Utiliser un compte locataire

StorageGRID software

NetApp
December 03, 2025

Sommaire

Utiliser un compte locataire

Utiliser un compte locataire

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

Qu'est-ce qu'un compte locataire ?

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

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

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

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

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

Comment créer un compte locataire

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

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

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

Configurer les locataires S3

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

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

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

Comment se connecter et se déconnecter

Sign in à Tenant Manager

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

Avant de commencer

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

```
https://FQDN_or_Admin_Node_IP/

https://FQDN_or_Admin_Node_IP:port/

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

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

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

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

Étapes

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

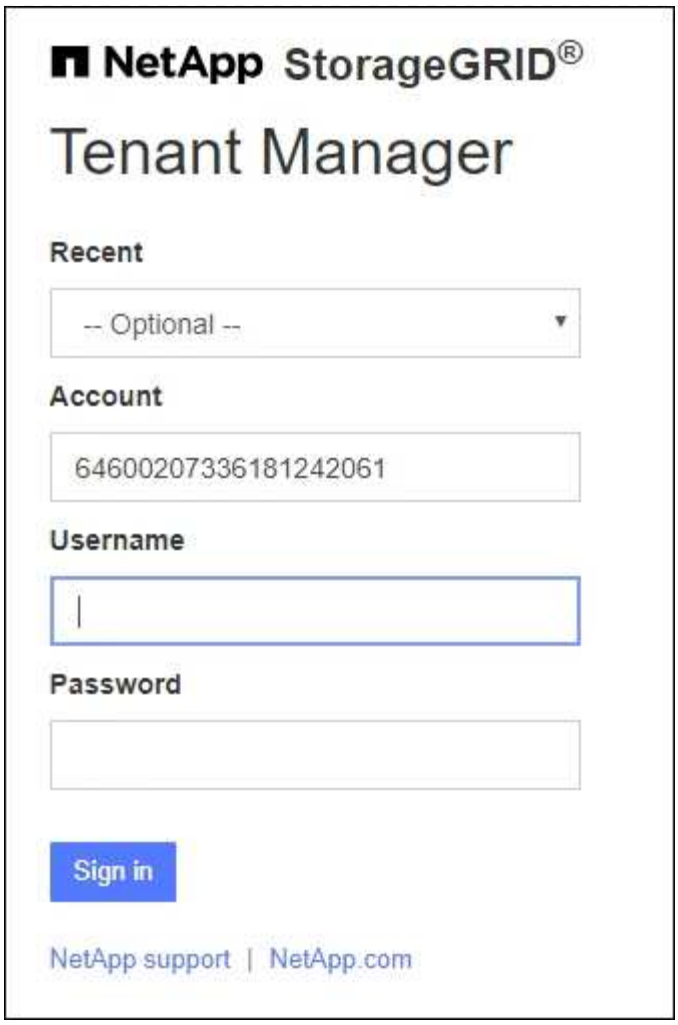
   L'écran de connexion qui s'affiche dépend de l'URL que vous avez saisie et de la configuration de l'authentification unique (SSO) pour StorageGRID.

Ne pas utiliser SSO

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

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

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



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

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

iii. Sélectionnez * Sign in*.

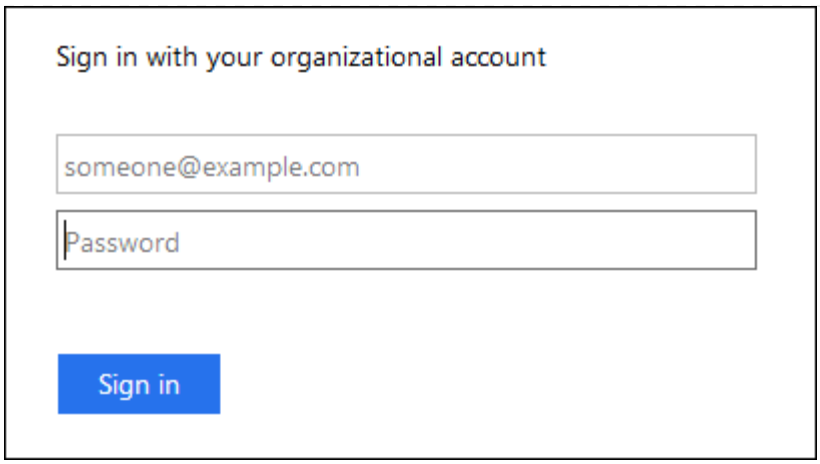
Le tableau de bord du gestionnaire de locataires apparaît.

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

Utilisation de SSO

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

◦ La page SSO de votre organisation. Par exemple:



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

- La page de connexion SSO du gestionnaire de locataires.

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

ii. Sélectionnez * Sign in*.

iii. Sign in avec vos informations d'identification SSO standard sur la page de connexion SSO de votre organisation.

Le tableau de bord du gestionnaire de locataires apparaît.

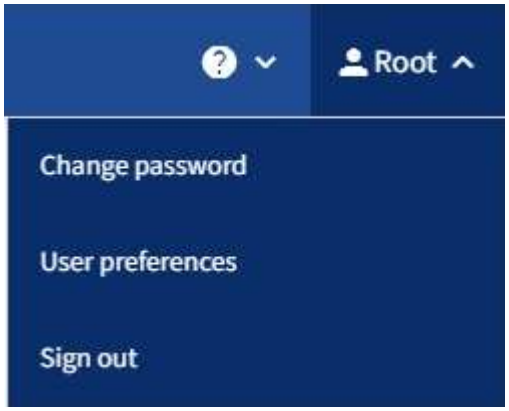
Déconnexion de Tenant Manager

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

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

Étapes

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



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

   - Si SSO n'est pas utilisé :

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

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

   - Si SSO est activé :

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

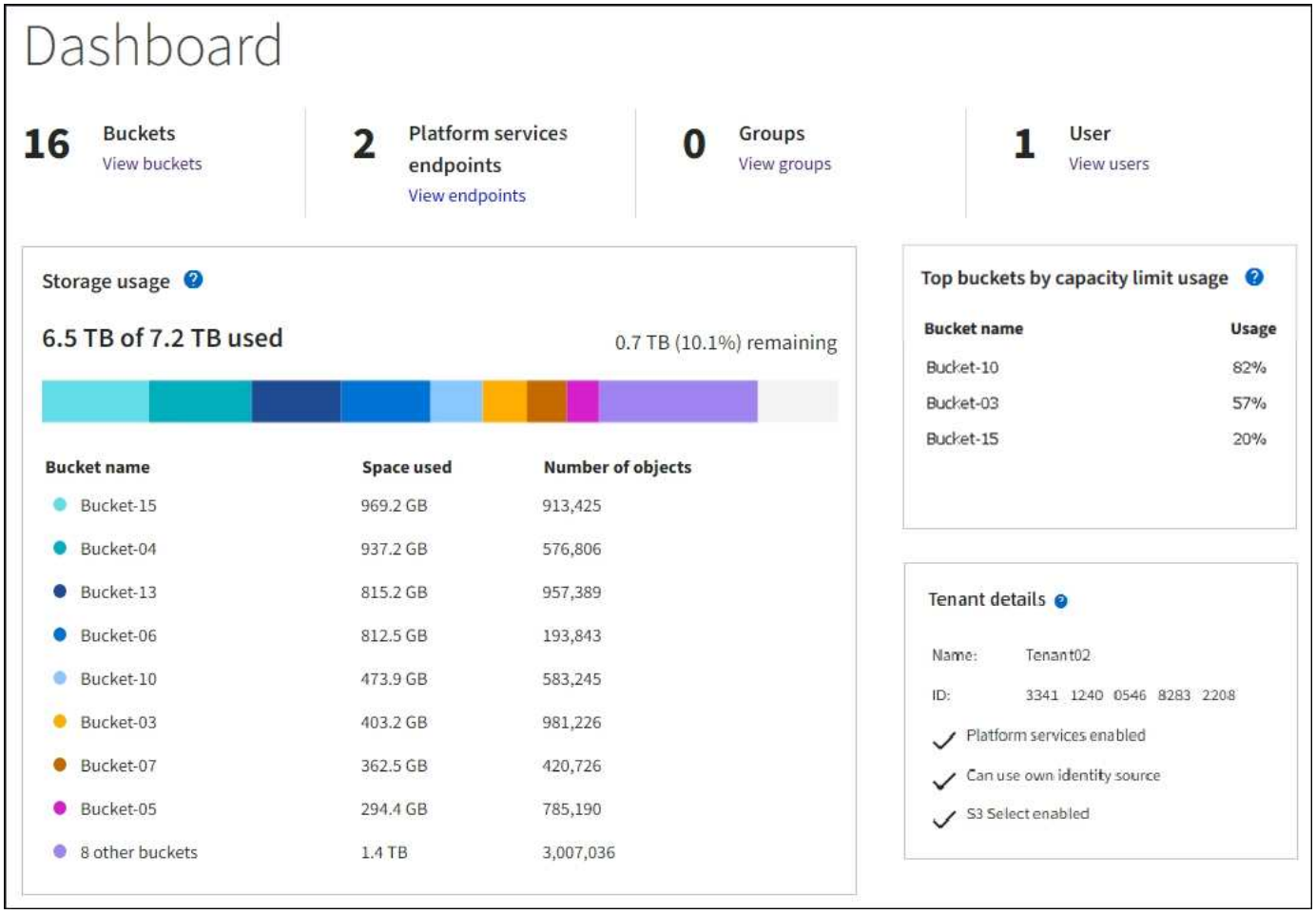
Si SSO est activé et que vous êtes également connecté au Gestionnaire de grille, vous devez également vous déconnecter du Gestionnaire de grille pour vous déconnecter de SSO.

Comprendre le tableau de bord du Tenant Manager

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

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

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



Informations sur le compte du locataire

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

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

Utilisation du stockage et des quotas

Le panneau Utilisation du stockage contient les informations suivantes :

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

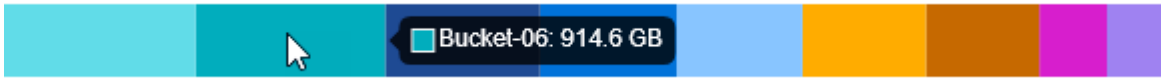
  Cette valeur indique la quantité totale de données d'objet téléchargées et ne représente pas l'espace utilisé pour stocker des copies de ces objets et leurs métadonnées.

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

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

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

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



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

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

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

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

Alertes d'utilisation des quotas

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

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

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

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

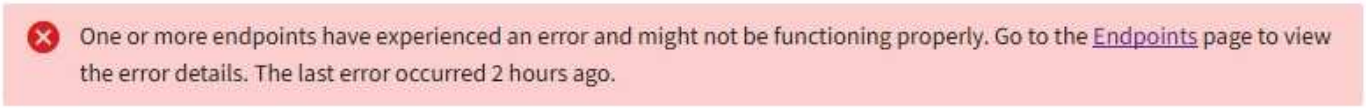
Utilisation de la limite de capacité

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

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

Erreurs de point de terminaison

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



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

API de gestion des locataires

Comprendre l'API de gestion des locataires

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

L'API de gestion des locataires :

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

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

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

Opérations API

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

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

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

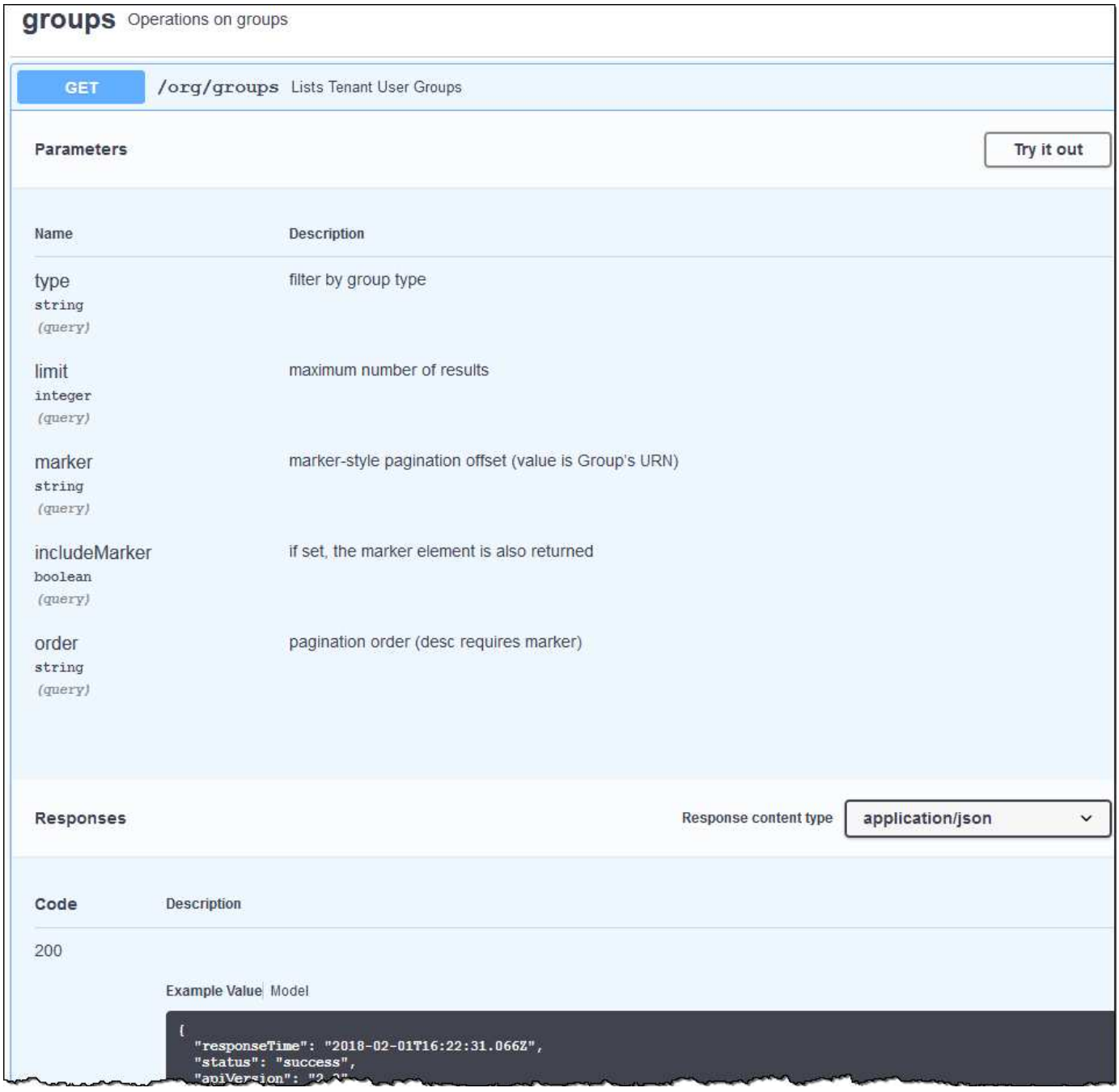
  Pour plus d'informations sur l'amélioration de la sécurité de l'authentification, consultez"Protection contre la falsification de requêtes intersites" .

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

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

Détails de l'opération

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



Émettre des requêtes API

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

Étapes

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

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

Gestion des versions de l'API de gestion des locataires

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

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

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

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

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

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

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

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

Les demandes obsolètes sont marquées comme obsolètes des manières suivantes :

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

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

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

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

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

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

Spécifier une version d'API pour une requête

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

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

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

Protection contre la falsification de requêtes intersites (CSRF)

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

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

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

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

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

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

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

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

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

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

Utiliser les connexions de la fédération de grille

Cloner des groupes de locataires et des utilisateurs

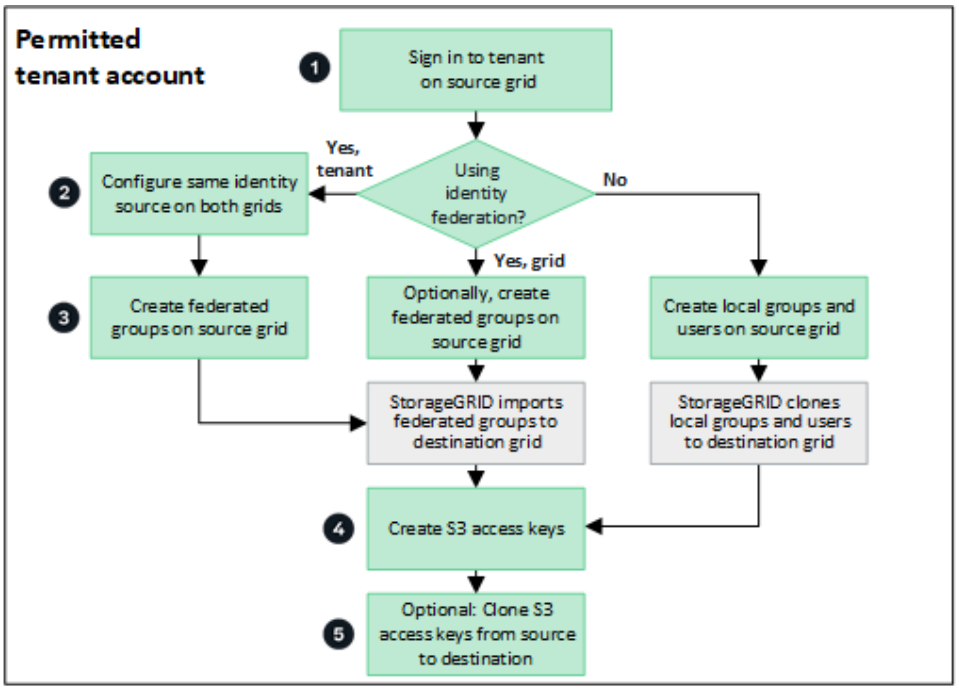
Si un locataire a été créé ou modifié pour utiliser une connexion de fédération de grille, ce locataire est répliqué d'un système StorageGRID (le locataire source) vers un autre système StorageGRID (le locataire réplica). Une fois le locataire répliqué, tous les groupes et utilisateurs ajoutés au locataire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

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

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

Flux de travail du locataire pour le clonage de compte

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



Voici les principales étapes du flux de travail :

1 Sign in au locataire

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

2 En option, configurer la fédération d'identité

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

3 Créer des groupes et des utilisateurs

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

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

4 Créer des clés d'accès S3

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

5 En option, clonez les clés d'accès S3

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

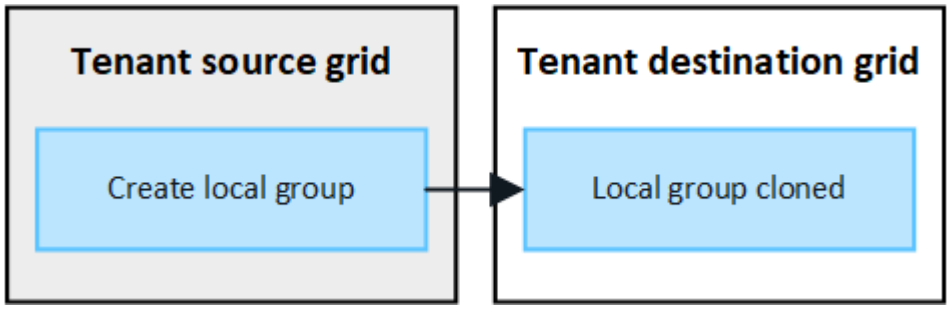
Comment les groupes, les utilisateurs et les clés d'accès S3 sont-ils clonés ?

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

Les groupes locaux créés sur la grille source sont clonés

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

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

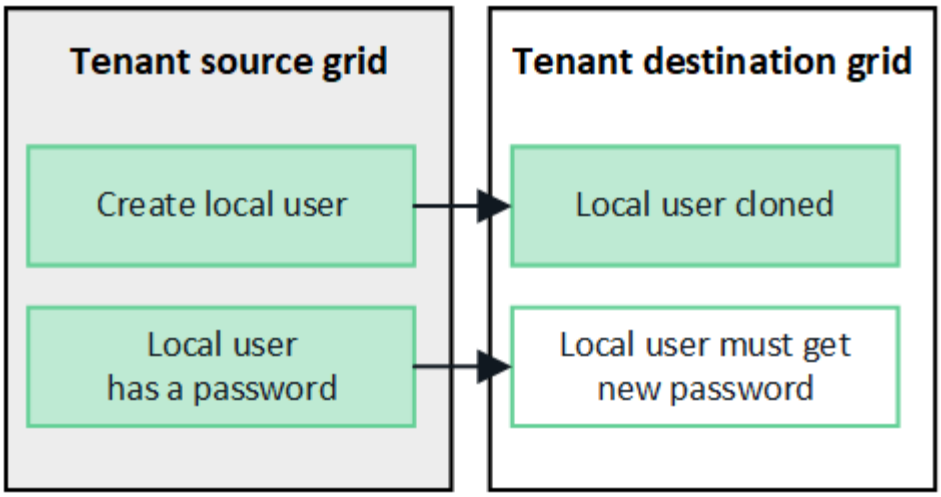


> Tous les utilisateurs que vous sélectionnez lorsque vous créez un groupe local sur la grille source ne sont pas inclus lorsque le groupe est cloné sur la grille de destination. Pour cette raison, ne sélectionnez pas d'utilisateurs lorsque vous créez le groupe. Sélectionnez plutôt le groupe lorsque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

Les utilisateurs locaux créés sur la grille source sont clonés

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

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

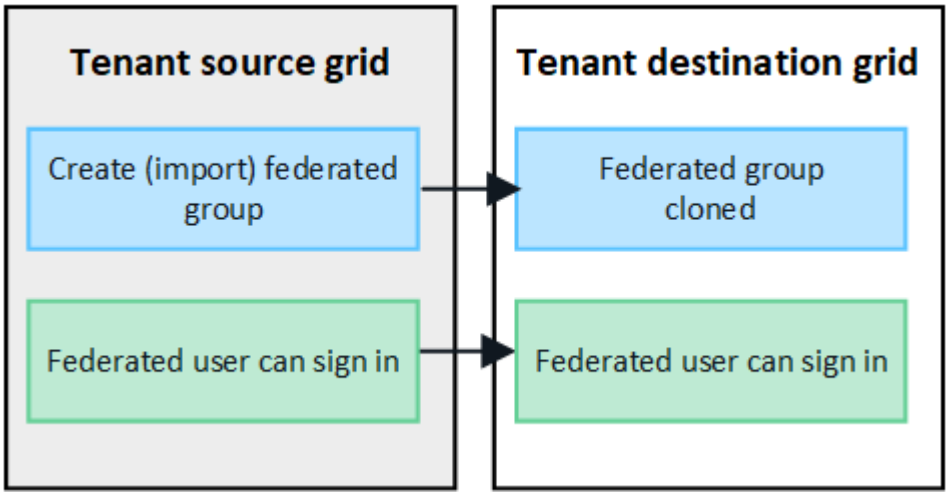


Les groupes fédérés créés sur la grille source sont clonés

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

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

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

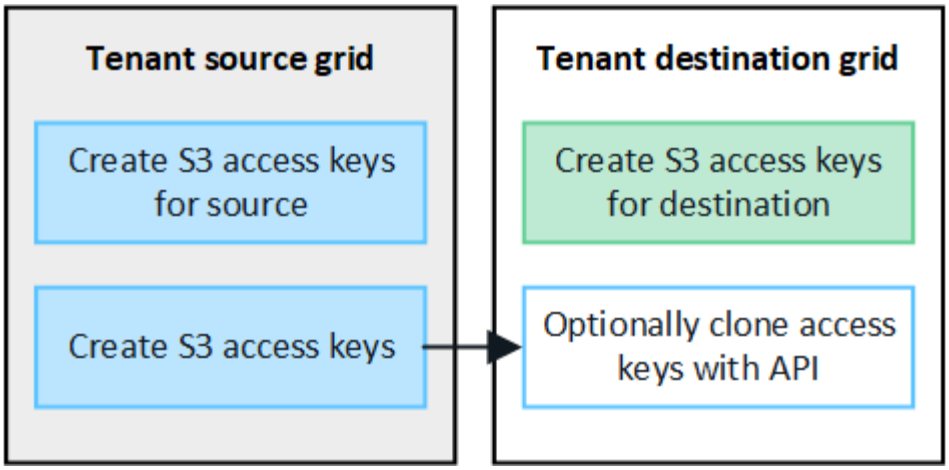


Les clés d'accès S3 peuvent être clonées manuellement

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

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

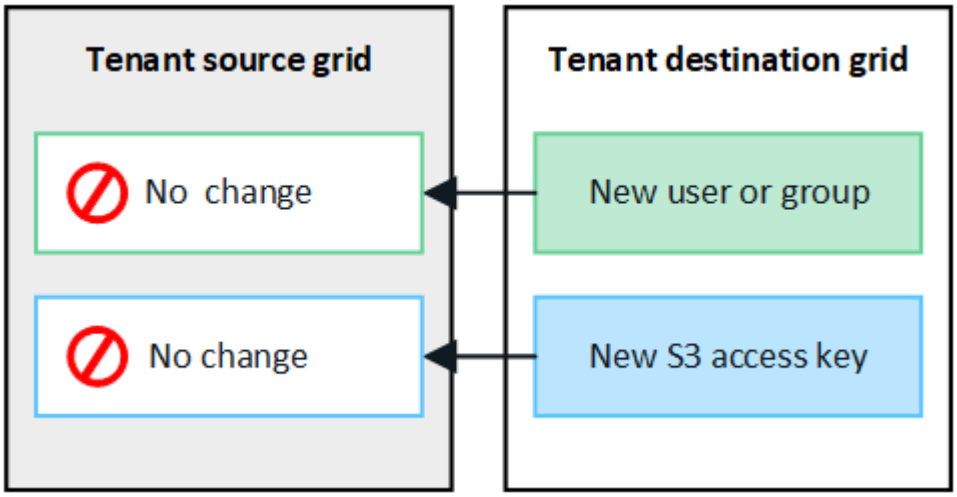
- Si vous n'avez pas besoin d'utiliser les mêmes clés pour chaque grille, vous pouvez"créez vos propres clés d'accès" ou"créer les clés d'accès d'un autre utilisateur" sur chaque grille.
- Si vous devez utiliser les mêmes clés sur les deux grilles, vous pouvez créer des clés sur la grille source, puis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



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

