Utilisez un compte de locataire

StorageGRID

NetApp
October 03, 2025

Sommaire

Utilisez un compte de locataire

Utilisez un compte de locataire : présentation

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

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

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

Il est possible d'utiliser des comptes de tenant pour isoler les objets stockés par différentes entités. Par exemple, vous pouvez utiliser plusieurs comptes locataires pour l'une de ces utilisations :

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

> Si vous utilisez le protocole client S3, vous pouvez également utiliser des compartiments S3 et des règles de compartiment pour isoler les objets entre les différents départements d'une entreprise. Il n'est pas nécessaire de créer des comptes de tenant distincts. Voir la Instructions d'implémentation des applications client S3.

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

Comment créer un compte de locataire

Les comptes de locataire sont créés par un Administrateur du grid StorageGRID utilisant le gestionnaire de grille. Lors de la création d'un compte de locataire, l'administrateur du grid spécifie les informations suivantes :

- Nom d'affichage du locataire (l'ID de compte du locataire est attribué automatiquement et ne peut pas être modifié).
- Si le compte de locataire utilise S3 ou Swift.
- Pour les comptes de locataire S3 : si le compte de locataire est autorisé à utiliser des services de plateforme. Si l'utilisation des services de plateforme est autorisée, la grille doit être configurée pour prendre en charge leur utilisation.
- Éventuellement, un quota de stockage pour le compte du locataire, soit le nombre maximal de gigaoctets, téraoctets ou pétaoctets disponibles pour les objets du locataire. Le quota de stockage d'un locataire représente une quantité logique (taille d'objet), et non une quantité physique (taille sur disque).
- Si la fédération des identités est activée pour le système StorageGRID, quel groupe fédéré a l'autorisation d'accès racine pour configurer le compte de tenant.
- Si l'authentification unique (SSO) n'est pas utilisée pour le système StorageGRID, que le compte de tenant utilise son propre référentiel d'identité ou partage le référentiel d'identité de la grille et le mot de passe initial de l'utilisateur racine local du locataire.

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

Configurez les locataires S3

Après un Le compte de locataire S3 est créé, Vous pouvez accéder au Gestionnaire de tenant pour effectuer des tâches telles que :

- Configuration de la fédération des identités (sauf si le référentiel d'identité est partagé avec la grille) ou création de groupes et d'utilisateurs locaux
- Gestion des clés d'accès S3
- Création et gestion des compartiments S3, notamment des compartiments conformes
- Utilisation des services de plate-forme (si activé)
- Contrôle de l'utilisation du stockage

> Vous devez avoir la possibilité de créer et de gérer des compartiments S3 avec le Gestionnaire des locataires Les clés d'accès S3 et utilisent l'API REST S3 pour ingérer et gérer les objets.

Configurez les locataires Swift

Après un Le compte de locataire Swift est créé, Vous pouvez accéder au Gestionnaire de tenant pour effectuer des tâches telles que :

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

> Les utilisateurs Swift doivent disposer de l'autorisation d'accès racine pour accéder au gestionnaire de locataires. Toutefois, l'autorisation accès racine ne permet pas aux utilisateurs de s'authentifier dans le système API REST Swift pour créer des conteneurs et ingérer des objets. Les utilisateurs doivent disposer de l'autorisation Administrateur Swift pour s'authentifier dans l'API REST de Swift.

Utilisez le Gestionnaire de locataires

Le gestionnaire de locataires permet de gérer tous les aspects d'un compte de locataire StorageGRID.

Vous pouvez utiliser le gestionnaire des locataires pour surveiller l'utilisation du stockage d'un compte de locataire et gérer les utilisateurs avec une fédération des identités ou en créant des groupes et des utilisateurs locaux. Pour les comptes locataires S3, vous pouvez également gérer des clés S3, gérer des compartiments S3 et configurer les services de plateforme.

Comment se connecter et se déconnecter

Connectez-vous au Gestionnaire de locataires

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

Ce dont vous avez besoin

- Vous devez disposer de vos identifiants de connexion.
- Vous devez disposer d'une URL pour accéder au Gestionnaire de locataires, telle que fournie par votre administrateur de grid. L'URL se présente comme l'un de ces exemples :

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

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

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

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

  L'URL contient toujours le nom de domaine complet (FQDN) ou l'adresse IP utilisée pour accéder à un nœud d'administration, et peut également inclure un numéro de port, l'ID de compte de locataire à 20 chiffres, ou les deux.

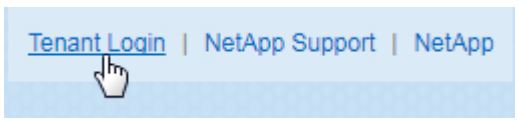
- Si l'URL n'inclut pas l'ID de compte à 20 chiffres du locataire, vous devez avoir cet ID de compte.
- Vous devez utiliser un navigateur web pris en charge.
- Les cookies doivent être activés dans votre navigateur Web.
- Vous devez disposer d'autorisations d'accès spécifiques.

Étapes

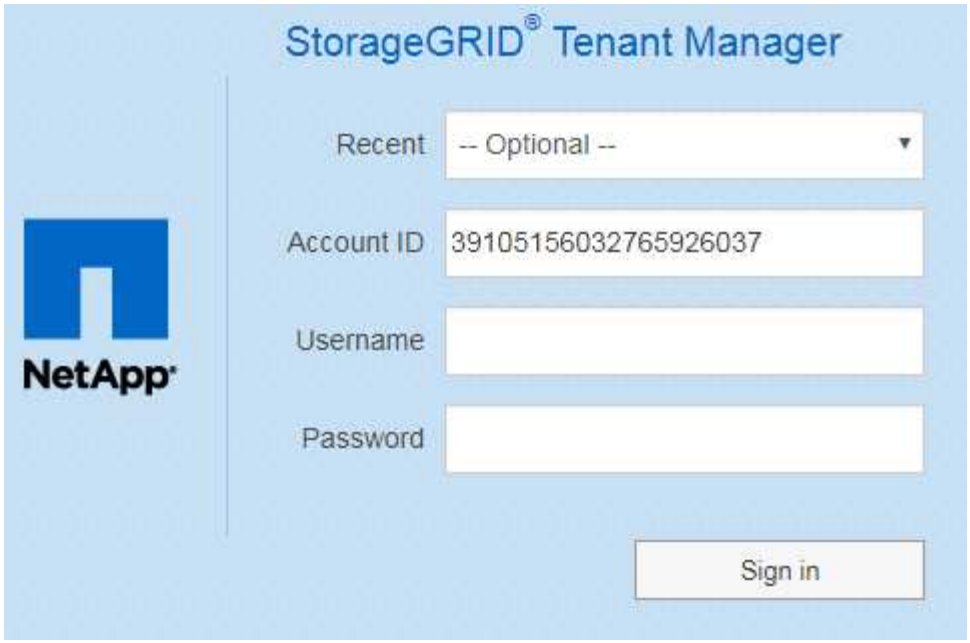
1. Lancez un navigateur web pris en charge.
2. Dans la barre d'adresse du navigateur, entrez l'URL d'accès au Gestionnaire de locataires.
3. Si vous êtes invité à recevoir une alerte de sécurité, installez le certificat à l'aide de l'assistant d'installation du navigateur.
4. Connectez-vous au Gestionnaire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

   L'écran de connexion que vous voyez dépend de l'URL que vous avez saisie et de l'utilisation de SSO (Single Sign-on) par votre organisation. Vous verrez l'un des écrans suivants :

   - Page de connexion de Grid Manager. Cliquez sur le lien **tenant Login** dans le coin supérieur droit.

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



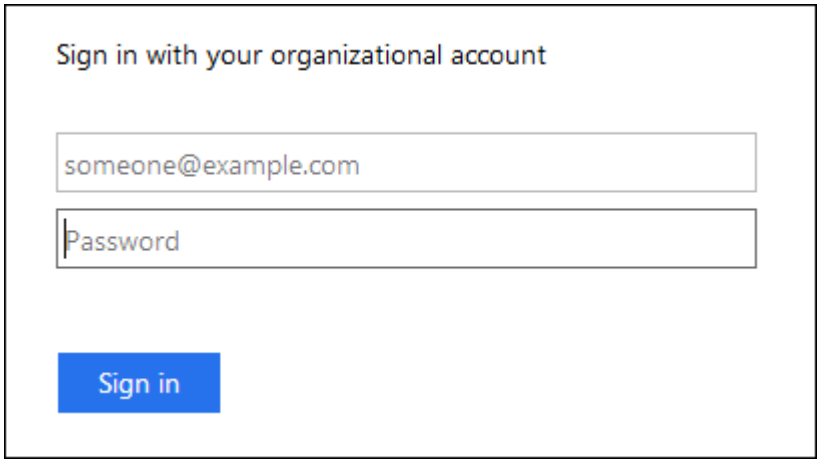
i. Si l'ID de compte à 20 chiffres du locataire ne s'affiche pas, sélectionnez le nom du compte du locataire s'il apparaît dans la liste des comptes récents ou saisissez l'ID du compte.

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

iii. Cliquez sur **connexion**.

Le tableau de bord de tenant Manager s'affiche.

◦ La page SSO de votre entreprise, si SSO est activé sur le grid. Par exemple :



Entrez vos informations d'identification SSO standard, puis cliquez sur **connexion**.

◦ Page de connexion SSO du Gestionnaire de locataires.

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

ii. Cliquez sur **connexion**.

iii. Connectez-vous à l'aide de vos identifiants SSO standard sur la page de connexion SSO de votre entreprise.

Le tableau de bord de tenant Manager s'affiche.

5. Si vous avez reçu un mot de passe initial de quelqu'un d'autre, modifiez votre mot de passe pour sécuriser votre compte. Sélectionnez ***username*** **Modifier le mot de passe**.

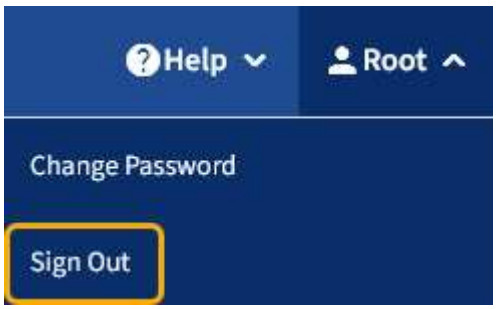
> Si l'authentification SSO est activée pour le système StorageGRID, vous ne pouvez pas modifier votre mot de passe à partir du Gestionnaire de locataires.

Déconnectez-vous du Gestionnaire de locataires

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

Étapes

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



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

- Si SSO n'est pas utilisé :

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

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

- Si SSO est activé :

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

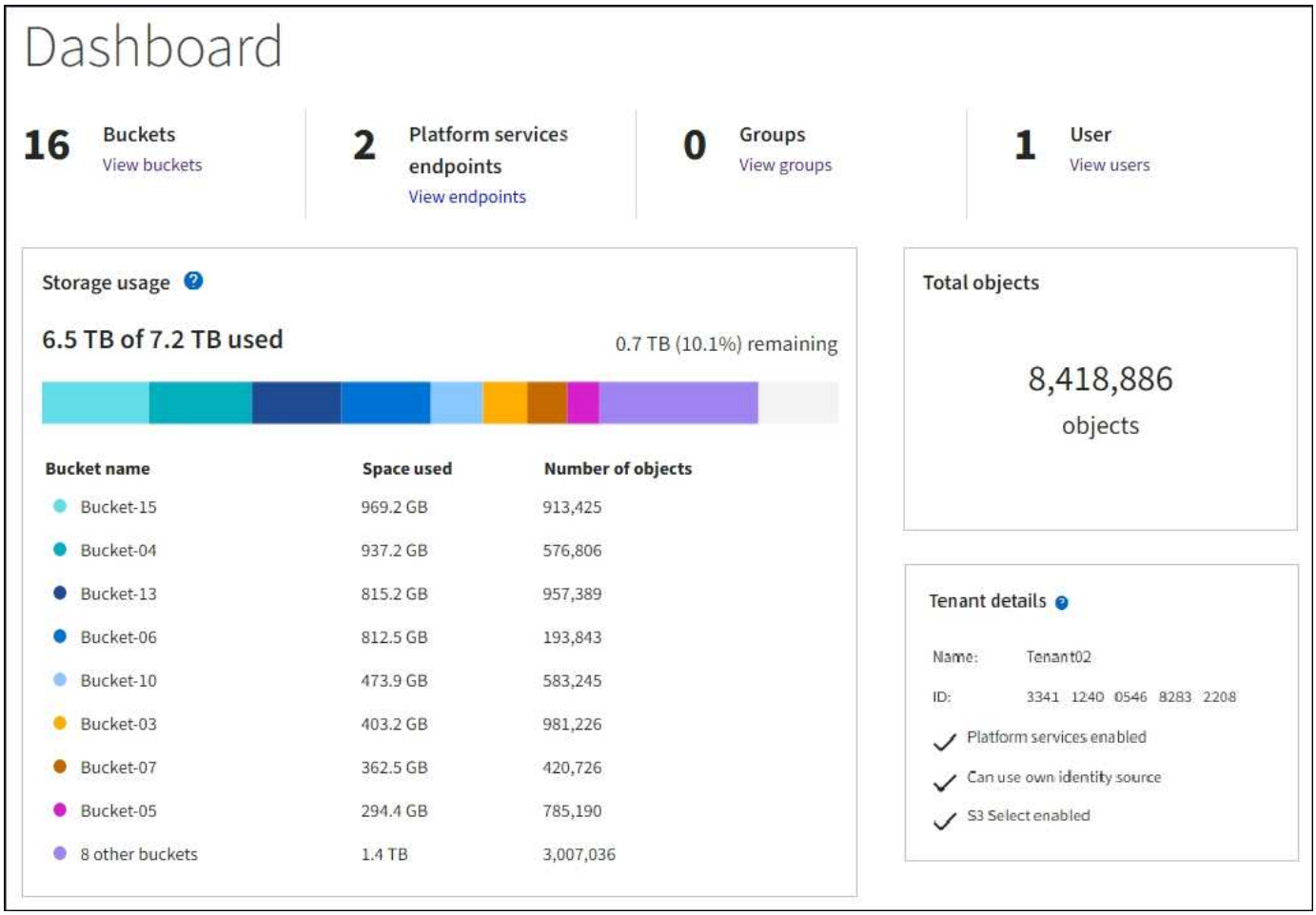
> Si SSO est activé et que vous êtes également connecté à Grid Manager, vous devez également vous déconnecter de Grid Manager pour vous déconnecter de SSO.

Compréhension du tableau de bord de tenant Manager

Le tableau de bord de tenant Manager présente la configuration des comptes d'un locataire ainsi que la quantité d'espace utilisé par les objets dans les compartiments (S3) ou les conteneurs (Swift) du locataire. Si le locataire dispose d'un quota, le tableau de bord affiche la part du quota utilisée et la quantité restante. En cas d'erreurs liées au compte du locataire, les erreurs sont affichées sur le tableau de bord.

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

Lorsque des objets ont été téléchargés, le Tableau de bord ressemble à l'exemple suivant :



Récapitulatif du compte de locataire

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

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

Vous pouvez sélectionner les liens pour afficher les détails.

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

- Nombre total d'objets pour le locataire.

  Pour un compte S3, si aucun objet n'a été ingéré et que vous disposez de l'autorisation d'accès racine, les instructions relatives à la mise en route s'affichent au lieu du nombre total d'objets.

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

Utilisation du stockage et des quotas

Le panneau utilisation du stockage contient les informations suivantes :

- Volume des données d'objet pour le locataire.

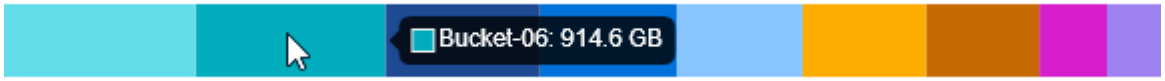
Cette valeur indique la quantité totale de données d'objet chargées et ne représente pas l'espace utilisé pour stocker les copies de ces objets et leurs métadonnées.

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

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

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

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



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

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

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

Alertes d'utilisation des quotas

Si les alertes d'utilisation des quotas ont été activées dans Grid Manager, elles s'affichent dans le Gestionnaire de locataires lorsque le quota est faible ou dépassé, comme suit :

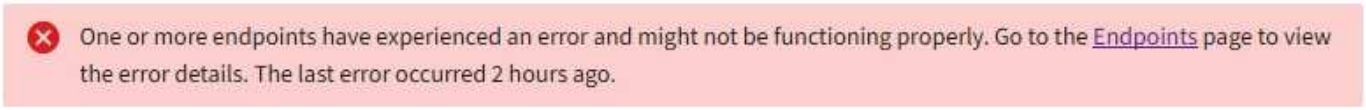
Si 90 % ou plus du quota d'un locataire a été utilisé, l'alerte **usage du quota de locataire élevé** est déclenchée. Pour plus d'informations, consultez la référence des alertes dans les instructions de surveillance et de dépannage de StorageGRID.

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

Pour afficher des informations supplémentaires et gérer les règles et notifications relatives aux alertes, reportez-vous aux instructions de surveillance et de dépannage de StorageGRID.

Erreurs de point final

Si vous avez utilisé Grid Manager pour configurer un ou plusieurs terminaux pour les services de plateforme, le tableau de bord du Gestionnaire de locataires affiche une alerte si des erreurs de point final se sont produites au cours des sept derniers jours.



Pour afficher des détails sur une erreur de point final, sélectionnez noeuds finaux pour afficher la page noeuds finaux.

Informations associées

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

Surveiller et résoudre les problèmes

API de gestion des locataires

Compréhension de l'API de gestion des locataires

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

L'API de gestion des locataires :

- Utilise la plate-forme API open source swagger. Swagger fournit une interface utilisateur intuitive qui

permet aux développeurs et aux non-développeurs d'interagir avec l'API. L'interface utilisateur swagger fournit des détails complets et de la documentation pour chaque opération API.

- Utilisations gestion des versions pour prendre en charge les mises à niveau sans interruption.

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

Étapes

1. Connectez-vous au Gestionnaire de locataires.
2. Dans la partie supérieure du Gestionnaire de tenant, sélectionnez l'icône d'aide et sélectionnez **Documentation API**.

