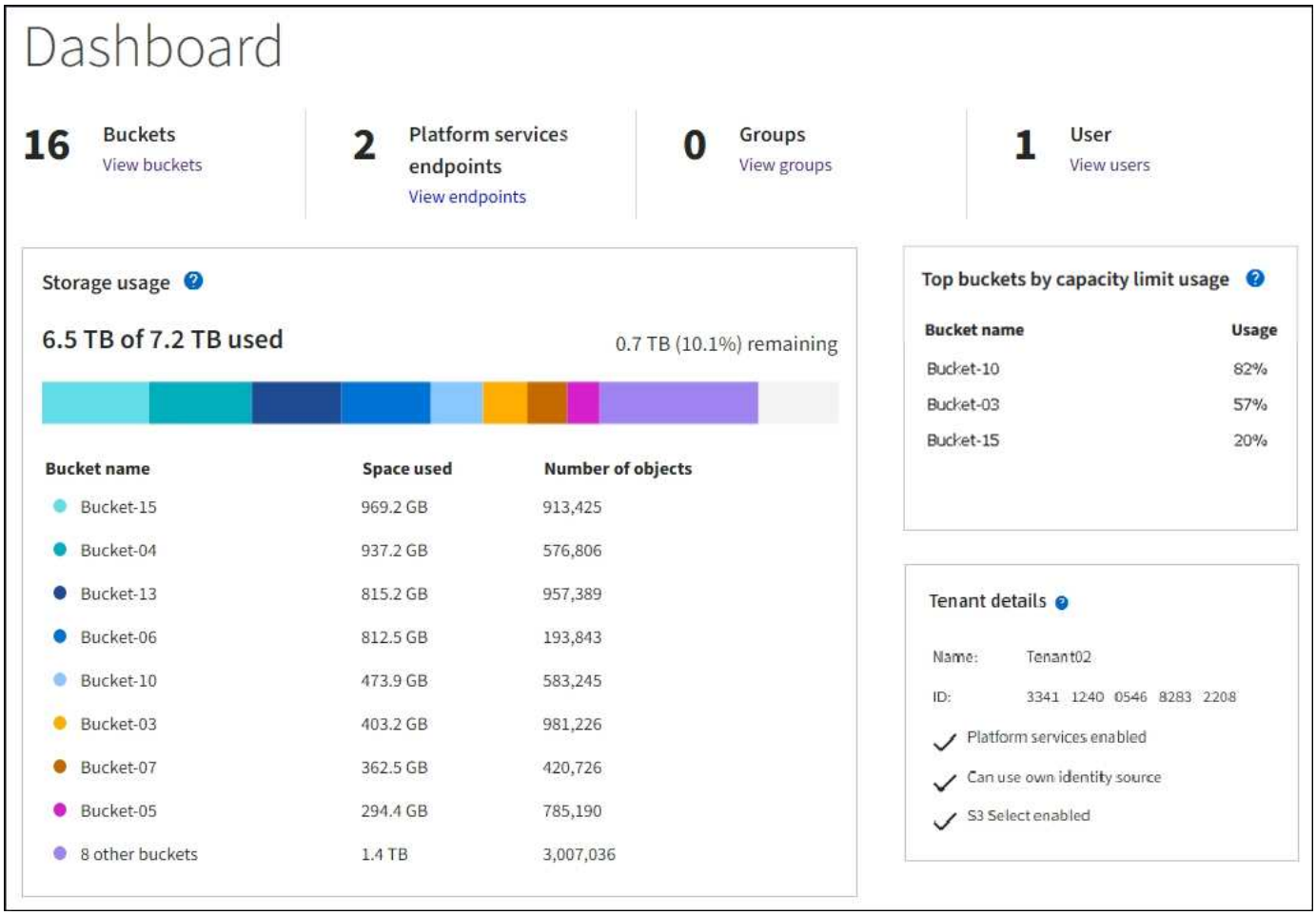
> Si SSO est activé et que vous êtes également connecté à Grid Manager, vous devez également vous déconnecter de Grid Manager pour vous déconnecter de SSO.

Présentation du tableau de bord du gestionnaire de locataires

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

> La taille logique de tous les objets appartenant à ce locataire inclut les téléchargements multipartites incomplets et en cours. La taille n'inclut pas l'espace physique supplémentaire utilisé pour les politiques ILM. Les valeurs de l'espace utilisé sont des estimations. Ces estimations sont affectées par le moment des ingestions, la connectivité réseau et l'état du nœud.

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



Informations sur le compte locataire

Le haut du tableau de bord affiche le nombre de compartiments ou de conteneurs, de groupes et d'utilisateurs configurés. Il affiche également le nombre de noeuds finaux de services de plate-forme, s'ils ont été configurés. Sélectionnez les liens pour afficher les détails.

Selon votre configuration et les options dont vous disposez, le reste du tableau de bord affiche différentes combinaisons de consignes, d'utilisation du stockage, d'informations sur l'objet et de données sur le "autorisations de gestion des locataires"locataire.

Utilisation du stockage et des quotas

Le panneau utilisation du stockage contient les informations suivantes :

- Volume des données d'objet pour le locataire.

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

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

L'utilisation des quotas est basée sur des estimations internes et peut être dépassée dans certains cas. Par exemple, StorageGRID vérifie le quota lorsqu'un locataire commence à charger des objets et rejette les nouvelles ingère si le locataire a dépassé le quota. Cependant, StorageGRID ne prend pas en compte la taille du téléchargement actuel lors de la détermination du dépassement du quota. Si des objets sont supprimés, un locataire peut temporairement empêcher le téléchargement de nouveaux objets jusqu'au recalcul de l'utilisation du quota. Le calcul de l'utilisation des quotas peut prendre 10 minutes ou plus.

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

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

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

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

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

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

Alertes d'utilisation des quotas

Si les alertes d'utilisation des quotas ont été activées dans Grid Manager, ces alertes apparaissent dans le gestionnaire de locataires lorsque le quota est faible ou dépassé, comme suit :

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

  Demandez à votre administrateur de grid d'augmenter le quota.

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

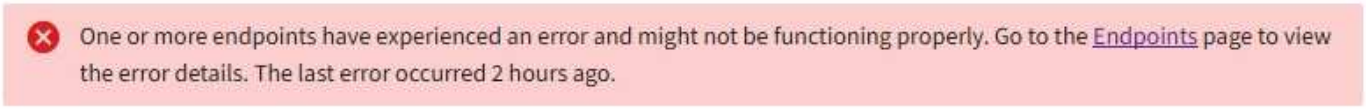
utilisation limitée de la capacité

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

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

Erreurs de point final

Si vous avez utilisé le gestionnaire de grille pour configurer un ou plusieurs points de terminaison pour les services de plateforme, le tableau de bord du gestionnaire de locataires affiche une alerte si des erreurs de point de terminaison se sont produites au cours des sept derniers jours.



Pour "erreurs de noeud final des services de plate-forme"afficher des détails sur , sélectionnez **noeuds finaux** pour afficher la page noeuds finaux.

API de gestion des locataires

Compréhension de l'API de gestion des locataires

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

L'API de gestion des locataires :

- Utilise la plate-forme API open source swagger. Swagger fournit une interface utilisateur intuitive qui permet aux développeurs et aux non-développeurs d'interagir avec l'API. L'interface utilisateur swagger fournit des détails complets et de la documentation pour chaque opération API.
- Utilise "gestion des versions pour prendre en charge les mises à niveau sans interruption".

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

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

Opérations API

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

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

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

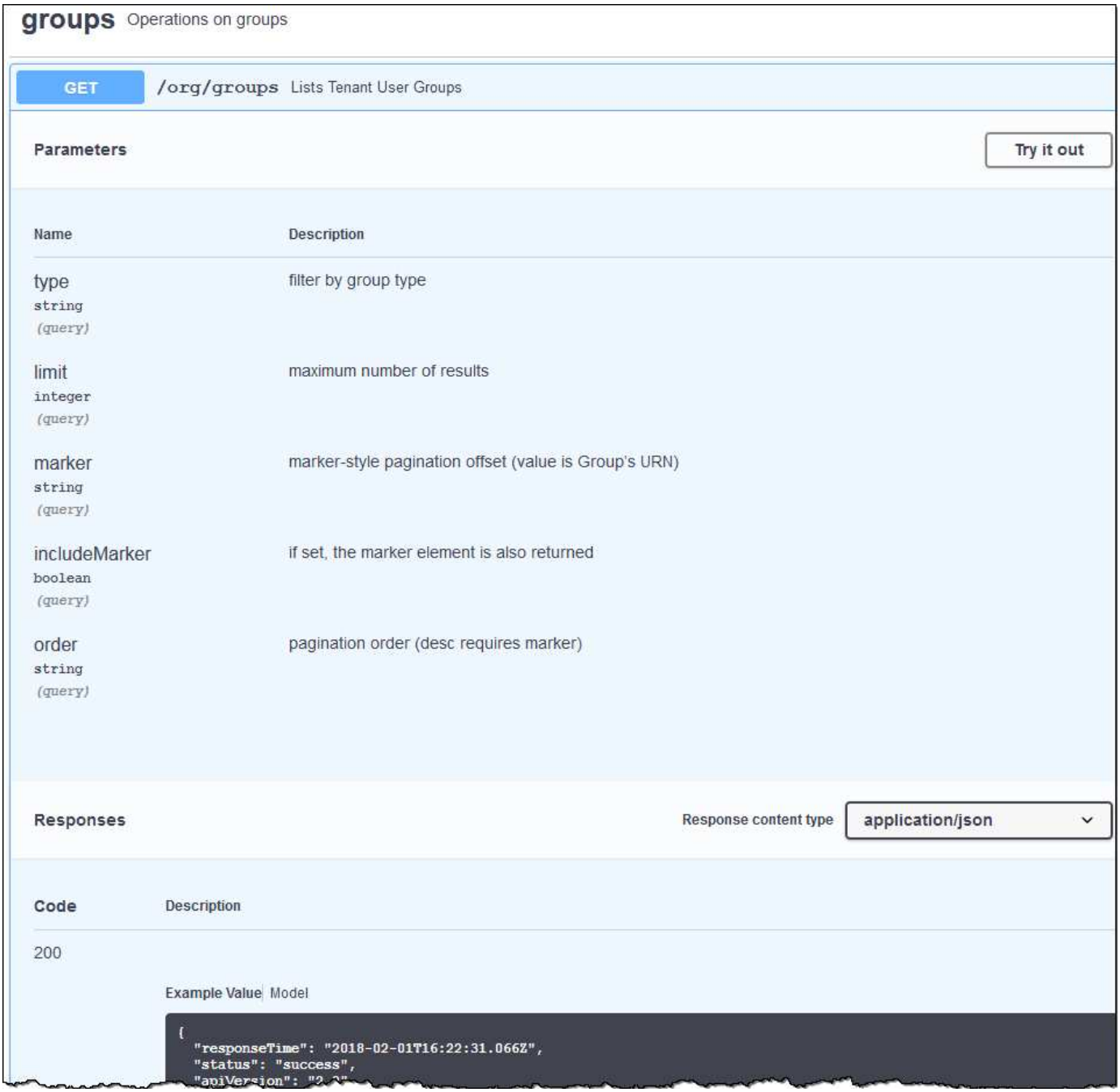
  Pour plus d'informations sur l'amélioration de la sécurité d'authentification, reportez-vous à la section "Protéger contre la contrefaçon de demandes intersites".

  > Si l'authentification unique (SSO) est activée pour le système StorageGRID, vous devez effectuer différentes étapes pour l'authentification. Voir la "Instructions d'utilisation de l'API de gestion de grille".

- **Config** : opérations liées à la version du produit et aux versions de l'API de gestion des locataires. Vous pouvez lister la version du produit ainsi que les versions principales de l'API prises en charge par cette version.
- **conteneurs** : opérations sur les buckets S3.
- **Désactivé-features** : opérations permettant d'afficher les fonctions qui auraient pu être désactivées.
- **Noeuds finaux** : opérations pour gérer un noeud final. Les terminaux permettent à un compartiment S3 d'utiliser un service externe pour la réplication StorageGRID CloudMirror, les notifications ou l'intégration de la recherche.
- **Grid-federation-connections** : opérations sur les connexions de fédération de grille et la réplication de grille transversale.
- **Groupes** : opérations de gestion des groupes de locataires locaux et de récupération des groupes de locataires fédérés à partir d'un référentiel d'identité externe.
- **Identity-source** : opérations permettant de configurer un référentiel d'identité externe et de synchroniser manuellement les informations relatives au groupe fédéré et à l'utilisateur.
- **ilm** : opérations sur les paramètres de gestion du cycle de vie de l'information (ILM).
- **Régions** : opérations permettant de déterminer quelles régions ont été configurées pour le système StorageGRID.
- **s3** : opérations de gestion des clés d'accès S3 pour les utilisateurs locataires.
- **s3-object-lock** : opérations sur les paramètres globaux de verrouillage d'objet S3, utilisées pour prendre en charge la conformité réglementaire.
- **Utilisateurs** : opérations pour afficher et gérer les utilisateurs locataires.

Détails de l'opération

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



Émettre des requêtes API

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

Étapes

1. Sélectionnez l'action HTTP pour afficher les détails de la demande.
2. Déterminez si la demande nécessite des paramètres supplémentaires, tels qu'un ID de groupe ou d'utilisateur. Ensuite, obtenir ces valeurs. Vous devrez peut-être d'abord lancer une autre demande d'API pour obtenir les informations dont vous avez besoin.
3. Déterminez si vous devez modifier l'exemple de corps de la demande. Si c'est le cas, vous pouvez sélectionner **modèle** pour connaître les exigences de chaque champ.

4. Sélectionnez **essayez-le**.
5. Fournir tous les paramètres requis ou modifier le corps de la demande selon les besoins.
6. Sélectionnez **Exécuter**.
7. Vérifiez le code de réponse pour déterminer si la demande a réussi.

Gestion des versions de l'API de gestion des locataires

L'API de gestion des locataires utilise la gestion des versions pour prendre en charge les mises à niveau sans interruption.

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

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

La version majeure de l'API est incrémentée lorsque des modifications sont effectuées qui ne sont *pas compatibles* avec des versions plus anciennes. La version mineure de l'API est incrémentée lorsque des modifications qui sont *compatibles* avec des versions plus anciennes sont effectuées. Les modifications compatibles incluent l'ajout de nouveaux noeuds finaux ou de nouvelles propriétés.

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

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

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 accéder à l'ancienne version de l'API pour au moins une version de StorageGRID.

> Vous pouvez configurer les versions prises en charge. Pour plus d'informations, reportez-vous à la section **config** de la documentation de l'API swagger"API de gestion du grid". Vous devez désactiver la prise en charge de l'ancienne version après avoir mis à jour tous les clients API pour utiliser la nouvelle version.

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

- L'en-tête de réponse est « obsolète : vrai »
- Le corps de la réponse JSON inclut « obsolète » : vrai
- Un avertissement obsolète est ajouté à nms.log. Par exemple :

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

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

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

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

Spécifiez une version API pour une demande

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

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

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

Protection contre la contrefaçon de demandes intersites (CSRF)

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

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

StorageGRID contribue à la protection contre les attaques CSRF en utilisant des jetons CSRF. Lorsque cette option est activée, le contenu d'un cookie spécifique doit correspondre au contenu d'un en-tête spécifique ou d'un paramètre DE CORPS POST spécifique.

Pour activer la fonction, définissez le `csrfToken` paramètre sur `true` pendant l'authentification. La valeur par défaut est `false`.

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

Lorsque la valeur est true, un `GridCsrfToken` cookie est défini avec une valeur aléatoire pour les connexions au gestionnaire de tenant et le `AccountCsrfToken` cookie est défini avec une valeur aléatoire pour les connexions au gestionnaire de tenant.

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

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

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

> Les demandes qui ont un ensemble de cookies de token CSRF appliquent également l'en-tête « Content-Type: Application/json » pour toute demande qui attend un corps de requête JSON comme protection supplémentaire contre les attaques CSRF.

Utiliser les connexions de fédération de grille

Cloner des groupes de locataires et des utilisateurs

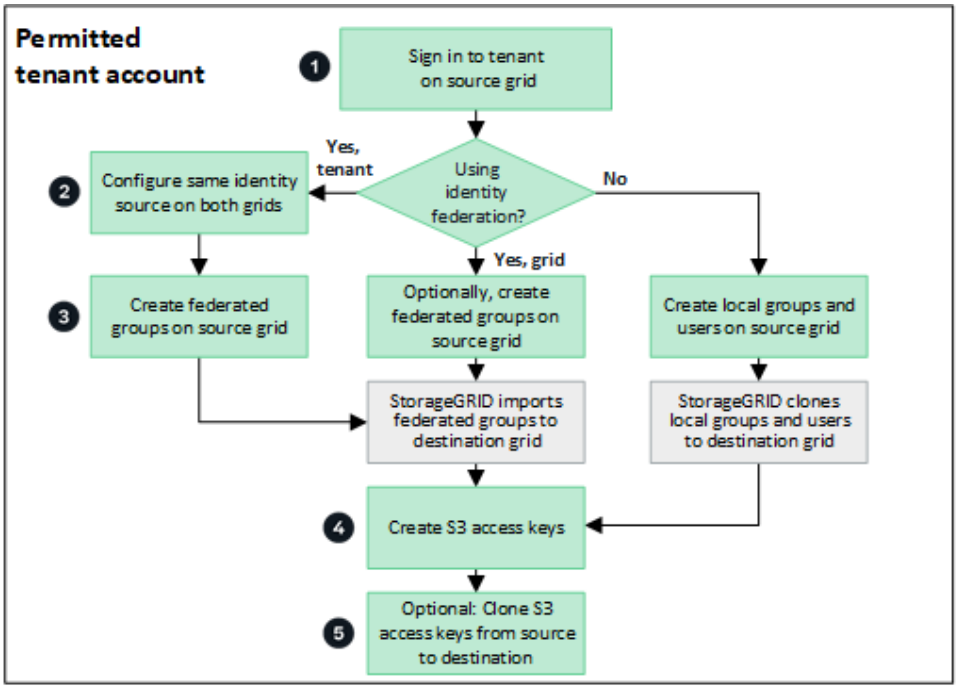
Si un locataire a été créé ou modifié pour utiliser une connexion de fédération de grille, ce dernier est répliqué d'un système StorageGRID (le locataire source) vers un autre système StorageGRID (le locataire de réplica). Une fois le tenant répliqué, tous les groupes et utilisateurs ajoutés au tenant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

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

Le clonage des informations de compte de locataire est requis pour les "réplication entre plusieurs grilles"objets de compartiment. Le fait de disposer des mêmes groupes de locataires et utilisateurs sur les deux grilles vous permet d'accéder aux compartiments et objets correspondants sur l'une ou l'autre grille.