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

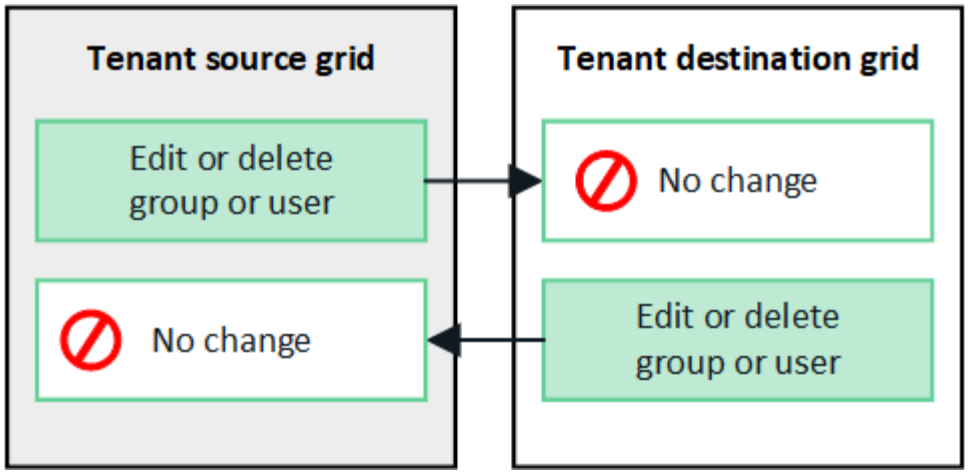
Le clonage se produit uniquement à partir de la grille source du locataire vers la grille de destination du locataire. Si vous créez ou importez des groupes et des utilisateurs sur la grille de destination du locataire, StorageGRID ne clonera pas ces éléments dans la grille source du locataire.



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

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

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



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

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

Avant de commencer

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

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

Clonez vos propres clés d'accès

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

Étapes

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

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

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

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

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

Cloner les clés d'accès d'un autre utilisateur

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

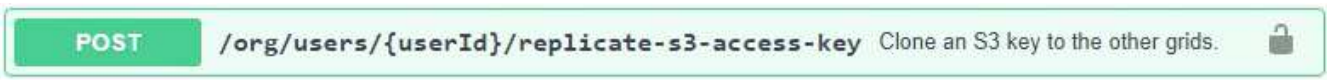
Étapes

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

      `GET /org/users`

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

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



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

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

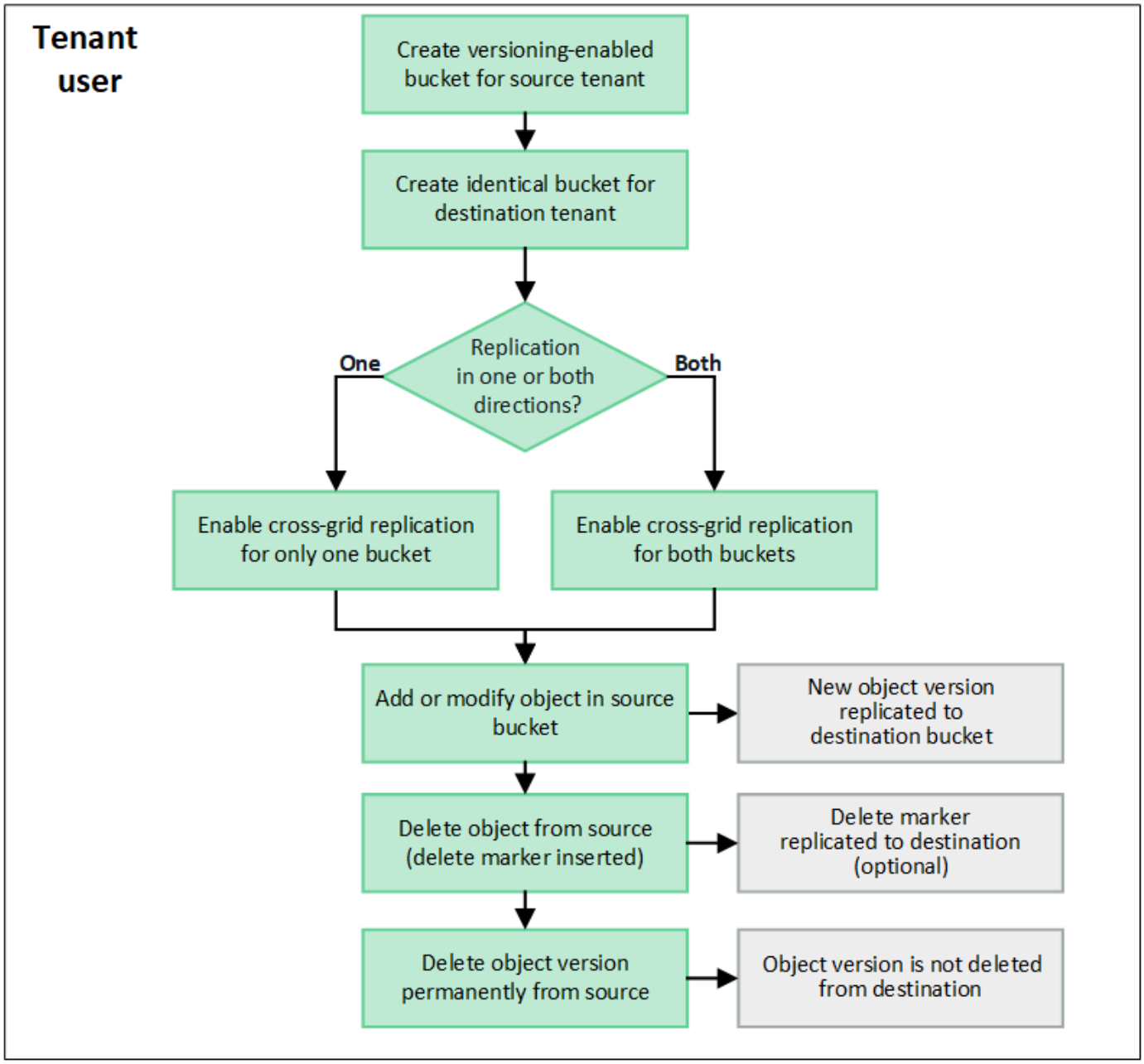
8. Si la clé expire, remplacez l'exemple d'entrée pour **expires** par la date et l'heure d'expiration sous forme de chaîne au format de données-heure ISO 8601 (par exemple, `2023-02-28T22:46:33-08:00`). Si la clé n'expire pas, entrez **null** comme valeur pour l'entrée **expires** (ou supprimez la ligne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

Gérer la réplication inter-réseaux

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

Flux de travail pour la réplication inter-grille

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



Configurer la réplication inter-grille

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

Avant de commencer

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

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

Créer deux buckets identiques

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

Étapes

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

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

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

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

Activer la réplication inter-réseaux

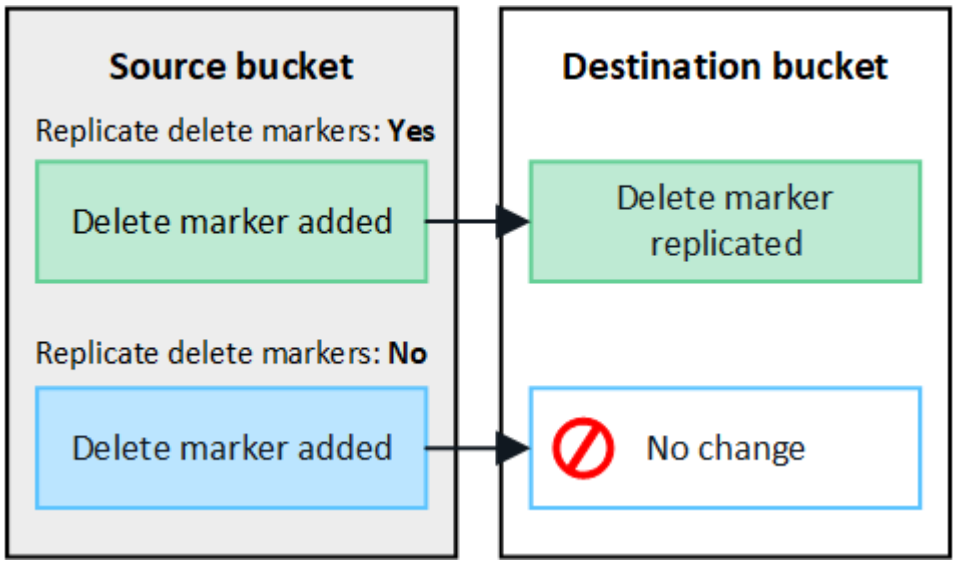
Vous devez effectuer ces étapes avant d'ajouter des objets à l'un ou l'autre des compartiments.

Étapes

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

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

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



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

Voir"Qu'est-ce que la réplication inter-réseau" pour plus de détails.

a. Vous pouvez également modifier le paramètre de la catégorie d'audit **Réplication inter-grille** pour gérer le volume des messages d'audit :
   - **Erreur** (par défaut) : seules les demandes de réplication inter-grille ayant échoué sont incluses dans la sortie d'audit.
   - **Normal** : toutes les demandes de réplication inter-grille sont incluses, ce qui augmente considérablement le volume de sortie d'audit.

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

c. Sélectionnez **Activer et tester**.

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

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

Réplication des tests entre les grilles

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

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

Avant de commencer

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

Étapes

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

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

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

Désactiver la réplication inter-grille

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

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

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

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

Avant de commencer

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

Étapes

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

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

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

Afficher les connexions de la fédération de grille

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

Avant de commencer

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

Étapes

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

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

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

2. Vous pouvez également sélectionner un nom de bucket pour"afficher les détails du godet" .

Effacer la dernière erreur

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

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

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

Étapes

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

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

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

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

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

Gérer les groupes et les utilisateurs

Utiliser la fédération d'identité

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

Configurer la fédération d'identité pour Tenant Manager

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

Avant de commencer

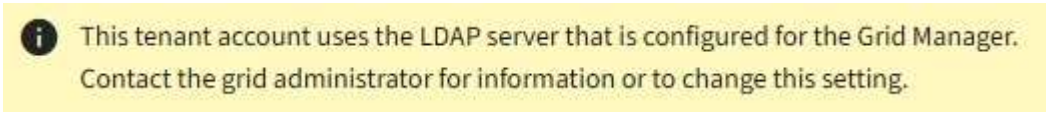
- Vous êtes connecté au Tenant Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous appartenez à un groupe d'utilisateurs qui possède le"Autorisation d'accès root" .
- Vous utilisez Active Directory, Azure AD, OpenLDAP ou Oracle Directory Server comme fournisseur d'identité.

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

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

À propos de cette tâche

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

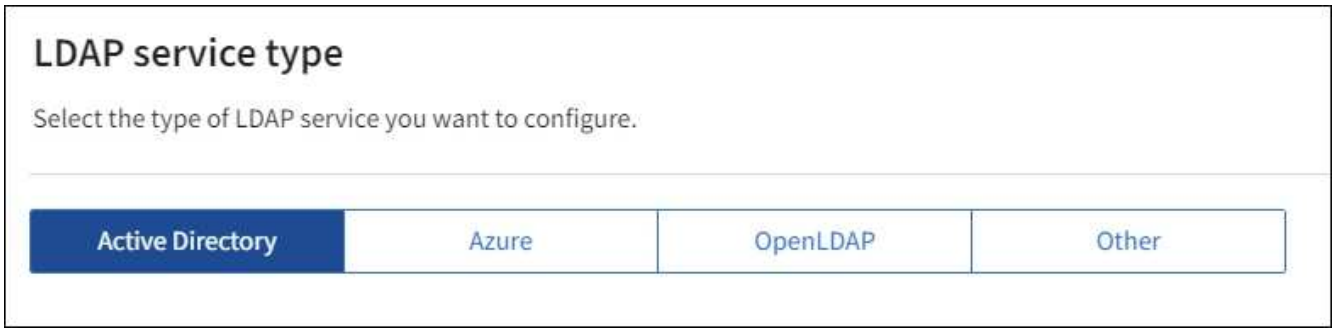


Entrer la configuration

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

Étapes

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



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

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

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

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

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

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

     - `sAMAccountName`ou `uid`

- `objectGUID`, `entryUUID` , ou `nsuniqueid`
- `cn`
- `memberOf`ou `isMemberOf`
- **Active Directory**: `objectSid` , `primaryGroupID` , `userAccountControl` , et `userPrincipalName`
- **Azuré**: `accountEnabled` et `userPrincipalName`

◦ **Mot de passe** : Le mot de passe associé au nom d'utilisateur.

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

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

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

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

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

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

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

Saisissez l'un de ces modèles :

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

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

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

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

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

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

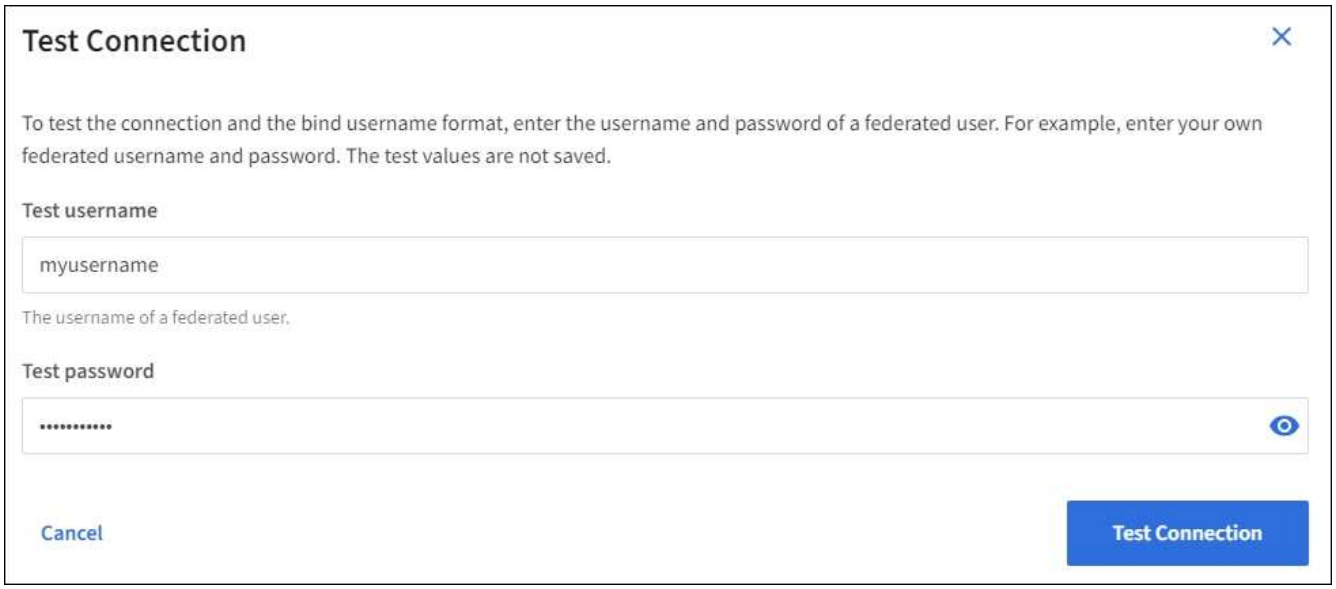
Tester la connexion et enregistrer la configuration

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

Étapes

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

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



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

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

Forcer la synchronisation avec la source d'identité

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

Étapes

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

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

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

Désactiver la fédération d'identité

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

À propos de cette tâche

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

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

Étapes

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

Directives pour la configuration du serveur OpenLDAP

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

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

Superpositions Memberof et refint

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

Indexage

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

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

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

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

Gérer les groupes de locataires

Créer des groupes pour un locataire S3

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

Avant de commencer

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

Accéder à l'assistant de création de groupe

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

Étapes

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

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

3. Sélectionnez **Créer un groupe**.

Choisissez un type de groupe

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

Étapes

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

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

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

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

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

Gérer les autorisations de groupe

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

Étapes

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

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

2. Sélectionnez une ou plusieurs autorisations pour ce groupe.

   Voir "Autorisations de gestion des locataires" .

3. Sélectionnez **Continuer**.

Définir la stratégie de groupe S3

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

Étapes

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

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

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

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

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

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

Ajouter des utilisateurs (groupes locaux uniquement)