Opérations d'API

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

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

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

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

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

- **Config** — opérations liées à la version du produit et aux versions de l'API tenant Management. Vous pouvez lister la version du produit ainsi que les versions principales de l'API prises en charge par cette version.
- **Conteneurs** — opérations sur des compartiments S3 ou des conteneurs Swift, comme suit :

  S3

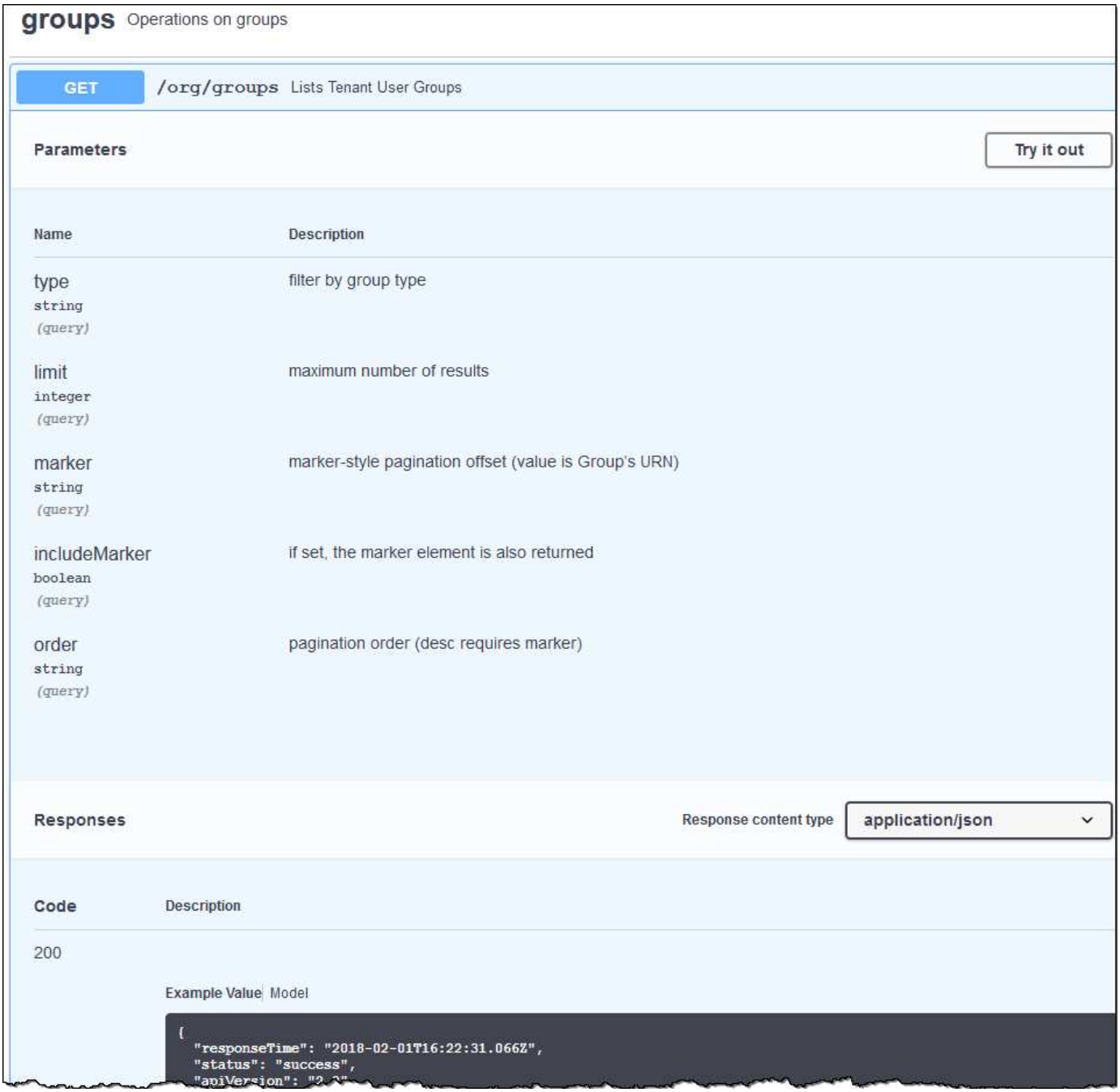
  - Création d'un compartiment (avec et sans l'activation du verrouillage objet S3)
  - Modifier la conservation par défaut du compartiment (pour les compartiments avec le verrouillage objet S3 activé)
  - Définissez le contrôle de cohérence pour les opérations effectuées sur les objets
  - Créer, mettre à jour et supprimer la configuration CORS d'un compartiment
  - Activez et désactivez les mises à jour de l'heure du dernier accès pour les objets
  - Gestion des paramètres de configuration des services de plateforme, notamment la réplication CloudMirror, les notifications et l'intégration de la recherche (notification-métadonnées)
  - Supprimer les compartiments vides

  Swift : définissez le niveau de cohérence utilisé pour les conteneurs

- **DESACTIVE-fonctions** — opérations pour afficher les fonctions qui pourraient avoir été désactivées.
- **Noeuds finaux** — opérations pour gérer un noeud final. Les terminaux permettent à un compartiment S3 d'utiliser un service externe pour la réplication StorageGRID CloudMirror, les notifications ou l'intégration de la recherche.
- **Groupes** — opérations pour gérer des groupes de locataires locaux et extraire des groupes de locataires fédérés à partir d'un référentiel d'identité externe.
- **Identity-source** — opérations pour configurer un référentiel d'identité externe et synchroniser manuellement les informations de groupe et d'utilisateur fédérés.
- **Régions** — opérations pour déterminer les régions qui ont été configurées pour le système StorageGRID.
- **s3** — opérations pour gérer les clés d'accès S3 pour les utilisateurs locataires.
- **s3-Object-lock** — opérations sur les paramètres globaux de verrouillage d'objet S3, utilisées pour prendre en charge la conformité réglementaire.
- **Utilisateurs** — opérations pour afficher et gérer les utilisateurs locataires.