Workflow des locataires pour le clone de compte

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



Voici les principales étapes du flux de travail :

1 Connectez-vous au locataire

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

2 Vous pouvez également configurer la fédération des identités

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

3 Créer des groupes et des utilisateurs

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

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

4 Création de clés d'accès S3

Vous pouvez "créez vos propres clés d'accès" ou "créez 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 **Vous pouvez également cloner les clés d'accès S3**

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

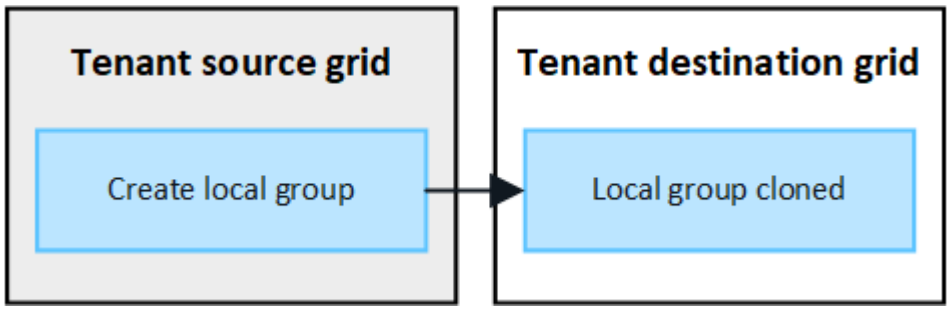
Comment les groupes, les utilisateurs et les clés d'accès S3 sont-ils clonés ?

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

Les groupes locaux créés dans la grille source sont clonés

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

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

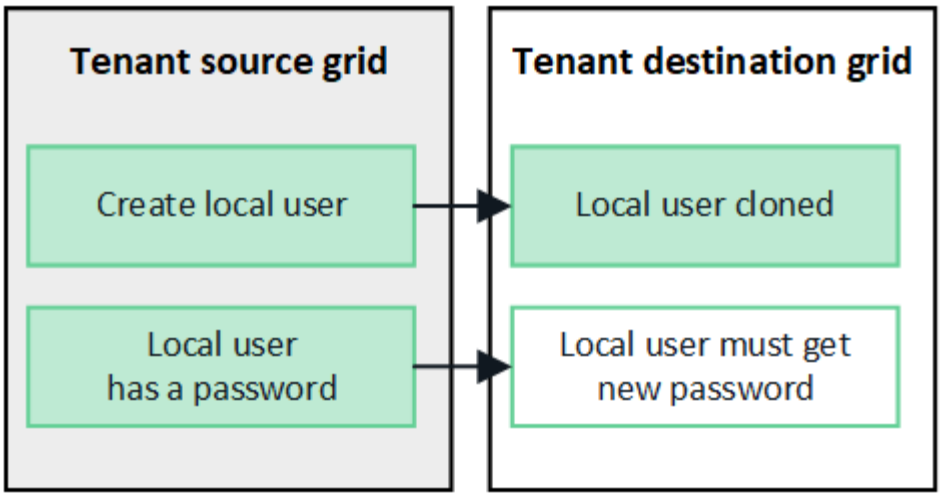


Tous les utilisateurs sélectionnés lors de la création d'un groupe local sur la grille source ne sont pas inclus lorsque le groupe est cloné dans la grille de destination. Pour cette raison, ne sélectionnez pas d'utilisateurs lorsque vous créez le groupe. Sélectionnez plutôt le groupe lorsque vous créez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

Les utilisateurs locaux créés dans la grille source sont clonés

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

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

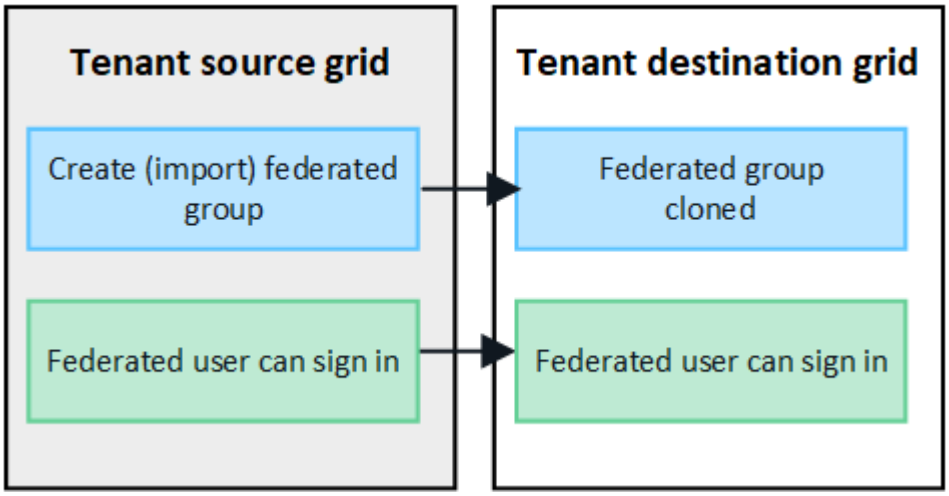


Les groupes fédérés créés dans la grille source sont clonés

En supposant que les conditions d'utilisation du clone de compte "authentification unique" "fédération des identités"soient remplies, les groupes fédérés que vous créez (importez) pour le locataire sur la grille source sont automatiquement clonés dans le locataire de la grille de destination.

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

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

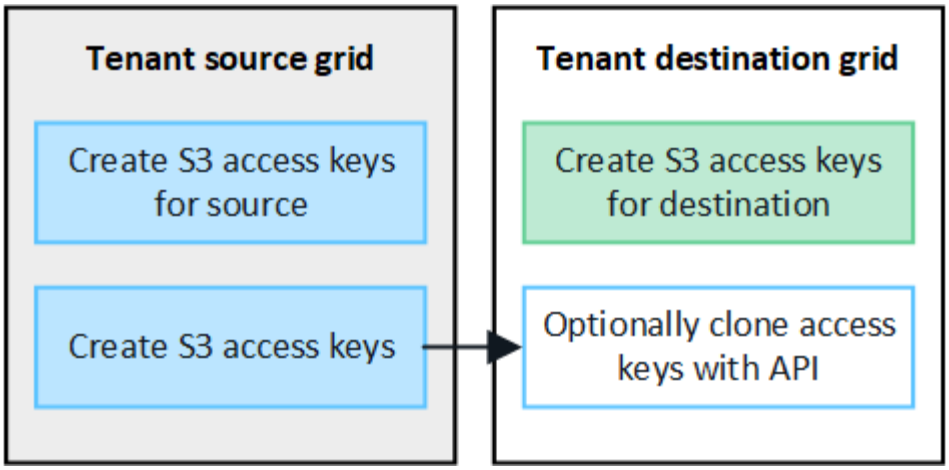


Les clés d'accès S3 peuvent être clonées manuellement

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

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

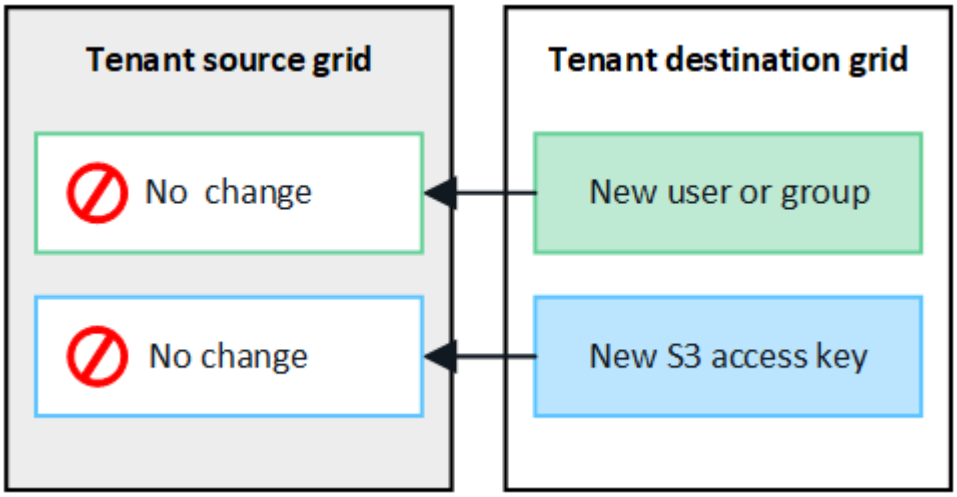
- Si vous n'avez pas besoin d'utiliser les mêmes touches pour chaque grille, vous pouvez "créez vos propres clés d'accès" ou "créez les clés d'accès d'un autre utilisateur" sur chaque grille.
- Si vous devez utiliser les mêmes clés sur les deux grilles, vous pouvez créer des clés sur la grille source,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



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

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

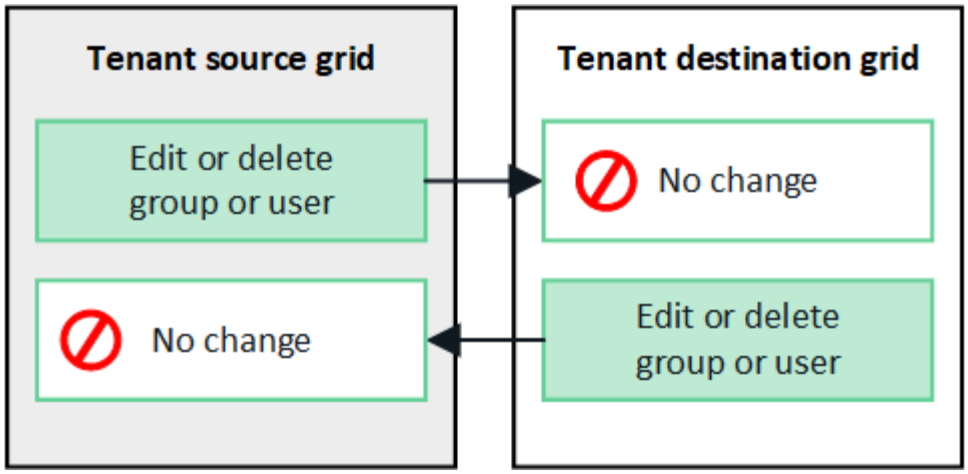
Le clonage s'effectue uniquement depuis la grille source du locataire vers la grille de destination du locataire. Si vous créez ou importez des groupes et des utilisateurs sur la grille de destination du locataire, StorageGRID ne les clonez pas dans la grille source du locataire.



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

Le clonage a lieu uniquement lorsque vous créez de nouveaux groupes et utilisateurs.

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



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

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

Avant de commencer

- Le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille**.
- La connexion de fédération de grille a un **état de connexion** de **connecté**.
- Vous êtes connecté au gestionnaire de locataires sur la grille source du locataire à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez vos propres informations d'identification S3 ou autorisations d'accès racine".
- Si vous clonez des clés d'accès pour un utilisateur local, l'utilisateur existe déjà sur les deux grilles.

> Lorsque vous clonez les clés d'accès S3 d'un utilisateur fédéré, ces deux clés sont ajoutées au locataire de destination.

Clonez vos propres clés d'accès

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

Étapes

1. À l'aide du gestionnaire de locataires sur la grille source "créez vos propres clés d'accès"et téléchargez le `.csv` fichier.
2. Dans le haut du Gestionnaire de locataires, sélectionnez l'icône d'aide et sélectionnez **documentation API**.
3. Dans la section **s3**, sélectionnez le noeud final suivant :

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

4. Sélectionnez **essayez-le**.
5. Dans la zone de texte **body**, remplacez les entrées d'exemple pour **accesskey** et **secretAccessKey** par les valeurs du fichier **.csv** que vous avez téléchargé.

   Veillez à conserver les guillemets doubles autour de chaque chaîne.

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

Cloner les clés d'accès d'un autre utilisateur

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

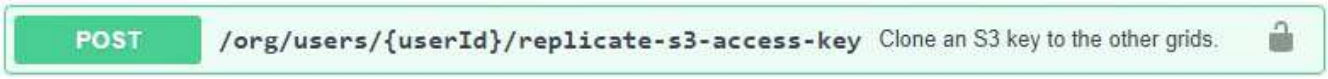
Étapes

1. À l'aide du gestionnaire de locataires sur la grille source "Créez les clés d'accès S3 de l'autre utilisateur"et téléchargez le `.csv` fichier.
2. Dans le haut du Gestionnaire de locataires, sélectionnez l'icône d'aide et sélectionnez **documentation API**.
3. Obtenez l'ID utilisateur. Vous aurez besoin de cette valeur pour cloner les clés d'accès des autres utilisateurs.
   a. Dans la section **Users**, sélectionnez le noeud final suivant :

      `GET /org/users`

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

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



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

   Veillez à conserver les guillemets doubles autour de la chaîne.

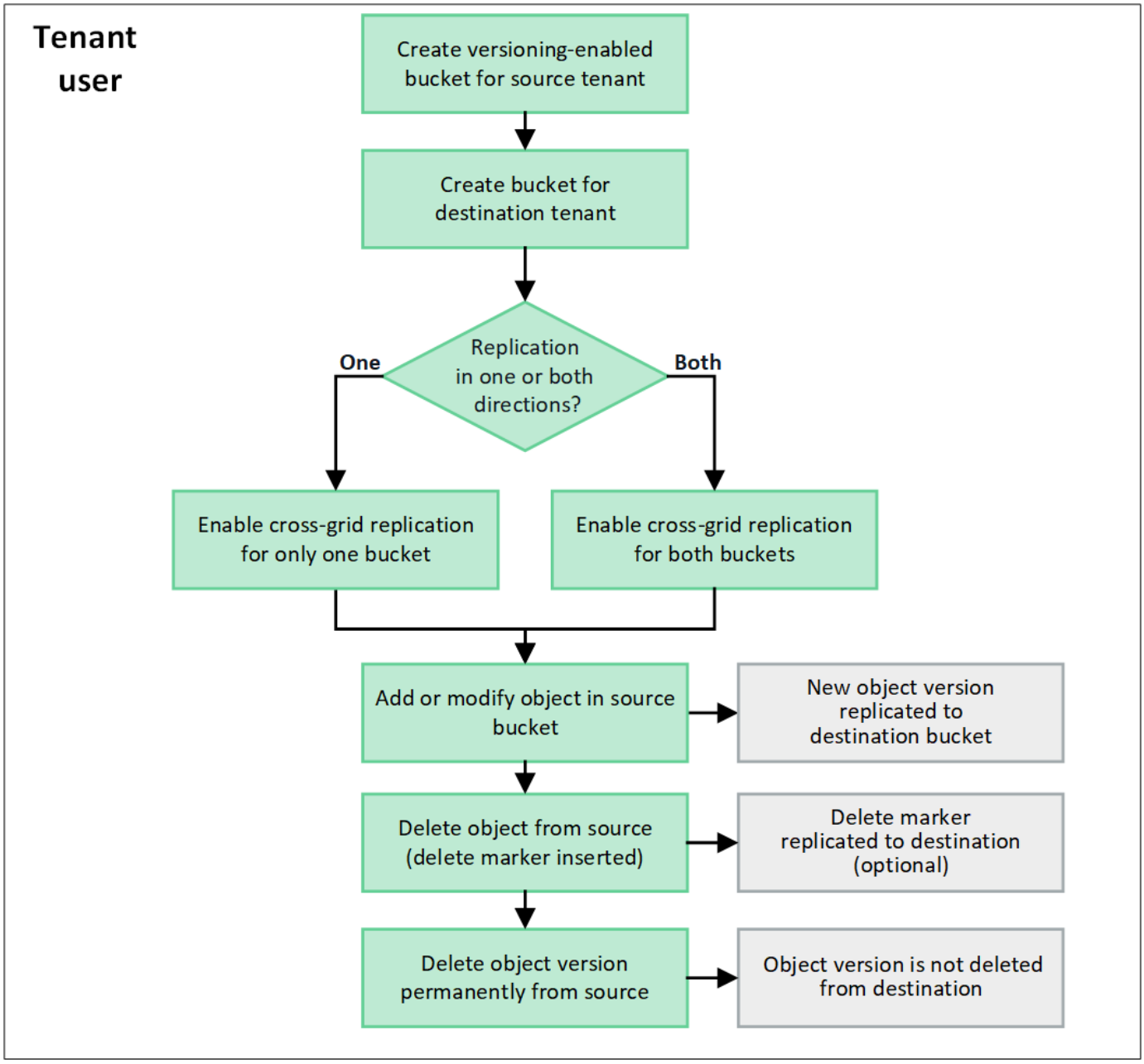
8. Si la clé expire, remplacez l'exemple de **expire** par la date et l'heure d'expiration sous forme de chaîne au format de données ISO 8601 (par exemple, `2023-02-28T22:46:33-08:00`). Si la clé n'expire pas, entrez **null** comme valeur pour l'entrée **Expires** (ou supprimez la ligne **Expires** et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

Gérer la réplication entre les grilles

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

Flux de production pour la réplication entre les grilles

Le diagramme de flux de travail résume les étapes à suivre pour configurer la réplication inter-grille entre les buckets de deux grilles. Ces étapes sont décrites plus en détail sous le diagramme.



Configurer la réplication entre les grilles

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

Avant de commencer

- Vous avez examiné les exigences relatives à la réplication inter-grille. "Qu'est-ce que la réplication cross-grid" .
- Vous utilisez un"navigateur web pris en charge" .
- Le compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et des comptes locataires identiques existent sur les deux grilles. "Gérez les locataires autorisés pour la connexion de fédération de grille" .
- L'utilisateur locataire sous lequel vous vous connectez existe déjà sur les deux grilles et appartient à un groupe d'utilisateurs qui possède le"Autorisation d'accès racine" .

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

Créer deux buckets

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

Étapes

1. En commençant à partir de l'une des grilles de la connexion de fédération de grille, créez un nouveau compartiment :
   a. Connectez-vous au compte de tenant à l'aide des informations d'identification d'un utilisateur de tenant qui existe sur les deux grilles.

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

   b. Suivez les instructions à "Créer un compartiment S3".

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

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

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

Activer la réplication entre les grilles

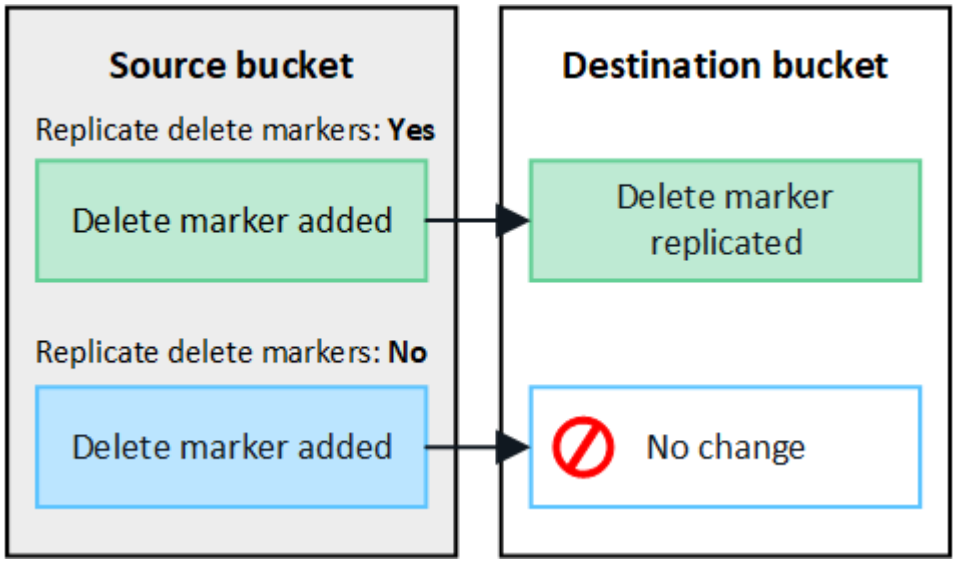
Vous devez effectuer ces étapes avant d'ajouter des objets à l'un ou l'autre compartiment.