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

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

Étapes

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

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

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

Créer des groupes pour un locataire Swift

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

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

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

Avant de commencer

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

Accéder à l’assistant de création de groupe

Étapes

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

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

Choisissez un type de groupe

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

Étapes

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

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

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

Gérer les autorisations de groupe

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

Étapes

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

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

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

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

Définir la politique de groupe Swift

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

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

Ajouter des utilisateurs (groupes locaux uniquement)

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

Étapes

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

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

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

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

Autorisations de gestion des locataires

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

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

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

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

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

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

Autorisation	Description	Détails
Accès root	Fournit un accès complet au gestionnaire de locataires et à l'API de gestion des locataires.	Les utilisateurs Swift doivent disposer de l'autorisation d'accès root pour se connecter au compte locataire.
Administrateur	Locataires rapides seulement. Fournit un accès complet aux conteneurs et objets Swift pour ce compte locataire	Les utilisateurs Swift doivent disposer de l'autorisation d'administrateur Swift pour effectuer des opérations avec l'API REST Swift.
Gérez vos propres identifiants S3	Permet aux utilisateurs de créer et de supprimer leurs propres clés d'accès S3.	Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu **STOCKAGE (S3)** > **Mes clés d'accès S3**.
Voir tous les seaux	• Locataires S3 * : permet aux utilisateurs d'afficher tous les buckets et configurations de buckets. • Locataires Swift * : permet aux utilisateurs Swift d'afficher tous les conteneurs et configurations de conteneurs à l'aide de l'API de gestion des locataires.	Les utilisateurs qui ne disposent pas de l'autorisation Afficher tous les buckets ou Gérer tous les buckets ne voient pas l'option de menu **Buckets**. 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. Vous ne pouvez attribuer cette autorisation qu'aux groupes Swift à partir de l'API de gestion des locataires. Vous ne pouvez pas attribuer cette autorisation aux groupes Swift à l'aide du gestionnaire de locataires.

Autorisation	Description	Détails
Gérer tous les compartiments	• Locataires S3 * : permet aux utilisateurs d'utiliser le gestionnaire de locataires et l'API de gestion des locataires pour créer et supprimer des compartiments S3 et pour gérer les paramètres de tous les compartiments S3 du compte de locataire, quels que soient les compartiments S3 ou les stratégies de groupe. • Locataires Swift * : permet aux utilisateurs Swift de contrôler la cohérence des conteneurs Swift à l'aide de l'API de gestion des locataires.	Les utilisateurs qui ne disposent pas de l'autorisation Afficher tous les buckets ou Gérer tous les buckets ne voient pas l'option de menu **Buckets**. 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. Vous ne pouvez attribuer cette autorisation qu'aux groupes Swift à partir de l'API de gestion des locataires. Vous ne pouvez pas attribuer cette autorisation aux groupes Swift à l'aide du gestionnaire de locataires.
Gérer les points de terminaison	Permet aux utilisateurs d'utiliser Tenant Manager ou l'API Tenant Management pour créer ou modifier des points de terminaison de service de plateforme, qui sont utilisés comme destination pour les services de plateforme StorageGRID .	Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu **Points de terminaison des services de plateforme**.
Utiliser l'onglet Console S3	Associée à l'autorisation Afficher tous les buckets ou Gérer tous les buckets, cette option permet aux utilisateurs d'afficher et de gérer les objets à partir de l'onglet Console S3 sur la page de détails d'un bucket.	

Gérer les groupes

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

Avant de commencer

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

Afficher ou modifier le groupe

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

Étapes

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 locataire.

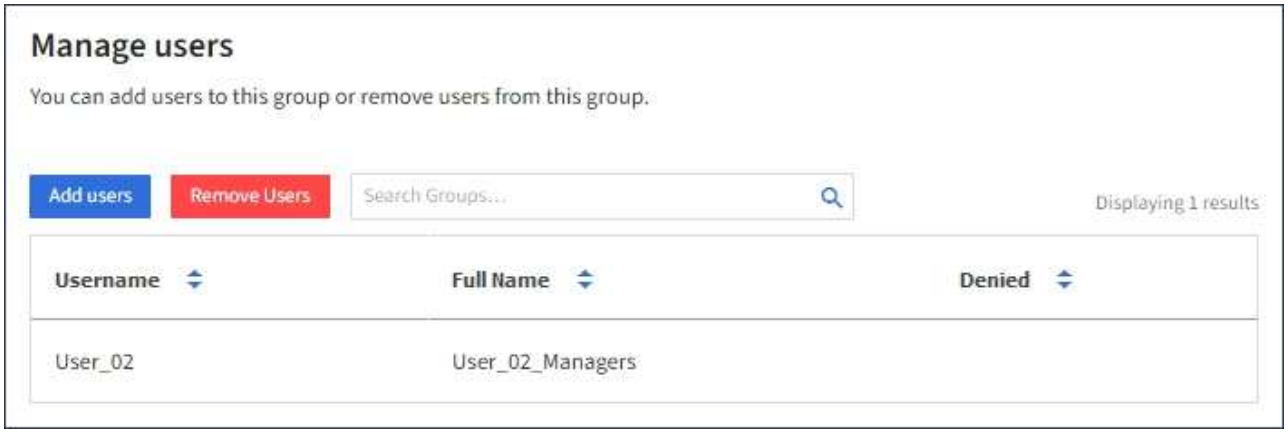
   Si le compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous

visualisez les groupes sur la grille source du locataire :

- Un message de bannière indique que si vous modifiez ou supprimez un groupe, vos modifications ne seront pas synchronisées avec l'autre grille.
- Si nécessaire, un message de bannière indique si les groupes n'ont pas été clonés sur le locataire sur la grille de destination. Tu peuxréessayer un clonage de groupe ça a échoué.

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

a. Sélectionnez l'onglet Utilisateurs.



b. Sélectionnez **Ajouter des utilisateurs**.

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

Un message de réussite apparaît dans le coin supérieur droit.

8. Pour supprimer les utilisateurs locaux du groupe :

a. Sélectionnez l'onglet Utilisateurs.

b. Sélectionnez **Supprimer les utilisateurs**.

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

Un message de réussite apparaît dans le coin supérieur droit.

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

Groupe en double

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

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

Étapes

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

Réessayer le clonage du groupe

Pour réessayer un clonage qui a échoué :

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

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

Supprimer un ou plusieurs groupes

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

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

Étapes

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

   Une boîte de dialogue de confirmation apparaît.
4. Sélectionnez **Supprimer le groupe** ou **Supprimer les groupes**.

Gérer les utilisateurs locaux

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

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

Avant de commencer

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

Créer un utilisateur local

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

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

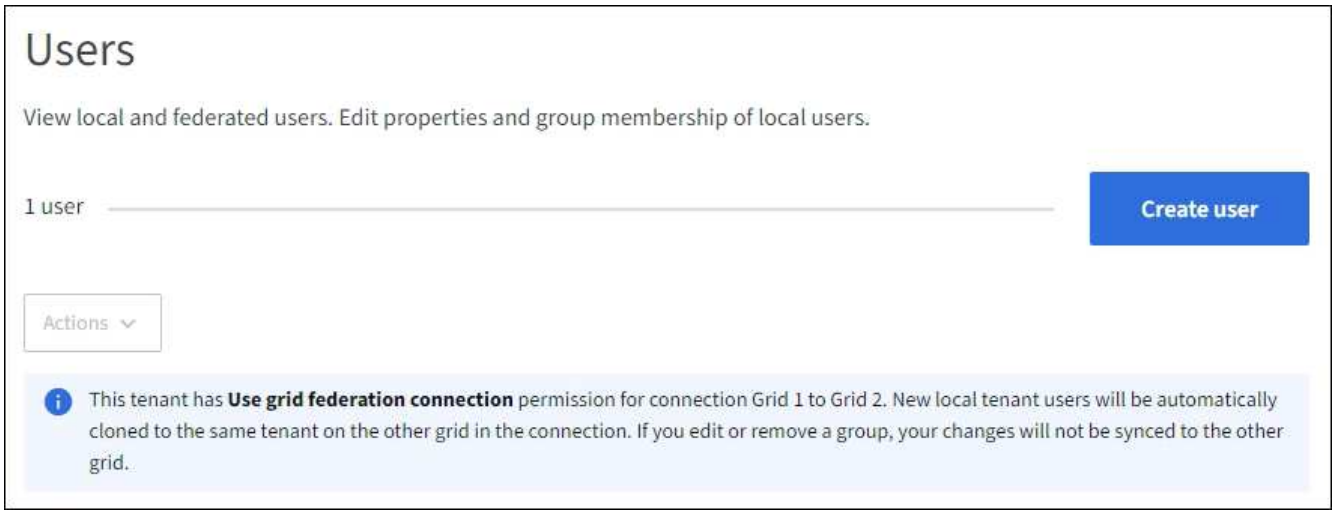
Les utilisateurs Swift qui n'appartiennent à aucun groupe ne disposent pas d'autorisations de gestion ni d'accès au conteneur Swift.

Accéder à l'assistant de création d'utilisateur

Étapes

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

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



2. Sélectionnez **Créer un utilisateur**.

Entrez les informations d'identification

Étapes

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

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

Champ	Description
Nom d'utilisateur	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 de locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, une erreur de clonage se produira si le même **Nom d'utilisateur** existe déjà pour le locataire sur la grille de destination.
Mot de passe et confirmation du mot de passe	Le mot de passe que l'utilisateur utilisera initialement lors de la connexion.
Refuser l'accès	Sélectionnez **Oui** pour empêcher cet utilisateur de se connecter au compte locataire, même s'il appartient toujours à un ou plusieurs groupes. Par exemple, sélectionnez **Oui** pour suspendre temporairement la possibilité pour un utilisateur de se connecter.

2. Sélectionnez **Continuer**.

Affecter à des groupes

Étapes

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

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

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

2. Sélectionnez **Créer un utilisateur**.

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

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

Afficher ou modifier l'utilisateur local

Étapes

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

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

- Un message de bannière indique que si vous modifiez ou supprimez un utilisateur, vos modifications ne seront pas synchronisées avec l'autre grille.
- Si nécessaire, un message de bannière indique si les utilisateurs n'ont pas été clonés sur le locataire sur la grille de destination. Vous pouvez réessayer un clone d'utilisateur qui a échoué .

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

      Vous ne pouvez pas changer le nom d'utilisateur.

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

Utilisateur local en double

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

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

Étapes

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

Réessayer le clonage de l'utilisateur

Pour réessayer un clonage qui a échoué :

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

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

Supprimer un ou plusieurs utilisateurs locaux

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

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

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

Étapes

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

   Une boîte de dialogue de confirmation apparaît.
4. Sélectionnez **Supprimer l'utilisateur** ou **Supprimer les utilisateurs**.

Gérer les clés d’accès S3

Gérer les clés d’accès S3

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

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

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

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

Créez vos propres clés d’accès S3

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

Avant de commencer

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

À propos de cette tâche