Détails de l'opération

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



Émettre des requêtes API

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

Étapes

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

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

Gestion des versions de l'API de gestion des locataires

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

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

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

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

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

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

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

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

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

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

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

Spécifiez la version de l'API pour la demande

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

```
curl https://[IP-Address]/api/v3/grid/accounts

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

Protection contre la contrefaçon de demandes intersites (CSRF)

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

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

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

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

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

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

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

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

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

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

Gérez l'accès au système

Utiliser la fédération des identités

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

Configurez la fédération des identités pour le gestionnaire des locataires

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

Ce dont vous avez besoin

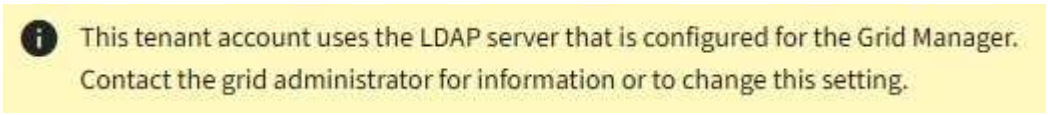
- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous disposez d'autorisations d'accès spécifiques.
- Vous utilisez Active Directory, Azure AD, OpenLDAP ou Oracle Directory Server comme fournisseur d'identité.

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

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

Description de la tâche

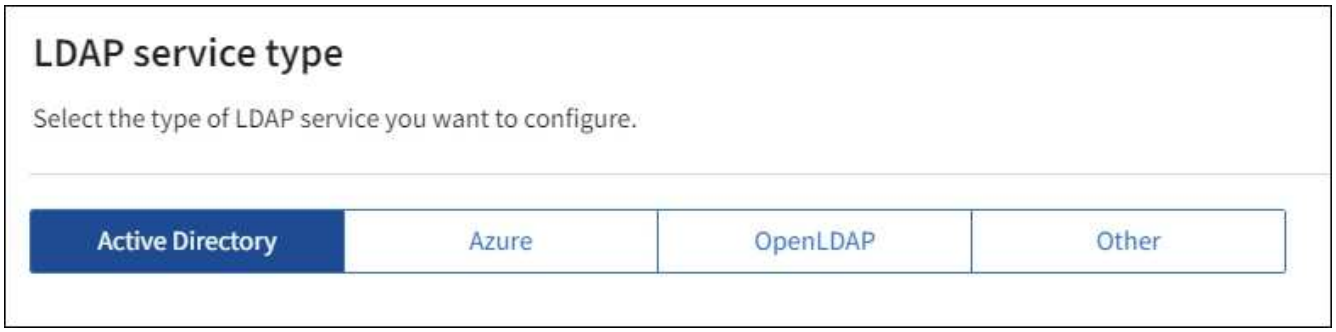
La configuration d'un service de fédération des identités pour votre locataire dépend de la configuration de votre compte locataire. Votre locataire peut partager le service de fédération des identités configuré pour Grid Manager. Si ce message s'affiche lorsque vous accédez à la page Fédération des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



Entrez la configuration

Étapes

1. Sélectionnez **ACCESS MANAGEMENT identity federation**.
2. Sélectionnez **Activer la fédération d'identités**.
3. Dans la section Type de service LDAP, sélectionnez le type de service LDAP que vous souhaitez configurer.



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

4. Si vous avez sélectionné **autre**, renseignez les champs de la section attributs LDAP. Dans le cas contraire, passez à l'étape suivante.
   - **Nom unique utilisateur** : nom de l'attribut qui contient l'identifiant unique d'un utilisateur LDAP. Cet attribut est équivalent à `sAMAccountName` Pour Active Directory et `uid` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `uid`.
   - **UUID d'utilisateur** : nom de l'attribut qui contient l'identifiant unique permanent d'un utilisateur LDAP. Cet attribut est équivalent à `objectGUID` Pour Active Directory et `entryUUID` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `nsuniqueid`. La valeur de chaque utilisateur pour l'attribut spécifié doit être un nombre hexadécimal à 32 chiffres au format 16 octets ou chaîne, où les tirets sont ignorés.
   - **Nom unique de groupe** : nom de l'attribut qui contient l'identifiant unique d'un groupe LDAP. Cet attribut est équivalent à `sAMAccountName` Pour Active Directory et `cn` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `cn`.
   - **UUID de groupe** : nom de l'attribut qui contient l'identificateur unique permanent d'un groupe LDAP.

Cet attribut est équivalent à `objectGUID` Pour Active Directory et `entryUUID` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `nsuniqueid`. La valeur de chaque groupe pour l'attribut spécifié doit être un nombre hexadécimal à 32 chiffres au format 16 octets ou chaîne, où les tirets sont ignorés.

5. Pour tous les types de services LDAP, entrez les informations de connexion réseau et de serveur LDAP requises dans la section configurer le serveur LDAP.
   - **Nom d'hôte** : le nom de domaine complet (FQDN) ou l'adresse IP du serveur LDAP.
   - **Port** : port utilisé pour se connecter au serveur LDAP.

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

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

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

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

     - `sAMAccountName` ou `uid`
     - `objectGUID`, `entryUUID`, ou `nsuniqueid`
     - `cn`
     - `memberOf` ou `isMemberOf`
     - **Active Directory** : `objectSid`, `primaryGroupID`, `userAccountControl`, et `userPrincipalName`
     - **Azure**: `accountEnabled` et `userPrincipalName`
   - **Mot de passe** : mot de passe associé au nom d'utilisateur.
   - **DN de base de groupe** : chemin complet du nom distinctif (DN) pour une sous-arborescence LDAP que vous voulez rechercher des groupes. Dans l'exemple Active Directory (ci-dessous), tous les groupes dont le nom unique est relatif au DN de base (DC=storagegrid,DC=exemple,DC=com) peuvent être utilisés comme groupes fédérés.

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

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

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

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

     Il est recommandé de fournir le format **Bind username** car il peut permettre aux utilisateurs de se

connecter si StorageGRID ne parvient pas à se lier avec le compte de service.

Entrez l'un des motifs suivants :

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

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

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

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

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

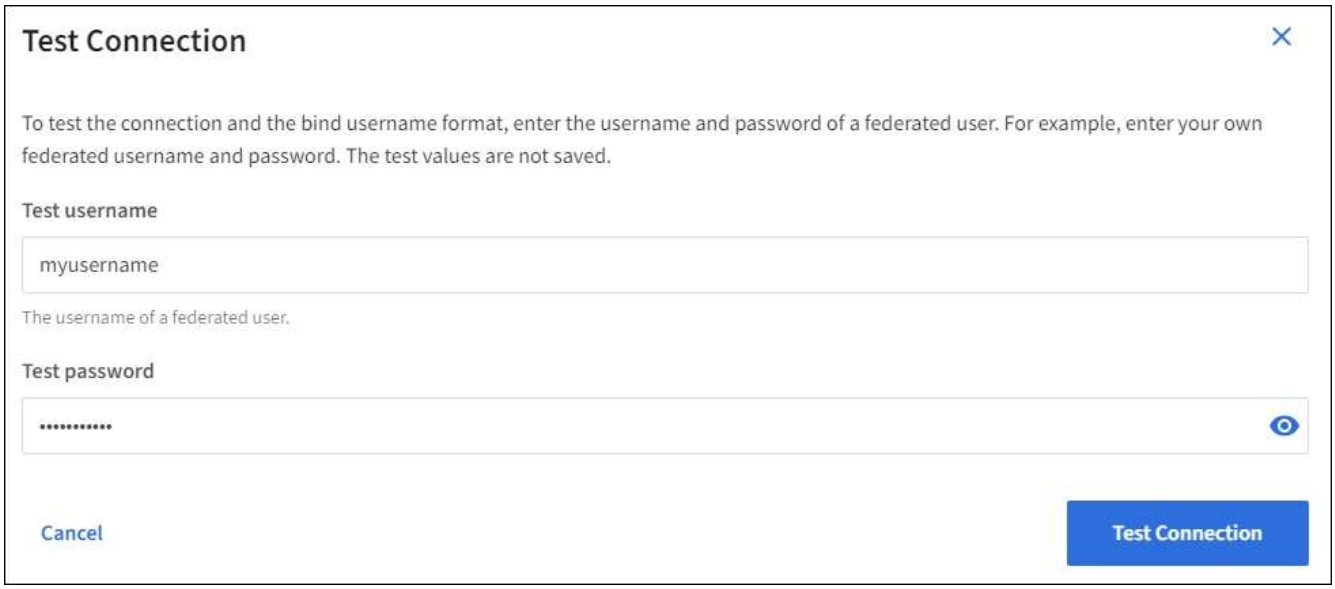
     Si vous sélectionnez ce paramètre, copiez et collez le certificat de sécurité personnalisé dans la zone de texte certificat de l'autorité de certification.

Testez la connexion et enregistrez la configuration

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

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

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



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

Forcer la synchronisation avec le référentiel d'identité

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

Étapes

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

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

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

Désactiver la fédération des identités

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

Description de la tâche

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

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

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

- La synchronisation entre le système StorageGRID et le référentiel d'identité ne se produira pas et des alertes ou des alarmes ne seront pas émises pour les comptes qui n'ont pas été synchronisés.
- La case à cocher **Activer la fédération d'identités** est désactivée si l'authentification unique (SSO) est définie sur **Enabled** ou **Sandbox mode**. Le statut SSO sur la page connexion unique doit être **désactivé** avant de pouvoir désactiver la fédération d'identités. Voir Désactiver l'authentification unique.

Étapes

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

Instructions de configuration du serveur OpenLDAP

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

> Pour les référentiels d'identité qui ne sont pas ActiveDirectory ou Azure, StorageGRID ne bloque pas automatiquement l'accès S3 des utilisateurs désactivés en externe. Pour bloquer l'accès S3, supprimez toute clé S3 pour l'utilisateur et supprimez l'utilisateur de tous les groupes.

Recouvrements de memberOf et de raffint

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

Indexation

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

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

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

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

Gérer les groupes

Créez des groupes pour un locataire S3

Vous pouvez gérer les autorisations des groupes d'utilisateurs S3 en important des

groupes fédérés ou en créant des groupes locaux.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs qui dispose de l'autorisation accès racine. Voir Autorisations de gestion des locataires.
- Si vous envisagez d'importer un groupe fédéré, vous avez configuré la fédération des identités et le groupe fédéré existe déjà dans le référentiel d'identité configuré.

Pour plus d'informations sur S3, reportez-vous à la section Utilisation de S3.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT Groups**.

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

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

4. Entrez le nom du groupe.
   - **Groupe local** : saisissez à la fois un nom d'affichage et un nom unique. Vous pouvez modifier le nom d'affichage ultérieurement.
   - **Groupe fédéré** : saisissez le nom unique. Pour Active Directory, le nom unique est le nom associé à l' `sAMAccountName` attribut. Pour OpenLDAP, le nom unique est le nom associé à `uid` attribut.
5. Sélectionnez **Continuer**.
6. Sélectionnez un mode d'accès. Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini

sur lecture seule, l'utilisateur dispose d'un accès en lecture seule à tous les paramètres et fonctions sélectionnés.

- **Read-write** (valeur par défaut) : les utilisateurs peuvent se connecter au Gestionnaire de locataires et gérer la configuration du locataire.
- **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent pas apporter de modifications ni effectuer d'opérations dans le Gestionnaire des locataires ou l'API de gestion des locataires. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.

7. Sélectionnez les autorisations de groupe pour ce groupe.

   Reportez-vous aux informations sur les autorisations de gestion des locataires.

8. Sélectionnez **Continuer**.
9. Sélectionnez une stratégie de groupe pour déterminer quelles autorisations d'accès S3 seront attribuées aux membres de ce groupe.