Étapes

1. À partir d'une grille dont vous voulez répliquer les objets, activez "réplication multigrille dans une direction":
   a. Connectez-vous au compte du locataire pour le compartiment.
   b. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.
   c. Sélectionnez le nom du compartiment dans le tableau pour accéder à la page de détails du compartiment.
   d. Sélectionnez l'onglet **réplication multigrille**.
   e. Sélectionnez **Activer** et consultez la liste des exigences.
   f. Si toutes les exigences ont été satisfaites, sélectionnez la connexion de fédération de grille que vous souhaitez utiliser.

g. Vous pouvez également modifier le paramètre **replicate delete markers** pour déterminer ce qui se passe sur la grille de destination si un client S3 envoie une demande de suppression à la grille source qui n'inclut pas d'ID de version :

   - **Yes** (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 bucket source mais n'est pas répliqué dans le bucket de destination.



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

Se référer à"Qu'est-ce que la réplication cross-grid" pour plus de détails.

a. Vous pouvez également modifier le paramètre de la catégorie d'audit **réplication multigrille** pour gérer le volume des messages d'audit :

   - **Erreur** (par défaut) : seules les demandes de réplication inter-grille en échec sont incluses dans la sortie d'audit.
   - **Normal** : toutes les demandes de réplication inter-grille sont incluses, ce qui augmente considérablement le volume de la sortie d'audit.

b. Vérifiez 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 apparaît. Les objets ajoutés à ce bucket sont désormais automatiquement répliqués sur l'autre grille. La **réplication inter-grille** est affichée comme une fonctionnalité activée sur la page des détails du bucket.

2. Si vous le souhaitez, accédez au compartiment correspondant sur l'autre grille et "activez la réplication entre les grilles dans les deux sens".

Tester la réplication entre les grilles

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

Avant de commencer

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

Étapes

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

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

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

Désactiver la réplication entre les grilles

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

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

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

> Vous ne pouvez pas réactiver la réplication sauf si les deux compartiments sont vides.

Avant de commencer

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

Étapes

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

      Après quelques instants, un message de réussite s'affiche. Les nouveaux objets ajoutés à ce compartiment ne peuvent plus être automatiquement répliqués sur l'autre grille. **La réplication multigrille** n'est plus affichée comme fonction activée sur la page compartiments.
2. Si la réplication inter-grille a été configurée pour se produire dans les deux directions, allez dans le compartiment correspondant sur l'autre grille et arrêtez la réplication inter-grille dans l'autre direction.

Afficher les connexions de fédération de grille

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

Avant de commencer

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

Étapes

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

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

Colonne	Description
Nom de la connexion	Les connexions de fédération de grille que ce locataire a l'autorisation d'utiliser.

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

2. Si vous le souhaitez, sélectionnez un nom de compartiment à "afficher les détails du compartiment".

efface la dernière erreur

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

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

> Cette colonne affiche uniquement la dernière erreur de réplication inter-grille à se produire ; les erreurs précédentes qui se sont peut-être produites ne seront pas affichées.

Étapes

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

   Par exemple, cette erreur indique que le compartiment de destination de la réplication inter-grid était dans un état non valide, probablement parce que la gestion de version a été suspendue ou que le verrouillage d'objet S3 a été activé.

2. Effectuez toutes les actions recommandées. Par exemple, si la gestion des versions a été suspendue dans le compartiment de destination pour la réplication inter-grid, réactivez la gestion des versions pour ce compartiment.

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

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

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

Gestion des groupes et des utilisateurs

Utiliser la fédération des identités

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

Configurez la fédération des identités pour le gestionnaire des locataires

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

Avant de commencer

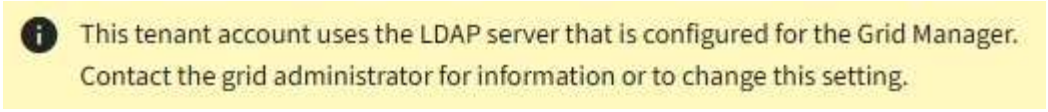
- Vous êtes connecté au gestionnaire de locataires à l'aide d'un"navigateur web pris en charge" .
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".
- Vous utilisez Active Directory, Microsoft Entra ID, OpenLDAP ou Oracle Directory Server comme fournisseur d'identité.

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

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

Description de la tâche

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

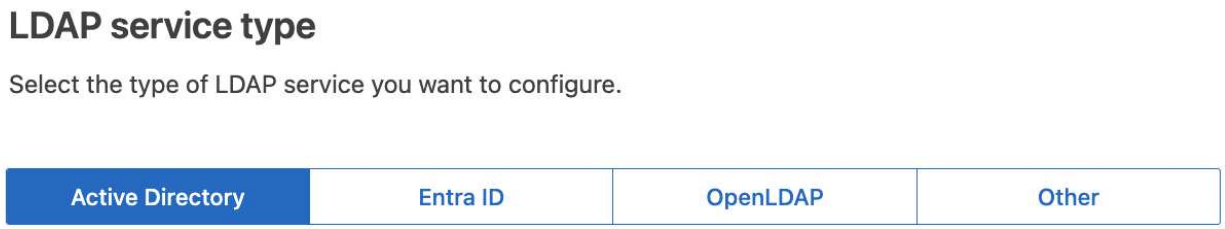


Entrez la configuration

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

Étapes

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

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

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

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

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

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

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

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

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

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

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

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

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

  Entrez l'un des motifs suivants :

  - **Modèle UserPrincipalName (AD et Entra ID)**: `[USERNAME]@example.com`
  - **Modèle de nom de connexion de niveau inférieur (AD et Entra ID)**: `example\[USERNAME]`

- **Motif de nom distinctif** : `CN=[USERNAME],CN=Users,DC=example,DC=com`

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

6. Dans la section transport Layer Security (TLS), sélectionnez un paramètre de sécurité.
   - **Utiliser STARTTLS** : Utilisez STARTTLS pour sécuriser les communications avec le serveur LDAP. Il s'agit de l'option recommandée pour Active Directory, OpenLDAP ou Autre, mais cette option n'est pas prise en charge pour 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'utilisation de l'option **Ne pas utiliser TLS** n'est pas prise en charge si votre serveur Active Directory applique la signature LDAP. Vous devez utiliser STARTTLS ou LDAPS.

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

     Si vous sélectionnez ce paramètre, copiez et collez le certificat de sécurité personnalisé dans la zone de texte certificat de l'autorité de certification.

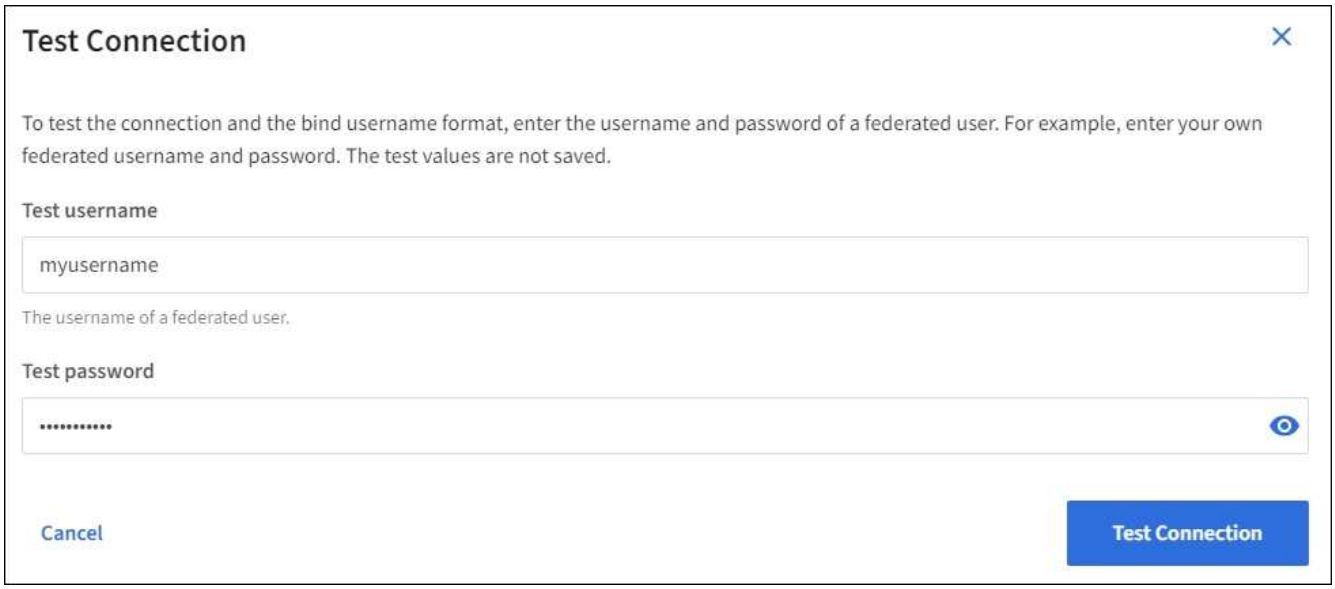
Testez la connexion et enregistrez la configuration

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

Étapes

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

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



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

Forcer la synchronisation avec le référentiel d'identité

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

Étapes

1. Accédez à la page fédération des identités.
2. Sélectionnez **serveur de synchronisation** en haut de la page.

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

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

Désactiver la fédération des identités

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

Description de la tâche

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

- Les utilisateurs fédérés ne pourront pas se connecter.
- Les utilisateurs fédérés qui sont actuellement connectés conservent l'accès au système StorageGRID

jusqu'à l'expiration de leur session, mais ils ne pourront pas se connecter après l'expiration de leur session.

- La synchronisation entre le système StorageGRID et la source d'identité ne se produira pas et les alertes ne seront pas générées pour les comptes qui n'ont pas été synchronisés.
- La case à cocher **Activer la fédération d'identité** est désactivée si l'état de l'authentification unique (SSO) est **Activé** ou **Mode Sandbox**. Le statut SSO sur la page d'authentification unique doit être **Désactivé** avant de pouvoir désactiver la fédération d'identité. Voir "Désactiver l'authentification unique" .

Étapes

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

Instructions de configuration du serveur OpenLDAP

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

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

Recouvrements de memberOf et de raffint

Les recouvrements de membre et de raffinage doivent être activés. Pour plus d'informations, reportez-vous aux instructions relatives à la maintenance des membres de groupe inversé dans le "Documentation OpenLDAP : version 2.4 - Guide de l'administrateur".

Indexation

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

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

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

Reportez-vous aux informations sur la maintenance de l'appartenance à "Documentation OpenLDAP : version 2.4 - Guide de l'administrateur"un groupe inversé dans le .

Gestion des groupes de locataires

Créez des groupes pour un locataire S3

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

Avant de commencer

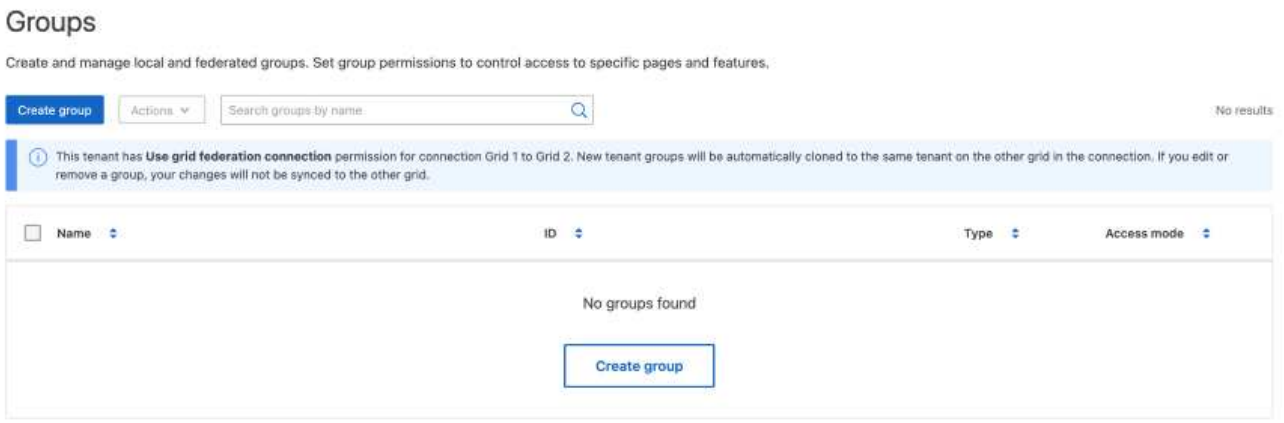
- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".
- Si vous prévoyez d'importer un groupe fédéré, vous avez "fédération des identités configurée"et le groupe fédéré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

Accédez à l'assistant de création de groupe

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

Étapes

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



3. Sélectionnez **Créer groupe**.

Choisissez un type de groupe

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

Étapes

1. Sélectionnez l'onglet **Groupe local** pour créer un groupe local ou sélectionnez l'onglet **Groupe fédéré** pour importer un groupe à partir du référentiel d'identité configuré précédemment.

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

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

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

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

3. Sélectionnez **Continuer**.

Gérer les autorisations de groupe

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

Étapes

1. Pour **Access mode**, sélectionnez l'une des options suivantes :
   - **Lecture-écriture** (par défaut) : les utilisateurs peuvent se connecter au gestionnaire de locataires et gérer la configuration du locataire.
   - **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent pas apporter de modifications ni exécuter d'opérations dans le gestionnaire de locataires ou l'API de gestion des locataires. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.

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

2. Sélectionnez une ou plusieurs autorisations pour ce groupe.

   Voir "Autorisations de gestion des locataires".

3. Sélectionnez **Continuer**.

Définissez la règle de groupe S3

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

Étapes

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

Stratégie de groupe	Description
Aucun accès à S3	Par défaut. Les utilisateurs de ce groupe n'ont pas accès aux ressources S3, sauf si l'accès est accordé avec une règle de compartiment. Si vous sélectionnez cette option, seul l'utilisateur root peut accéder aux ressources S3 par défaut.

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 afficher la liste des objets et lire les données d'objet, les métadonnées et les balises. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe en lecture seule s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
Accès complet	Les utilisateurs de ce groupe bénéficient d'un accès complet aux ressources S3, y compris les compartiments. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe à accès complet s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
Réduction des ransomwares	Cet exemple de règle 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 la gestion des versions d'objet est activée. Les utilisateurs de tenant Manager disposant de l'autorisation **gérer tous les compartiments** peuvent remplacer cette stratégie de groupe. Limitez l'autorisation gérer tous les compartiments aux utilisateurs de confiance et utilisez l'authentification multifacteur (MFA), le cas échéant.
Personnalisées	Les utilisateurs du groupe se voient accorder les autorisations que vous spécifiez dans la zone de texte.

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

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

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

Ajouter des utilisateurs (groupes locaux uniquement)

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

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

Étapes

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

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

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

Autorisations de gestion des locataires

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

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

- Afficher le tableau de bord
- Modifier son propre mot de passe (pour les utilisateurs locaux)

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

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

Vous pouvez attribuer les autorisations suivantes à un groupe.

Autorisations	Description	Détails
Accès racine	Donne un accès complet au gestionnaire des locataires et à l'API de gestion des locataires.	
Gérez vos identifiants S3	Permet aux utilisateurs de créer et de supprimer leurs propres clés d'accès S3.	Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu **STORAGE (S3)** > **My S3 Access keys**.

Autorisations	Description	Détails
Afficher tous les compartiments	Permet aux utilisateurs d'afficher tous les buckets et configurations de buckets.	Les utilisateurs qui ne disposent pas de l'autorisation Afficher tous les compartiments ou gérer tous les compartiments ne voient pas l'option de menu **compartiments**. Cette autorisation est remplacée par l'autorisation Gérer tous les buckets. Cela n'affecte pas les stratégies de groupe ou de compartiment S3 utilisées par les clients S3 ou la console S3.
Gestion de tous les compartiments	Permet aux utilisateurs d'utiliser Tenant Manager et l'API Tenant Management pour créer et supprimer des compartiments S3 et pour gérer les paramètres de tous les compartiments S3 du compte locataire, quels que soient les compartiments S3 ou les stratégies de groupe.	Les utilisateurs qui ne disposent pas de l'autorisation Afficher tous les compartiments ou gérer tous les compartiments ne voient pas l'option de menu **compartiments**. Cette autorisation remplace l'autorisation Afficher tous les buckets. Cela n'affecte pas les stratégies de groupe ou de compartiment S3 utilisées par les clients S3 ou la console S3.
Gestion des terminaux	Permet aux utilisateurs d'utiliser le gestionnaire de locataires ou l'API de gestion des locataires pour créer ou modifier des terminaux de service de plateforme, qui sont utilisés comme destination pour les services de plateforme StorageGRID.	Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu **Platform Services Endpoints**.
Utilisez l'onglet de la console S3	Associé à l'autorisation Afficher tous les compartiments ou gérer tous les compartiments, permet aux utilisateurs d'afficher et de gérer des objets à partir de l'onglet de la console S3 de la page de détails d'un compartiment.	

Gérer les groupes

Gérez vos groupes de locataires selon vos besoins pour afficher, modifier ou dupliquer un groupe, etc.

Avant de commencer

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

Afficher ou modifier un groupe

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

Étapes

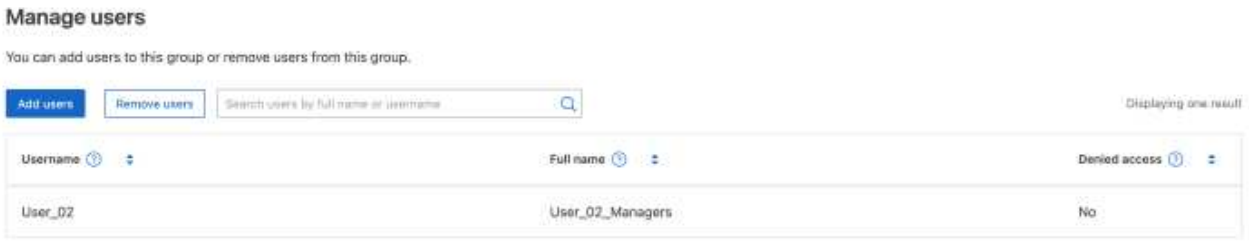
1. Sélectionnez **Gestion des accès** > **Groupes**.
2. Consultez les informations fournies sur la page groupes, qui répertorie les informations de base pour tous les groupes locaux et fédérés pour ce compte de tenant.