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

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

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

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

Étapes

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

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

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

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

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

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

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

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

6. Sélectionnez **Terminer**.

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

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

Afficher vos clés d'accès S3

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

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

Avant de commencer

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

Étapes

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

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

   Les clés expirées sont supprimées automatiquement.

Supprimez vos propres clés d'accès S3

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

Avant de commencer

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

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

Étapes

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

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

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

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

Avant de commencer

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

À propos de cette tâche

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

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

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

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

Étapes

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

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

     > La date d'expiration peut être au maximum de cinq ans à compter de la date actuelle. Le délai d'expiration peut être d'au moins une minute à partir de l'heure actuelle.
5. Sélectionnez **Créer une clé d'accès**.

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

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

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

7. Sélectionnez **Terminer**.

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

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

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

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

Avant de commencer

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

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

Étapes

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

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

   Les clés expirées sont supprimées automatiquement.

Informations connexes

- "Créer les clés d'accès S3 d'un autre utilisateur"
- "Supprimer les clés d'accès S3 d'un autre utilisateur"

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

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

Avant de commencer

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

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

Étapes

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

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

Gérer les buckets S3

Créer un bucket S3

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

Avant de commencer

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

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

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

> Chaque grille peut contenir un maximum de 100 000 buckets.

Accéder à l'assistant

Étapes

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

Entrez les détails

Étapes

1. Saisissez les détails du bucket.

Champ	Description
Nom du bucket	Un nom pour le bucket qui respecte ces règles : • Doit être unique sur chaque système StorageGRID (pas seulement unique au sein du compte locataire). • Doit être conforme au DNS. • Doit contenir au moins 3 et pas plus de 63 caractères. • Chaque étiquette doit commencer et se terminer par une lettre minuscule ou un chiffre et ne peut utiliser que des lettres minuscules, des chiffres et des traits d'union. • Ne doit pas contenir de points dans les demandes de style hébergé virtuellement. Les points entraîneront des problèmes avec la vérification du certificat générique du serveur. Pour plus d'informations, consultez le "Documentation d'Amazon Web Services (AWS) sur les règles de dénomination des buckets" . **Remarque** : vous ne pouvez pas modifier le nom du bucket après l'avoir créé.
Région	La région du seau. 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. **Remarque** : vous ne pouvez pas modifier la région après avoir créé le bucket.

2. Sélectionnez **Continuer**.

Gérer les paramètres

Étapes

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

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

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

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

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

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

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

   > Votre administrateur de réseau doit vous donner la permission de"utiliser les fonctionnalités spécifiques de S3 Object Lock" .

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

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

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

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

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

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

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

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

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

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

5. Sélectionnez **Créer un bucket**.

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

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

Afficher les détails du godet

Vous pouvez afficher les buckets dans votre compte locataire.

Avant de commencer

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

Étapes

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

   La page Buckets apparaît.

2. Consultez le tableau récapitulatif pour chaque compartiment.

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

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

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

   Fonctionnalités activées
   La liste des fonctionnalités activées pour le bucket.

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

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

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

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

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

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

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

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

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

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

Capacité

Si défini, la limite de capacité du bucket.

Date de création

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

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

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

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

Appliquer une balise de stratégie ILM à un bucket

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

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

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

Avant de commencer

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

Étapes

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

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

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

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

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

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

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

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

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

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

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

Gérer la politique de compartiment

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

Avant de commencer

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

Étapes

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

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

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

Gérer la cohérence des buckets

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

Avant de commencer

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

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

Directives relatives à la cohérence des seaux

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

Modifier la cohérence du bucket

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

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

Étapes

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

   La page des détails du bucket apparaît.

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

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

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

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

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

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

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

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

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

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

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

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

Avant de commencer

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

À propos de cette tâche

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

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

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

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

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

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

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

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

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

Demande de liste d'objets ou de versions d'objets	Non	Non	Non	Non
Demande de copie d'un objet d'un bucket à un autre	• 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
Demande de finalisation d'un téléchargement en plusieurs parties	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé

Étapes

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