   - **Pas d'accès S3** : par défaut. Les utilisateurs de ce groupe n'ont pas accès aux ressources S3, sauf si l'accès est accordé avec une règle de compartiment. Si vous sélectionnez cette option, seul l'utilisateur root peut accéder aux ressources S3 par défaut.
   - **Accès en lecture seule** : les utilisateurs de ce groupe ont accès en lecture seule aux ressources S3. Par exemple, les utilisateurs de ce groupe peuvent afficher la liste des objets et lire les données d'objet, les métadonnées et les balises. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe en lecture seule s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
   - **Accès complet** : les utilisateurs de ce groupe ont accès aux ressources S3, y compris aux compartiments. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe à accès complet s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
   - **Custom** : les utilisateurs du groupe disposent des autorisations que vous spécifiez dans la zone de texte. Pour plus d'informations sur les règles de groupe, notamment la syntaxe du langage et des exemples, reportez-vous aux instructions de mise en œuvre d'une application client S3.
10. Si vous avez sélectionné **personnalisé**, entrez la stratégie de groupe. Chaque stratégie de groupe a une taille limite de 5,120 octets. Vous devez entrer une chaîne au format JSON valide.

    Dans cet exemple, les membres du groupe sont uniquement autorisés à répertorier et accéder à un dossier correspondant à leur nom d'utilisateur (préfixe de clé) dans le champ spécifié. Notez que les autorisations d'accès à partir d'autres stratégies de groupes et de la règle de compartiment doivent être prises en compte lors de la détermination de la confidentialité de ces dossiers.

11. Sélectionnez le bouton qui s'affiche, selon que vous créez un groupe fédéré ou local :
    - Groupe fédéré : **Créer groupe**
    - Groupe local : **Continuer**

    Si vous créez un groupe local, STEP 4 (Ajouter des utilisateurs) apparaît après avoir sélectionné **Continuer**. Cette étape n'apparaît pas pour les groupes fédérés.

12. Cochez la case de chaque utilisateur que vous souhaitez ajouter au groupe, puis sélectionnez **Créer groupe**.

    Vous pouvez également enregistrer le groupe sans ajouter d'utilisateurs. Vous pouvez ajouter des utilisateurs au groupe ultérieurement ou sélectionner le groupe lorsque vous ajoutez de nouveaux utilisateurs.

13. Sélectionnez **Terminer**.

    Le groupe que vous avez créé apparaît dans la liste des groupes. L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Créez des groupes pour un locataire Swift

Vous pouvez gérer les autorisations d'accès pour un compte de locataire Swift en important des groupes fédérés ou en créant des groupes locaux. Au moins un groupe doit disposer de l'autorisation Administrateur Swift, qui est requise pour gérer les conteneurs et les objets d'un compte de locataire Swift.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs qui dispose de l'autorisation accès racine.
- Si vous envisagez d'importer un groupe fédéré, vous avez configuré la fédération des identités et le groupe fédéré existe déjà dans le référentiel d'identité configuré.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT Groups**.

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

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

4. Entrez le nom du groupe.
   - **Groupe local** : saisissez à la fois un nom d'affichage et un nom unique. Vous pouvez modifier le nom d'affichage ultérieurement.
   - **Groupe fédéré** : saisissez le nom unique. Pour Active Directory, le nom unique est le nom associé à l'`sAMAccountName` attribut. Pour OpenLDAP, le nom unique est le nom associé à `uid` attribut.
5. Sélectionnez **Continuer**.
6. Sélectionnez un mode d'accès. Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur lecture seule, l'utilisateur dispose d'un accès en lecture seule à tous les paramètres et fonctions sélectionnés.
   - **Read-write** (valeur par défaut) : les utilisateurs peuvent se connecter au Gestionnaire de locataires et gérer la configuration du locataire.
   - **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne

peuvent pas apporter de modifications ni effectuer d'opérations dans le Gestionnaire des locataires ou l'API de gestion des locataires. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.

7. Définissez l'autorisation Groupe.
   - Cochez la case **accès racine** si les utilisateurs doivent se connecter au Gestionnaire de locataires ou à l'API de gestion des locataires. (Valeur par défaut)
   - Désélectionnez la case **accès racine** si les utilisateurs n'ont pas besoin d'accéder au Gestionnaire de locataires ou à l'API de gestion des locataires. Par exemple, désélectionnez la case à cocher pour les applications qui n'ont pas besoin d'accéder au locataire. Attribuez ensuite l'autorisation **Swift Administrator** pour permettre à ces utilisateurs de gérer des conteneurs et des objets.
8. Sélectionnez **Continuer**.
9. Cochez la case **Administrateur Swift** si l'utilisateur doit pouvoir utiliser l'API REST Swift.

   Les utilisateurs Swift doivent disposer de l'autorisation d'accès racine pour accéder au gestionnaire de locataires. Toutefois, l'autorisation accès racine ne permet pas aux utilisateurs de s'authentifier auprès de l'API REST Swift pour créer des conteneurs et ingérer des objets. Les utilisateurs doivent disposer de l'autorisation Administrateur Swift pour s'authentifier dans l'API REST de Swift.

10. Sélectionnez le bouton qui s'affiche, selon que vous créez un groupe fédéré ou local :
    - Groupe fédéré : **Créer groupe**
    - Groupe local : **Continuer**

      Si vous créez un groupe local, STEP 4 (Ajouter des utilisateurs) apparaît après avoir sélectionné **Continuer**. Cette étape n'apparaît pas pour les groupes fédérés.

11. Cochez la case de chaque utilisateur que vous souhaitez ajouter au groupe, puis sélectionnez **Créer groupe**.

    Vous pouvez également enregistrer le groupe sans ajouter d'utilisateurs. Vous pouvez ajouter des utilisateurs au groupe ultérieurement ou sélectionner le groupe lorsque vous créez de nouveaux utilisateurs.

12. Sélectionnez **Terminer**.

    Le groupe que vous avez créé apparaît dans la liste des groupes. L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Informations associées

Autorisations de gestion des locataires

Utiliser Swift

Autorisations de gestion des locataires

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

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

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

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

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

Vous pouvez attribuer les autorisations suivantes à un groupe. Notez que les locataires S3 et Swift disposent d'autorisations de groupe différentes. L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Autorisations	Description
Accès racine	Donne un accès complet au gestionnaire des locataires et à l'API de gestion des locataires. **Remarque :** les utilisateurs de Swift doivent disposer de l'autorisation d'accès racine pour se connecter au compte du locataire.
Administrateur	Les locataires Swift uniquement. Fournit un accès complet aux conteneurs et objets Swift pour ce compte de locataire **Remarque :** les utilisateurs de Swift doivent disposer de l'autorisation Administrateur Swift pour effectuer toutes les opérations avec l'API REST Swift.
Gérez vos propres identifiants S3	Locataires S3 uniquement. Permet aux utilisateurs de créer et de supprimer leurs propres clés d'accès S3. Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu **STORAGE (S3) My S3 Access Keys**.
Gérer toutes les rubriques	• Locataires S3 : permet aux utilisateurs d'utiliser le gestionnaire de locataires et l'API de gestion des locataires pour créer et supprimer des compartiments S3 et gérer les paramètres de tous les compartiments S3 du compte, indépendamment des règles du compartiment S3 ou du groupe. Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu **seaux**. • Locataires Swift : permet aux utilisateurs Swift de contrôler le niveau de cohérence des conteneurs Swift à l'aide de l'API de gestion des locataires. **Remarque :** vous pouvez uniquement attribuer l'autorisation gérer toutes les rubriques 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.

Autorisations	Description
Gérer les terminaux	Locataires S3 uniquement. Permet aux utilisateurs d'utiliser le Gestionnaire de locataires ou l'API de gestion des locataires pour créer ou modifier des terminaux, qui sont utilisés comme destination pour les services de plateforme StorageGRID. Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu **Platform services Endpoints**.

Informations associées

Utilisation de S3

Utiliser Swift

Afficher et modifier les détails du groupe

Lorsque vous affichez les détails d'un groupe, vous pouvez modifier le nom d'affichage, les autorisations, les règles et les utilisateurs appartenant au groupe.

Ce dont vous avez besoin

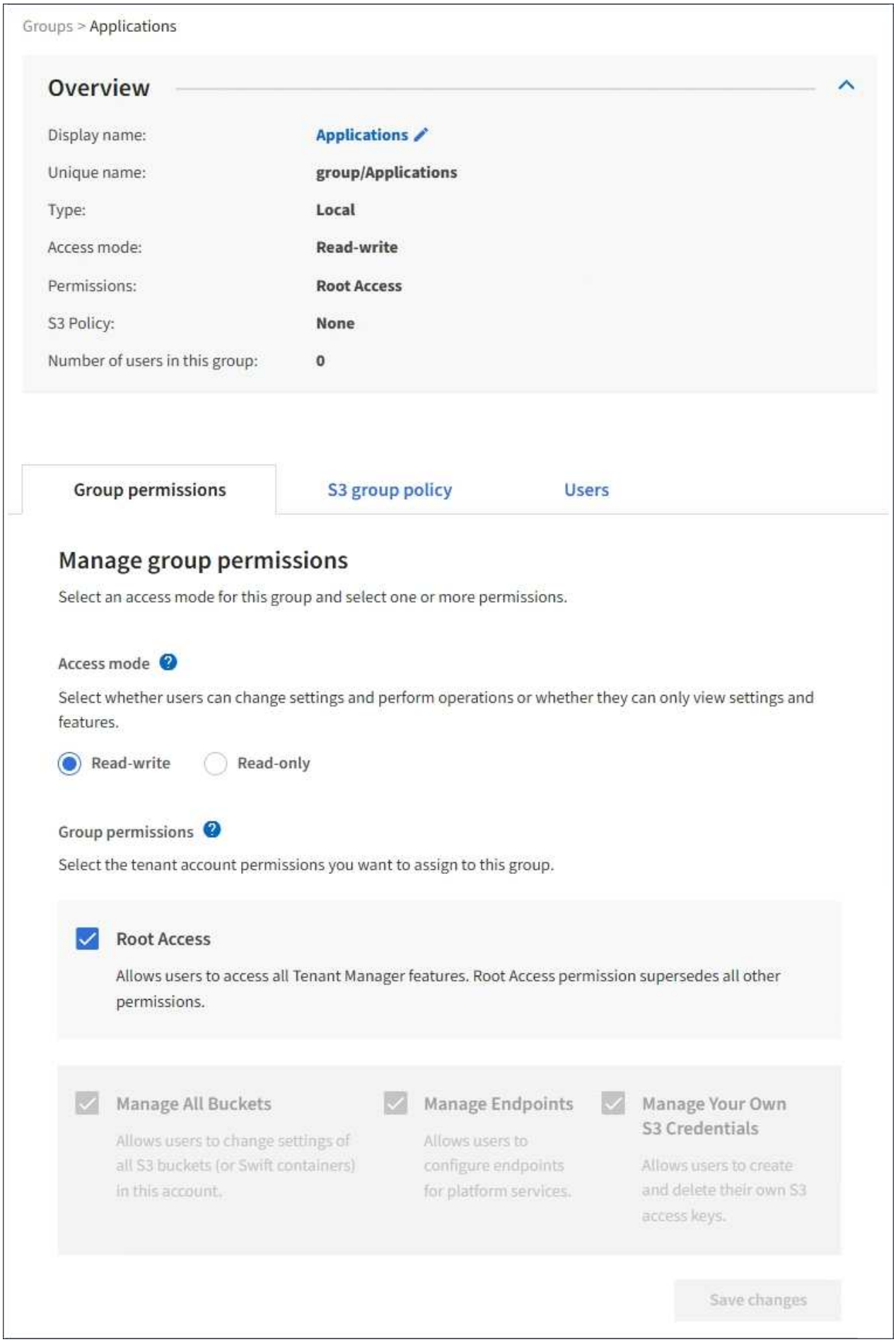
- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs qui dispose de l'autorisation accès racine.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT Groups**.
2. Sélectionnez le nom du groupe dont vous souhaitez afficher ou modifier les détails.

   Vous pouvez également sélectionner **actions Afficher les détails du groupe**.

   La page des détails du groupe s'affiche. L'exemple suivant montre la page des détails du groupe S3.


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. Modifiez les paramètres du groupe selon vos besoins.

> Pour vous assurer que vos modifications sont enregistrées, sélectionnez **Enregistrer les modifications** après avoir effectué des modifications dans chaque section. Lorsque vos modifications sont enregistrées, un message de confirmation s'affiche dans le coin supérieur droit de la page.

   a. Vous pouvez également sélectionner le nom d'affichage ou l'icône de modification pour mettre à jour le nom d'affichage.

      Vous ne pouvez pas modifier le nom unique d'un groupe. Vous ne pouvez pas modifier le nom d'affichage d'un groupe fédéré.

   b. Si vous le souhaitez, mettez à jour les autorisations.

   c. Pour les règles de groupe, apportez les modifications appropriées à votre locataire S3 ou Swift.

      - Si vous modifiez un groupe pour un locataire S3, vous pouvez choisir une autre règle de groupe S3. Si vous sélectionnez une règle S3 personnalisée, mettez à jour la chaîne JSON si nécessaire.
      - Si vous modifiez un groupe pour un locataire Swift, vous pouvez sélectionner ou désélectionner la case à cocher **Administrateur Swift**.

        Pour plus d'informations sur l'autorisation de l'administrateur Swift, reportez-vous aux instructions de création de groupes pour un locataire Swift.

   d. Si vous le souhaitez, vous pouvez ajouter ou supprimer des utilisateurs.

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