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

   - Un message de bannière indique que si vous modifiez ou supprimez un groupe, vos modifications ne seront pas synchronisées avec l'autre grille.
   - Si nécessaire, un message de bannière indique si les groupes n'ont pas été clonés dans le locataire sur la grille de destination. Vous pouvez réessayez un clone de groupe que cela a échoué.
3. Si vous souhaitez modifier le nom du groupe :
   a. Cochez la case du groupe.
   b. Sélectionnez **actions** > **Modifier le nom du groupe**.
   c. Saisissez le nouveau nom.
   d. Sélectionnez **Enregistrer les modifications.**
4. Si vous souhaitez afficher plus de détails ou apporter des modifications supplémentaires, effectuez l'une des opérations suivantes :
   - Sélectionnez le nom du groupe.
   - Cochez la case du groupe et sélectionnez **actions** > **Afficher les détails du groupe**.
5. Consultez la section Présentation, qui présente les informations suivantes pour chaque groupe :
   - Nom d'affichage
   - Nom unique
   - Type
   - Mode d'accès
   - Autorisations
   - Règle S3
   - Nombre d'utilisateurs dans ce groupe
   - Champs supplémentaires si le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous affichez le groupe sur la grille source du locataire :
     - État de clonage, soit **succès** soit **échec**
     - Une bannière bleue indiquant que si vous modifiez ou supprimez ce groupe, vos modifications ne seront pas synchronisées avec l'autre grille.
6. Modifiez les paramètres du groupe selon vos besoins. Se référer à"Créez des groupes pour un locataire S3" pour plus de détails sur ce qu'il faut saisir.
   a. Dans la section vue d'ensemble, modifiez le nom d'affichage en sélectionnant le nom ou l'icône d'édition .
   b. Dans l'onglet **autorisations de groupe**, mettez à jour les autorisations et sélectionnez **Enregistrer les modifications**.
   c. Dans l'onglet **Stratégie de groupe**, apportez les modifications nécessaires et sélectionnez **Enregistrer les modifications**.

Sélectionnez éventuellement une autre stratégie de groupe S3 ou saisissez la chaîne JSON d'une stratégie personnalisée selon vos besoins.

7. Pour ajouter un ou plusieurs utilisateurs locaux existants au groupe :
   a. Sélectionnez l'onglet utilisateurs.



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

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

8. Pour supprimer des utilisateurs locaux du groupe :
   a. Sélectionnez l'onglet utilisateurs.
   b. Sélectionnez **Supprimer utilisateurs**.
   c. Sélectionnez les utilisateurs que vous souhaitez supprimer, puis sélectionnez **Supprimer utilisateurs**.

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

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

Dupliquer le groupe

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

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

Étapes

1. Sélectionnez **Gestion des accès** > **Groupes**.
2. Cochez la case du groupe que vous souhaitez dupliquer.
3. Sélectionnez **actions** > **Dupliquer le groupe**.
4. Voir"Créez des groupes pour un locataire S3" pour plus de détails sur ce qu'il faut saisir.
5. Sélectionnez **Créer groupe**.

Réessayez le clone de groupe

Pour réessayer un clone qui a échoué :

1. Sélectionnez chaque groupe indiquant *(échec du clonage)* sous le nom du groupe.
2. Sélectionnez **actions** > **groupes de clones**.
3. Consultez l'état de l'opération de clonage dans la page de détails de chaque groupe que vous êtes en train de cloner.

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

Supprimer un ou plusieurs groupes

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

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

Étapes

1. Sélectionnez **Gestion des accès** > **Groupes**.
2. Cochez la case correspondant à chaque groupe à supprimer.
3. Sélectionnez **actions** > **Supprimer groupe** ou **actions** > **Supprimer groupes**.

   Une boîte de dialogue de confirmation s'affiche.
4. Sélectionnez **Supprimer le groupe** ou **Supprimer les groupes**.

Configurer AssumeRole

Avant de commencer

Vous devez être administrateur pour configurer AssumeRole.

Description de la 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 en supposant que ce groupe est valide pour une durée limitée. La séance dure entre 15 minutes et 12 heures, et la séance par défaut est de 1 heure. Lorsque vous supprimez l'utilisateur de la politique de confiance S3 du groupe, l'utilisateur ne peut plus assumer ce groupe.

Étapes

1. Sélectionnez **Gestion des accès** > **Groupes**.
2. Cliquez sur le nom du groupe.
3. Sélectionnez l'onglet **Politique de confiance S3**.
4. Ajoutez votre politique de confiance S3, y compris une liste d'utilisateurs pouvant exécuter AssumeRole.
5. Sélectionnez **Enregistrer les modifications**.
6. Sélectionnez l'onglet **Stratégie de groupe S3**.

7. Modifiez la politique S3 pour spécifier uniquement les actions S3 requises pour les utilisateurs de confiance ajoutés dans la politique de confiance S3 de ce groupe.
8. Sélectionnez **Enregistrer les modifications**.