   La page des détails du bucket apparaît.

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

Modifier la version d'objet pour un bucket

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

Avant de commencer

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

À propos de cette tâche

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

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

Pour plus d'informations, consultez les éléments suivants :

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

Étapes

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

   La page des détails du bucket apparaît.

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

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

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

5. Sélectionnez **Enregistrer les modifications**.

Utilisez S3 Object Lock pour conserver les objets

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

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

Qu'est-ce que S3 Object Lock ?

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

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

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

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

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

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

Modes de rétention

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

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

Paramètres de conservation pour les versions d'objet

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

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

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

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

verrouillage d’objet S3" .

Paramètre de rétention par défaut pour les buckets

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

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

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

Voir"Créer un bucket S3" et"Mettre à jour la conservation par défaut du verrouillage des objets S3" .

Tâches de verrouillage d’objet S3

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

Administrateur de réseau

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

Utilisateur locataire

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

Exigences pour les buckets avec S3 Object Lock activé

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

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

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

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

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

1. **Objet ingéré**

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

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

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

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

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

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

Puis-je toujours gérer les buckets conformes hérités ?

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

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

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

Avant de commencer

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

Étapes

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

   La page des détails du bucket apparaît.

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

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

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

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

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

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

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

7. Sélectionnez **Enregistrer les modifications**.

Configurer le partage de ressources inter-origines (CORS)

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

Avant de commencer

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

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

- Le"Autorisation d'accès root" donne accès à toutes les demandes de configuration CORS.

À propos de cette tâche

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

Activer CORS pour un bucket

Étapes

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

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

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

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

   La page des détails du bucket apparaît.

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

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

Modifier le paramètre CORS

Étapes

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

Désactiver le paramètre CORS

Étapes

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

Supprimer les objets dans le bucket

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

Considérations et exigences

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

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

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

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

- Si le contrôle de version d'objet est activé pour un bucket, l'opération de suppression d'objets ne supprimera pas les marqueurs de suppression créés dans StorageGRID 11.7 ou une version antérieure. Consultez les informations sur la suppression d'objets dans un bucket dans"Comment les objets versionnés S3 sont supprimés" .
- Si vous utilisez"réplication inter-réseaux" , notez ce qui suit :
  - L'utilisation de cette option ne supprime aucun objet du bucket sur l'autre grille.
  - Si vous sélectionnez cette option pour le bucket source, l'alerte **Échec de la réplication inter-grille** sera déclenchée si vous ajoutez des objets au bucket de destination sur l'autre grille. Si vous ne pouvez pas garantir que personne n'ajoutera d'objets au seau sur l'autre grille,"désactiver la réplication inter-grille" pour ce bucket avant de supprimer tous les objets du bucket.

Avant de commencer

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

Étapes

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

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

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

   Menu Actions

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

   b. Sélectionnez **Actions** > **Supprimer les objets dans le bucket**.

   Page de détails

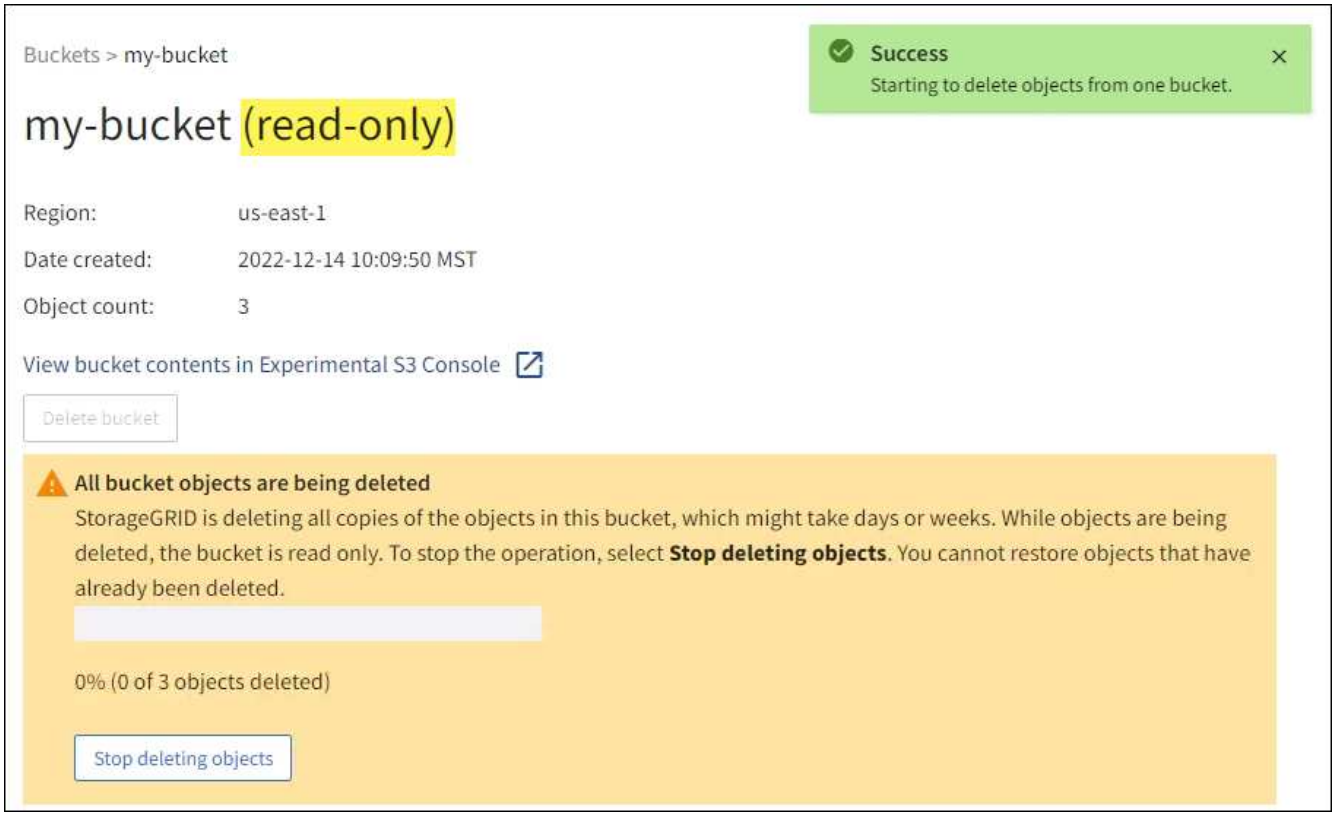
   a. Sélectionnez un nom de bucket pour afficher ses détails.

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

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

   Après quelques minutes :

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

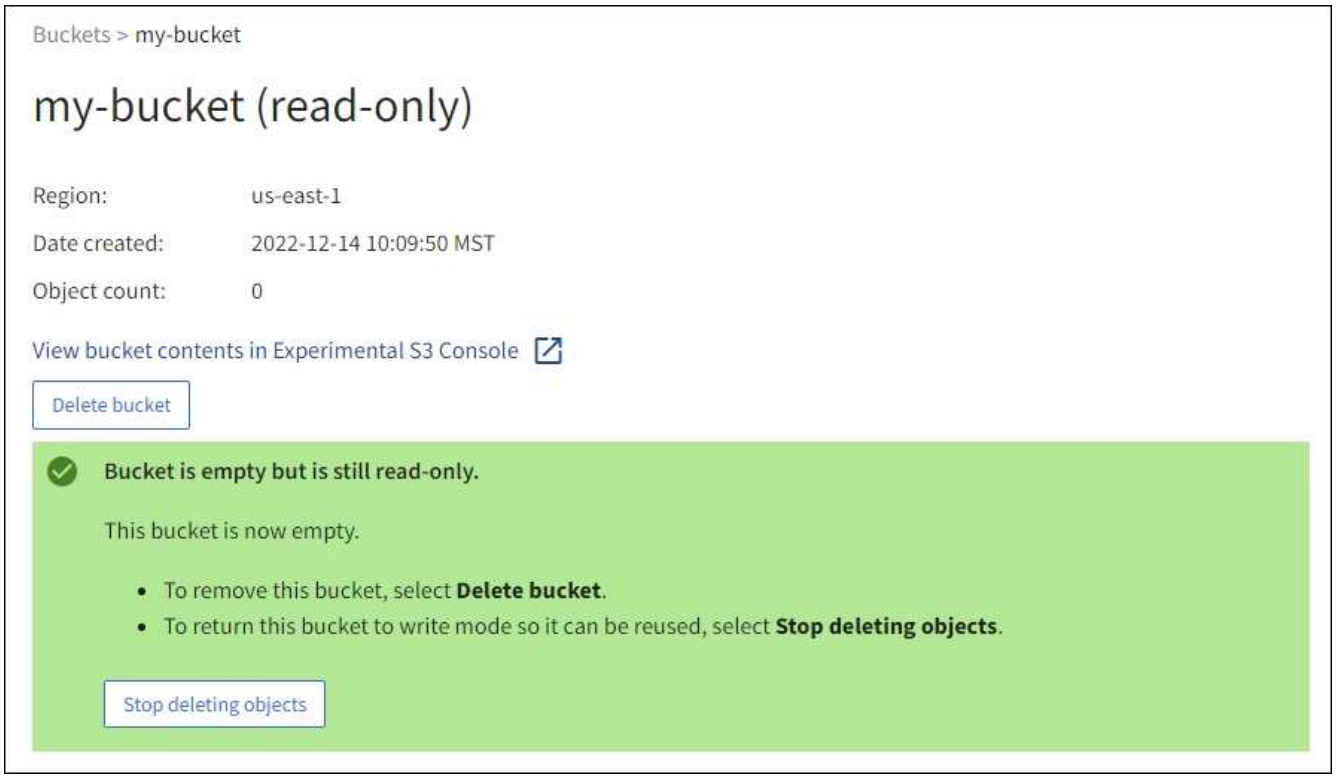


5. Si nécessaire, pendant que l'opération est en cours, sélectionnez **Arrêter la suppression des objets** pour arrêter le processus. Ensuite, si vous le souhaitez, sélectionnez **Supprimer les objets dans le bucket** pour reprendre le processus.

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

6. Attendez que l'opération soit terminée.

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



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

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

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

Supprimer le compartiment S3

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

Avant de commencer

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

À propos de cette tâche

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

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

Étapes

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

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

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

   Menu Actions

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

   b. Sélectionnez **Actions** > **Supprimer les buckets**.

   Page de détails

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

   b. Sélectionnez **Supprimer le bucket**.

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

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

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

Utiliser la console S3

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

La console S3 vous permet de :

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

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

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

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

Avant de commencer

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

Étapes

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

Informations Complémentaires

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

Gérer les services de la plateforme S3

Services de la plateforme S3

Présentation et considérations relatives aux services de la plateforme

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

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

Aperçu des services de la plateforme

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

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

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

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

Comment les services de la plateforme sont configurés

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

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

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

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

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

Service de plateforme	API REST S3	Se référer à
Réplication CloudMirror	• Réplication GetBucket • Réplication de PutBucket	• "Réplication CloudMirror" • "Opérations sur les godets"
Notifications	• Configuration de GetBucketNotification • Configuration de PutBucketNotification	• "Notifications" • "Opérations sur les godets"
Intégration de la recherche	• Configuration de la notification des métadonnées du bucket GET • Configuration des notifications de métadonnées du compartiment PUT	• "Intégration de la recherche" • "Opérations personnalisées StorageGRID"

Considérations relatives à l'utilisation des services de plateforme

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

Considération	Détails
Garanties de commande	StorageGRID garantit l'ordre des opérations sur un objet au sein d'un site. Tant que toutes les opérations sur un objet se déroulent sur le même site, l'état final de l'objet (pour la réplication) sera toujours égal à l'état dans StorageGRID. StorageGRID fait de son mieux pour ordonner les demandes lorsque des opérations sont effectuées sur les sites StorageGRID . Par exemple, si vous écrivez initialement un objet sur le site A, puis écrasez ultérieurement le même objet sur le site B, il n'est pas garanti que l'objet final répliqué par CloudMirror vers le bucket de destination soit l'objet le plus récent.