   L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Informations associées

Créez des groupes pour les locataires S3

Créez des groupes pour le locataire Swift

Ajouter des utilisateurs à un groupe local

Vous pouvez ajouter des utilisateurs à un groupe local si nécessaire.

Ce dont vous avez besoin

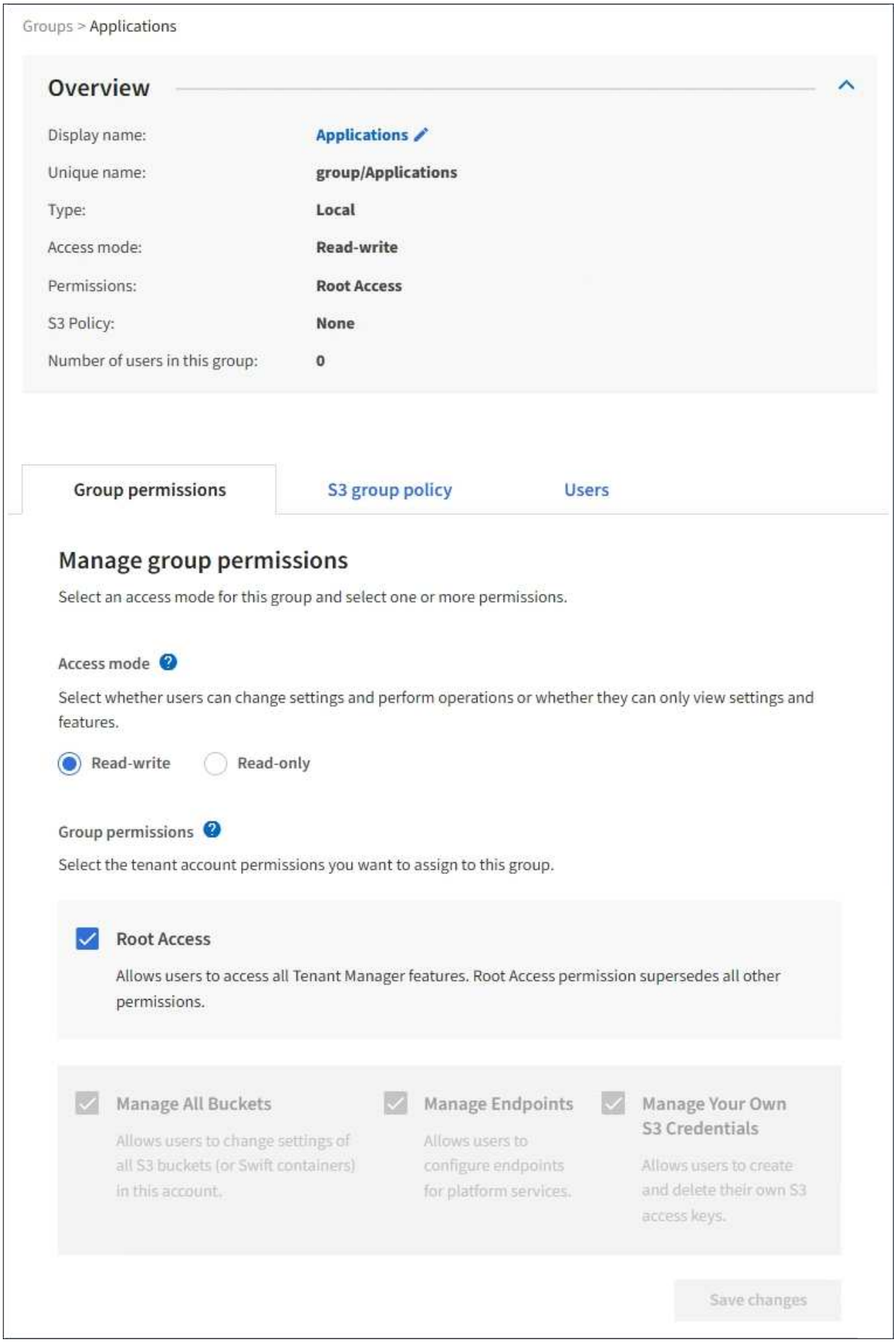
- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs qui dispose de l'autorisation accès racine.

Étapes

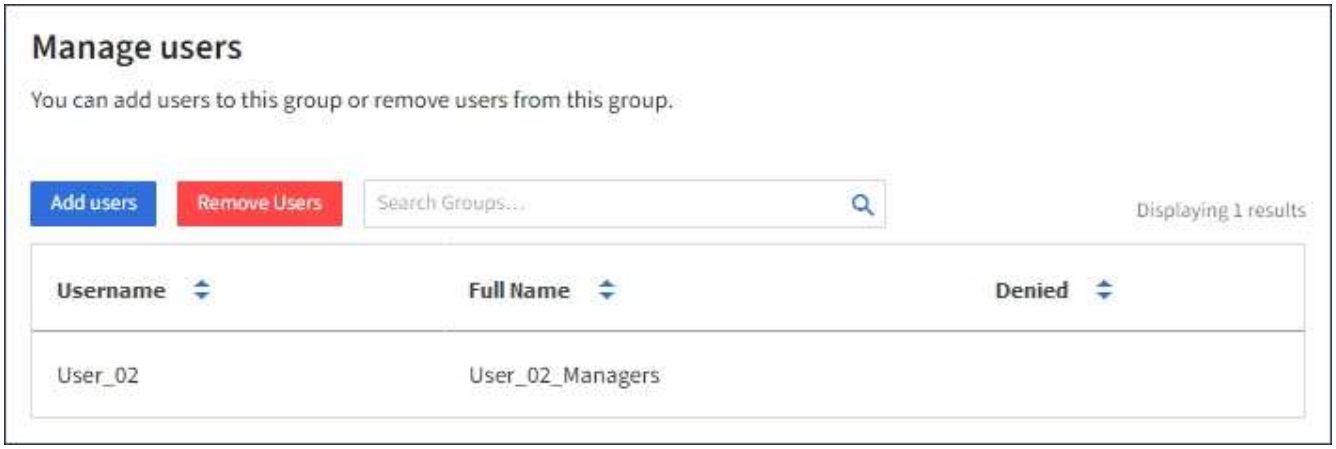
1. Sélectionnez **ACCESS MANAGEMENT Groups**.
2. Sélectionnez le nom du groupe local auquel vous souhaitez ajouter des utilisateurs.

   Vous pouvez également sélectionner **actions Afficher les détails du groupe**.

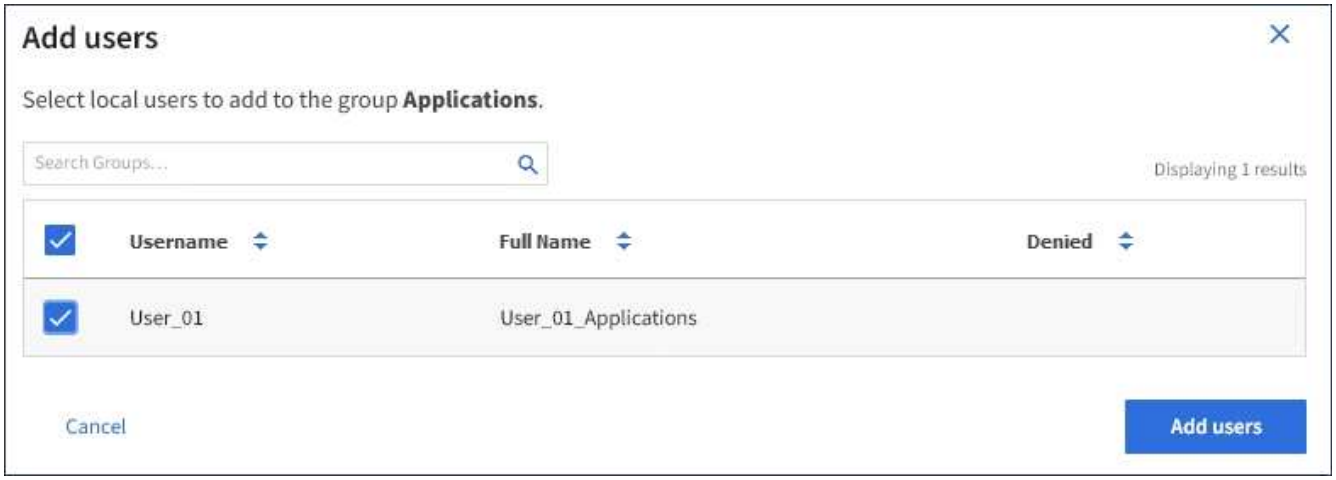
   La page des détails du groupe s'affiche.


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. Sélectionnez **utilisateurs**, puis **Ajouter utilisateurs**.



4. Sélectionnez les utilisateurs que vous souhaitez ajouter au groupe, puis sélectionnez **Ajouter utilisateurs**.



Un message de confirmation s'affiche dans le coin supérieur droit de la page. L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Modifier le nom du groupe

Vous pouvez modifier le nom d'affichage d'un groupe. Vous ne pouvez pas modifier le nom unique d'un groupe.

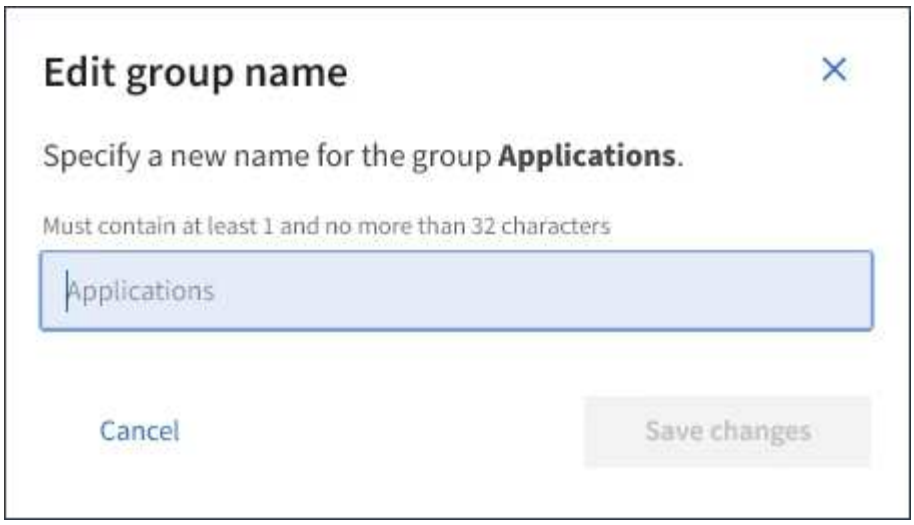
Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs qui dispose de l'autorisation accès racine. Voir Autorisations de gestion des locataires.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT Groups**.
2. Cochez la case du groupe dont vous souhaitez modifier le nom d'affichage.
3. Sélectionnez **actions Modifier le nom du groupe**.

   La boîte de dialogue Modifier le nom du groupe s'affiche.



4. Si vous modifiez un groupe local, mettez à jour le nom d'affichage selon vos besoins.

   Vous ne pouvez pas modifier le nom unique d'un groupe. Vous ne pouvez pas modifier le nom d'affichage d'un groupe fédéré.

5. Sélectionnez **Enregistrer les modifications**.

   Un message de confirmation s'affiche dans le coin supérieur droit de la page. L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Dupliquer le groupe

Vous pouvez créer de nouveaux groupes plus rapidement en dupliquant un groupe existant.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs qui dispose de l'autorisation accès racine. Voir Autorisations de gestion des locataires.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT Groups**.
2. Cochez la case correspondant au groupe que vous souhaitez dupliquer.
3. Sélectionnez **Dupliquer le groupe**. Pour plus d'informations sur la création d'un groupe, reportez-vous aux instructions de création de groupes pour Un locataire S3 ou pour Un locataire Swift.
4. Sélectionnez l'onglet **Groupe local** pour créer un groupe local ou sélectionnez l'onglet **Groupe fédéré** pour importer un groupe à partir du référentiel d'identité configuré précédemment.

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

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

d'affichage ultérieurement.

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

6. Sélectionnez **Continuer**.
7. Si nécessaire, modifiez les autorisations pour ce groupe.
8. Sélectionnez **Continuer**.
9. Si nécessaire, si vous copiez un groupe pour un locataire S3, vous pouvez sélectionner une autre stratégie à partir des boutons d'option **Ajouter une stratégie S3**. Si vous avez sélectionné une règle personnalisée, mettez à jour la chaîne JSON si nécessaire.
10. Sélectionnez **Créer groupe**.

Supprimer le groupe

Vous pouvez supprimer un groupe du système. Les utilisateurs appartenant uniquement à ce groupe ne pourront plus se connecter au Gestionnaire de locataires ni utiliser le compte de tenant.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs qui dispose de l'autorisation accès racine. Voir Autorisations de gestion des locataires.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT Groups**.

2. Cochez les cases des groupes que vous souhaitez supprimer.
3. Sélectionnez **actions Supprimer le groupe**.

   Un message de confirmation s'affiche.

4. Sélectionnez **Supprimer le groupe** pour confirmer la suppression des groupes indiqués dans le message de confirmation.

   Un message de confirmation s'affiche dans le coin supérieur droit de la page. L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Gérez les utilisateurs locaux

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

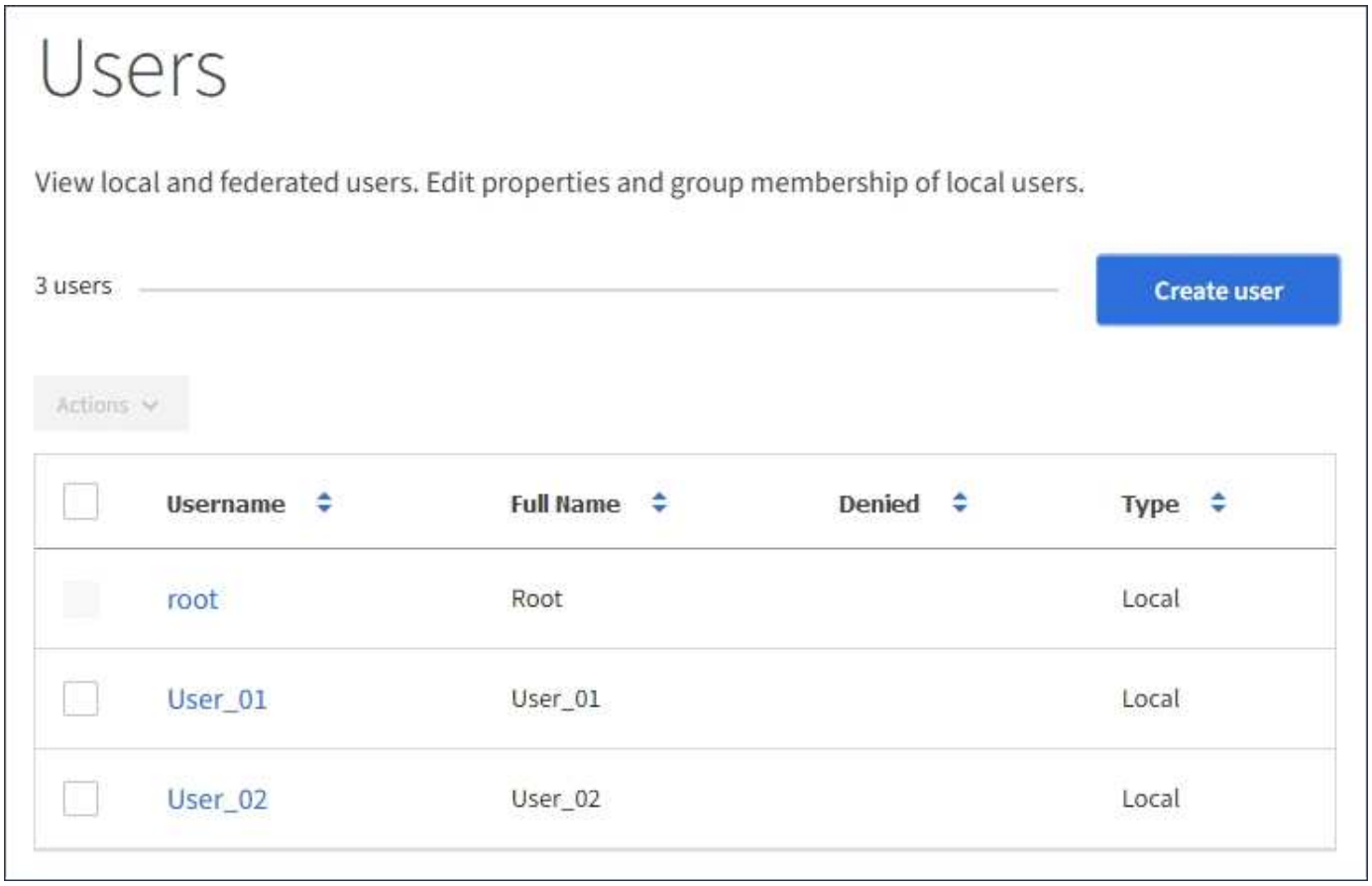
Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs en lecture/écriture doté de l'autorisation accès racine. Voir Autorisations de gestion des locataires.

> Si l'authentification unique 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, même s'ils peuvent utiliser les applications client S3 ou Swift pour accéder aux ressources du locataire en fonction des autorisations de groupe.

Accéder à la page utilisateurs

Sélectionnez **ACCESS MANAGEMENT Users**.



Créez des utilisateurs locaux

Vous pouvez créer des utilisateurs locaux et les attribuer à un ou plusieurs groupes locaux pour contrôler leurs autorisations d'accès.

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

Les utilisateurs Swift n'appartenant à aucun groupe ne disposent d'autorisations de gestion ni d'un accès au conteneur Swift.

Étapes

1. Sélectionnez **Créer utilisateur**.
2. Renseignez les champs suivants.
   - **Nom complet** : le nom complet de cet utilisateur, par exemple le prénom et le nom de famille d'une personne ou le nom d'une application.
   - **Nom d'utilisateur**: Le nom que cet utilisateur utilisera pour se connecter. Les noms d'utilisateur doivent être uniques et ne peuvent pas être modifiés.
   - **Mot de passe** : mot de passe utilisé lorsque l'utilisateur ouvre une session.
   - **Confirmer le mot de passe** : saisissez le même mot de passe que celui que vous avez saisi dans le champ Mot de passe.
   - **Refuser l'accès**: Si vous sélectionnez **Oui**, cet utilisateur ne peut pas se connecter au compte de tenant, même si l'utilisateur peut toujours appartenir à un ou plusieurs groupes.

Par exemple, vous pouvez utiliser cette fonction pour suspendre temporairement la connexion d'un utilisateur.

3. Sélectionnez **Continuer**.
4. Attribuez l'utilisateur à un ou plusieurs groupes locaux.

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

5. Sélectionnez **Créer utilisateur**.

   L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Modifier les détails de l'utilisateur

Lorsque vous modifiez les détails d'un utilisateur, vous pouvez modifier le nom complet et le mot de passe de l'utilisateur, ajouter l'utilisateur à différents groupes et empêcher l'utilisateur d'accéder au locataire.

Étapes

1. Dans la liste utilisateurs, sélectionnez le nom de l'utilisateur dont vous souhaitez afficher ou modifier les détails.

   Vous pouvez également cocher la case de l'utilisateur, puis sélectionner **actions Afficher les détails de l'utilisateur**.

2. Apportez les modifications nécessaires aux paramètres utilisateur.
   a. Modifiez le nom complet de l'utilisateur selon vos besoins en sélectionnant le nom complet ou l'icône de modification Dans la section vue d'ensemble.

      Vous ne pouvez pas modifier le nom d'utilisateur.

   b. Dans l'onglet **Mot de passe**, modifiez le mot de passe de l'utilisateur si nécessaire.
   c. Dans l'onglet **Access**, permettez à l'utilisateur de se connecter (sélectionnez **non**) ou d'empêcher l'utilisateur de se connecter (sélectionnez **Oui**) selon les besoins.
   d. Dans l'onglet **groupes**, ajoutez l'utilisateur aux groupes ou supprimez l'utilisateur des groupes si nécessaire.
   e. Si nécessaire pour chaque section, sélectionnez **Enregistrer les modifications**.

      L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Utilisateurs locaux en double

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

Étapes

1. Dans la liste utilisateurs, sélectionnez l'utilisateur que vous souhaitez dupliquer.
2. Sélectionnez **Dupliquer l'utilisateur**.
3. Modifiez les champs suivants pour le nouvel utilisateur.
   - **Nom complet** : le nom complet de cet utilisateur, par exemple le prénom et le nom de famille d'une

personne ou le nom d'une application.

- **Nom d'utilisateur**: Le nom que cet utilisateur utilisera pour se connecter. Les noms d'utilisateur doivent être uniques et ne peuvent pas être modifiés.
- **Mot de passe** : mot de passe utilisé lorsque l'utilisateur ouvre une session.
- **Confirmer le mot de passe** : saisissez le même mot de passe que celui que vous avez saisi dans le champ Mot de passe.
- **Refuser l'accès**: Si vous sélectionnez **Oui**, cet utilisateur ne peut pas se connecter au compte de tenant, même si l'utilisateur peut toujours appartenir à un ou plusieurs groupes.

  Par exemple, vous pouvez utiliser cette fonction pour suspendre temporairement la connexion d'un utilisateur.

4. Sélectionnez **Continuer**.
5. Sélectionnez un ou plusieurs groupes locaux.

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

6. Sélectionnez **Créer utilisateur**.

   L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Supprimer des utilisateurs locaux

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

À l'aide du Gestionnaire de locataires, vous pouvez supprimer des utilisateurs locaux, mais pas des utilisateurs fédérés. Vous devez utiliser le référentiel d'identité fédéré pour supprimer des utilisateurs fédérés.

Étapes

1. Dans la liste utilisateurs, cochez la case de l'utilisateur local que vous souhaitez supprimer.
2. Sélectionnez **actions Supprimer l'utilisateur**.
3. Dans la boîte de dialogue de confirmation, sélectionnez **Supprimer l'utilisateur** pour confirmer que vous souhaitez supprimer l'utilisateur du système.

   L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Gestion des comptes de locataires S3

Gestion des clés d'accès S3

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

Description de la tâche

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

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

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

Créez vos propres clés d'accès S3

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

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez disposer de l'autorisation gérer vos propres informations d'identification S3. Voir Autorisations de gestion des locataires.

Description de la tâche

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

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

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

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

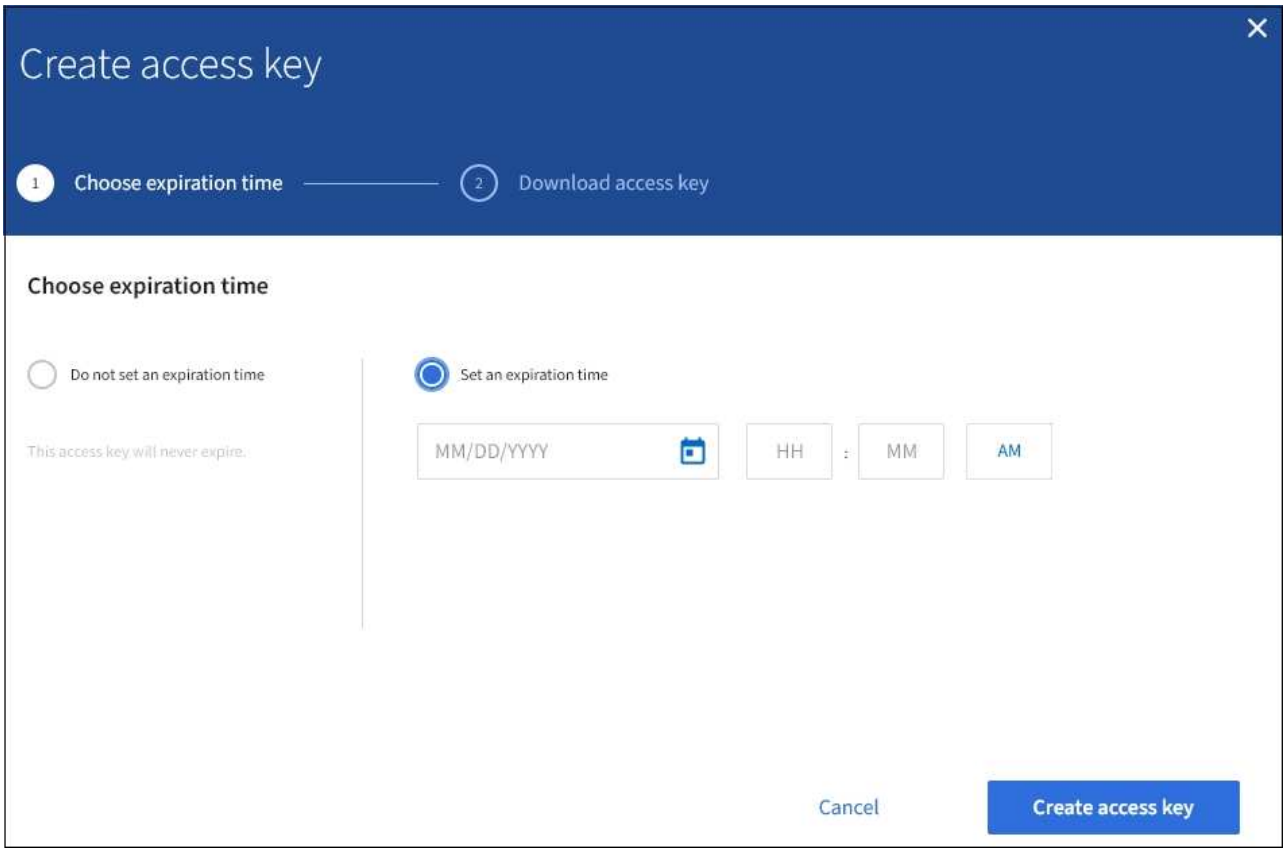
Étapes

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

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

2. Sélectionnez **Créer clé**.
3. Effectuez l'une des opérations suivantes :

- Sélectionnez **ne définissez pas d'heure d'expiration** pour créer une clé qui n'expire pas. (Valeur par défaut)