Exemple de politique de confiance S3 AssumeRole

```
{
    "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 répertoriés dans la politique de confiance S3 peuvent exécuter AssumeRole et recevoir des informations d'identification. Les autorisations finales sont déterminées par la politique de groupe, la politique de compartiment et la politique de session. "Utiliser les politiques d'accès" .

Gérer les utilisateurs

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

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

Avant de commencer

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

Créez un utilisateur local

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

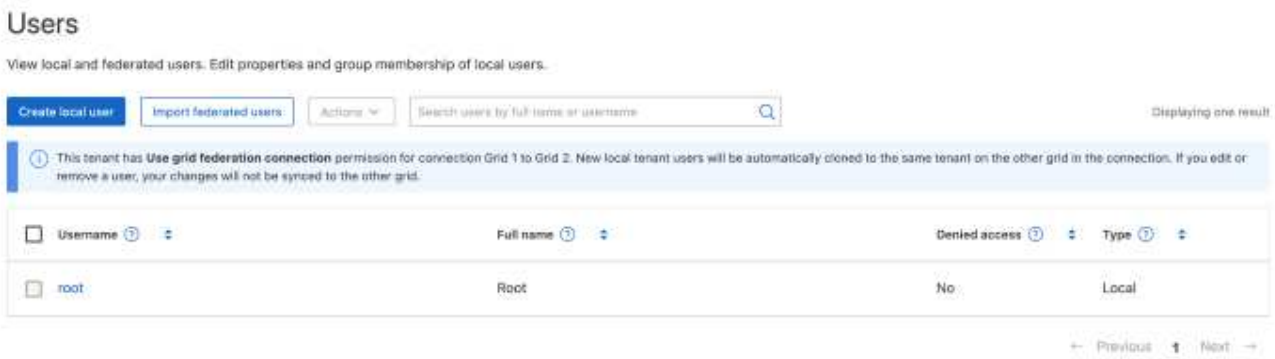
Les utilisateurs S3 qui n'appartiennent à aucun groupe ne disposent pas d'autorisations de gestion ni de règles de groupe S3 qui leur sont appliquées. Il est possible que les utilisateurs bénéficient d'un accès par compartiment S3 accordé via une règle de compartiment.

Accédez à l'assistant de création d'utilisateur

Étapes

1. Sélectionnez **Gestion des accès** > **Utilisateurs**.

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



2. Sélectionnez **Créer utilisateur**.

Entrez les informations d'identification

Étapes

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

Champ	Description
Nom complet	Le nom complet de cet utilisateur, par exemple le prénom et le nom d'une personne ou le nom d'une application.
Nom d'utilisateur	Le nom que cet utilisateur utilisera pour se connecter. Les noms d'utilisateur doivent être uniques et ne peuvent pas être modifiés. **Remarque** : si votre compte locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, une erreur de clonage se produit si le même **Nom d'utilisateur** existe déjà pour le locataire sur la grille de destination.

Champ	Description
Mot de passe et confirmer le mot de passe	Le mot de passe que l'utilisateur utilisera lors de sa connexion.
Refuser l'accès	Sélectionnez **Oui** pour empêcher cet utilisateur de se connecter au compte de tenant, même s'il appartient toujours à un ou plusieurs groupes. Par exemple, sélectionnez **Oui** pour suspendre temporairement la capacité d'un utilisateur à se connecter.

2. Sélectionnez **Continuer**.

Affecter à des groupes

Étapes

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

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

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

2. Sélectionnez **Créer utilisateur**.

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

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

Afficher ou modifier un utilisateur local

Étapes

1. Sélectionnez **Gestion des accès** > **Utilisateurs**.
2. Consultez les informations fournies sur la page utilisateurs, qui répertorie les informations de base pour tous les utilisateurs locaux et fédérés pour ce compte de tenant.

   Si le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous affichez l'utilisateur sur la grille source du locataire :

   - Un message de bannière indique que si vous modifiez ou supprimez un utilisateur, vos modifications ne seront pas synchronisées avec l'autre grille.
   - Si nécessaire, un message de bannière indique si les utilisateurs n'ont pas été clonés dans le locataire sur la grille de destination. Vous pouvez réessayez un clone utilisateur qui a échoué.
3. Si vous souhaitez modifier le nom complet de l'utilisateur :
   a. Cochez la case de l'utilisateur.

b. Sélectionnez **actions** > **Modifier le nom complet**.

c. Saisissez le nouveau nom.

d. Sélectionnez **Enregistrer les modifications.**

4. Si vous souhaitez afficher plus de détails ou apporter des modifications supplémentaires, effectuez l'une des opérations suivantes :
   - Sélectionnez le nom d'utilisateur.
   - Cochez la case de l'utilisateur et sélectionnez **actions** > **Afficher les détails de l'utilisateur**.
5. Consultez la section Présentation, qui présente les informations suivantes pour chaque utilisateur :
   - Nom complet
   - Nom d'utilisateur
   - Type d'utilisateur
   - Accès refusé
   - Mode d'accès
   - Appartenance à un groupe
   - Champs supplémentaires si le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous affichez l'utilisateur sur la grille source du locataire :
     - État de clonage, soit **succès** soit **échec**
     - Une bannière bleue indiquant que si vous modifiez cet utilisateur, vos modifications ne seront pas synchronisées avec l'autre grille.
6. Modifiez les paramètres utilisateur selon vos besoins. Voir Créer un utilisateur local pour plus de détails sur ce que vous devez saisir.

   a. Dans la section vue d'ensemble, modifiez le nom complet en sélectionnant le nom ou l'icône d'édition .

      Vous ne pouvez pas modifier le nom d'utilisateur.

   b. Dans l'onglet **Mot de passe**, modifiez le mot de passe de l'utilisateur et sélectionnez **Enregistrer les modifications**.

   c. Dans l'onglet **accès**, sélectionnez **non** pour permettre à l'utilisateur de se connecter ou sélectionnez **Oui** pour empêcher l'utilisateur de se connecter. Ensuite, sélectionnez **Enregistrer les modifications**.

   d. Dans l'onglet **clés 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 supprimer l'utilisateur des groupes. Sélectionnez ensuite **Enregistrer les modifications**.
7. Confirmez que vous avez sélectionné **Enregistrer les modifications** pour chaque section que vous avez modifiée.

Importer des utilisateurs fédérés

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

Étapes

1. Sélectionnez **Gestion des accès** > **Utilisateurs**.

2. Sélectionnez **Importer les utilisateurs fédérés**.
3. Saisissez l'UUID ou le nom d'utilisateur d'un ou 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 **Importer les utilisateurs fédérés**.

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

Dupliquer l'utilisateur local

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

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

Étapes

1. Sélectionnez **Gestion des accès** > **Utilisateurs**.
2. Cochez la case correspondant à l'utilisateur que vous souhaitez dupliquer.
3. Sélectionnez **actions** > **Dupliquer utilisateur**.
4. Voir Créer un utilisateur local pour plus de détails sur ce que vous devez saisir.
5. Sélectionnez **Créer utilisateur**.

Réessayez le clone utilisateur

Pour réessayer un clone qui a échoué :

1. Sélectionnez chaque utilisateur qui indique *(échec du clonage)* sous le nom d'utilisateur.
2. Sélectionnez **actions** > **Cloner les utilisateurs**.
3. Consultez l'état de l'opération de clonage sur la page de détails de chaque utilisateur que vous êtes en train de cloner.

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

Supprimez un ou plusieurs utilisateurs locaux

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

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

Vous devez utiliser le référentiel d'identité fédéré pour supprimer des utilisateurs fédérés.

Étapes

1. Sélectionnez **Gestion des accès** > **Utilisateurs**.
2. Cochez la case correspondant à chaque utilisateur à supprimer.
3. Sélectionnez **actions** > **Supprimer utilisateur** ou **actions** > **Supprimer utilisateurs**.

   Une boîte de dialogue de confirmation s'affiche.

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

Gestion des clés d'accès S3

Gestion des clés d'accès S3

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

Les clés d'accès S3 peuvent être gérées de la manière suivante :

- Les utilisateurs disposant de l'autorisation **gérer vos propres informations d'identification S3** peuvent créer ou supprimer leurs propres clés d'accès S3.
- Les utilisateurs disposant de l'autorisation **Root Access** peuvent gérer les clés d'accès du compte root S3 et de tous les autres utilisateurs. Les clés d'accès racine offrent un accès complet à toutes les compartiments et objets du locataire, sauf si une règle de compartiment est explicitement désactivée.

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

Créez vos propres clés d'accès S3

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

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez vos propres informations d'identification S3 ou autorisations d'accès racine".

Description de la tâche

Vous pouvez créer une ou plusieurs clés d'accès S3 qui vous permettent de créer et de gérer des compartiments pour votre compte de locataire. Après avoir créé une nouvelle clé d'accès, mettez à jour

l'application avec votre nouvel ID de clé d'accès et votre clé d'accès secrète. Pour des raisons de sécurité, ne créez pas plus de clés que nécessaire et supprimez les clés que vous n'utilisez pas. Si vous n'avez qu'une seule clé et que vous êtes sur le point d'expirer, créez une nouvelle clé avant l'expiration de l'ancienne, puis supprimez l'ancienne.

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

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

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

Étapes

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

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

2. Sélectionnez **Créer clé**.
3. Effectuez l'une des opérations suivantes :
   - Sélectionnez **ne définissez pas d'heure d'expiration** pour créer une clé qui n'expire pas. (Valeur par défaut)
   - Sélectionnez **définissez une heure d'expiration** et définissez la date et l'heure d'expiration.

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

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

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

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

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

6. Sélectionnez **Terminer**.

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

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

Affichez vos clés d'accès S3

Si vous utilisez un locataire S3 et que vous disposez de la "autorisation appropriée", vous pouvez afficher la liste de vos clés d'accès S3. Vous pouvez trier la liste en fonction de l'heure d'expiration afin de déterminer quelles clés vont bientôt expirer. Si nécessaire, vous pouvez "créer de nouvelles clés" ou "supprimer les clés" que vous n'utilisez plus.

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

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs possédant les informations d'identification Manage Your Own S3 "permission".

Étapes

1. Sélectionnez **STORAGE (S3)** > **Mes clés d'accès**.
2. À partir de la page Mes clés d'accès, triez toutes les clés d'accès existantes par **heure d'expiration** ou **ID de clé d'accès**.
3. Au besoin, créez de nouvelles clés ou supprimez les clés que vous n'utilisez plus.

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

   Les clés expirées sont supprimées automatiquement.

Supprimez vos propres clés d'accès S3

Si vous utilisez un locataire S3 et que vous disposez des autorisations appropriées, vous pouvez supprimer vos propres clés d'accès S3. Une fois la clé d'accès supprimée, elle ne peut plus être utilisée pour accéder aux objets et aux compartiments du compte du locataire.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Gérez vos propres identifiants S3".

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

Étapes

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

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

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

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

Avant de commencer

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

Description de la tâche

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

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

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

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

Étapes

1. Sélectionnez **Gestion des accès** > **Utilisateurs**.
2. Sélectionnez l'utilisateur dont vous souhaitez gérer les clés d'accès S3.

   La page de détails utilisateur s'affiche.

3. Sélectionnez **touches d'accès**, puis **touche Créer**.
4. Effectuez l'une des opérations suivantes :
   - Sélectionnez **ne pas définir de délai d'expiration** pour créer une clé qui n'expire pas. (Valeur par défaut)
   - Sélectionnez **définissez une heure d'expiration** et définissez la date et l'heure d'expiration.

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

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

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

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

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

7. Sélectionnez **Terminer**.

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

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

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

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

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine".

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

Étapes

1. Sélectionnez **Gestion des accès** > **Utilisateurs**.
2. Sur la page utilisateurs, sélectionnez l'utilisateur dont vous souhaitez afficher les clés d'accès S3.
3. Dans la page Détails de l'utilisateur, sélectionnez **touches d'accès**.
4. Trier les clés par **heure d'expiration** ou **ID de clé d'accès**.
5. Si nécessaire, créez de nouvelles clés et supprimez manuellement les clés que le n'est plus utilisé.

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

   Les clés expirées sont supprimées automatiquement.

Informations associées

- "Créez les clés d'accès S3 d'un autre utilisateur"
- "Supprimez les clés d'accès S3 d'un autre utilisateur"

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

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

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine".

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

Étapes

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

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

Gestion des compartiments S3

Créer un compartiment S3

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

Avant de commencer

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

> Les autorisations permettant de définir ou de modifier les propriétés de verrouillage d'objet S3 des compartiments ou des objets peuvent être accordées par"politique de compartiment ou règle de groupe" .

- Si vous prévoyez d'activer le verrouillage objet S3 pour un compartiment, un administrateur du grid a activé le paramètre de verrouillage objet S3 global pour le système StorageGRID. Vous avez également passé en revue les exigences relatives aux compartiments et aux objets S3 Object Lock.
- Si chaque locataire dispose de 5,000 compartiments, chaque nœud de stockage de la grille dispose d'au moins 64 Go de RAM.

> Chaque grille peut contenir un maximum de 100 000 buckets, y compris"seaux de branches" .

Accéder à l'assistant

Étapes

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

Entrez les détails

Étapes

1. Entrez les détails du compartiment.

Champ	Description
Nom du compartiment	Nom du compartiment conforme aux règles suivantes : • Il doit être unique sur chaque système StorageGRID (et pas seulement au sein du compte du locataire). • Doit être conforme DNS. • Doit contenir au moins 3 et 63 caractères. • Chaque étiquette doit commencer et se terminer par une lettre ou un chiffre en minuscules et ne peut utiliser que des lettres minuscules, des chiffres et des tirets. • Ne doit pas contenir de périodes dans les demandes de type hébergement virtuel. Les périodes provoquera des problèmes avec la vérification du certificat générique du serveur. Pour plus d'informations, voir "Documentation Amazon Web Services (AWS) sur les règles d'attribution de nom de compartiment". **Remarque** : vous ne pouvez pas modifier le nom du compartiment après avoir créé le compartiment.
Région	La région du godet. Votre administrateur StorageGRID gère les régions disponibles. La région d'un bucket peut affecter la politique de protection des données appliquée aux objets. Par défaut, tous les buckets sont créés dans le `us-east-1` région. 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. **Remarque** : vous ne pouvez pas modifier la région après avoir créé le compartiment.

2. Sélectionnez **Continuer**.

Gérer les paramètres

Étapes

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

   Activez la gestion des versions d'objet si vous souhaitez stocker chaque version de chaque objet dans ce compartiment. Vous pouvez ensuite récupérer les versions précédentes d'un objet si nécessaire.

   Vous devez activer le contrôle de version des objets si :

   ◦ Le bucket sera utilisé pour la réplication inter-grille.
   ◦ Vous souhaitez créer un"seau de branche" de ce seau.

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

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

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

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

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

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

> Votre administrateur de grille doit vous donner l'autorisation de "Utiliser les fonctionnalités spécifiques du verrouillage objet S3".

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

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

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

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

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

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

4. Vous pouvez également sélectionner **Activer la limite de capacité**, saisir une valeur et sélectionner l'unité de capacité.

   La limite de capacité est la capacité maximale disponible pour les objets de ce compartiment. 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 godet est illimitée. Pour plus d'informations, reportez-vous à la section "Utilisation limitée de la capacité" .

5. Si vous le souhaitez, sélectionnez **Activer la limite du nombre d'objets**.

   La limite du nombre d'objets est le nombre maximal d'objets que ce bucket 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 godet est créé et ajouté au tableau sur la page godets.

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

Vous pouvez également"créer des compartiments de branches" selon les besoins.

Afficher les détails du compartiment

Vous pouvez afficher les compartiments de votre compte de locataire.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Accès racine, gestion de tous les compartiments ou autorisation Afficher tous les compartiments". Ces autorisations remplacent les paramètres d'autorisation dans les stratégies de groupe ou de compartiment.

Étapes

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

   La page compartiments s'affiche.

2. Consultez le tableau récapitulatif pour chaque compartiment.

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

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

Nom

Nom unique du compartiment, qui ne peut pas être modifié.

Fonctionnalités activées

Liste des fonctions activées pour le compartiment.

Verrouillage d'objet S3

Indique si le verrouillage d'objet S3 est activé pour le compartiment.

Cette colonne apparaît uniquement si le verrouillage objet S3 est activé pour la grille. Cette colonne affiche également des informations pour tous les compartiments conformes existants.

Région

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

Nombre d'objets

Nombre d'objets dans ce compartiment. Si la gestion des versions des compartiments est activée, les versions d'objets non actuelles sont incluses dans cette valeur.

Lorsque des objets sont ajoutés ou supprimés, il est possible que cette valeur ne soit pas mise à jour immédiatement.

Espace utilisé

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

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

Du stockage

Pourcentage utilisé de la limite de capacité du godet, si un pourcentage a été défini.

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 télécharger des objets et rejette de nouvelles ingests dans ce compartiment si le locataire a dépassé la limite de capacité. Cependant, StorageGRID ne prend pas en compte la taille du téléchargement actuel lorsqu'il détermine si la limite de capacité a été dépassée. En cas de suppression d'objets, un locataire peut temporairement empêcher le chargement 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.

Cette valeur indique la taille logique et non la taille physique nécessaire au stockage des objets et de leurs métadonnées.

Capacité

S'il est défini, la limite de capacité du godet.

Date de création

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. Affichez le récapitulatif en haut de la page Web pour confirmer les détails du compartiment, tels que le nombre de régions et d'objets.

b. Affichez les barres d'utilisation de la limite de capacité et 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. Au besoin, sélectionnez **Supprimer les objets dans le compartiment** et **Supprimer le compartiment**.

> Soyez attentif aux mises en garde qui apparaissent lorsque vous sélectionnez chacune de ces options. Pour plus d'informations, se reporter à :
>
> - "Supprime tous les objets d'un compartiment"
> - "Supprimer un compartiment" (le godet doit être vide)

d. Afficher ou modifier les paramètres du compartiment dans chacun des onglets, selon les besoins.

- **S3 Console** : permet d'afficher les objets du compartiment. Pour plus d'informations, reportez-vous "Utiliser la console S3"à .
- **Options de compartiment** : afficher ou modifier les paramètres des options. Certains paramètres, tels que S3 Object Lock, ne peuvent pas être modifiés après la création du compartiment.
  - "Gestion de la cohérence des compartiments"
  - "Mises à jour de l'heure du dernier accès"
  - "Limite de capacité"
  - "Limite du nombre d'objets"
  - "Gestion des versions d'objet"
  - "Verrouillage d'objet S3"
  - "Rétention de compartiments par défaut"
  - "Gérer la réplication entre les grilles" (si autorisé pour le locataire)
- **Platform services**: "Gestion des services de plateforme" (Si autorisé pour le locataire)
- **Accès au compartiment** : afficher ou modifier les paramètres des options. Vous devez disposer d'autorisations d'accès spécifiques.
  - Configure"CORS pour les buckets et les objets" ainsi, le bucket et les objets qu'il contient seront accessibles aux applications Web dans d'autres domaines.
  - "Contrôler l'accès des utilisateurs" Pour un compartiment S3 et les objets dans ce compartiment.
- **Branches** : afficher la liste des branches du bucket. "Créer un nouveau bucket de branches ou gérer des buckets de branches" .

Qu'est-ce qu'un bucket de branche ?

Un bucket de branche fournit un accès aux objets d'un bucket tels qu'ils existaient à un moment donné.

Vous créez un bucket de branche à partir d'un bucket existant. Une fois que vous avez créé un bucket de branche, le bucket d'origine à partir duquel il a été créé est appelé le *bucket de base*. De plus, vous pouvez créer un bucket de branche à partir d'un autre bucket de branche.

Un bucket 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 buckets de base :

- "Verrouillage d'objet S3"
- "Réplication entre plusieurs grilles"pour les godets de base
- "Politiques de compartiments"pour les buckets versionnés pour nettoyer les anciennes versions d'objets

Notez les caractéristiques suivantes des compartiments de branche :

- Vous pouvez accéder aux objets dans les compartiments de branche en utilisant"Console S3 pour télécharger des objets" .
- Lorsque les clients accèdent aux objets d'un bucket de branche, le bucket de branche"politiques d'accès" , plutôt que les politiques du compartiment de base, déterminent si l'accès est accordé ou refusé.
- Les objets créés dans un bucket de base sont évalués en fonction de la manière dont"Règles ILM" appliquer au bucket de base. Les objets créés dans un bucket de branche sont évalués en fonction de la manière dont les règles ILM s'appliquent au bucket de branche.
- La réplication inter-grille n'est pas prise en charge pour les buckets de branche.
- Les services de plateforme ne sont pas pris en charge pour les buckets de branches.

Exemples d'utilisation de compartiments de branchement

- Vous pouvez utiliser un bucket de branche pour supprimer les objets corrompus en créant un bucket de branche à partir d'un moment antérieur à la corruption, puis en pointant les applications vers le bucket de branche au lieu du bucket de base qui contient les objets corrompus.
- Vous enregistrez des données dans un bucket versionné. Une vulnérabilité accidentelle a provoqué l'ingestion de nombreux objets indésirables après le temps *T*. Vous pouvez créer un compartiment de branche pour la valeur Avant l'heure, *T*, et rediriger les opérations client vers ce compartiment de branche. Ensuite, seuls les objets ingérés avant l'heure Avant *T* sont exposés aux clients.

Opérations sur les objets dans les compartiments de branche

- Une opération d'objet PUT sur un bucket de branche crée un objet dans la branche.
- Une opération d'objet GET sur un bucket de branche récupère un objet de la branche. Si l'objet n'existe pas dans le bucket de branche, l'objet est récupéré à partir du bucket de base.
- Les suppressions d'objets des compartiments de branche se produisent comme suit :

Fonctionnement	Cible	Résultat	Visibilité des objets dans le bucket de base	Visibilité des objets dans le bucket de branche
Supprimer sans ID de version	Godet de base	Le marqueur de suppression est créé uniquement pour le compartiment de base	HEAD/GET renvoie L'objet n'existe pas, mais des versions spécifiques sont toujours accessibles	HEAD/GET renvoie L'objet existe et des versions spécifiques sont toujours accessibles Le marqueur de suppression aurait été créé après le bucket de branche `beforeTime` .

Fonctionnement	Cible	Résultat	Visibilité des objets dans le bucket de base	Visibilité des objets dans le bucket de branche
Supprimer avec l'ID de version	Godet de base	La version d'objet spécifique est supprimée pour le bucket de base et de branche	HEAD/GET renvoie La version de l'objet n'existe pas	HEAD/GET renvoie La version de l'objet n'existe pas
Supprimer sans ID de version	Seau à branches	Le marqueur de suppression est créé uniquement pour le compartiment de branche	HEAD/GET renvoie l'objet (l'objet bucket de base n'est pas affecté)	HEAD/GET renvoie L'objet n'existe pas
Supprimer avec l'ID de version	Seau à branches	La version d'objet spécifique est supprimée uniquement pour le bucket de branche	HEAD/GET renvoie une version d'objet spécifique (l'objet de compartiment de base n'est pas affecté)	HEAD/GET renvoie La version de l'objet n'existe pas

Voir aussi"Suppression d'objets avec version S3" .

Gérer les compartiments de branches

Utilisez le gestionnaire de locataires pour créer et afficher les détails des compartiments de branches.

Avant de commencer

- Vous vous êtes connecté au gestionnaire de locataires à l'aide d'un"navigateur web pris en charge" .
- Vous appartenez à un groupe d'utilisateurs disposant de l'accès Root ou"Autorisations de gestion de tous les compartiments" . Ces autorisations remplacent les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.
- Le bucket de base à partir duquel vous souhaitez créer une branche a"contrôle de version activé" .
- Vous êtes le propriétaire du bucket de base.

Description de la tâche

Notez les informations suivantes pour les compartiments de branches :

- Les autorisations permettant de définir les propriétés de verrouillage d'objet S3 des buckets ou des objets peuvent être accordées par"politique de compartiment ou règle de groupe" .
- Si vous suspendez le contrôle de version sur le bucket de base, le contenu du bucket de base ne sera plus visible dans ses buckets de branche.

Après avoir configuré et créé un bucket de branche, vous ne pouvez pas modifier la configuration.

Créer un bucket de branche

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.
2. Sélectionnez le bucket à partir duquel vous souhaitez créer une branche (le « bucket de base »).
3. Sur la page des détails du bucket, sélectionnez **Branches** > **Créer un bucket de branche**.

   Le bouton **Créer un bucket de branche** est désactivé si le contrôle de version n'est pas activé pour le bucket de base.

Entrez les détails

Étapes

1. Saisissez les détails du compartiment de branche.

Champ	Description
Nom du bucket de branche	Un nom pour le bucket de branche qui respecte ces règles : • Il doit être unique sur chaque système StorageGRID (et pas seulement au sein du compte du locataire). • Doit être conforme DNS. • Doit contenir au moins 3 et 63 caractères. • Chaque étiquette doit commencer et se terminer par une lettre ou un chiffre en minuscules et ne peut utiliser que des lettres minuscules, des chiffres et des tirets. • Ne doit pas contenir de périodes dans les demandes de type hébergement virtuel. Les périodes provoquera des problèmes avec la vérification du certificat générique du serveur. Pour plus d'informations, voir "Documentation Amazon Web Services (AWS) sur les règles d'attribution de nom de compartiment". **Remarque** : vous ne pouvez pas modifier le nom après avoir créé le bucket de branche.
Région (ne peut pas être modifiée pour les compartiments de branche)	La région du bucket de branche. La région du bucket de branche doit correspondre à la région du bucket de base, ce champ est donc désactivé pour les buckets de branche.
Avant le temps	L'heure limite pour que les versions d'objet créées dans le bucket de base soient accessibles à partir du bucket de branche. Le bucket de branche donne accès aux versions d'objet créées avant l'heure Before. Avant le temps, il doit y avoir une date et une heure qui sont passées. Cela ne peut pas être une date future.

Champ	Description
Type de godet de branche	• **Lecture-écriture** : Vous pouvez ajouter ou supprimer des objets ou des versions d'objets dans le bucket de branche. • **Lecture seule** : vous ne pouvez pas modifier les objets dans le bucket de branche. **Remarque** : vous pouvez définir le type de compartiment de branche en lecture seule uniquement si le compartiment 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 **Continuer**.

Gérer les paramètres de l'objet (facultatif)

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

Étapes

1. Si le paramètre global de verrouillage d'objet S3 est activé, activez éventuellement le verrouillage d'objet S3 pour le compartiment de branche. Pour activer le verrouillage d'objet S3, le bucket de branche doit être un bucket en lecture-écriture.

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

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

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

   > Votre administrateur de grille doit vous donner l'autorisation de "Utiliser les fonctionnalités spécifiques du verrouillage objet S3".

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

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

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

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

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

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

3. En option, sélectionnez **Activer la limite de capacité**.

   La limite de capacité est la capacité maximale disponible pour le bucket de branche. 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 du bucket de branche est illimitée. Consultez "Utilisation limitée de la capacité" pour plus d'informations.

   > Ce paramètre s'applique uniquement aux objets directement ingérés dans le bucket de branche, et non aux objets visibles depuis le bucket de base via le bucket de branche.

4. En option, sélectionnez **Activer la limite du nombre d'objets**.

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

Ce paramètre s'applique uniquement aux objets directement ingérés dans le bucket de branche, et non aux objets visibles depuis le bucket de base via le bucket de branche.

5. Sélectionnez **Créer un compartiment**.

   Le bucket de branche est créé et ajouté à la table sur la page Buckets.

6. En option, sélectionnez **Accéder à la page des détails du bucket** pour"afficher les détails du bucket de branche" et effectuer une configuration supplémentaire.