Suppressions d'objets pilotées par ILM	Pour correspondre au comportement de suppression d'AWS CRR et d'Amazon Simple Notification Service, les demandes de notification d'événements et CloudMirror ne sont pas envoyées lorsqu'un objet dans le compartiment source est supprimé en raison des règles StorageGRID ILM. Par exemple, aucune demande de notification CloudMirror ou d'événement n'est envoyée si une règle ILM supprime un objet après 14 jours. En revanche, les demandes d'intégration de recherche sont envoyées lorsque des objets sont supprimés en raison de l'ILM.
Utilisation des points de terminaison Kafka	Pour les points de terminaison Kafka, le protocole TLS mutuel n'est pas pris en charge. Par conséquent, si vous avez `ssl.client.auth` réglé sur `required` dans la configuration de votre courtier Kafka, cela peut entraîner des problèmes de configuration du point de terminaison Kafka. L'authentification des points de terminaison Kafka utilise les types d'authentification suivants. Ces types sont différents de ceux utilisés pour l'authentification d'autres points de terminaison, tels qu'Amazon SNS, et nécessitent des informations d'identification de nom d'utilisateur et de mot de passe. • SASL/PLAIN • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 **Remarque :** les paramètres de proxy de stockage configurés ne s'appliquent pas aux points de terminaison des services de la plateforme Kafka.

Considérations relatives à l'utilisation du service de réplication CloudMirror

Considération	Détails
État de réplication	StorageGRID ne prend pas en charge le `x-amz-replication-status` en-tête.

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

Comprendre le service de réplication CloudMirror

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

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

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

CloudMirror et ILM

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

CloudMirror et réplication inter-grille

La réplication CloudMirror présente des similitudes et des différences importantes avec la fonctionnalité de réplication inter-grille. "Comparer la réplication inter-grille et la réplication CloudMirror" .

CloudMirror et buckets S3

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

Buckets existants

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

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

Plusieurs buckets de destination

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

Buckets versionnés ou non versionnés

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

Suppression, boucles de réplication et événements

Comportement de suppression

Il s'agit du même comportement de suppression que le service Amazon S3, la réplication interrégionale (CRR). La suppression d'un objet dans un bucket source ne supprime jamais un objet répliqué dans la destination. Si les buckets source et de destination sont tous deux versionnés, le marqueur de suppression

est répliqué. Si le bucket de destination n'est pas versionné, la suppression d'un objet dans le bucket source ne réplique pas le marqueur de suppression dans le bucket de destination ni ne supprime l'objet de destination.

Protection contre les boucles de réplication

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

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

Événements dans le bucket de destination

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

Comprendre les notifications pour les buckets

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

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

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

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

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

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

- s3 : Objet supprimé :
- s3:ObjectRemoved:Supprimer
- s3 : Objet supprimé : Supprimer le marqueur créé
- s3 : Restauration d'objet : Publication

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

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

Comprendre le service d'intégration de recherche

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

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

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

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

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

Intégration de la recherche et buckets S3

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

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

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

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

Notifications de recherche

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

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

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

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

Service d'intégration de recherche et Elasticsearch

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

Gérer les points de terminaison des services de la plateforme

Configurer les points de terminaison des services de la plateforme

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

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

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

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

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

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

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

Points de terminaison pour la réplication CloudMirror

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

Points de terminaison pour les notifications

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

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

Points de terminaison pour le service d’intégration de recherche

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

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

métadonnées de l'objet au point de terminaison.

Informations connexes

"Administrer StorageGRID"

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

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

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

éléments URN

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

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

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

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

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

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

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

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

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

URN pour les services hébergés sur AWS et GCP

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

- Réplication CloudMirror :

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

- Notifications:

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

- Intégration de la recherche :

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

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

URN pour les services hébergés localement

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

- Réplication CloudMirror :

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

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

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

- Notifications:

  Spécifiez un point de terminaison Amazon Simple Notification Service :

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

  Spécifiez un point de terminaison Kafka :

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

- Intégration de la recherche :

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

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

Créer un point de terminaison des services de plateforme

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

Avant de commencer

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

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

  - Nom de ressource unique (URN)

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

- Informations d'authentification (si nécessaire) :

Points de terminaison d'intégration de recherche

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

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

Points de terminaison de réplication CloudMirror

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

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

Points de terminaison Amazon SNS

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

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

Points de terminaison Kafka

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

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

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

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

Étapes

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

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

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

Utilisez l'un des formats suivants :

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

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

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

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

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

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

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

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

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

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

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

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

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

Points de terminaison d'intégration de recherche

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

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

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

Points de terminaison de réplication CloudMirror

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

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

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

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

Points de terminaison Amazon SNS

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

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

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

Points de terminaison Kafka

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

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

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

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

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

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

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

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

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

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

Informations connexes

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