- Sélectionnez **définissez une heure d'expiration** et définissez la date et l'heure d'expiration.

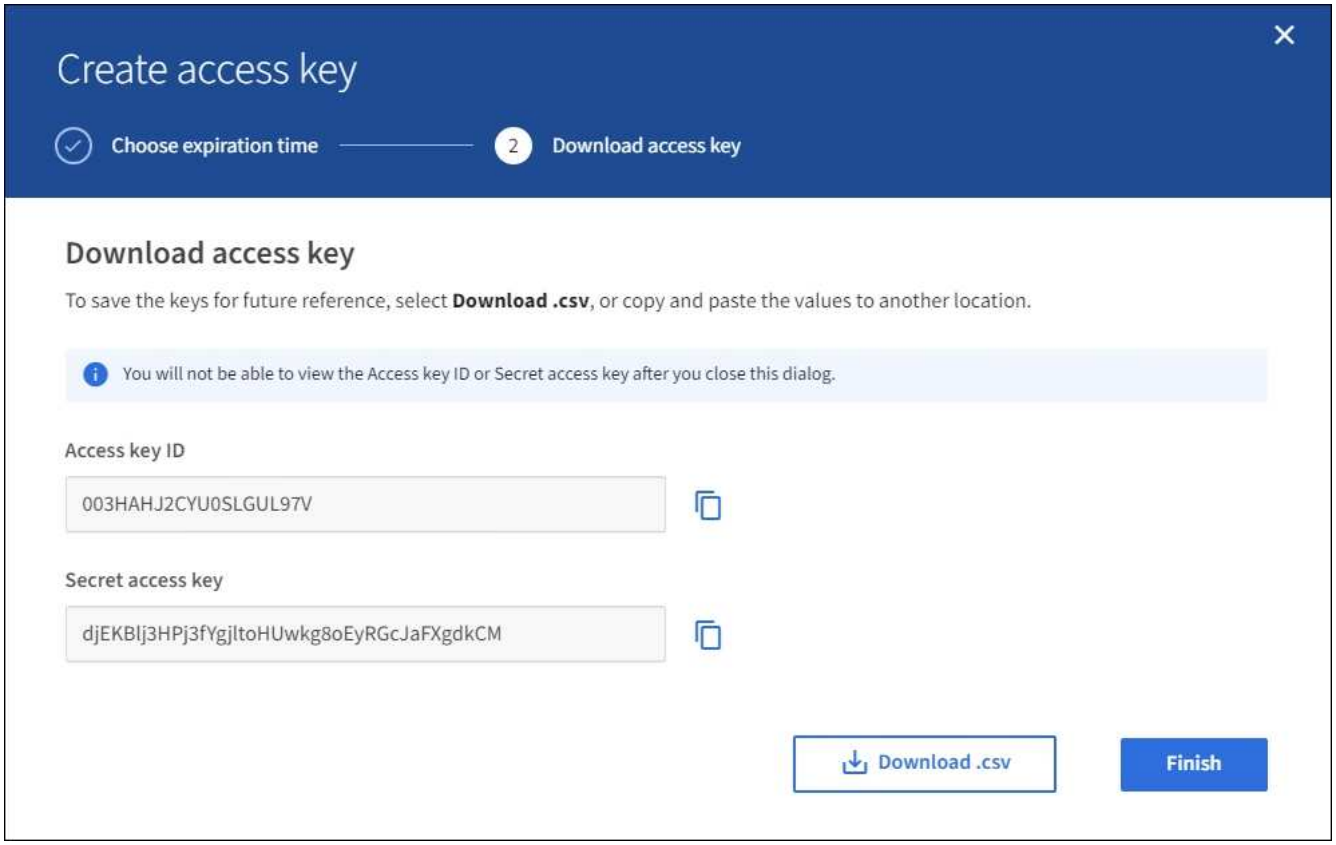


4. Sélectionnez **Créer une clé d'accès**.

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

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

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



6. Sélectionnez **Terminer**.

   La nouvelle clé apparaît sur la page Mes clés d'accès. L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Affichez vos clés d'accès S3

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

Ce dont vous avez besoin

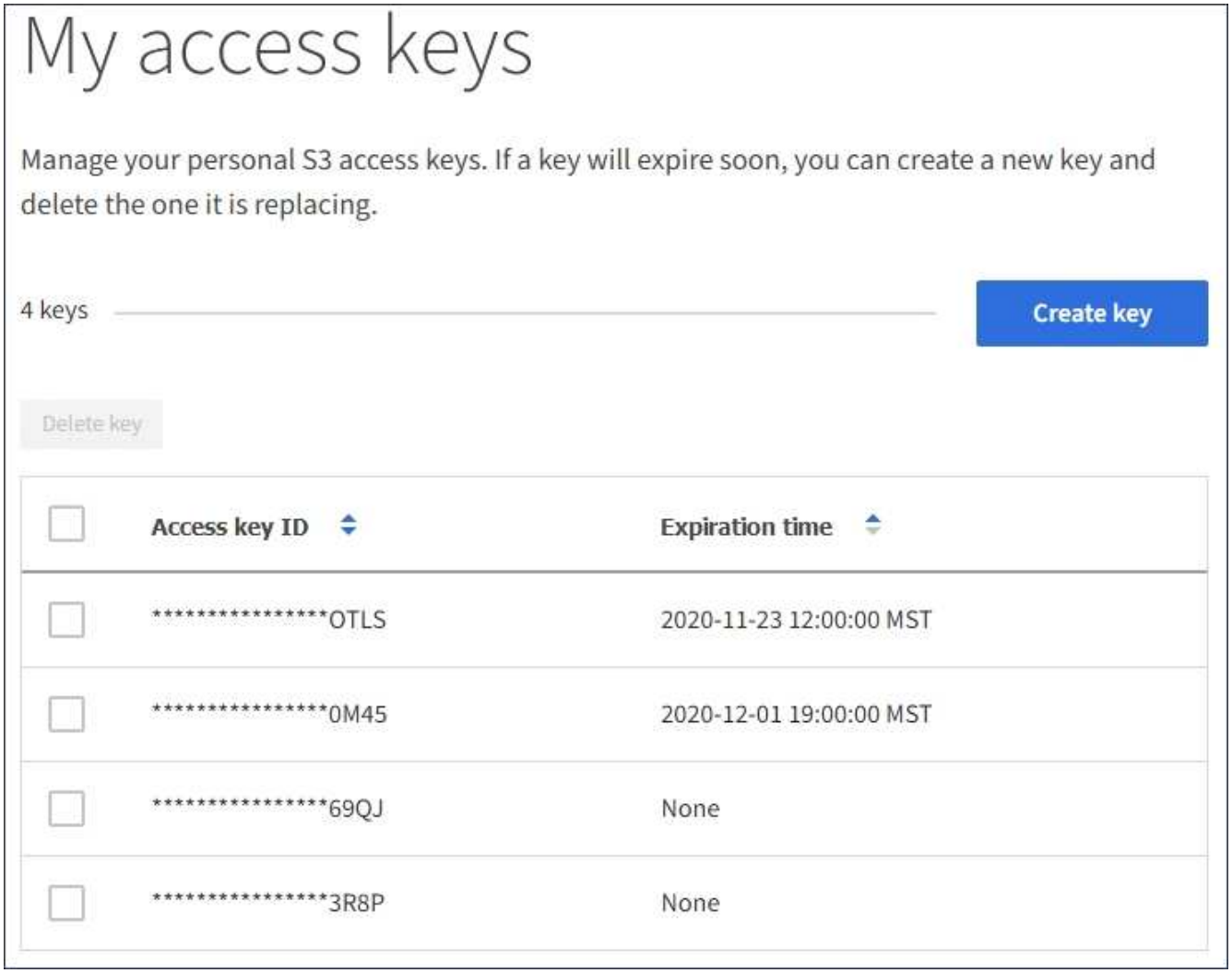
- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez disposer de l'autorisation gérer vos propres informations d'identification S3.

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

Étapes

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

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



2. Trier les clés par **heure d'expiration** ou **ID de clé d'accès**.
3. Si nécessaire, créez de nouvelles clés et supprimez manuellement les clés que vous n'utilisez plus.

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

   Les clés expirées sont supprimées automatiquement.

Informations associées

Créez vos propres clés d'accès S3

Supprimez vos propres clés d'accès S3

Supprimez vos propres clés d'accès S3

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

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez disposer de l'autorisation gérer vos propres informations d'identification S3. Voir Autorisations de gestion des locataires.

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

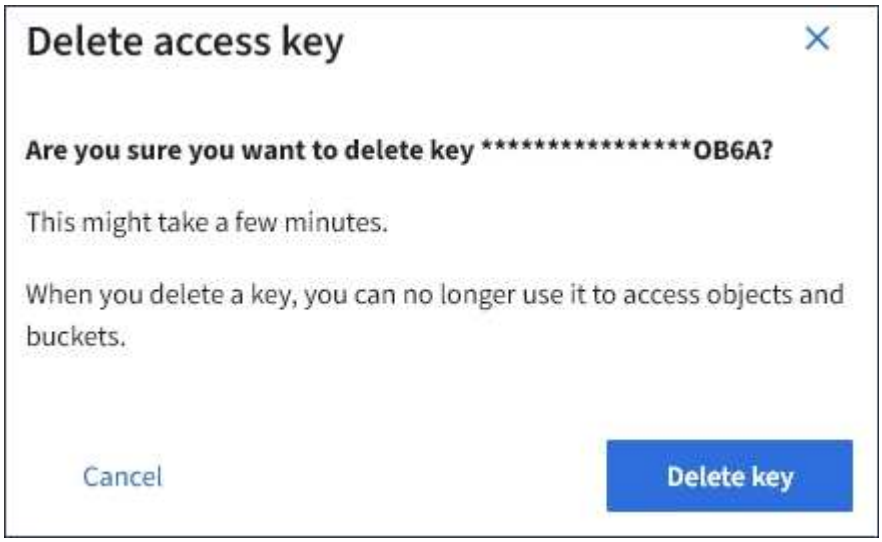
Étapes

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

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

2. Cochez la case correspondant à chaque clé d'accès que vous souhaitez supprimer.
3. Sélectionnez **Supprimer la touche**.

   Une boîte de dialogue de confirmation s'affiche.



4. Sélectionnez **Supprimer la touche**.

   Un message de confirmation s'affiche dans le coin supérieur droit de la page. L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

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

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

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez disposer de l'autorisation accès racine.

Description de la tâche

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

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

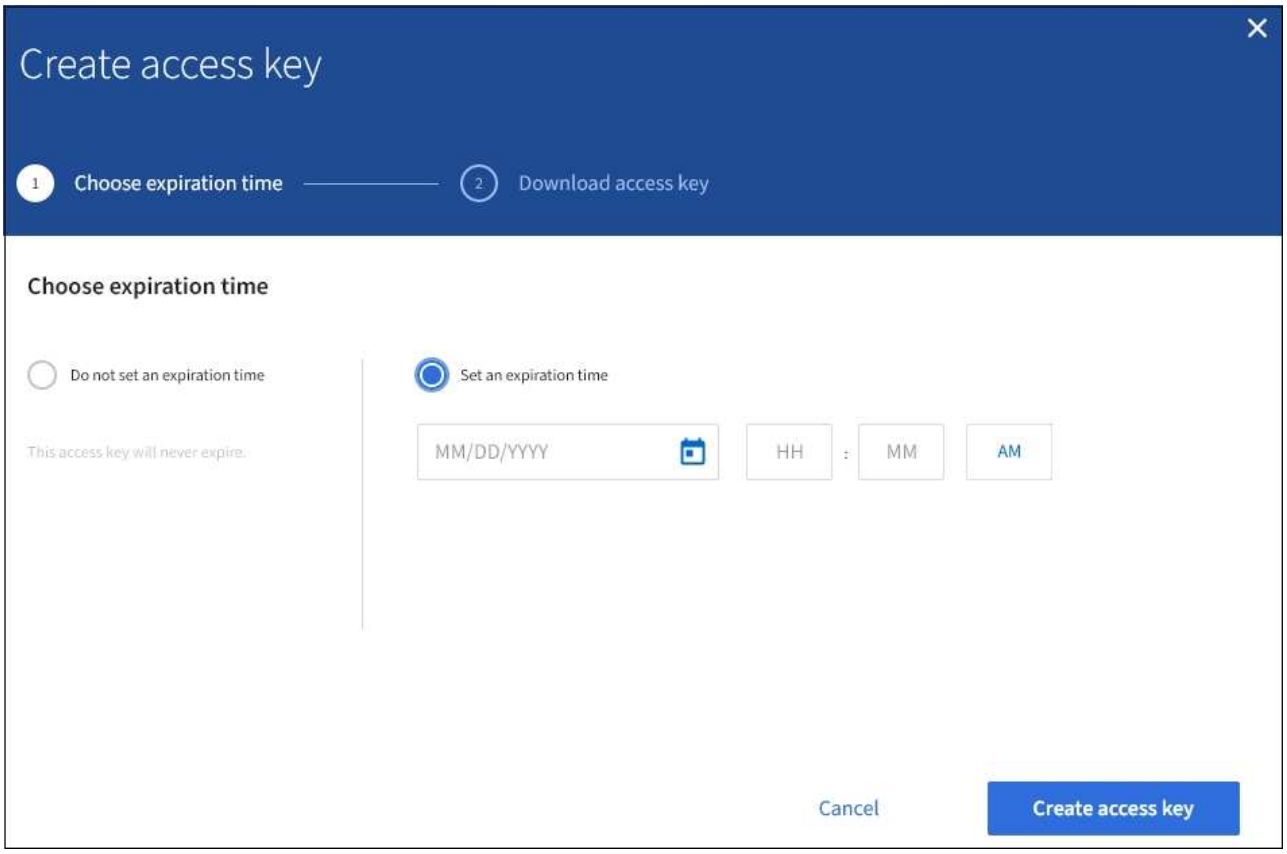
- Définissez un délai d'expiration pour les clés afin de limiter l'accès de l'utilisateur à une certaine période. La définition d'un délai d'expiration court peut aider à réduire le risque si l'ID de clé d'accès et la clé secrète sont exposés accidentellement. Les clés expirées sont supprimées automatiquement.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

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

Étapes

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

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

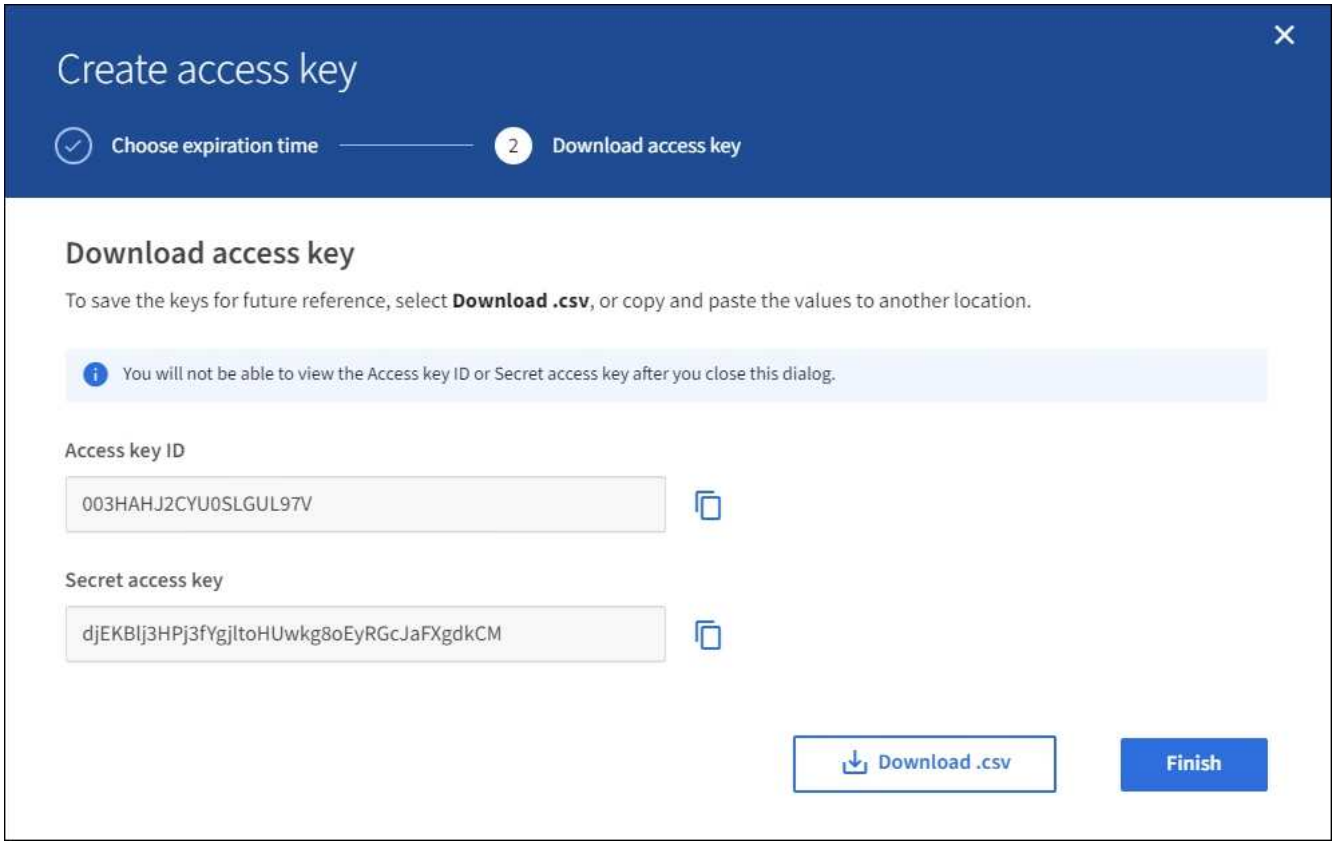


5. Sélectionnez **Créer une clé d'accès**.

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

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

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



7. Sélectionnez **Terminer**.

   La nouvelle clé est répertoriée dans l'onglet touches d'accès de la page des détails de l'utilisateur. L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Informations associées

Autorisations de gestion des locataires

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

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

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez disposer de l'autorisation accès racine.

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

Étapes

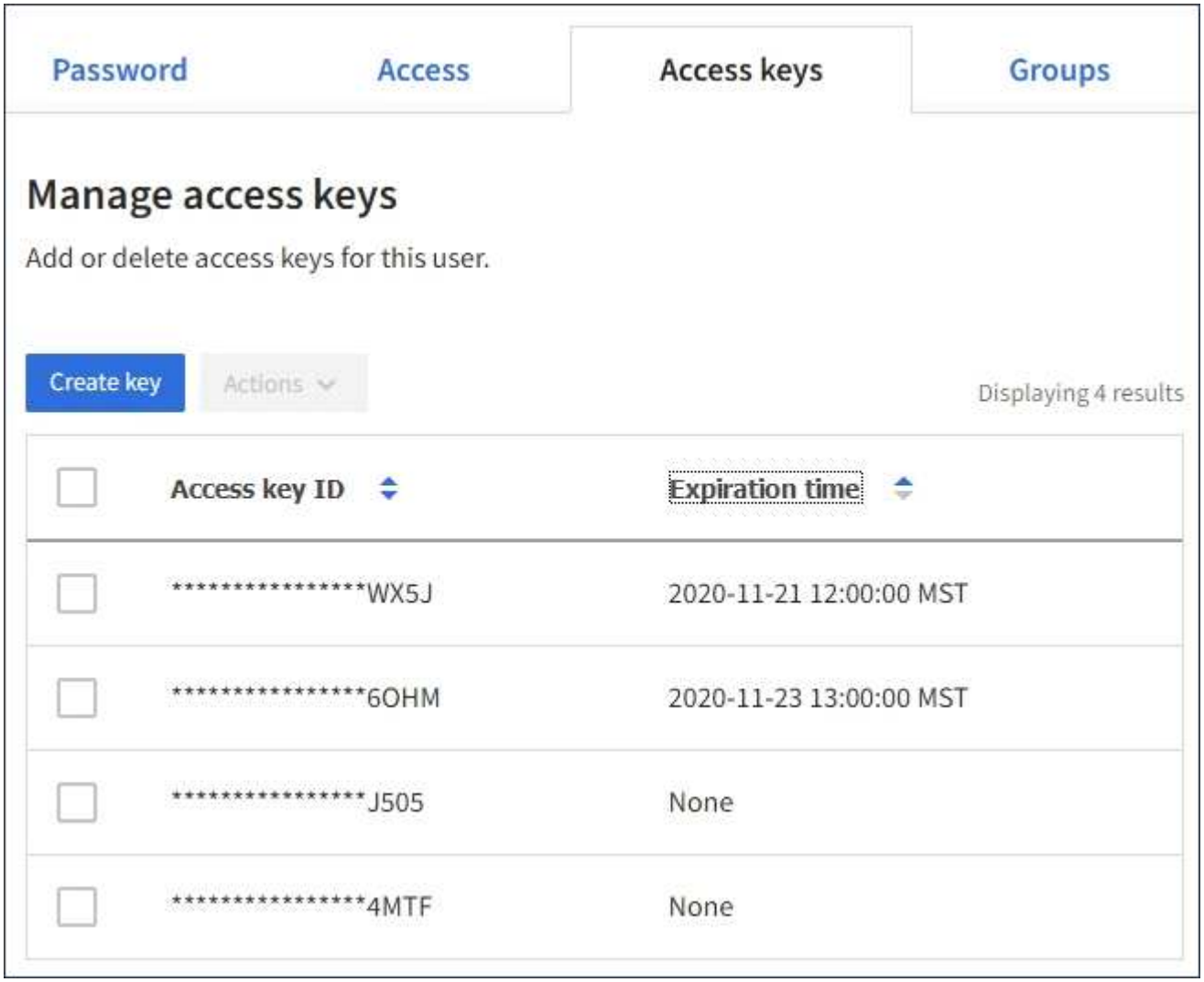
1. Sélectionnez **ACCESS MANAGEMENT Users**.

   La page utilisateurs s'affiche et répertorie les utilisateurs existants.

2. Sélectionnez l'utilisateur dont vous souhaitez afficher les clés d'accès S3.

   La page Détails de l'utilisateur s'affiche.

3. Sélectionnez **touches d'accès**.



4. Trier les clés par **heure d'expiration** ou **ID de clé d'accès**.
5. Si nécessaire, créez de nouvelles clés et supprimez manuellement les clés que le n'est plus utilisé.

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

   Les clés expirées sont supprimées automatiquement.

Informations associées

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

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

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

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

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez disposer de l'autorisation accès racine. Voir Autorisations de gestion des locataires.

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

Étapes

1. Sélectionnez **ACCESS MANAGEMENT Users**.

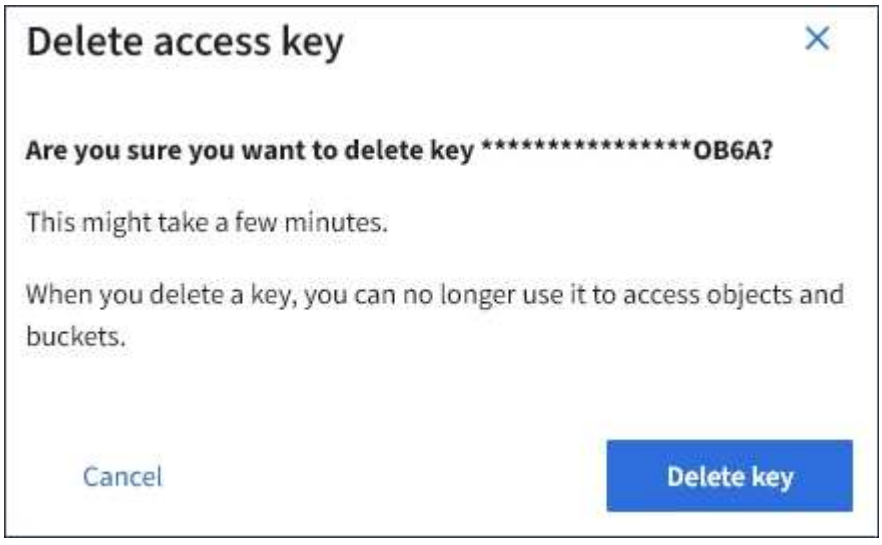
   La page utilisateurs s'affiche et répertorie les utilisateurs existants.

2. Sélectionnez l'utilisateur dont vous souhaitez gérer les clés d'accès S3.

   La page Détails de l'utilisateur s'affiche.

3. Sélectionnez **touches d'accès**, puis cochez la case pour chaque clé d'accès que vous souhaitez supprimer.
4. Sélectionnez **actions Supprimer la touche sélectionnée**.

   Une boîte de dialogue de confirmation s'affiche.



5. Sélectionnez **Supprimer la touche**.

   Un message de confirmation s'affiche dans le coin supérieur droit de la page. L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Gestion des compartiments S3

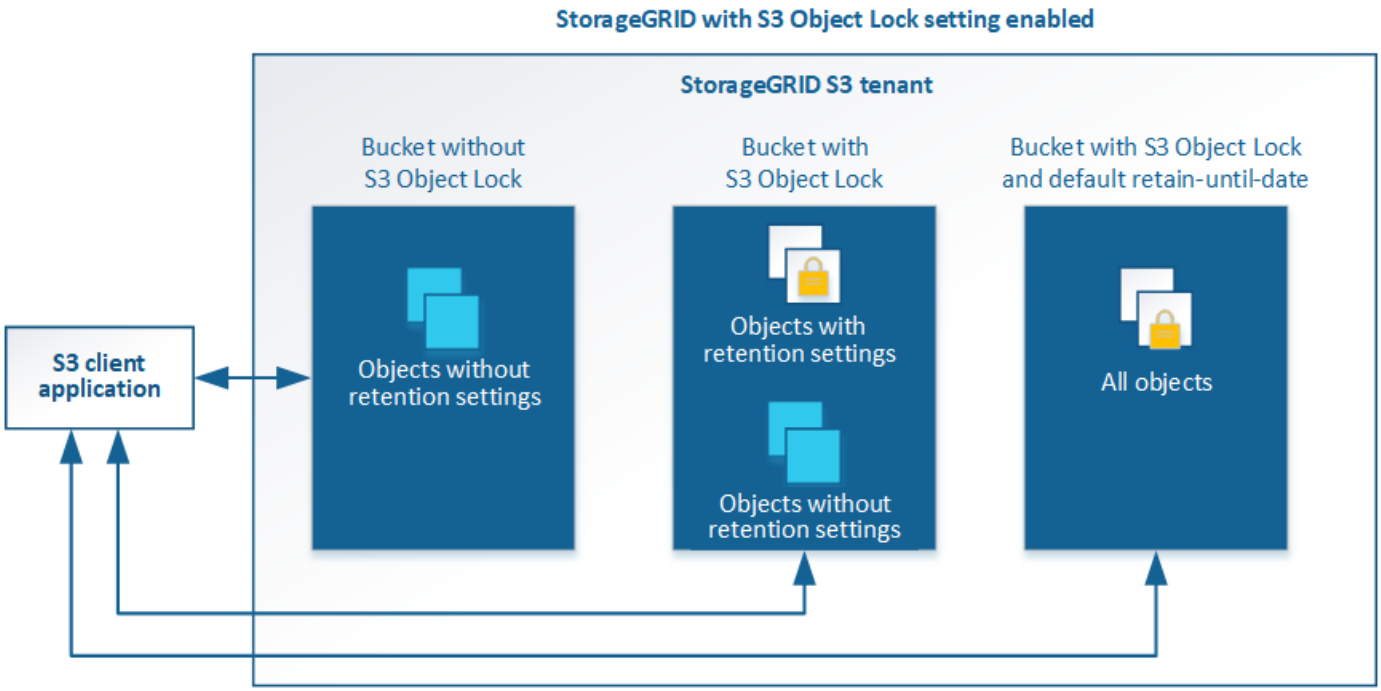
Utilisez la fonction de verrouillage d'objet S3 avec les locataires

Vous pouvez utiliser la fonctionnalité de verrouillage d'objet S3 dans StorageGRID si vos objets doivent être conformes aux exigences réglementaires en matière de conservation.

Qu'est-ce que le verrouillage objet S3 ?

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

Comme illustré dans la figure, lorsque le paramètre global de verrouillage d'objet S3 est activé pour un système StorageGRID, un compte de locataire S3 peut créer des compartiments avec ou sans verrouillage d'objet S3 activé. Si un compartiment est doté du verrouillage objet S3 activé, les applications client S3 peuvent éventuellement spécifier des paramètres de conservation pour toute version d'objet dans ce compartiment. Des paramètres de conservation doivent être spécifiés pour être protégés par le verrouillage d'objet S3.



La fonctionnalité de verrouillage d'objet StorageGRID S3 fournit un mode de conservation unique équivalent au mode de conformité Amazon S3. Par défaut, une version d'objet protégé ne peut être écrasée ou supprimée par aucun utilisateur. La fonction de verrouillage d'objet StorageGRID S3 ne prend pas en charge un mode de gouvernance et n'autorise pas les utilisateurs disposant d'autorisations spéciales à contourner les paramètres de rétention ou à supprimer des objets protégés.

Si un compartiment est doté de l'option de verrouillage des objets S3, l'application client S3 peut spécifier la ou les deux paramètres de conservation de niveau objet suivants lors de la création ou de la mise à jour d'un objet :

- **Conserver-jusqu'à-date** : si la date-à-jour d'une version d'objet est à l'avenir, l'objet peut être récupéré, mais ne peut pas être modifié ou supprimé. Si nécessaire, la date de conservation d'un objet peut être augmentée, mais cette date ne peut pas être réduite.

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

Vous pouvez également spécifiez un mode de conservation par défaut et la période de conservation par défaut pour le compartiment. Elles sont appliquées à chaque objet ajouté au compartiment qui ne spécifie pas ses propres paramètres de rétention.

Pour plus de détails sur ces paramètres, reportez-vous à la section Utilisez le verrouillage d'objet S3.

Gestion des compartiments conformes aux ancienne génération

La fonction de verrouillage d'objet S3 remplace la fonction de conformité disponible dans les versions StorageGRID précédentes. Si vous avez créé des compartiments conformes à l'aide d'une version précédente de StorageGRID, vous pouvez continuer à gérer les paramètres de ces compartiments. Toutefois, vous ne pouvez plus créer de compartiments conformes. Pour en savoir plus, consultez l'article de la base de connaissance NetApp.

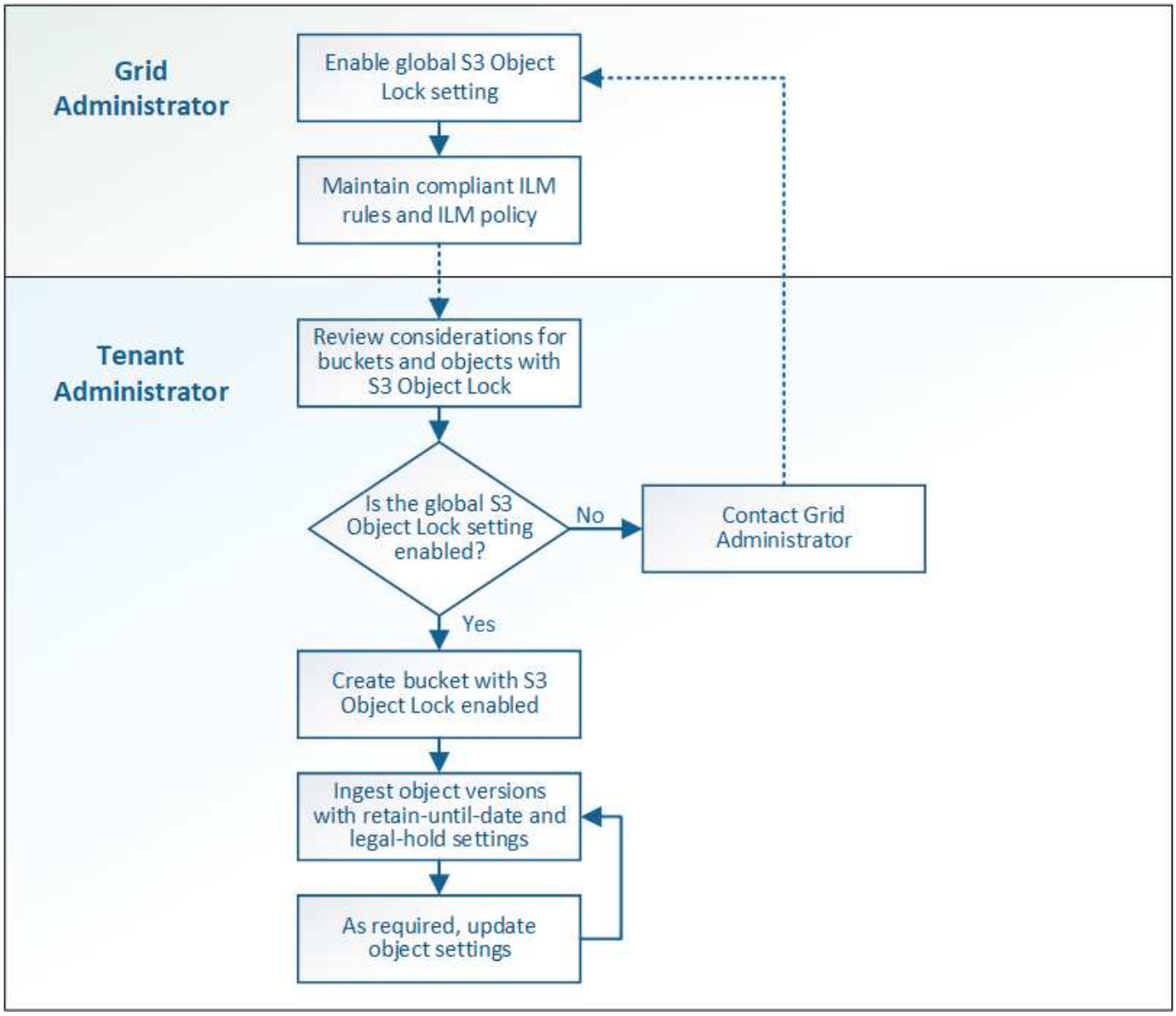
"Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5"

Workflow de verrouillage d'objet S3

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

Avant de créer des compartiments avec le verrouillage d'objet S3 activé, l'administrateur de la grille doit activer le paramètre de verrouillage d'objet S3 global pour l'ensemble du système StorageGRID. L'administrateur du grid doit également s'assurer que La gestion du cycle de vie de l'information (ILM Est « conforme » ; il doit répondre aux exigences des compartiments lorsque le verrouillage d'objet S3 est activé. Pour plus d'informations, contactez votre administrateur de la grille ou consultez les instructions relatives à la gestion des objets avec la gestion du cycle de vie des informations.

Une fois que le paramètre de verrouillage d'objet S3 global a été activé, vous pouvez créer des compartiments avec le verrouillage d'objet S3 activé. Vous pouvez ensuite utiliser l'application client S3 pour spécifier les paramètres de conservation pour chaque version d'objet.



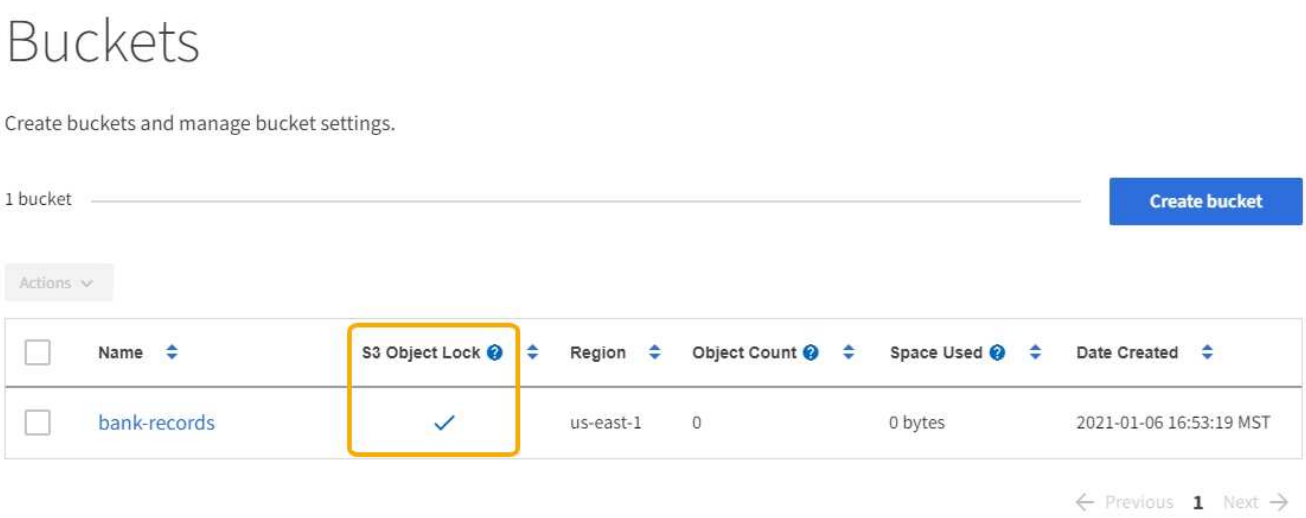
Conditions requises pour le verrouillage d'objet S3

Avant d'activer le verrouillage d'objet S3 pour un compartiment, vérifiez les exigences relatives aux compartiments et aux objets S3 Object Lock ainsi que le cycle de vie des objets dans des compartiments où le verrouillage d'objet S3 est activé.

Conditions requises pour les compartiments avec verrouillage objet S3 activé

- Si le paramètre global de verrouillage objet S3 est activé pour le système StorageGRID, vous pouvez utiliser le gestionnaire de locataires, l'API de gestion des locataires ou l'API REST S3 pour créer des compartiments avec le verrouillage objet S3 activé.

  Dans cet exemple, le gestionnaire des locataires affiche un compartiment avec le verrouillage objet S3 activé.



- Si vous prévoyez d'utiliser le verrouillage d'objet S3, vous devez activer le verrouillage d'objet S3 lors de la création du compartiment. Vous ne pouvez pas activer le verrouillage d'objet S3 pour un compartiment existant.
- Le contrôle de version de compartiment est requis avec le verrouillage d'objet S3. Lorsque le verrouillage d'objet S3 est activé pour un compartiment, StorageGRID active automatiquement le contrôle de version pour ce compartiment.
- Une fois que vous avez créé un compartiment avec le verrouillage d'objet S3 activé, vous ne pouvez pas désactiver le verrouillage d'objet S3 ou suspendre la gestion des versions pour ce compartiment.