   Sur la page Détails du bucket, certaines options de configuration liées à la modification des objets sont désactivées pour les buckets en lecture seule.

Applique une balise de règle ILM à un compartiment

Vous pouvez choisir une balise de règle ILM à appliquer à un compartiment en fonction de vos besoins en stockage objet.

La politique ILM contrôle l'emplacement du stockage des données objet et leur suppression au bout d'une période donnée. Votre administrateur du grid crée des règles ILM et les attribue aux balises de règles ILM lors de l'utilisation de plusieurs règles actives.

Évitez de fréquemment réaffecter le tag de stratégie d'un compartiment. Sinon, des problèmes de performances risquent de se produire.

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 "Accès racine, gestion de tous les compartiments ou autorisation Afficher tous les compartiments". Ces autorisations remplacent les paramètres d'autorisation dans les stratégies de groupe ou de compartiment.

Étapes

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

   La page compartiments s'affiche. Si nécessaire, vous pouvez trier les informations par colonne, ou vous pouvez avancer et revenir à la liste.

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

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

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

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

compartiment.

> La modification de la balise de règle ILM d'un compartiment déclenche la réévaluation des règles ILM de tous les objets du compartiment. Si la nouvelle règle conserve des objets pendant une durée limitée, les objets plus anciens seront supprimés.

5. Sélectionnez le bouton radio correspondant à l'étiquette que vous souhaitez affecter au compartiment.
6. Sélectionnez **Enregistrer les modifications**. Une nouvelle balise de compartiment S3 sera définie dans le compartiment avec la clé `NTAP-SG-ILM-BUCKET-TAG` et la valeur du nom de la balise de règle ILM.

> Assurez-vous que vos applications S3 ne remplacent pas accidentellement ou ne suppriment pas 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 de nouveau évalués par rapport à la règle ILM par défaut.

> Définissez et modifiez les balises de règles ILM à l'aide uniquement du gestionnaire de locataires ou de l'API du gestionnaire de locataires sur lequel la balise de règle ILM est validée. Ne modifiez pas la `NTAP-SG-ILM-BUCKET-TAG` balise de stratégie ILM à l'aide de l'API S3 PutBucketTagging ou de l'API S3 DeleteBuckeTagging.

> La modification de la balise de règle attribuée à un compartiment a un impact temporaire sur les performances, tandis que la réévaluation des objets est effectuée à l'aide de la nouvelle règle ILM.

Gestion de la règle de compartiment

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

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine". Les autorisations Afficher tous les compartiments et gérer tous les compartiments permettent uniquement l'affichage.
- Vous avez vérifié que le nombre de nœuds de stockage et de sites requis 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 apportées à ces paramètres risquent de ne pas être disponibles.

Étapes

1. Sélectionnez **godets**, puis sélectionnez le compartiment que vous souhaitez gérer.
2. Sur la page de détails du compartiment, sélectionnez **accès au compartiment** > **Stratégie de compartiment**.
3. Effectuez l'une des opérations suivantes :
   - Entrez une stratégie de compartiment en cochant la case **Enable policy**. Entrez ensuite une chaîne au format JSON valide.

     Chaque politique de compartiment a une taille limite de 20,480 octets.

   - Modifiez une règle existante en modifiant la chaîne.

- Désactivez une stratégie en désélectionnant **Activer la stratégie**.

Pour plus d'informations sur les règles de compartiment, notamment la syntaxe du langage et des exemples, reportez-vous à la section "Exemples de politiques de compartiments".

Gestion de la cohérence des compartiments

Les valeurs de cohérence peuvent être utilisées pour spécifier la disponibilité des modifications des paramètres de compartiment, ainsi que pour fournir un équilibre entre la disponibilité des objets au sein d'un compartiment et la cohérence de ces objets entre plusieurs nœuds de stockage et sites. Vous pouvez modifier les valeurs de cohérence pour qu'elles soient différentes des valeurs par défaut afin que les applications client puissent répondre à leurs besoins opérationnels.

Avant de commencer

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

Instructions de cohérence des compartiments

La cohérence des compartiments détermine la cohérence des applications client qui affectent les objets au sein de ce compartiment S3. En général, vous devez utiliser la cohérence **Read-After-New-write** pour vos compartiments.

modifiez la cohérence des compartiments

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

> Lorsque vous modifiez la cohérence d'un compartiment, seuls les objets ingérés après la modification sont garantis pour respecter le paramètre révisé.

Étapes

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

   La page des détails du compartiment s'affiche.
3. Dans l'onglet **Bucket options**, sélectionnez ** accordéon.
4. Sélectionnez une cohérence pour les opérations effectuées sur les objets de ce compartiment.
   - **Tous** : fournit le plus haut niveau de cohérence. Tous les nœuds reçoivent les données immédiatement, sinon la requête échoue.
   - **Strong-global** : garantit la cohérence lecture après écriture pour toutes les demandes client sur tous les sites.
   - **Strong-site** : garantit la cohérence lecture après écriture pour toutes les demandes client au sein d'un

site.

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

5. Sélectionnez **Enregistrer les modifications**.

Que se passe-t-il lorsque vous modifiez les paramètres de compartiment

Les compartiments ont plusieurs paramètres qui affectent le comportement des compartiments et des objets dans ces compartiments.

Les paramètres de compartiment suivants utilisent la cohérence **strong** par défaut. Si au moins deux nœuds de stockage ne sont disponibles dans aucun site, ou si un site n'est pas disponible, toute modification de ces paramètres peut ne pas être disponible.

- "Suppression du compartiment vide en arrière-plan"
- "Heure du dernier accès"
- "Cycle de vie des compartiments"
- "Politique des compartiments"
- "Balisage du compartiment"
- "Gestion des versions de compartiment"
- "Verrouillage d'objet S3"
- "Chiffrement des compartiments"

La valeur de cohérence pour la gestion des versions des compartiments, le verrouillage objet S3 et le chiffrement des compartiments ne peut pas être définie sur une valeur qui n'est pas parfaitement cohérente.

Les paramètres de compartiment suivants n'utilisent pas une cohérence élevée et offrent une plus grande disponibilité en cas de modification. Les modifications apportées à ces paramètres peuvent prendre un certain temps avant d'avoir un effet.

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

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

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

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

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

Avant de commencer

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

Description de la tâche

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

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

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

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

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

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

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

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

Type de demande	Comportement si l'heure du dernier accès est désactivée (par défaut)		Comportement si l'heure du dernier accès est activée	
	Heure du dernier accès mise à jour ?	Objet ajouté à la file d'attente d'évaluation ILM ?	Heure du dernier accès mise à jour ?	Objet ajouté à la file d'attente d'évaluation ILM ?
Demande de récupération des métadonnées d'un objet lorsqu'une opération HEAD est émise	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
Demander de copier un objet d'un compartiment à un autre	• Non, pour la copie source • Oui, pour la copie de destination	• Non, pour la copie source • Oui, pour la copie de destination	• Oui, pour la copie source • Oui, pour la copie de destination	• Oui, pour la copie source • Oui, pour la copie de destination
Demander de terminer un téléchargement partitionné	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** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.
2. Sélectionnez le nom du compartiment dans la table.

   La page des détails du compartiment s'affiche.

3. Dans l'onglet **Bucket options**, sélectionnez l'accordéon **Last Access Time Updates**.

4. Activer ou désactiver les mises à jour des heures du dernier accès.
5. Sélectionnez **Enregistrer les modifications**.

Modifiez le contrôle de version d'objet pour un compartiment

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

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez tous les compartiments ou l'autorisation d'accès racine". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.
- Vous avez vérifié que le nombre de nœuds de stockage et de sites requis 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 apportées à ces paramètres risquent de ne pas être disponibles.

Description de la tâche

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

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

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

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

Étapes

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

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

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

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

5. Sélectionnez **Enregistrer les modifications**.

Utilisez le verrouillage d'objet S3 pour conserver les objets

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

Votre administrateur de grille doit vous donner l'autorisation d'utiliser des fonctions spécifiques de verrouillage d'objet S3.

Qu'est-ce que le verrouillage objet S3 ?

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

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

Un compartiment sans S3 Object Lock ne peut contenir que des objets sans paramètres de rétention spécifiés. Aucun objet ingéré ne possède de paramètres de conservation.

Un compartiment avec S3 Object Lock peut contenir des objets avec et sans paramètres de conservation spécifiés par les applications client S3. Certains objets ingérés auront des paramètres de conservation.

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

En effet, tous les objets nouvellement ingérés ont des paramètres de conservation lorsque la conservation par défaut est configurée. Les objets existants sans paramètres de conservation d'objet ne sont pas affectés.

Modes de rétention

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

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

Paramètres de conservation pour les versions d'objet

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

- **Mode de conservation** : conformité ou gouvernance.
- **Conserver-jusqu'à-date**: Si la date de conservation d'une version d'objet est dans le futur, l'objet peut être récupéré, mais il ne peut pas être supprimé.
- **Mise en garde légale** : l'application d'une mise en garde légale à une version d'objet verrouille immédiatement cet objet. Par exemple, vous devrez peut-être mettre une obligation légale sur un objet lié à une enquête ou à un litige juridique. Une obligation légale n'a pas de date d'expiration, mais reste en place jusqu'à ce qu'elle soit explicitement supprimée. Les dispositions légales sont indépendantes de la date de conservation.

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

  Pour plus de détails sur les paramètres de l'objet, reportez-vous à la section "Utilisez l'API REST S3 pour configurer le verrouillage objet S3".

Paramètre de rétention par défaut pour les compartiments

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

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

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

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

Tâches de verrouillage d'objet S3

Les listes suivantes destinées aux administrateurs du grid et aux utilisateurs de locataires contiennent des tâches de haut niveau relatives à l'utilisation de la fonction S3 Object Lock.

Administrateur du grid

- Activez le paramètre de verrouillage d'objet S3 global pour l'ensemble du système StorageGRID.
- Assurez-vous que les politiques de gestion du cycle de vie des informations (ILM) sont *conformes*; c'est-à"Exigences des compartiments avec le verrouillage objet S3 activé"-dire qu'elles respectent le .
- Si nécessaire, autorisez un locataire à utiliser le mode de conservation Compliance. Sinon, seul le mode gouvernance est autorisé.
- Si nécessaire, définissez une période de conservation maximale pour un locataire.

Utilisateur locataire

- Considérations relatives aux compartiments et aux objets avec le verrouillage d'objet S3
- Si nécessaire, contactez l'administrateur de la grille pour activer le paramètre global S3 Object Lock et définir les autorisations.
- Créez des compartiments avec le verrouillage d'objet S3 activé.
- Vous pouvez également configurer les paramètres de conservation par défaut d'un compartiment :
  - Mode de conservation par défaut : gouvernance ou conformité, si l'administrateur du grid l'autorise.
  - Période de conservation par défaut : doit être inférieure ou égale à la période de conservation maximale définie par l'administrateur du grid.
- Utilisez l'application client S3 pour ajouter des objets et définir éventuellement la conservation propre à l'objet :
  - Mode de rétention. Gouvernance ou conformité, si l'administrateur du grid l'autorise.
  - Conserver la date de fin : doit être inférieur ou égal à ce qui est autorisé par la période de conservation maximale définie par l'administrateur de la grille.

Conditions requises pour les compartiments avec verrouillage objet S3 activé

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

- La réplication CloudMirror n'est pas prise en charge pour les compartiments avec le verrouillage objet S3 activé.

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

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

Cycle de vie des objets dans des compartiments avec verrouillage objet S3 activé

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

1. **Entrée d'objet**

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

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

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

2. **Conservation et suppression d'objets**

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

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

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

La fonction de verrouillage d'objet S3 remplace la fonction de conformité disponible dans les versions StorageGRID précédentes. Si vous avez créé des compartiments conformes à l'aide d'une version précédente de StorageGRID, vous pouvez continuer à gérer les paramètres de ces compartiments. Toutefois, vous ne pouvez plus créer de compartiments conformes. Pour obtenir des instructions, reportez-vous à la section "Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5".

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

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

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez tous les compartiments ou l'autorisation d'accès racine". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.
- Le verrouillage des objets S3 est activé globalement pour votre système StorageGRID et vous avez activé le verrouillage des objets S3 lorsque vous avez créé le compartiment. Voir "Utilisez le verrouillage d'objet S3 pour conserver les objets".

Étapes

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

   La page des détails du compartiment s'affiche.

3. Dans l'onglet **Bucket options**, sélectionnez l'accordéon **S3 Object Lock**.
4. En option, activez ou désactivez **rétention par défaut** pour ce compartiment.

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

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

Mode de rétention par défaut	Description
La gouvernance	• Les utilisateurs disposant de l' `s3:BypassGovernanceRetention`autorisation peuvent utiliser l' `x-amz-bypass-governance-retention: true`en-tête de la demande pour contourner les paramètres de rétention. • Ces utilisateurs peuvent supprimer une version d'objet avant d'atteindre sa date de conservation jusqu'à. • Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

Mode de rétention par défaut	Description
La conformité	• L'objet ne peut pas être supprimé tant que sa date de conservation jusqu'à n'est pas atteinte. • La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être réduite. • La date de conservation de l'objet jusqu'à ne peut pas être supprimée tant que cette date n'est pas atteinte. **Remarque** : votre administrateur de grille doit vous permettre d'utiliser le mode de conformité.

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

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

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

7. Sélectionnez **Enregistrer les modifications**.

Configurer StorageGRID CORS pour les buckets et les objets

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

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Pour les demandes de configuration GET CORS, vous appartenez à un groupe d'utilisateurs qui a le "Autorisation gérer tous les compartiments ou Afficher tous les compartiments". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.
- Pour les demandes de configuration PUT CORS, vous appartenez à un groupe d'utilisateurs qui a le "Autorisations de gestion de tous les compartiments". Cette autorisation remplace les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.
- Le "Autorisation d'accès racine" permet d'accéder à toutes les demandes de configuration CORS.

Description de la tâche

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

Activer le CORS pour un godet

Étapes

1. Utilisez un éditeur de texte pour créer le fichier XML requis. Cet exemple montre le code XML utilisé pour activer le code commande pour un compartiment S3. Détails :
   - Permet à n'importe quel domaine d'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 demande sont autorisés

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

   Pour plus d'informations sur le XML de configuration CORS, reportez-vous àla section "Documentation Amazon Web Services (AWS) : guide de l'utilisateur d'Amazon simple Storage Service".

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

   La page des détails du compartiment s'affiche.

4. Dans l'onglet **Bucket Access**, sélectionnez l'accordéon **Cross-Origin Resource Sharing (CORS)**.
5. Cochez la case **Activer CORS**.
6. Collez le fichier XML de configuration CORS dans la zone de texte.
7. Sélectionnez **Enregistrer les modifications**.

Modifier le paramètre CORS

Étapes

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

Désactiver le paramètre CORS

Étapes

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

Informations associées

"Configurer StorageGRID CORS pour une interface de gestion"

Supprime les objets du compartiment

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

Considérations et exigences

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

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

  Un compartiment qui utilise le verrouillage d'objet S3 restera à l'état **Suppression d'objets : lecture seule** jusqu'à ce que la date de conservation soit atteinte pour tous les objets et que toutes les mises en suspens légales soient supprimées.

- Pendant la suppression des objets, l'état du compartiment est **Suppression d'objets : lecture seule**. Dans cet état, vous ne pouvez pas ajouter de nouveaux objets au compartiment.
- Une fois tous les objets supprimés, le compartiment reste à l'état en lecture seule. Vous pouvez effectuer l'une des opérations suivantes :
  - Ramener le compartiment en mode écriture et le réutiliser pour de nouveaux objets
  - Supprimez le compartiment
  - Conservez le compartiment en mode lecture seule pour réserver son nom pour une utilisation ultérieure
- Si la gestion des versions d'objet est activée dans un compartiment, les marqueurs de suppression créés dans StorageGRID 11.8 ou version ultérieure peuvent être supprimés à l'aide des opérations de suppression d'objets dans un compartiment.
- Si la gestion des versions d'objet est activée dans un compartiment, l'opération de suppression d'objets ne supprime pas les marqueurs de suppression créés dans StorageGRID 11.7 ou une version antérieure. Voir les informations sur la suppression d'objets dans un compartiment dans "Suppression d'objets avec version S3".
- Si vous utilisez "réplication entre plusieurs grilles", notez ce qui suit :
  - L'utilisation de cette option ne supprime aucun objet du compartiment de l'autre grille.

- Si vous sélectionnez cette option pour le compartiment source, l'alerte **échec de réplication multigrille** est déclenchée si vous ajoutez des objets au compartiment de destination sur l'autre grille. Si vous ne pouvez pas garantir que personne n'ajoute d'objets au compartiment de l'autre grille avant de supprimer tous les objets "désactiver la réplication entre les grilles"du compartiment.

Avant de commencer

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

Étapes

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

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

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

   Menu actions

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

   b. Sélectionnez **actions** > **Supprimer les objets dans le compartiment**.

   Page de détails

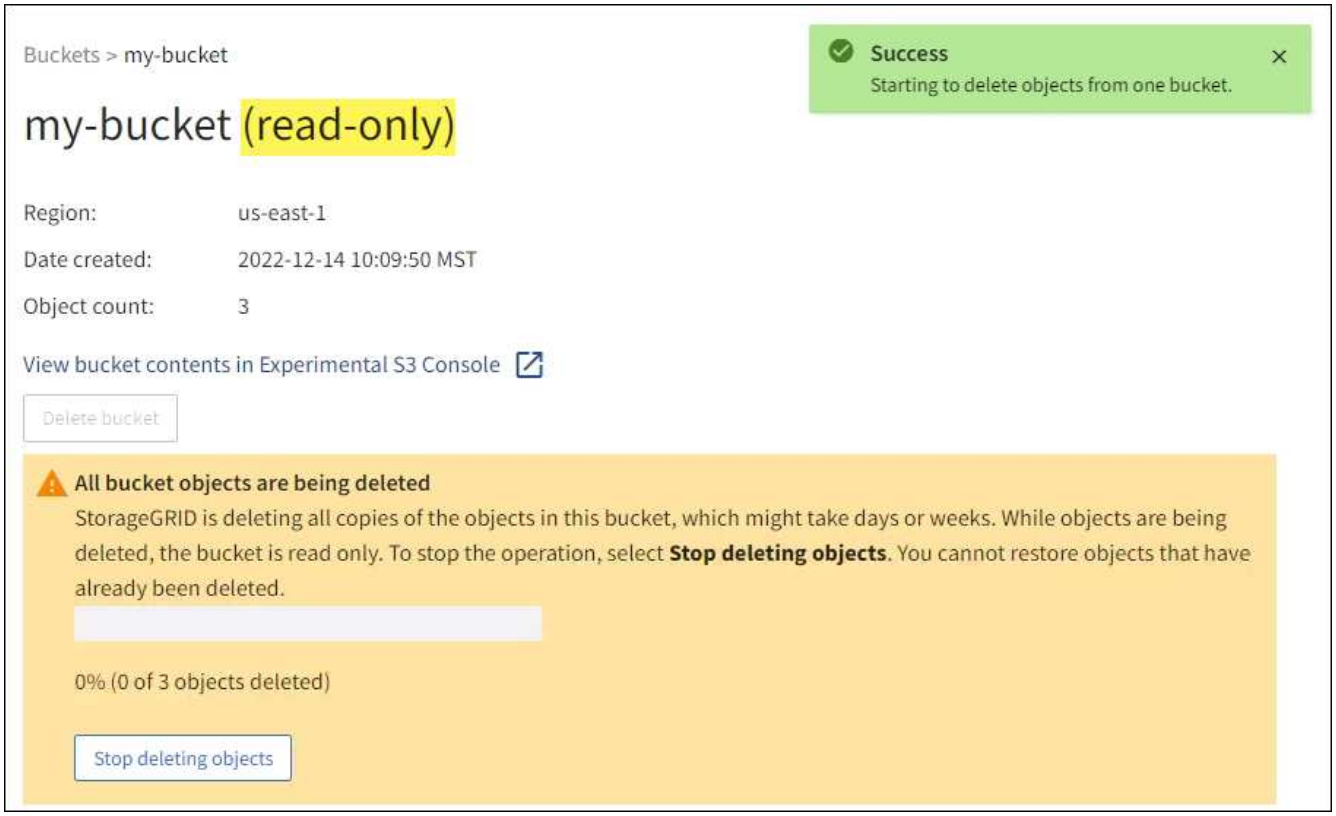
   a. Sélectionnez un nom de compartiment pour afficher ses détails.

   b. Sélectionnez **Supprimer les objets dans le compartiment**.

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

   Au bout de quelques minutes :

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

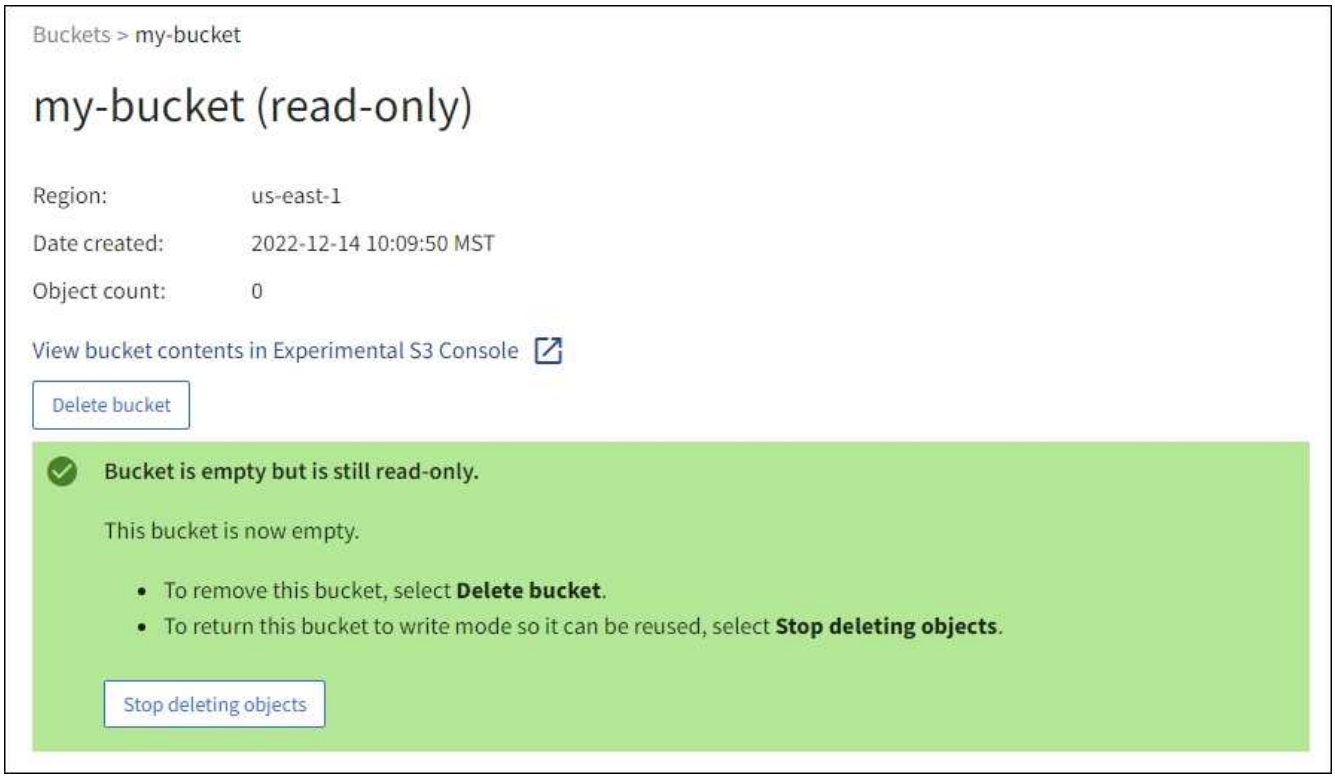


5. Si nécessaire pendant l'exécution de l'opération, sélectionnez **Arrêter la suppression d'objets** pour arrêter le processus. Sélectionnez ensuite **Supprimer les objets dans le compartiment** pour reprendre le processus.

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

6. Attendez la fin de l'opération.

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



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

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

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

Supprimez le compartiment S3

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

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez tous les compartiments ou l'autorisation d'accès racine". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.
- Les compartiments à supprimer sont vides. Si les rubriques que vous souhaitez supprimer sont *not* vides,

"supprimez des objets du compartiment".

Description de la tâche

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

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

Étapes

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

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

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

   Menu actions

   a. Cochez la case correspondant à chaque compartiment à supprimer.

   b. Sélectionnez **actions** > **Supprimer des compartiments**.

   Page de détails

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

   b. Sélectionnez **Supprimer le compartiment**.

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

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

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

Utiliser la console S3

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

Avec la console S3, vous pouvez :

- Télécharger, télécharger, renommer, copier, déplacer, et supprimer des objets
- Affichez, restaurez, téléchargez et supprimez des versions d'objet
- Recherche d'objets par préfixe
- Gérer les balises d'objet
- Afficher les métadonnées d'objet
- Afficher, créer, renommer, copier, déplacer, et supprimez des dossiers

La console S3 améliore l'expérience utilisateur dans les cas les plus courants. Elle n'a pas été conçue pour remplacer les opérations de l'interface de ligne de commande ou de l'API dans tous les cas.

Si les opérations sont trop longues avec la console S3 (en minutes ou en heures, par exemple), tenez compte des points suivants :

- Réduction du nombre d'objets sélectionnés
- Accédez à vos données à l'aide de méthodes non graphiques (API ou interface de ligne de commande)

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Si vous souhaitez gérer des objets, vous appartenez à un groupe d'utilisateurs disposant de l'autorisation d'accès racine. Vous pouvez également appartenir à un groupe d'utilisateurs disposant de l'autorisation utiliser l'onglet de la console S3 et de l'autorisation Afficher tous les compartiments ou gérer tous les compartiments. Voir "Autorisations de gestion des locataires".
- Une stratégie de groupe ou de compartiment S3 a été configurée pour l'utilisateur. Voir "Utilisez les règles d'accès au compartiment et au groupe" .
- Vous connaissez l'ID de clé d'accès de l'utilisateur et la clé d'accès secrète. Vous disposez éventuellement d'un `.csv` fichier contenant ces informations. Voir la "instructions pour la création de clés d'accès".

Étapes

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

Informations supplémentaires

- **Recherche par préfixe** : la fonction de recherche par préfixe recherche uniquement les objets commençant par un mot spécifique par rapport au dossier en cours. La recherche n'inclut pas les objets qui contiennent le mot ailleurs. Cette règle s'applique également aux objets dans les dossiers. Par exemple, une recherche de `folder1/folder2/somefile-` renvoie des objets se trouvant dans le `folder1/folder2/` dossier et commence par le mot `somefile-`.
- **Glisser-déposer** : vous pouvez faire glisser et déposer des fichiers du gestionnaire de fichiers de votre ordinateur vers la console S3. Cependant, vous ne pouvez pas télécharger de dossiers.
- **Opérations sur les dossiers** : lorsque vous déplacez, copiez ou renommez un dossier, tous les objets du dossier sont mis à jour un par un, ce qui peut prendre du temps.
- **Suppression permanente lorsque la gestion des versions de compartiment est désactivée** : lorsque vous écrasez ou supprimez un objet dans un compartiment avec la gestion des versions désactivée, l'opération est permanente. Voir "Modifiez le contrôle de version d'objet pour un compartiment".

Gérez les services de la plateforme S3

Services de plateforme S3

Présentation et éléments à prendre en compte pour les services de plateforme

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

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

Présentation des services de plateforme

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

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

Toute combinaison de services de plateforme peut être configurée pour un seul compartiment S3. Par exemple, vous pouvez configurer à la fois le "Service CloudMirror" et le "notifications" dans un compartiment StorageGRID S3 afin de mettre en miroir des objets spécifiques vers Amazon simple Storage Service (S3), tout en envoyant une notification sur chacun de ces objets à une application de surveillance tierce pour vous aider à suivre vos dépenses AWS.

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

Configuration des services de plate-forme

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

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

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

- Si vous souhaitez que tous les objets dont les clés commencent par `/images` soient répliqués sur 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.

Le format du XML de configuration est régi par les API REST S3 utilisées pour mettre en œuvre les services

de plateforme StorageGRID :

Service de plateforme	L'API REST S3	Reportez-vous à la section
Réplication CloudMirror	• GetBuckeReplication • PutBuckeReplication	• "Réplication CloudMirror" • "Opérations sur les compartiments"
Notifications	• GetBucketNotifationConfiguration • PutBucketNotifationConfiguration	• "Notifications" • "Opérations sur les compartiments"
Intégration de la recherche	• CONFIGURATION DES notifications de métadonnées de compartiment • CONFIGURATION de notification des métadonnées de compartiment	• "Intégration de la recherche" • "Opérations personnalisées StorageGRID"

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

Réflexion	Détails
Surveillance des terminaux de destination	Vous devez surveiller la disponibilité de chaque point final de destination. Si la connexion au point final de destination est perdue pendant une période prolongée et qu'il existe un important retard de requêtes, les demandes client supplémentaires (telles QUE LES requêtes ENVOYÉES) à StorageGRID échoueront. Vous devez réessayer ces demandes ayant échoué lorsque le noeud final devient accessible.
Limitation du terminal de destination	Le logiciel StorageGRID peut canaliser les demandes S3 entrantes pour un compartiment si le taux d'envoi des demandes dépasse le taux à partir duquel le terminal de destination peut recevoir les demandes. La restriction ne se produit que lorsqu'il existe un arriéré de demandes en attente d'envoi vers le noeud final de destination. Le seul effet visible est que les requêtes S3 entrantes prennent plus de temps à s'exécuter. Si vous commencez à détecter les performances beaucoup plus lentes, vous devez réduire le taux d'entrée ou utiliser un terminal avec une capacité plus élevée. Si l'carnet de commandes des requêtes continue d'augmenter, les opérations S3 des clients (par EXEMPLE, LES requêtes PUT) finiront par échouer. Les demandes CloudMirror sont plus susceptibles d'être affectées par les performances du terminal de destination, car ces demandes impliquent généralement plus de transfert de données que les demandes d'intégration de recherche ou de notification d'événements.

Réflexion	Détails
Garanties de commande	StorageGRID garantit l'ordre des opérations sur un objet d'un site. Tant que toutes les opérations relatives à un objet se trouvent sur le même site, l'état final de l'objet (pour la réplication) sera toujours égal à l'état dans StorageGRID. StorageGRID tente également de commander des demandes lorsque des opérations sont effectuées sur des sites StorageGRID. Par exemple, si vous écrivez un objet initialement sur le site A, puis que vous le remplacez par un autre objet au niveau du site B, le dernier objet répliqué par CloudMirror vers le compartiment de destination n'est pas garanti que ce nouvel objet soit.
Suppressions d'objets basées sur des règles ILM	Pour correspondre au comportement de suppression des CRR AWS et 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 demande de notification de CloudMirror ou d'événement n'est envoyée si une règle ILM supprime un objet au bout de 14 jours. Au contraire, les demandes d'intégration de la recherche sont envoyées lorsque les objets sont supprimés du fait de ILM.
À l'aide des terminaux Kafka	Pour les terminaux Kafka, le protocole TLS mutuel n'est pas pris en charge. Par conséquent, si vous avez `ssl.client.auth` défini sur `required` dans la configuration de votre courtier Kafka, cela peut entraîner des problèmes de configuration du terminal Kafka. L'authentification des terminaux Kafka utilise les types d'authentification suivants. Ces types sont différents de ceux utilisés pour l'authentification d'autres terminaux, tels qu'Amazon SNS, et nécessitent des informations d'identification de nom d'utilisateur et de mot de passe. • SASL/SIMPLE • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 **Remarque :** les paramètres du proxy de stockage configuré ne s'appliquent pas aux noeuds finaux des services de la plateforme Kafka.