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

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

Avant de commencer

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

À propos de cette tâche

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

Étapes

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

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

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

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

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

Modifier le point de terminaison des services de la plateforme

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

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

Avant de commencer

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

Étapes

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

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

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

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

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

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

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

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

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

Supprimer le point de terminaison des services de la plateforme

Vous pouvez supprimer un point de terminaison si vous ne souhaitez plus utiliser le

service de plateforme associé.

Avant de commencer

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

Étapes

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

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

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

   > Si vous supprimez un point de terminaison de services de plateforme en cours d'utilisation, le service de plateforme associé sera désactivé pour tous les buckets qui utilisent le point de terminaison. Toutes les demandes qui n'ont pas encore été traitées seront abandonnées. Toutes les nouvelles demandes continueront d'être générées jusqu'à ce que vous modifiiez la configuration de votre bucket pour ne plus référencer l'URN supprimée. StorageGRID signalera ces demandes comme des erreurs irrécupérables.

3. Sélectionnez **Actions** > **Supprimer le point de terminaison**.

   Un message de confirmation apparaît.

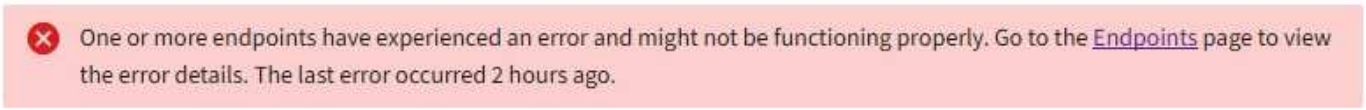
4. Sélectionnez **Supprimer le point de terminaison**.

Résoudre les erreurs de point de terminaison des services de plateforme

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

Déterminer si une erreur s'est produite

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



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

Étapes

1. Dans la liste des points de terminaison, sélectionnez le point de terminaison qui présente l'erreur.
2. Sur la page des détails du point de terminaison, sélectionnez **Connexion**. Cet onglet affiche uniquement l'erreur la plus récente pour un point de terminaison et indique depuis combien de temps l'erreur s'est produite. Erreurs qui incluent l'icône X rouge  survenu au cours des 7 derniers jours.

Vérifiez si l'erreur est toujours d'actualité

Certaines erreurs peuvent continuer à s'afficher dans la colonne **Dernière erreur** même après avoir été résolues. Pour voir si une erreur est actuelle ou pour forcer la suppression d'une erreur résolue du tableau :

Étapes

1. Sélectionnez le point de terminaison.

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

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

La sélection de **Tester la connexion** amène StorageGRID à valider que le point de terminaison des services de la plateforme existe et qu'il est accessible avec les informations d'identification actuelles. La connexion au point de terminaison est validée à partir d'un nœud sur chaque site.

Résoudre les erreurs de point de terminaison

Vous pouvez utiliser le message **Dernière erreur** sur la page des détails du point de terminaison pour vous aider à déterminer la cause de l'erreur. Certaines erreurs peuvent nécessiter de modifier le point de terminaison pour résoudre le problème. Par exemple, une erreur CloudMirroring peut se produire si StorageGRID ne peut pas accéder au bucket S3 de destination car il ne dispose pas des autorisations d'accès appropriées ou si la clé d'accès a expiré. Le message est « Les informations d'identification du point de terminaison ou l'accès à la destination doivent être mis à jour » et les détails sont « AccessDenied » ou « InvalidAccessKeyId ».

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

Étapes

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

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

Lorsque StorageGRID valide un point de terminaison de services de plateforme, il confirme que les informations d'identification du point de terminaison peuvent être utilisées pour contacter la ressource de destination et effectue une vérification des autorisations de base. Cependant, StorageGRID ne valide pas toutes les autorisations requises pour certaines opérations de services de plateforme. Pour cette raison, si vous recevez une erreur lorsque vous tentez d'utiliser un service de plateforme (par exemple « 403 Forbidden »), vérifiez les autorisations associées aux informations d'identification du point de terminaison.

Informations connexes

- **Administrer StorageGRID › Résoudre les problèmes des services de la plateforme**
- "Créer un point de terminaison des services de plateforme"
- "Tester la connexion pour le point de terminaison des services de la plateforme"
- "Modifier le point de terminaison des services de la plateforme"

Configurer la réplication CloudMirror

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

Avant de commencer

- Les services de plateforme ont été activés pour votre compte locataire par un administrateur StorageGRID .
- Vous avez déjà créé un bucket pour servir de source de réplication.
- Le point de terminaison que vous souhaitez utiliser comme destination pour la réplication CloudMirror existe déjà et vous disposez de son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le"Gérer tous les buckets ou l'autorisation d'accès root" . Ces autorisations remplacent les paramètres d'autorisation dans les stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du gestionnaire de locataires.

À propos de cette tâche

La réplication CloudMirror copie les objets d'un bucket source vers un bucket de destination spécifié dans un point de terminaison.

Pour obtenir des informations générales sur la réplication de bucket et comment la configurer, consultez "Documentation Amazon Simple Storage Service (S3) : Réplication d'objets" . Pour plus d'informations sur la manière dont StorageGRID implémente GetBucketReplication, DeleteBucketReplication et PutBucketReplication, consultez le"Opérations sur les godets" .

> La réplication CloudMirror présente des similitudes et des différences importantes avec la fonctionnalité de réplication inter-grille. Pour en savoir plus, voir"Comparer la réplication inter-grille et la réplication CloudMirror" .

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

- Lorsque vous créez et appliquez un XML de configuration de réplication de compartiment valide, il doit utiliser l'URN d'un point de terminaison de compartiment S3 pour chaque destination.
- La réplication n'est pas prise en charge pour les buckets source ou de destination avec le verrouillage d'objet S3 activé.
- Si vous activez la réplication CloudMirror sur un bucket contenant des objets, les nouveaux objets ajoutés au bucket sont répliqués, mais les objets existants dans le bucket ne sont pas répliqués. Vous devez mettre à jour les objets existants pour déclencher la réplication.
- Si vous spécifiez une classe de stockage dans le XML de configuration de réplication, StorageGRID utilise cette classe lors de l'exécution d'opérations sur le point de terminaison S3 de destination. Le point de terminaison de destination doit également prendre en charge la classe de stockage spécifiée. Assurez-vous de suivre toutes les recommandations fournies par le fournisseur du système de destination.

Étapes

1. Activer la réplication pour votre bucket source :
   - Utilisez un éditeur de texte pour créer le XML de configuration de réplication requis pour activer la réplication, comme spécifié dans l'API de réplication S3.
   - Lors de la configuration du XML :
     - Notez que StorageGRID ne prend en charge que la version V1 de la configuration de réplication. Cela signifie que StorageGRID ne prend pas en charge l'utilisation du `Filter` élément pour les règles et suit les conventions V1 pour la suppression des versions d'objet. Consultez la documentation Amazon sur la configuration de la réplication pour plus de détails.
     - Utilisez l'URN d'un point de terminaison de compartiment S3 comme destination.
     - Ajoutez éventuellement le `<StorageClass>` élément et spécifiez l'un des éléments suivants :
       - `STANDARD`: La classe de stockage par défaut. Si vous ne spécifiez pas de classe de stockage lorsque vous téléchargez un objet, le `STANDARD` la classe de stockage est utilisée.
       - `STANDARD_IA`: (Standard - accès peu fréquent.) Utilisez cette classe de stockage pour les données auxquelles on accède moins fréquemment, mais qui nécessitent néanmoins un accès rapide en cas de besoin.
       - `REDUCED_REDUNDANCY`:Utilisez cette classe de stockage pour les données non critiques et reproductibles qui peuvent être stockées avec moins de redondance que les `STANDARD` classe de stockage.
     - Si vous spécifiez un `Role` dans la configuration XML, il sera ignoré. Cette valeur n'est pas utilisée par StorageGRID.

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

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

   La page des détails du bucket apparaît.

4. Sélectionnez **Services de plateforme** > **Réplication**.
5. Cochez la case **Activer la réplication**.
6. Collez le XML de configuration de réplication dans la zone de texte et sélectionnez **Enregistrer les modifications**.

> Les services de plateforme doivent être activés pour chaque compte de locataire par un administrateur StorageGRID à l'aide de Grid Manager ou de l'API Grid Management. Contactez votre administrateur StorageGRID si une erreur se produit lorsque vous enregistrez le XML de configuration.

7. Vérifiez que la réplication est correctement configurée :
   a. Ajoutez un objet au bucket source qui répond aux exigences de réplication telles que spécifiées dans la configuration de réplication.

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

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

      Pour les petits objets, la réplication se produit rapidement.

Informations connexes

"Créer un point de terminaison des services de plateforme"

Configurer les notifications d'événements

Vous activez les notifications pour un bucket en créant un XML de configuration de notification et en utilisant le gestionnaire de locataires pour appliquer le XML à un bucket.

Avant de commencer