- Vous pouvez également configurer la conservation par défaut d'un compartiment. Lors du téléchargement d'une version d'objet, la conservation par défaut est appliquée à la version de l'objet. Vous pouvez remplacer la valeur par défaut du compartiment en spécifiant un mode de rétention et une date de conservation dans la demande de téléchargement d'une version d'objet.
- La configuration du cycle de vie des compartiments est prise en charge pour les compartiments de cycle de vie des objets S3.
- La réplication CloudMirror n'est pas prise en charge pour les compartiments avec le verrouillage objet S3 activé.

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

- Pour protéger la version d'un objet, l'application client S3 doit configurer la conservation par défaut du compartiment ou spécifier les paramètres de conservation dans chaque demande de téléchargement.
- Vous pouvez augmenter la valeur de conservation jusqu'à la date d'une version d'objet, mais vous ne pouvez jamais la diminuer.
- Si vous êtes averti d'une action légale ou d'une enquête réglementaire en attente, vous pouvez conserver les informations pertinentes en plaçant une mise en garde légale sur une version d'objet. Lorsqu'une version d'objet est soumise à une conservation légale, cet objet ne peut pas être supprimé de StorageGRID, même si elle a atteint sa date de conservation. Dès que la mise en attente légale est levée, la version de l'objet peut être supprimée si la date de conservation a été atteinte.
- Le verrouillage d'objet S3 requiert l'utilisation de compartiments avec version. Les paramètres de conservation s'appliquent aux versions d'objet individuelles. Une version d'objet peut avoir à la fois un paramètre de conservation à la date et un paramètre de conservation légal, l'un mais pas l'autre, ou l'autre. La spécification d'un paramètre de conservation à la date ou d'un paramètre de conservation légal pour un objet protège uniquement la version spécifiée dans la demande. Vous pouvez créer de nouvelles versions de l'objet, tandis que la version précédente de l'objet reste verrouillée.

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

Chaque objet enregistré dans un compartiment avec l'option de verrouillage d'objet S3 passe en trois étapes :

1. **Entrée d'objet**
   - Lorsque vous ajoutez une version d'objet dans un compartiment lorsque le verrouillage objet S3 est activé, l'application client S3 peut spécifier des paramètres de conservation pour l'objet (conservation à la date, conservation légale ou les deux). StorageGRID génère ensuite les métadonnées de cet objet, qui incluent un identificateur d'objet unique (UUID) et la date et l'heure d'ingestion.
   - Lors de l'ingestion d'une version d'objet avec paramètres de conservation, les données et les métadonnées S3 définies par l'utilisateur ne peuvent pas être modifiées.
   - StorageGRID stocke les métadonnées objet indépendamment des données de l'objet. Elle conserve trois copies de toutes les métadonnées d'objet sur chaque site.
2. **Rétention d'objet**
   - Plusieurs copies de l'objet sont stockées par StorageGRID. Le nombre et le type exacts de copies ainsi que les emplacements de stockage sont déterminés par les règles conformes de la politique ILM active.
3. **Suppression d'objet**
   - Un objet peut être supprimé lorsque sa date de conservation est atteinte.
   - Impossible de supprimer un objet en attente légale.

Créer un compartiment S3

Vous pouvez utiliser le Gestionnaire des locataires pour créer des compartiments S3 pour les données d'objet. Lorsque vous créez un compartiment, vous devez spécifier son nom et sa région. Si le paramètre global de verrouillage d'objet S3 est activé pour le système StorageGRID, vous pouvez activer le verrouillage d'objet S3 pour le compartiment.

Ce dont vous avez besoin

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous appartenez à un groupe d'utilisateurs possédant l'autorisation gérer toutes les rubriques ou accès racine. Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.

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

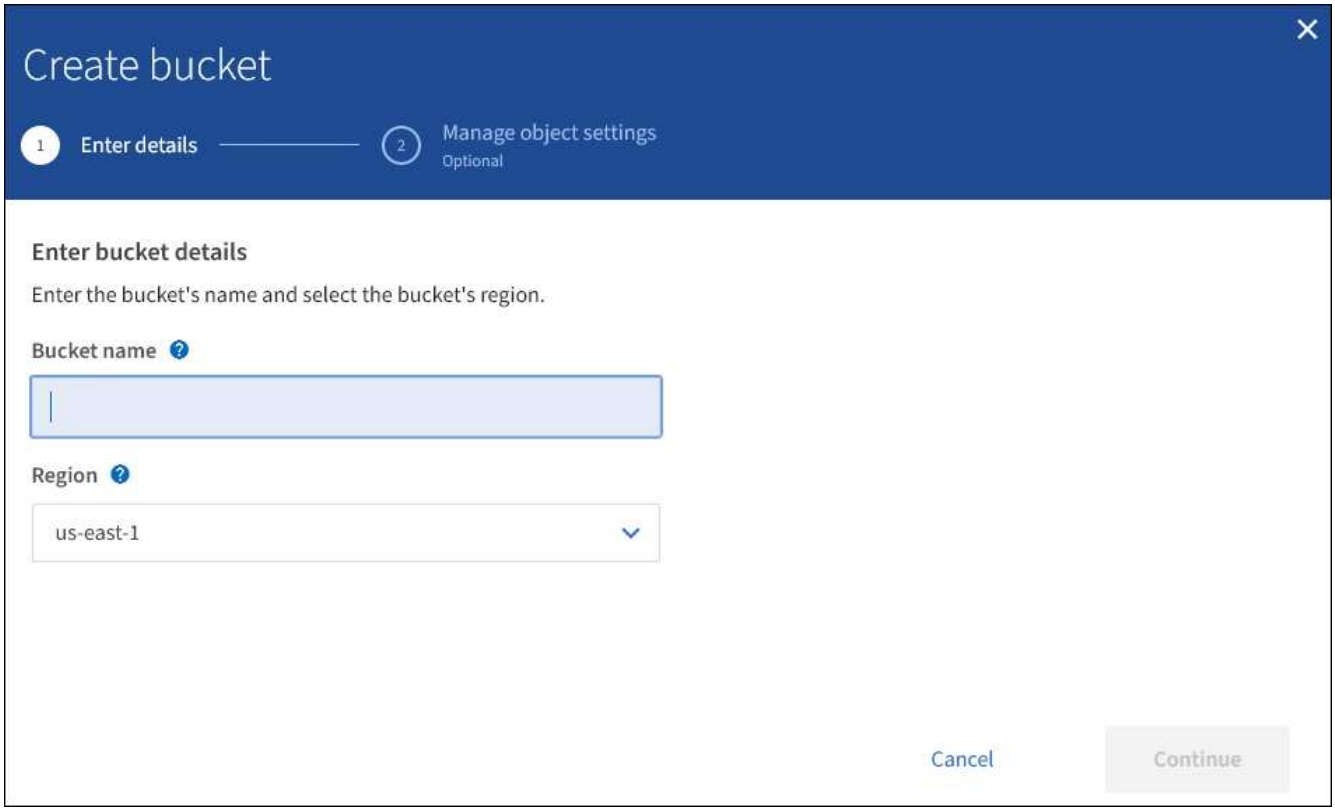
- Si vous prévoyez de créer un compartiment avec le verrouillage d'objet S3, vous avez activé le paramètre de verrouillage d'objet S3 global pour le système StorageGRID et vous avez examiné les exigences relatives aux compartiments et aux objets de verrouillage d'objet S3.

  Utilisez le verrouillage d'objet S3

Étapes

1. Sélectionnez **STOCKAGE (S3) seaux**.

2. Sélectionnez **Créer un compartiment**.



3. Entrer un nom unique pour le compartiment.

> Vous ne pouvez pas modifier le nom d'un compartiment après sa création.

Les noms de compartiment doivent être conformes aux règles suivantes :

- Il doit être unique sur chaque système StorageGRID (et pas seulement au sein du compte du locataire).
- Doit être conforme DNS.
- Doit contenir au moins 3 caractères et pas plus de 63 caractères.
- Chaque étiquette doit commencer et se terminer par une lettre ou un chiffre en minuscules et ne peut utiliser que des lettres minuscules, des chiffres et des tirets.
- Ne doit pas utiliser de périodes dans des demandes de type hébergement virtuel. Les périodes provoquera des problèmes avec la vérification du certificat générique du serveur.

> Pour plus d'informations, reportez-vous à la section "Documentation Amazon Web Services (AWS) sur les règles d'attribution de nom de compartiment".

4. Sélectionnez la région de ce compartiment.

L'administrateur StorageGRID gère les régions disponibles. Ce compartiment peut affecter la règle de protection des données appliquée aux objets. Par défaut, tous les compartiments sont créés dans le `us-east-1` région.

> Vous ne pouvez pas modifier la région après avoir créé le compartiment.

5. Sélectionnez **Continuer**.
6. Activez éventuellement le contrôle de version d'objet pour le compartiment.

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

7. Si la section verrouillage d'objet S3 s'affiche, activez éventuellement le verrouillage d'objet S3 pour le compartiment.

   > Vous ne pouvez pas activer ou désactiver le verrouillage d'objet S3 après la création du compartiment.

   La section verrouillage d'objet S3 s'affiche uniquement si le paramètre verrouillage d'objet S3 global est activé.

   Le verrouillage objet S3 doit être activé pour le compartiment avant qu'une application client S3 puisse spécifier des paramètres de conservation à une date et de conservation légale pour les objets ajoutés au compartiment.

   Si vous activez le verrouillage des objets S3 pour un compartiment, le contrôle de version des compartiments est automatiquement activé. Vous pouvez également spécifiez un mode de conservation par défaut et la période de conservation par défaut pour le compartiment qui sont appliquées à chaque objet ingéré dans le compartiment qui ne spécifie pas ses propres paramètres de conservation.

8. Sélectionnez **Créer un compartiment**.

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

Informations associées

Gestion des objets avec ILM

Compréhension de l'API de gestion des locataires

Utilisation de S3

Affichez les détails du compartiment S3

Vous pouvez afficher la liste des compartiments et des paramètres de compartiment dans votre compte de locataire.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.

Étapes

1. Sélectionnez **STOCKAGE (S3) seaux**.

   La page rubriques s'affiche et répertorie toutes les rubriques du compte locataire.

2. Passer en revue les informations relatives à chaque godet.

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

   - Nom : nom unique du compartiment, qui ne peut pas être modifié.
   - Verrouillage de l'objet S3 : indique si le verrouillage de l'objet S3 est activé pour ce compartiment.

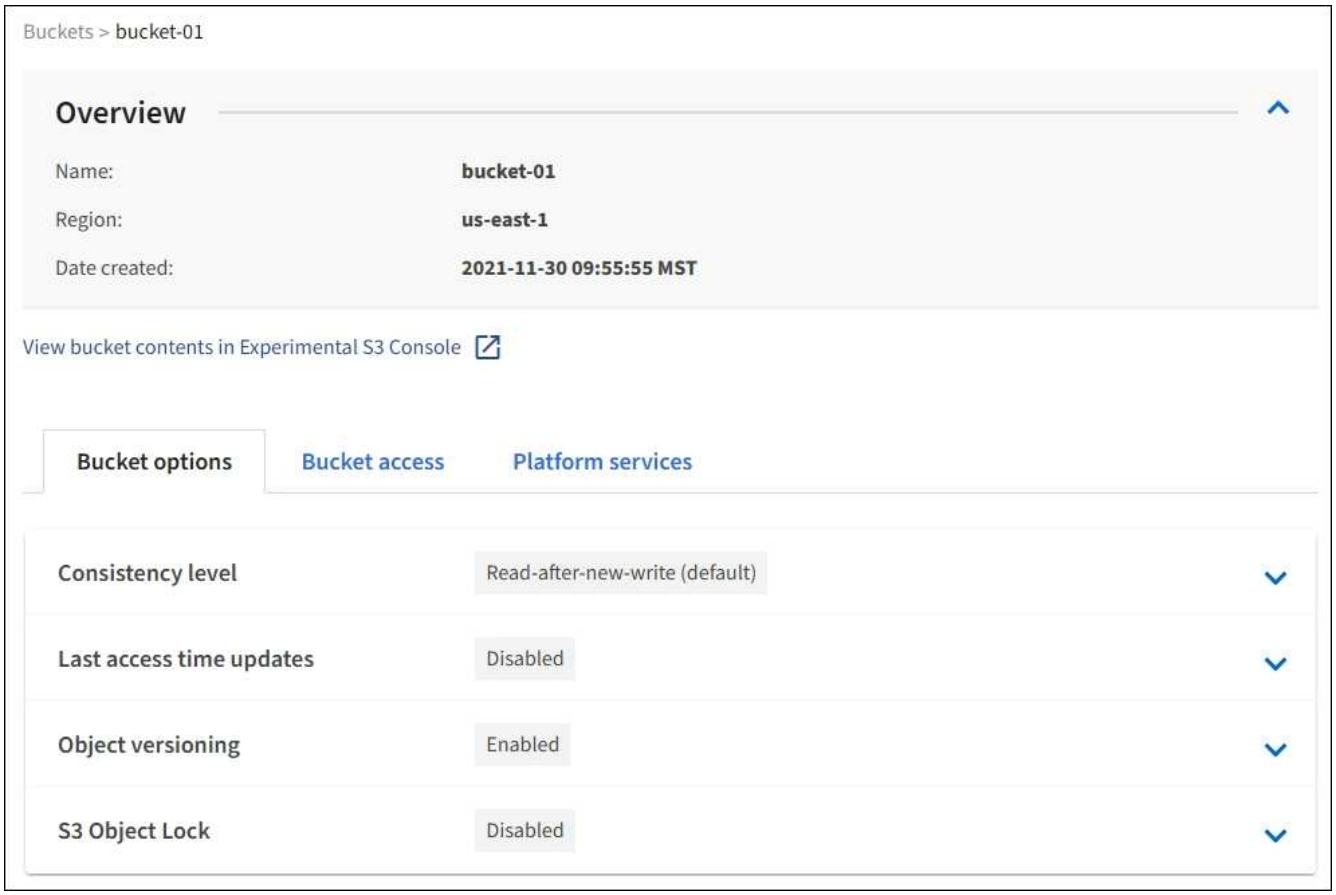
     Cette colonne n'est pas affichée si le paramètre de verrouillage d'objet S3 global est désactivé. Cette colonne affiche également des informations pour tous les compartiments conformes existants.

   - Région : région du godet, qui ne peut pas être modifiée.
   - Nombre d'objets : nombre d'objets dans ce compartiment.
   - Espace utilisé : taille logique de tous les objets de ce compartiment. La taille logique n'inclut pas l'espace réel requis pour les copies répliquées ou avec code d'effacement, ni pour les métadonnées d'objet.
   - Date de création : date et heure de création du compartiment.

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

3. Pour afficher et gérer les paramètres d'un compartiment, sélectionnez le nom du compartiment.

   La page des détails du compartiment vous permet d'afficher et de modifier les paramètres des options du compartiment, de l'accès au compartiment, et services de plateforme.



Modifiez le niveau de cohérence

Si vous utilisez un locataire S3, vous pouvez utiliser le gestionnaire des locataires ou l'API de gestion des locataires pour modifier le contrôle de cohérence pour les opérations effectuées sur les objets dans des compartiments S3.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs possédant l'autorisation gérer toutes les rubriques ou accès racine. Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments. Voir Autorisations de gestion des locataires.

Description de la tâche

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

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

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

Étapes

1. Sélectionnez **STOCKAGE (S3) seaux**.
2. Sélectionnez le nom du compartiment dans la liste.

   La page des détails du compartiment s'affiche.

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

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

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

Ces instructions s'appliquent uniquement aux systèmes StorageGRID qui incluent au moins une règle ILM utilisant l'option **dernier accès** dans ses instructions de placement. Vous pouvez ignorer ces instructions si votre système StorageGRID n'inclut pas une telle règle.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs possédant l'autorisation gérer toutes les rubriques ou accès racine. Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments. Voir Autorisations de gestion des locataires.

Heure de dernier accès est l'une des options disponibles pour l'instruction de placement **temps de référence** pour une règle ILM. La définition de l'heure de référence d'une règle sur heure du dernier accès permet aux administrateurs de la grille de spécifier que les objets doivent être placés dans certains emplacements de stockage en fonction de la date de récupération de ces objets (lecture ou visualisation).

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

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

Voir les instructions de gestion des objets avec la gestion du cycle de vie des informations.