Considérations relatives à l'utilisation du service de réplication CloudMirror

Réflexion	Détails
État de la réplication	StorageGRID ne prend pas en charge la `x-amz-replication-status` barre de coupe.

Réflexion	Détails
Taille de l'objet	La taille maximale des objets qui peuvent être répliqués dans un compartiment de destination par le service de réplication CloudMirror est de 5 Tio, soit la même que la taille maximale de l'objet *pris en charge*. **Remarque** : la taille *recommandée* maximale pour une opération PutObject unique est de 5 Gio (5,368,709,120 octets). Si vos objets sont supérieurs à 5 Gio, utilisez le téléchargement partitionné.
Gestion des versions du compartiment et ID de version	Si le compartiment S3 source de StorageGRID est activé pour la gestion des versions, vous devez également activer la gestion des versions pour le compartiment de destination. Lors de l'utilisation du contrôle de version, notez que l'ordre des versions d'objet dans le compartiment de destination est meilleur effort et n'est pas garanti par le service CloudMirror, en raison des limites du protocole S3. **Remarque** : les ID de version du compartiment source dans StorageGRID ne sont pas liés aux ID de version du compartiment de destination.
Balisage des versions d'objets	Le service CloudMirror ne réplique pas les requêtes PutObjectTagging ou DeleteObjectTagging qui fournissent un ID de version, en raison des limitations du protocole S3. Étant donné que les ID de version de la source et de la destination ne sont pas liés, il n'est pas possible de s'assurer qu'une mise à jour de balise vers un ID de version spécifique sera répliquée. En revanche, le service CloudMirror réplique les requêtes PutObjectTagging ou DeleteObjectTagging qui ne spécifient pas d'ID de version. Ces demandes mettent à jour les balises pour la clé la plus récente (ou la dernière version si le compartiment est versionné). Les ings normaux avec des étiquettes (et non les mises à jour de marquage) sont également répliqués.
Téléchargements partitionnés et `ETag` valeurs	Lors de la mise en miroir d'objets qui ont été téléchargés à l'aide d'un téléchargement partitionné, le service CloudMirror ne conserve pas les pièces. Par conséquent, la `ETag` valeur de l'objet symétrique sera différente de celle `ETag` de l'objet d'origine.
Chiffrement des objets avec SSE-C (chiffrement côté serveur avec clés fournies par le client)	Le service CloudMirror ne prend pas en charge les objets cryptés avec SSE-C. si vous essayez d'ingérer un objet dans le compartiment source pour la réplication CloudMirror et que la demande inclut les en-têtes de requête SSE-C, l'opération échoue.
Compartiment avec verrouillage objet S3 activé	La réplication n'est pas prise en charge pour les compartiments source ou de destination lorsque le verrouillage d'objet S3 est activé.

Présentation du service de réplication CloudMirror

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.

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

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

CloudMirror et ILM

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

CloudMirror et réplication intergrille

La réplication CloudMirror présente des similarités et des différences importantes avec la fonction de réplication multigrille. Reportez-vous à la "Comparez la réplication entre les grilles et la réplication CloudMirror".

Compartiments CloudMirror et S3

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

Compartiments existants

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

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

Compartiments de destination multiples

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

Compartiments avec ou sans version

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

Suppression, boucles de réplication et événements

Comportement de suppression

Est identique au comportement de suppression du service Amazon S3, réplication interrégionale (CRR). La suppression d'un objet dans un compartiment source ne supprime jamais un objet répliqué dans la destination. Si le compartiment source et le compartiment de destination sont multiversion, le marqueur de suppression est répliqué. Si le compartiment de destination n'est pas versionné, la suppression d'un objet dans le compartiment source ne réplique pas le marqueur de suppression dans le compartiment de destination ni ne supprime l'objet de destination.

Protection contre les boucles de réplication

Comme les objets sont répliqués dans le compartiment de destination, StorageGRID les marque comme « réplicas ». Un compartiment StorageGRID de destination ne réplique pas les objets marqués comme répliques, ce qui vous protège contre les boucles de réplication accidentelles. Ce marquage de réplica est interne à StorageGRID et ne vous empêche pas d'utiliser AWS CRR lors de l'utilisation d'un compartiment Amazon S3 comme destination.

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

Événements dans le 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 du fait des opérations effectuées pour garantir le succès de la livraison. Dans de rares cas, lorsque le même objet est mis à jour simultanément depuis deux sites StorageGRID ou plus, il peut ne pas correspondre au ordre d'événements du compartiment source.

Description des notifications pour les compartiments

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

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

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

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

Les notifications d'événements StorageGRID suivent l'API Amazon S3 avec quelques restrictions.

- Les types d'événements suivants sont pris en charge :

- s3:ObjectCreated :
- s3:ObjectCreated:put
- s3:ObjectCreated:Post
- s3:ObjectCreated:Copier
- s3:ObjectCreated:CompleteMultipartUpload
- s3:objet Removed :
- s3:ObjectRemoved:Supprimer
- s3:ObjectRemoved:DeleteMarkerCreated
- s3:ObjectRestore:Post

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

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

Comprendre le service d'intégration de la recherche

Si vous souhaitez utiliser un service externe de recherche et d'analyse de données pour vos métadonnées d'objet, vous pouvez activer l'intégration de la recherche pour un compartiment S3.

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

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

Même si l'intégration avec Elasticsearch peut être configurée dans un compartiment avec S3 Object Lock activé, les métadonnées S3 Object Lock (y compris la date de conservation jusqu'à et l'état de conservation légale) des objets ne seront pas incluses dans les métadonnées envoyées à Elasticsearch.

Étant donné que le service d'intégration de recherche envoie des métadonnées d'objet à une destination, son XML de configuration est appelé « XML de configuration de notification_métadonnées_ ». Ce XML de configuration est différent du XML de configuration de notification utilisé pour activer les notifications *événement*.

Intégration de la recherche et compartiments S3

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

Les notifications 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 de l'objet et de toutes les métadonnées utilisateur.

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

Rechercher des notifications

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

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

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

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

Service d'intégration de la recherche et Elasticsearch

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

Gérez les terminaux des services de plateforme

Configurer les terminaux des services de plateforme

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

L'accès aux services de plateforme est activé par locataire par administrateur StorageGRID. Pour créer ou utiliser un noeud final de services de plate-forme, vous devez être un utilisateur locataire disposant de l'autorisation gérer les noeuds finaux ou accès racine, dans une grille dont la mise en réseau a été configurée pour permettre aux noeuds de stockage d'accéder aux ressources de noeuds finaux externes. Pour un seul locataire, vous pouvez configurer un maximum de 500 terminaux de services de plateforme. Pour plus d'informations, contactez votre administrateur StorageGRID.

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

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

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

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

Terminaux pour la réplication CloudMirror

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

Terminaux pour les notifications

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

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

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

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

Informations associées

"Administrer StorageGRID"

Spécifiez l'URN du terminal des services de plateforme

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

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

Éléments DE RETOUR

L'URN d'un noeud final de services de plate-forme doit commencer par ou `urn:mysite` par `arn:aws` , 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 noeud final 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 noeud final CloudMirror hébergé sur StorageGRID, vous devez ajouter `s3` à 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	Ressource spécifique
Réplication CloudMirror	`bucket-name`
Notifications	`sns-topic-name` ou `kafka-topic-name` **Remarque :** pour les points de terminaison webhook, l'élément final de l'URN peut être n'importe quelle chaîne, à condition que l'URN du point de terminaison soit unique.
Intégration de la recherche	`domain-name/index-name/type-name` **Remarque :** si le cluster Elasticsearch est **NOT** configuré pour créer automatiquement des index, vous devez créer l'index manuellement avant de créer le noeud final.

Urns pour les services hébergés sur AWS et GCP

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

- Réplication CloudMirror :

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

- Notifications :

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

- Intégration de la recherche :

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

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

Urnes pour des services hébergés localement

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

exemple :

- Réplication CloudMirror :

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

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

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

- Notifications :

  Spécifiez un point de terminaison Amazon simple notification Service :

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

  Spécifiez un terminal Kafka :

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

  Spécifiez un point de terminaison de webhook :

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

- Intégration de la recherche :

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

> Pour les noeuds finaux d'intégration de recherche hébergés localement, l' `domain-name`élément peut être n'importe quelle chaîne tant que l'URN du noeud final est unique.

Créer un terminal de services de plate-forme

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

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Les services de plateforme ont été activés pour votre compte de locataire par un administrateur StorageGRID.

- Vous appartenez à un groupe d'utilisateurs qui possède le "Gestion des noeuds finaux ou des autorisations d'accès racine".
- La ressource référencée par le point de terminaison des services de la plateforme a été créée :
  - Réplication CloudMirror : compartiment S3
  - Notification d'événement : rubrique Amazon Simple Notification Service (Amazon SNS), rubrique Kafka ou point de terminaison webhook
  - Notification de recherche : index Elasticsearch, si le cluster de destination n'est pas configuré pour créer automatiquement des index.
- Vous disposez des informations relatives à la ressource de destination :
  - Hôte et port pour l'URI (Uniform Resource identifier)

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

  - Nom de ressource unique (URN)

    "Spécifiez l'URN du terminal des services de plateforme"

  - Informations d'authentification (si nécessaire) :

Rechercher les terminaux d'intégration

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

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

Terminaux de réplication CloudMirror

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

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

Terminaux Amazon SNS

Pour les terminaux Amazon SNS, vous pouvez utiliser les informations d'identification suivantes :

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

Les terminaux Kafka

Pour les terminaux Kafka, vous pouvez utiliser les identifiants suivants :

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

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

- Si les fonctions de sécurité de Elasticsearch sont activées, vous disposez du privilège Monitor cluster pour les tests de connectivité et du privilège write index ou des privilèges index and delete index pour les mises à jour de documents.

Étapes

1. Sélectionnez **STORAGE (S3)** > **Platform services Endpoints**. La page noeuds finaux des services de plate-forme s'affiche.
2. Sélectionnez **Créer un noeud final**.
3. Entrez un nom d'affichage pour décrire brièvement le point final et son objectif.

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

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

   Utilisez l'un des formats suivants :

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Rechercher les terminaux d'intégration

Entrez ou téléchargez les informations d'identification d'un point final d'intégration de recherche.

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

Type d'authentification	Description	Informations d'identification
Anonyme	Fournit un accès anonyme à la destination. Fonctionne uniquement pour les terminaux dont la sécurité est désactivée.	Pas d'authentification.
Clé d'accès	Utilise des identifiants de style AWS pour authentifier les connexions avec la destination.	• ID de clé d'accès • Clé d'accès secrète
HTTP de base	Utilise un nom d'utilisateur et un mot de passe pour authentifier les connexions à la destination.	• Nom d'utilisateur • Mot de passe

Terminaux de réplication CloudMirror

Entrez ou téléchargez les informations d'identification d'un point final de réplication CloudMirror.

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

Type d'authentification	Description	Informations d'identification
Anonyme	Fournit un accès anonyme à la destination. Fonctionne uniquement pour les terminaux dont la sécurité est désactivée.	Pas d'authentification.
Clé d'accès	Utilise des identifiants de style AWS pour authentifier les connexions avec la destination.	• ID de clé d'accès • Clé d'accès secrète

Type d'authentification	Description	Informations d'identification
CAP (portail d'accès C2S)	Utilise des certificats et des clés pour authentifier les connexions à la destination.	• URL des informations d'identification temporaires • Certificat autorité de certification du serveur (téléchargement de fichiers PEM) • Certificat client (téléchargement de fichier PEM) • Clé privée client (téléchargement de fichiers PEM, format crypté OpenSSL ou format de clé privée non crypté) • Phrase de passe de clé privée du client (facultatif)

Terminaux Amazon SNS

Saisissez ou téléchargez les informations d'identification d'un terminal Amazon SNS.

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

Type d'authentification	Description	Informations d'identification
Anonyme	Fournit un accès anonyme à la destination. Fonctionne uniquement pour les terminaux dont la sécurité est désactivée.	Pas d'authentification.
Clé d'accès	Utilise des identifiants de style AWS pour authentifier les connexions avec la destination.	• ID de clé d'accès • Clé d'accès secrète

Les terminaux Kafka

Entrez ou téléchargez les identifiants d'un terminal Kafka.

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

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

Type d'authentification	Description	Informations d'identification
SASL/SIMPLE	Utilise un nom d'utilisateur et un mot de passe avec du texte brut pour authentifier les connexions à la destination.	• Nom d'utilisateur • Mot de passe
SASL/SCRAM-SHA-256	Utilise un nom d'utilisateur et un mot de passe à l'aide d'un protocole de réponse de vérification et d'un hachage SHA-256 pour authentifier les connexions à la destination.	• Nom d'utilisateur • Mot de passe
SASL/SCRAM-SHA-512	Utilise un nom d'utilisateur et un mot de passe à l'aide d'un protocole de réponse de vérification et d'un hachage SHA-512 pour authentifier les connexions à la destination.	• Nom d'utilisateur • Mot de passe

Sélectionnez **utiliser la délégation prise de l'authentification** 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 **Continuer**.
9. Sélectionnez un bouton radio pour **Vérifier les certificats** pour choisir comment la connexion TLS au point de terminaison est vérifiée.

La plupart des points finaux

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

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

Points de terminaison Webhook uniquement

Vérifiez la connexion TLS pour les points de terminaison webhook.

Type de vérification du certificat	Description
TLS	Valide le certificat du serveur pour les connexions TLS à la ressource de point de terminaison.
mTLS	Valide les certificats client et serveur pour les connexions TLS mutuelles à la ressource de point de terminaison.
Désactivées	La vérification du certificat est désactivée. Cette option n'est pas sécurisée.
Utiliser un certificat d'autorité de certification personnalisé	Le certificat CA personnalisé est utilisé pour vérifier l'identité du serveur lors de la connexion au point de terminaison.

Lorsque vous sélectionnez **mTLS**, ces options deviennent disponibles.

Type de vérification du certificat	Description
Ne pas vérifier le certificat du serveur	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.

Type de vérification du certificat	Description
Certificat client	Le certificat client est utilisé pour vérifier l'identité du client lors de la connexion au point de terminaison.
Clé privée du client	La clé privée du certificat client. S'il est chiffré, il doit utiliser le format traditionnel PKCS #1 (le format PKCS #8 n'est pas pris en charge).
Mot de passe de la clé privée du client	La phrase secrète permettant de décrypter la clé privée du client. Si la clé privée n'est pas chiffrée, laissez ce champ vide.

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

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

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

Informations associées

- "Spécifiez l'URN du terminal des services de plateforme"
- "Configurez la réplication CloudMirror"
- "Configurer les notifications d'événements"
- "Configurez le service d'intégration de la recherche"

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

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

Avant de commencer

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

Description de la tâche

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

Étapes

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

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

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

   La page des détails du point final s'affiche.

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

Modifier le point final des services de plate-forme

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

Avant de commencer

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

Étapes

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

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

2. Sélectionnez le point final que vous souhaitez modifier.

   La page des détails du point final s'affiche.

3. Sélectionnez **Configuration**.
4. Modifiez la configuration du noeud final selon les besoins.

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

   a. Pour modifier le nom d'affichage du noeud final, sélectionnez l'icône de modification .
   b. Modifiez l'URI si nécessaire.
   c. Si nécessaire, modifiez le type d'authentification.
      - Pour l'authentification par clé d'accès, modifiez la clé selon vos besoins en sélectionnant **Modifier la clé S3** et en collant une nouvelle ID de clé d'accès et une nouvelle clé d'accès secrète. Si vous devez annuler vos modifications, sélectionnez **Revert S3 key edit**.

- Pour l'authentification CAP (C2S Access Portal), modifiez l'URL des informations d'identification temporaires ou la phrase de passe de la clé privée du client facultative et téléchargez de nouveaux certificats et fichiers de clés selon les besoins.

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

d. Si nécessaire, modifiez la méthode de vérification des certificats.

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

Supprimer le noeud final des services de plate-forme

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

Avant de commencer

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

Étapes

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

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

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

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

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

   Un message de confirmation s'affiche.

4. Sélectionnez **Supprimer le point final**.

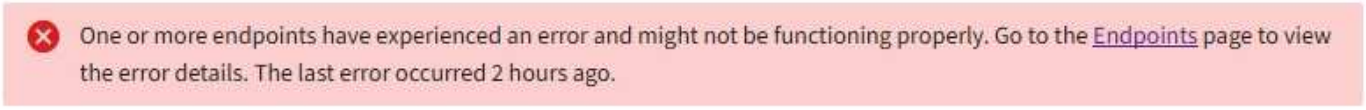
Dépanner les erreurs de point final des services de plate-forme

Si une erreur se produit lorsque StorageGRID tente de communiquer avec un noeud final de services de plate-forme, un message s'affiche sur le tableau de bord. Sur la page noeuds finaux des services de plate-forme, la colonne dernière erreur indique il y a

combien de temps l'erreur s'est produite. Aucune erreur ne s'affiche si les autorisations associées aux informations d'identification d'un noeud final sont incorrectes.

Déterminez si l'erreur s'est produite

Si des erreurs de noeud final de services de plateforme se sont produites au cours des 7 derniers jours, le tableau de bord du gestionnaire de locataires affiche un message d'alerte. Vous pouvez accéder à la page noeuds finaux des services de plate-forme pour obtenir plus de détails sur l'erreur.



La même erreur qui s'affiche sur le tableau de bord s'affiche également en haut de la page noeuds finaux Platform Services. Pour afficher un message d'erreur plus détaillé :

Étapes

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

Vérifiez si l'erreur est toujours à jour

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

Étapes

1. Sélectionnez l'extrémité.

   La page des détails du point final s'affiche.

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

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

Résoudre les erreurs de point final

Vous pouvez utiliser le message **dernière erreur** sur la page des détails du noeud final pour déterminer ce qui est à l'origine de l'erreur. Certaines erreurs peuvent vous obliger à modifier le noeud final pour résoudre le problème. Par exemple, une erreur CloudMirroring peut se produire si StorageGRID ne parvient pas à accéder au compartiment S3 de destination, car il ne dispose pas des autorisations d'accès correctes ou si la clé d'accès a expiré. Le message est "les informations d'identification du noeud final ou l'accès à la destination doivent être mis à jour" et les détails sont "AccessDenied" ou "InvalidAccessKeyId".

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

Étapes

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

Identifiants de point de terminaison avec autorisations insuffisantes

Lorsque StorageGRID valide un terminal de services de plateforme, il confirme que les identifiants du terminal peuvent être utilisés pour contacter la ressource de destination et il vérifie les autorisations de base. Cependant, StorageGRID ne valide pas toutes les autorisations requises pour certaines opérations de services de plateforme. Pour cette raison, si vous recevez une erreur lors de la tentative d'utilisation d'un service de plate-forme (tel que « 403 interdit »), vérifiez les autorisations associées aux informations d'identification du noeud final.

Informations associées

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

Configurez la réplication CloudMirror

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

Avant de commencer

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

Description de la tâche

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

Pour des informations générales sur la réplication de compartiment et la configuration de celle-ci, reportez-vous à la section "Documentation d'Amazon simple Storage Service (S3) : réplication d'objets". Pour plus d'informations sur la manière dont StorageGRID implémente GetBuckeReplication, DeleteBuckeReplication et PutBuckeReplication, reportez-vous au "Opérations sur les compartiments".

> La réplication CloudMirror présente des similarités et des différences importantes avec la fonction de réplication multigrille. Pour en savoir plus, voir "Comparez la réplication entre les grilles et la réplication CloudMirror".

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

- Lorsque vous créez et appliquez un XML de configuration de réplication de compartiment valide, il doit utiliser l'URN d'un terminal de compartiment S3 pour chaque destination.
- La réplication n'est pas prise en charge pour les compartiments source ou de destination lorsque le verrouillage d'objet S3 est activé.
- Si vous activez la réplication CloudMirror sur un compartiment qui contient des objets, les nouveaux objets ajoutés au compartiment sont répliqués, mais les objets existants du compartiment ne sont pas répliqués. Vous devez mettre à jour des objets existants pour déclencher la réplication.
- Si vous spécifiez une classe de stockage dans le fichier XML de configuration de réplication, StorageGRID utilise cette classe lors des opérations sur le terminal S3 de destination. Le noeud final de destination doit également prendre en charge la classe de stockage spécifiée. Veillez à suivre les recommandations fournies par le fournisseur du système de destination.

Étapes

1. Activer la réplication pour le compartiment source :
   - Utilisez un éditeur de texte pour créer le XML de configuration de réplication requis pour activer la réplication, comme spécifié dans l'API de réplication S3.
   - Lors de la configuration du XML :
     - Notez que StorageGRID ne prend en charge que le V1 de la configuration de la réplication. Cela signifie que StorageGRID ne prend pas en charge l'utilisation de `Filter` l'élément pour les règles et respecte les conventions V1 pour la suppression des versions d'objet. Pour plus d'informations, reportez-vous à la documentation Amazon sur la configuration de la réplication.
     - Utiliser l'URN d'un terminal du compartiment S3 comme destination.
     - Si vous le souhaitez, ajoutez l'élément et spécifiez l'une des options `<StorageClass>` suivantes :
       - `STANDARD`: La classe de stockage par défaut. Si vous ne spécifiez pas de classe de stockage lorsque vous téléchargez un objet, la `STANDARD` classe de stockage est utilisée.
       - `STANDARD_IA`: (Standard - accès peu fréquent.) Utilisez cette classe de stockage pour les données moins consultées, mais qui nécessitent 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 `STANDARD` classe de stockage.
     - 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** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.
3. Sélectionnez le nom du compartiment source.

   La page des détails du compartiment s'affiche.

4. Sélectionnez **Platform Services** > **Replication**.
5. Cochez la case **Activer la réplication**.
6. Collez le XML de configuration de réplication dans la zone de texte et sélectionnez **Enregistrer les modifications**.

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

7. Vérifiez que la réplication est configurée correctement :
   a. Ajoutez un objet au compartiment source qui répond aux exigences de réplication telles que spécifiées dans la configuration de la réplication.

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

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

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

Informations associées

"Créer un terminal de services de plate-forme"

Configurer les notifications d'événements

Vous activez les notifications pour un compartiment en créant un XML de configuration de notification et en utilisant le gestionnaire de locataires pour appliquer le XML à un compartiment.

Avant de commencer

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

Description de la tâche

Vous configurez les notifications d'événements en associant le XML de configuration de notification à un bucket source. Le XML de configuration de notification suit les conventions S3 pour la configuration des

notifications de compartiment, avec la rubrique Amazon SNS de destination, la rubrique Kafka ou le point de terminaison webhook spécifié comme URN d'un point de terminaison.

Pour obtenir des informations générales sur les notifications d'événements et leur configuration, reportez-vous au "Documentation Amazon". Pour plus d'informations sur la manière dont StorageGRID implémente l'API de configuration des notifications de compartiment S3, reportez-vous au "Instructions d'implémentation des applications client S3".

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

- Lorsque vous créez et appliquez un XML de configuration de notification valide, il doit utiliser l'URN d'un noeud final de notification d'événement pour chaque destination.
- Bien que la notification d'événement puisse être configurée sur un compartiment avec le verrouillage objet S3 activé, les métadonnées de verrouillage objet S3 (y compris la date de conservation jusqu'à et l'état de conservation légale) des objets ne seront pas incluses dans les messages de notification.
- Une fois que vous avez configuré les notifications d'événements, chaque fois qu'un événement spécifié se produit pour un objet dans le compartiment source, une notification est générée et envoyée à la rubrique Amazon SNS, à la rubrique 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 sont envoyées uniquement pour les actions qui sont effectuées après l'enregistrement de la configuration de notification.

Étapes

1. Activer les notifications pour le compartiment source :
   - Utilisez un éditeur de texte pour créer le XML de configuration de notification requis pour activer les notifications d'événement, comme spécifié dans l'API de notification S3.
   - Lors de la configuration du XML, utilisez l'URN d'un terminal de notification d'événements comme sujet de destination.

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

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

3. Sélectionnez le nom du compartiment source.

   La page des détails du compartiment s'affiche.

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

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

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

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

      Dans 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 envoyée à la rubrique Amazon SNS de destination, à la rubrique Kafka ou au point de terminaison du webhook.

      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 remise.