- Les services de plateforme ont été activés pour votre compte locataire par un administrateur StorageGRID .
- Vous avez déjà créé un bucket pour servir de source de notifications.
- Le point de terminaison que vous souhaitez utiliser comme destination pour les notifications d'événements existe déjà et vous disposez de son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le"Gérer tous les buckets ou l'autorisation d'accès root" . Ces autorisations remplacent les paramètres d'autorisation dans les stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du gestionnaire de locataires.

À propos de cette tâche

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

Pour obtenir des informations générales sur les notifications d'événements et comment les configurer, reportez-vous à la "Documentation Amazon" . Pour plus d'informations sur la manière dont StorageGRID implémente l'API de configuration des notifications de compartiment S3, reportez-vous à la"instructions pour la mise en œuvre des applications clientes S3" .

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

- Lorsque vous créez et appliquez un XML de configuration de notification valide, il doit utiliser l'URN d'un point de terminaison de notifications d'événements pour chaque destination.
- Bien que la notification d'événement puisse être configurée sur un bucket avec le verrouillage d'objet S3

activé, les métadonnées du verrouillage d'objet S3 (y compris la date de conservation et le statut de conservation légale) des objets ne seront pas incluses dans les messages de notification.

- Une fois que vous avez configuré les notifications d'événements, chaque fois qu'un événement spécifié se produit pour un objet dans le compartiment source, une notification est générée et envoyée à la rubrique Amazon SNS ou Kafka utilisée comme point de terminaison de destination.
- Si vous activez les notifications d'événements pour un compartiment contenant des objets, les notifications sont envoyées uniquement pour les actions effectuées après l'enregistrement de la configuration de notification.

Étapes

1. Activer les notifications pour votre bucket source :
   - Utilisez un éditeur de texte pour créer le XML de configuration de notification requis pour activer les notifications d'événements, comme spécifié dans l'API de notification S3.
   - Lors de la configuration du XML, utilisez l'URN d'un point de terminaison de notifications d'événements comme rubrique de destination.

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. Dans le gestionnaire de locataires, sélectionnez **STOCKAGE (S3)** > **Buckets**.
3. Sélectionnez le nom du bucket source.

   La page des détails du bucket apparaît.

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

> Les services de plateforme doivent être activés pour chaque compte de locataire par un administrateur StorageGRID à l'aide de Grid Manager ou de l'API Grid Management. Contactez votre administrateur StorageGRID si une erreur se produit lorsque vous enregistrez le XML de configuration.

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

   a. Exécutez une action sur un objet dans le bucket source qui répond aux exigences de déclenchement d’une notification telle que configurée dans le XML de configuration.

      Dans l’exemple, une notification d’événement est envoyée chaque fois qu’un objet est créé avec le `images/` préfixe.

   b. Confirmez qu’une notification a été envoyée à la rubrique Amazon SNS ou Kafka de destination.

      Par exemple, si votre rubrique de destination est hébergée sur Amazon SNS, vous pouvez configurer le service pour qu’il vous envoie un e-mail lorsque la notification est envoyée.

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


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

Informations connexes

"Comprendre les notifications pour les buckets"

"Utiliser l'API REST S3"

"Créer un point de terminaison des services de plateforme"

Configurer le service d'intégration de recherche

Vous activez l'intégration de recherche pour un bucket en créant un XML d'intégration de recherche et en utilisant le gestionnaire de locataires pour appliquer le XML au bucket.

Avant de commencer

- Les services de plateforme ont été activés pour votre compte locataire par un administrateur StorageGRID .
- Vous avez déjà créé un bucket S3 dont vous souhaitez indexer le contenu.
- Le point de terminaison que vous souhaitez utiliser comme destination pour le service d'intégration de recherche existe déjà et vous disposez de son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le"Gérer tous les buckets ou l'autorisation d'accès root" . Ces autorisations remplacent les paramètres d'autorisation dans les stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du gestionnaire de locataires.

À propos de cette tâche

Une fois que vous avez configuré le service d'intégration de recherche pour un bucket source, la création d'un objet ou la mise à jour des métadonnées ou des balises d'un objet déclenche l'envoi des métadonnées de l'objet au point de terminaison de destination.

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

Étapes

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

      Les objets peuvent être filtrés sur le préfixe du nom de l'objet. Par exemple, vous pouvez envoyer des métadonnées pour des objets avec le préfixe `images` vers une destination et des métadonnées pour les objets avec le préfixe `videos` à un autre. Les configurations dont les préfixes se chevauchent ne sont pas valides et sont rejetées lorsqu'elles sont soumises. Par exemple, une configuration qui inclut une règle pour les objets avec le préfixe `test` et une deuxième règle pour les objets avec le préfixe `test2` n'est pas autorisé.

      Au besoin, reportez-vous à laexemples pour la configuration des métadonnées XML .

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>/Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

Éléments dans le XML de configuration des notifications de métadonnées :

Nom	Description	Obligatoire
Configuration des notifications de métadonnées	Balise de conteneur pour les règles utilisées pour spécifier les objets et la destination des notifications de métadonnées. Contient un ou plusieurs éléments de règle.	Oui
Règle	Balise de conteneur pour une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié. Les règles avec des préfixes qui se chevauchent sont rejetées. Inclus dans l'élément MetadataNotificationConfiguration.	Oui
ID	Identifiant unique de la règle. Inclus dans l'élément Règle.	Non
Statut	Le statut peut être « Activé » ou « Désactivé ». Aucune action n'est entreprise 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 de l'objet sont envoyées. Doit être l'URN d'un point de terminaison 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 points de terminaison sont configurés à l'aide de l'API Tenant Manager ou Tenant Management. Ils prennent la forme suivante : • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` Le point de terminaison doit être configuré avant que le XML de configuration ne soit soumis, sinon la configuration échouera avec une erreur 404. L'URN est incluse dans l'élément Destination.	Oui

2. Dans le gestionnaire de locataires, sélectionnez **STOCKAGE (S3)** > **Compartiments**.
3. Sélectionnez le nom du bucket source.

   La page des détails du bucket apparaît.

4. Sélectionnez **Services de plateforme** > **Intégration de recherche**
5. Cochez la case **Activer l'intégration de la recherche**.
6. Collez la configuration de notification des métadonnées dans la zone de texte et sélectionnez **Enregistrer les modifications**.

   > ⓘ Les services de plateforme doivent être activés pour chaque compte de locataire par un administrateur StorageGRID à l'aide de Grid Manager ou de l'API de gestion. Contactez votre administrateur StorageGRID si une erreur se produit lorsque vous enregistrez le XML de configuration.

7. Vérifiez que le service d'intégration de recherche est correctement configuré :
   a. Ajoutez un objet au bucket source qui répond aux exigences de déclenchement d'une notification de métadonnées comme spécifié dans le XML de configuration.

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

   b. Confirmez qu'un document JSON contenant les métadonnées et les balises de l'objet a été ajouté à l'index de recherche spécifié dans le point de terminaison.

Après avoir terminé

Si nécessaire, vous pouvez désactiver l'intégration de la recherche pour un bucket en utilisant l'une des méthodes suivantes :

- Sélectionnez **STOCKAGE (S3)** > **Compartiments** et décochez la case **Activer l'intégration de la recherche**.
- Si vous utilisez directement l'API S3, utilisez une demande de notification de métadonnées DELETE Bucket. Consultez les instructions pour implémenter les applications clientes S3.

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

Dans cet exemple, les métadonnées d'objet pour tous les objets sont envoyées vers la même destination.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Exemple : Configuration de notification de métadonnées avec deux règles

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

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Format de notification des métadonnées

Lorsque vous activez le service d'intégration de recherche pour un bucket, un document JSON est généré et envoyé au point de terminaison de destination chaque fois que des métadonnées ou des balises d'objet sont ajoutées, mises à jour ou supprimées.

Cet exemple montre un exemple de JSON qui pourrait être généré lorsqu'un objet avec la clé `SGWS/Tagging.txt` est créé dans un bucket nommé `test` . Le `test` le bucket n'est pas versionné, donc le `versionId` la balise est vide.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Champs inclus dans le document JSON

Le nom du document inclut le nom du bucket, le nom de l'objet et l'ID de version s'il est présent.

Informations sur le bucket et l'objet

`bucket`: Nom du bucket

`key`: Nom de la clé de l'objet

`versionID`: Version de l'objet, pour les objets dans les buckets versionnés

`region`: Région de bucket, par exemple `us-east-1`

Métadonnées du système

`size`: Taille de l'objet (en octets) telle que visible par un client HTTP

`md5`: Hachage d'objet

Métadonnées de l'utilisateur

`metadata`:Toutes les métadonnées utilisateur pour l'objet, sous forme de paires clé-valeur

`key:value`

Mots-clés

`tags`:Toutes les balises d'objet définies pour l'objet, sous forme de paires clé-valeur

`key:value`

Comment afficher les résultats dans Elasticsearch

Pour les balises et les métadonnées utilisateur, StorageGRID transmet des dates et des nombres à Elasticsearch sous forme de chaînes ou de notifications d'événements S3. Pour configurer Elasticsearch afin

d’interpréter ces chaînes comme des dates ou des nombres, suivez les instructions Elasticsearch pour le mappage de champs dynamiques et pour le mappage des formats de date. Activez les mappages de champs dynamiques sur l’index avant de configurer le service d’intégration de recherche. Une fois qu’un document est indexé, vous ne pouvez pas modifier les types de champs du document dans l’index.