```
{
   "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 dans la rubrique de destination, vous avez configuré votre compartiment source pour les notifications StorageGRID.

Informations associées

- "Description des notifications pour les compartiments"
- "UTILISEZ L'API REST S3"
- "Créer un terminal de services de plate-forme"

Configurer le service d'intégration de la recherche

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

Avant de commencer

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

Description de la tâche

Une fois que vous avez configuré le service d'intégration de recherche pour un compartiment source, la création d'un objet ou la mise à jour des métadonnées ou des balises d'un objet déclenche l'envoi des métadonnées d'objet vers le terminal de destination.

Si vous activez le service d'intégration de recherche pour un compartiment qui contient déjà des objets, les notifications de métadonnées ne sont pas automatiquement envoyées pour les objets existants. Mettez à jour ces objets existants pour vous assurer 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 XML de notification de métadonnées requis pour activer l'intégration de la recherche.
    - Lors de la configuration du XML, utilisez l'URN d'un noeud final d'intégration de recherche comme destination.

      Les objets peuvent être filtrés sur le préfixe du nom de l'objet. Par exemple, vous pouvez envoyer des métadonnées pour les objets dont le préfixe est `images` donné à une destination, et des métadonnées pour les objets dont le préfixe est ajouté `videos` à une autre. Les configurations qui comportent des préfixes qui se chevauchent ne sont pas valides et sont rejetées lorsqu'elles sont soumises. Par exemple, une configuration qui inclut une règle pour les objets avec le préfixe `test` et une seconde règle pour les objets avec le préfixe `test2` n'est pas autorisée.

      Si nécessaire, reportez-vous à la Exemples pour le XML de configuration des métadonnées.

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>/Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

Éléments de la configuration de notification des métadonnées XML :

Nom	Description	Obligatoire
Configuration de la MetadaNotification Configuration	Balise de conteneur pour les règles utilisées pour spécifier les objets et la destination des notifications de métadonnées. Contient un ou plusieurs éléments de règle.	Oui
Règle	Balise de conteneur d'une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié. Les règles avec des préfixes qui se chevauchent sont rejetées. Inclus dans l'élément MetadaNotificationConfiguration.	Oui
ID	Identifiant unique de la règle. Inclus dans l'élément règle.	Non
État	L'état peut être « activé » ou « désactivé ». Aucune action n'est prise pour les règles désactivées. Inclus dans l'élément règle.	Oui
Préfixe	Les objets qui correspondent au préfixe sont affectés par la règle et leurs métadonnées sont envoyées à la destination spécifiée. Pour faire correspondre tous les objets, spécifiez un préfixe vide. Inclus dans l'élément règle.	Oui
Destination	Balise de conteneur pour la destination d'une règle. Inclus dans l'élément règle.	Oui

Nom	Description	Obligatoire
Urne	URN de la destination où les métadonnées d'objet sont envoyées. Doit être l'URN d'un terminal StorageGRID avec les propriétés suivantes : • `es` doit être le troisième élément. • L'URN doit se terminer par l'index et le type où les métadonnées sont stockées, sous la forme `domain-name/myindex/mytype`. Les terminaux sont configurés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Ils se présentent sous la forme suivante : • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` Le noeud final doit être configuré avant la soumission du XML de configuration, ou la configuration échouera avec une erreur 404. L'URNE est incluse dans l'élément destination.	Oui

2. Dans le Gestionnaire de locataires, sélectionnez **STORAGE (S3)** > **seaux**.
3. Sélectionnez le nom du compartiment source.

   La page des détails du compartiment s'affiche.

4. Sélectionnez **Platform Services** > **Search Integration**
5. Cochez la case **Activer l'intégration de la recherche**.
6. Collez la configuration de notification de métadonnées dans la zone de texte, puis sélectionnez **Enregistrer les modifications**.

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

7. Vérifiez que le service d'intégration de la recherche est configuré correctement :
   a. Ajoutez un objet au compartiment source qui répond aux exigences relatives au déclenchement d'une notification de métadonnées comme spécifié dans le XML de configuration.

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

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

Une fois que vous avez terminé

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

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

exemple : configuration de notification de métadonnées qui s'applique à tous les objets

Dans cet exemple, les métadonnées d'objet de tous les objets sont envoyées vers la même destination.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Exemple : configuration des notifications de métadonnées avec deux règles

Dans cet exemple, les métadonnées d'objet des objets qui correspondent au préfixe `/images` sont envoyées à une destination, tandis que les métadonnées d'objet des objets correspondant 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

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

Cet exemple montre un exemple de fichier JSON qui pourrait être généré lors de la création d'un objet avec la clé `SGWS/Tagging.txt` dans un compartiment nommé `test`. Le `test` compartiment n'est pas versionné, la balise est donc `versionId` vide.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Champs inclus dans le document JSON

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

Informations sur les compartiments et les objets

`bucket`: Nom du compartiment

`key`: Nom de clé d'objet

`versionID`: Version de l'objet, pour les objets dans les compartiments multiversion

`region`: Région du compartiment, par exemple `us-east-1`

Métadonnées de système

`size`: Taille de l'objet (en octets) visible par un client HTTP

`md5`: Hachage d'objet

Métadonnées d'utilisateur

`metadata`: Toutes les métadonnées utilisateur de l'objet, en tant que paires clé-valeur

`key:value`

Étiquettes

`tags`: Toutes les balises d'objet définies pour l'objet, en tant que paires clé-valeur

`key:value`

Affichage des résultats dans Elasticsearch

Pour les balises et les métadonnées d'utilisateur, StorageGRID transmet des dates et des chiffres à Elasticsearch en tant que chaînes ou notifications d'événement S3. Pour configurer Elasticsearch afin

d’interpréter ces chaînes comme des dates ou des chiffres, suivez les instructions Elasticsearch pour un mappage dynamique des champs et un mappage des formats de date. Activez les mappages de champs dynamiques sur l’index avant de configurer le service d’intégration de recherche. Une fois qu’un document est indexé, vous ne pouvez pas modifier les types de champ du document dans l’index.

Informations sur le copyright

Informations sur les marques commerciales