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

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

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

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

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

Type de demande	Comportement si l'heure du dernier accès est désactivée (par défaut)		Comportement si l'heure du dernier accès est activée	
	Heure du dernier accès mise à jour ?	Objet ajouté à la file d'attente d'évaluation ILM ?	Heure du dernier accès mise à jour ?	Objet ajouté à la file d'attente d'évaluation ILM ?
Demande de récupération d'un objet, de sa liste de contrôle d'accès ou de ses métadonnées	Non	Non	Oui.	Oui.
Demande de mise à jour des métadonnées d'un objet	Oui.	Oui.	Oui.	Oui.
Demander de copier un objet d'un compartiment à un autre	• Non, pour la copie source • Oui, pour la copie de destination	• Non, pour la copie source • Oui, pour la copie de destination	• Oui, pour la copie source • Oui, pour la copie de destination	• Oui, pour la copie source • Oui, pour la copie de destination

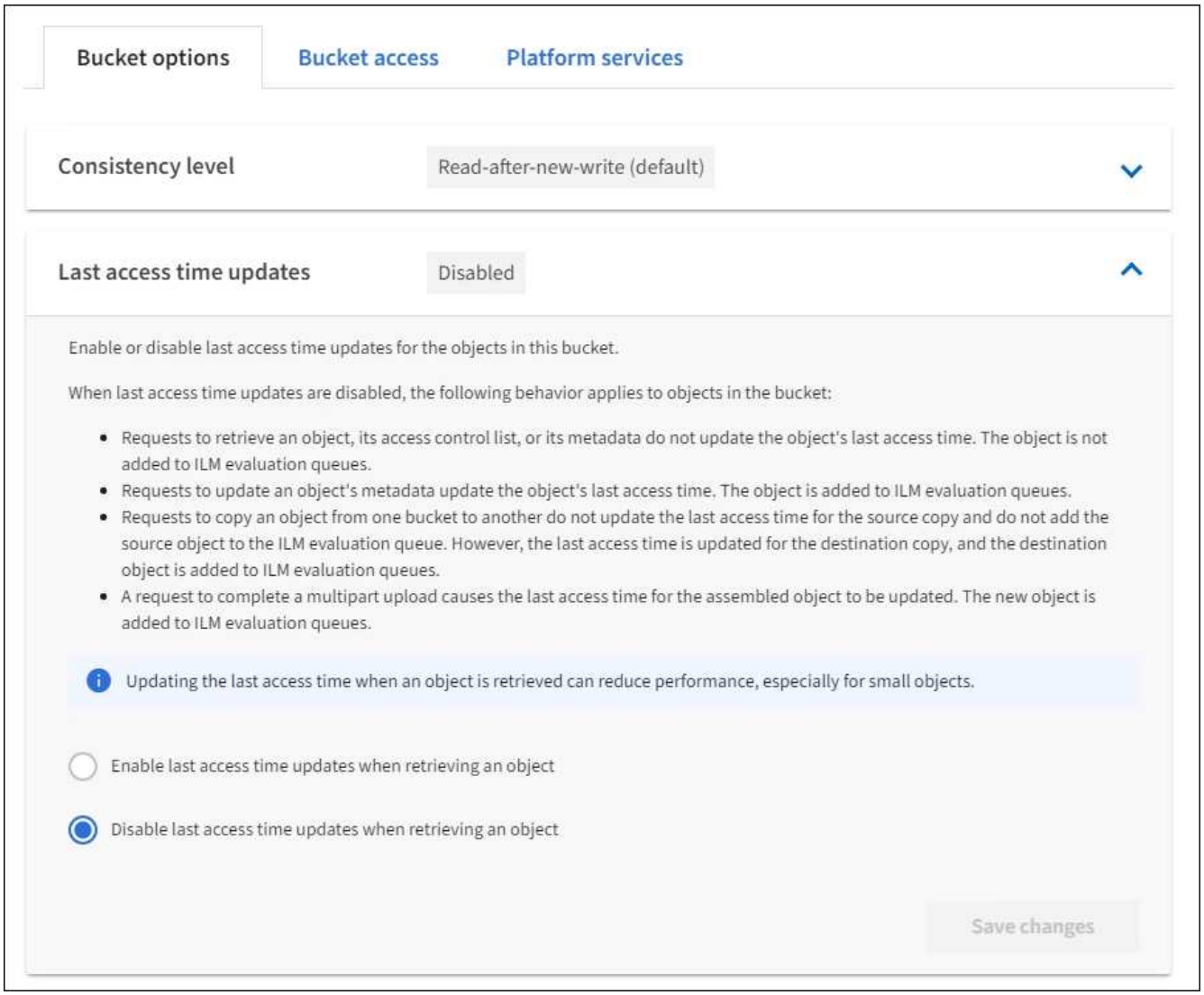
Demander de terminer un téléchargement partitionné	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé

Étapes

1. Sélectionnez **STOCKAGE (S3) seaux**.
2. Sélectionnez le nom du compartiment dans la liste.

   La page des détails du compartiment s'affiche.

3. Sélectionnez **Options de rubrique mises à jour des dernières temps d'accès**.
4. Sélectionnez le bouton radio approprié pour activer ou désactiver les dernières mises à jour des heures d'accès.



5. Sélectionnez **Enregistrer les modifications**.

Informations associées

Autorisations de gestion des locataires

Modifiez le contrôle de version d'objet pour un compartiment

Si vous utilisez un locataire S3, vous pouvez utiliser le Gestionnaire des locataires ou l'API de gestion des locataires pour modifier l'état des versions des compartiments S3.

Ce dont vous avez besoin

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous appartenez à un groupe d'utilisateurs possédant l'autorisation gérer toutes les rubriques ou accès racine. Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.

  Autorisations de gestion des locataires

Description de la tâche

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

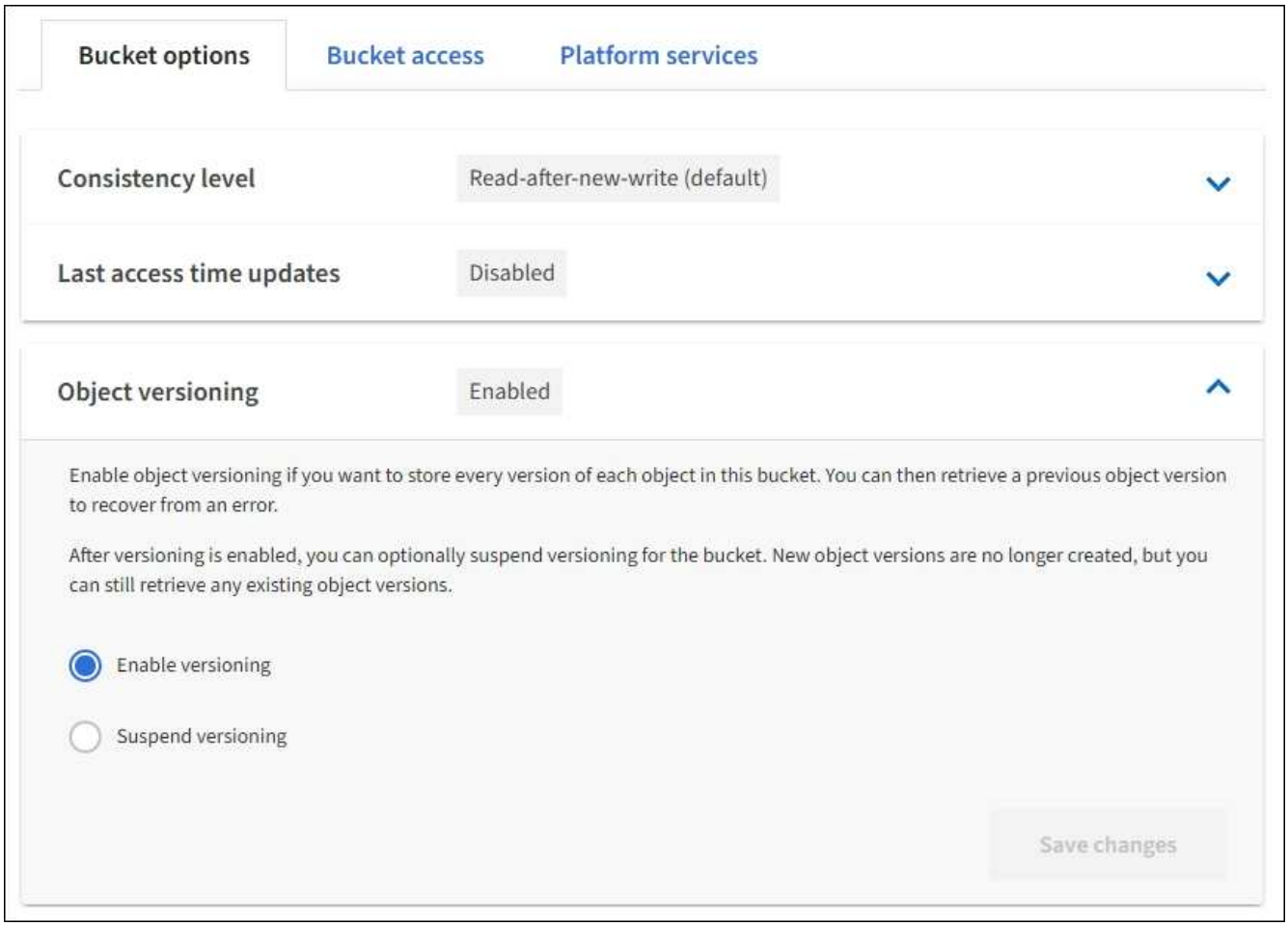
- Désactivé : le contrôle de version n'a jamais été activé
- Activé : la gestion des versions est activée
- Suspendu : la gestion des versions a déjà été activée et est suspendue

Gestion des versions d'objets S3

Règles et règles ILM pour les objets avec version S3 (exemple 4)

Étapes

1. Sélectionnez **STOCKAGE (S3) seaux**.
2. Sélectionnez le nom du compartiment dans la liste.
3. Sélectionnez **Options de rubrique gestion des versions d'objet**.



4. Sélectionnez un état de gestion des versions pour les objets de ce compartiment.

> Si le verrouillage d'objet S3 ou la conformité héritée est activée, les options **Object versionnage** sont désactivées.

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

5. Sélectionnez **Enregistrer les modifications**.

Configurer le partage de ressources inter-origine (CORS)

Vous pouvez configurer le partage de ressources inter-origine (CORS) pour un compartiment S3 si vous souhaitez que ce compartiment et les objets de ce

compartiment soient accessibles aux applications Web dans d'autres domaines.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs possédant l'autorisation gérer toutes les rubriques ou accès racine. Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.

Description de la tâche

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

Étapes

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

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

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

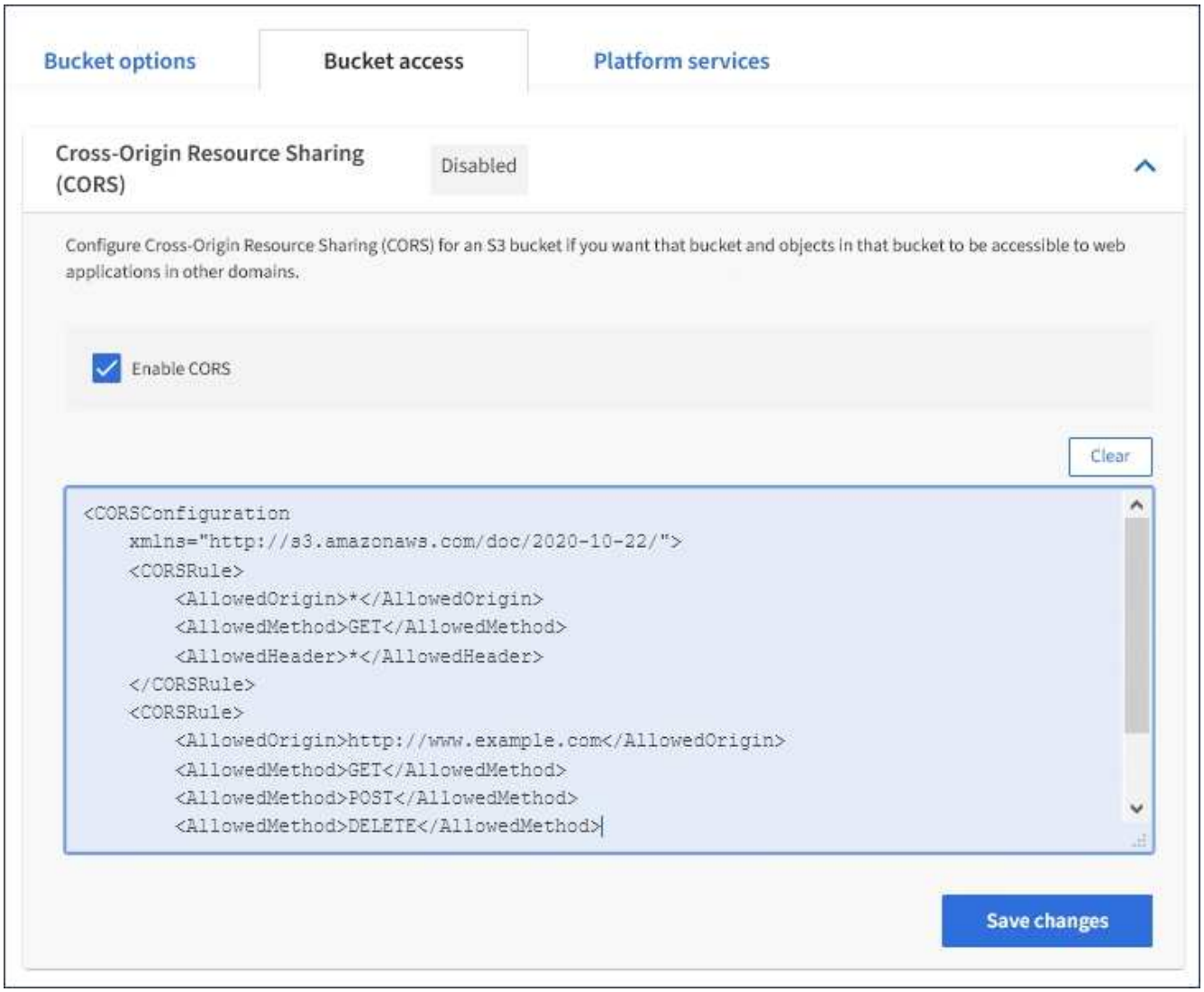
   Pour plus d'informations sur le XML de configuration CORS, voir "Documentation Amazon Web Services (AWS) : guide du développeur Amazon simple Storage Service".

2. Dans le Gestionnaire de locataires, sélectionnez **STORAGE (S3) seaux**.
3. Sélectionnez le nom du compartiment dans la liste.

   La page des détails du compartiment s'affiche.

4. Sélectionnez **accès au compartiment partage de ressources d'origine croisée (CORS)**.

5. Cochez la case **Activer CORS**.
6. Collez le code XML de configuration CORS dans la zone de texte, puis sélectionnez **Enregistrer les modifications**.



7. Pour modifier le paramètre CORS pour le compartiment, mettez à jour le code XML de configuration CORS dans la zone de texte ou sélectionnez **Clear** pour recommencer. Sélectionnez ensuite **Enregistrer les modifications**.
8. Pour désactiver CORS pour le compartiment, décochez la case **Activer CORS**, puis sélectionnez **Enregistrer les modifications**.

Supprimez le compartiment S3

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

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs possédant l'autorisation gérer toutes les rubriques ou accès racine. Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments. Voir Autorisations de gestion des locataires.

- Les compartiments à supprimer sont vides.

Description de la tâche

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

Si ce compartiment contient des objets ou des versions d'objet non actuelles, vous ne pouvez pas le supprimer. Pour plus d'informations sur la suppression des objets avec version S3, consultez le instructions de gestion des objets avec gestion du cycle de vie des informations.

Étapes

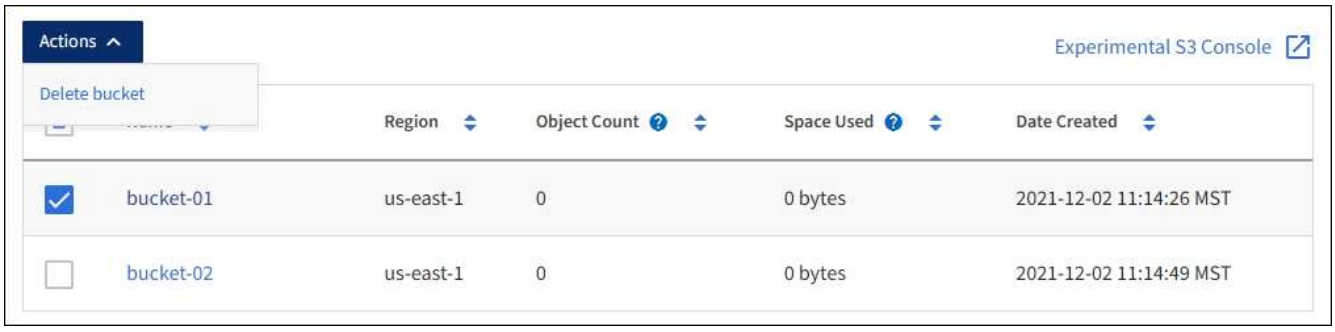
1. Sélectionnez **STOCKAGE (S3) seaux**.

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

2. Cochez la case du compartiment vide que vous souhaitez supprimer. Vous pouvez sélectionner plusieurs compartiments à la fois.

   Le menu actions est activé.

3. Dans le menu actions, sélectionnez **Supprimer le compartiment** (ou **Supprimer les compartiments** si vous en avez choisi plusieurs).



4. Lorsque la boîte de dialogue de confirmation s'affiche, sélectionnez **Oui** pour supprimer tous les

compartiments que vous avez choisis.

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

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

Utilisation de la console Experimental S3

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

Vous pouvez également utiliser la console S3 pour :

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

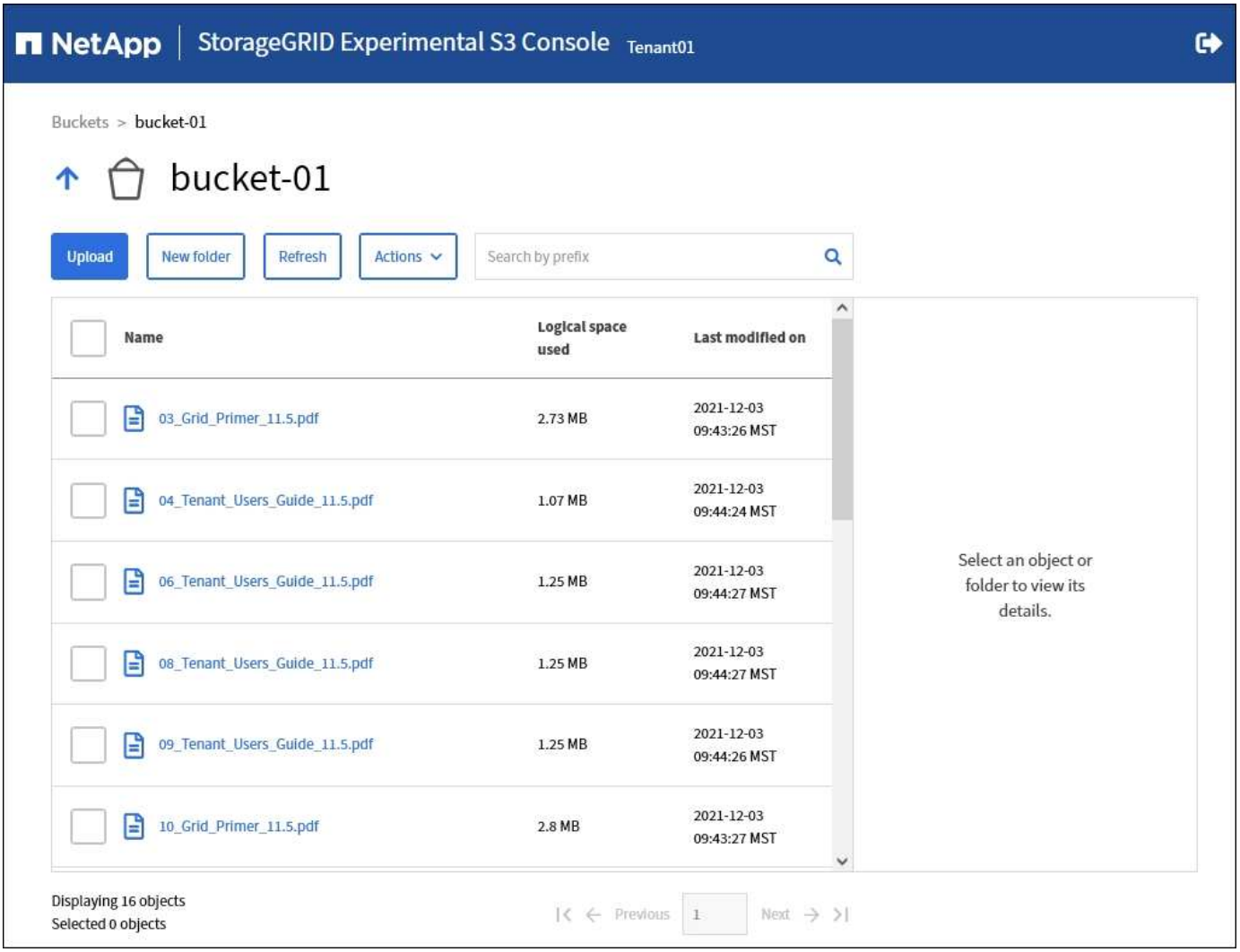
> La console S3 n'a pas été complètement testée et est marquée comme « expérimentale ». Il n'est pas destiné à la gestion en bloc des objets ou à une utilisation dans un environnement de production. Les locataires ne doivent utiliser la console S3 que lors de l'exécution de fonctions sur un petit nombre d'objets, par exemple lors du chargement d'objets pour simuler une nouvelle règle ILM, pour résoudre les problèmes d'ingestion ou via des grilles de validation technique ou non-production.

Ce dont vous avez besoin

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous disposez de l'autorisation gérer vos propres informations d'identification S3.
- Vous avez créé un compartiment.
- Vous connaissez l'ID de clé d'accès de l'utilisateur et la clé d'accès secrète. Si vous le souhaitez, vous avez un `.csv` fichier contenant ces informations. Voir la instructions pour la création de clés d'accès.

Étapes

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



Gérez les services de la plateforme S3

Qu’est-ce que les services de plateforme ?

Les services de plateforme StorageGRID peuvent vous aider à mettre en œuvre une stratégie de cloud hybride.

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

- **Réplication CloudMirror** : le Service de réplication StorageGRID CloudMirror Permet de mettre en miroir des objets spécifiques d’un compartiment StorageGRID vers une destination externe spécifiée.

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

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

- **Notifications**: Notifications d’événements par compartiment Sont utilisées pour envoyer des notifications sur des actions spécifiques effectuées sur des objets vers un service externe Amazon simple notification

Service™ (SNS) spécifié.

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

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

- **Service d'intégration de recherche** : service d'intégration de la recherche Elle permet d'envoyer des métadonnées d'objet S3 vers un index Elasticsearch spécifique où elles peuvent être recherchées ou analysées à l'aide du service externe.

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

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

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

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

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

Configuration des services de plate-forme

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

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

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

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

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

Service de plateforme	L'API REST S3
Réplication CloudMirror	• RÉPLICATION des compartiments • RÉPLICATION des compartiments
Notifications	• GET Bucket notification • PUT Bucket notification
Intégration de la recherche	• CONFIGURATION DES notifications de métadonnées de compartiment • CONFIGURATION de notification des métadonnées de compartiment Ces opérations sont personnalisées pour StorageGRID.

Pour plus d'informations sur l'implémentation de ces API par StorageGRID, consultez les instructions relatives à l'implémentation des applications client S3.

Informations associées

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

Utilisation de S3

Service de réplication CloudMirror

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

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

Si vous activez la réplication CloudMirror pour un compartiment existant, seuls les nouveaux objets ajoutés à ce compartiment sont répliqués. Tout objet existant dans le compartiment n'est pas répliqué. 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 les objets vers une destination AWS S3, notez qu'Amazon S3 limite la taille des métadonnées définies par l'utilisateur dans chaque en-tête de demande PUT à 2 Ko. Si un objet possède des métadonnées définies par l'utilisateur supérieures à 2 Ko, cet objet ne sera pas répliqué.

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

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

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

Lors de la réplication des objets dans le compartiment de destination, StorageGRID les désigne par « duplicaas ». Un compartiment StorageGRID de destination ne réplique pas les objets marqués comme répliques, ce qui vous protège des boucles de réplication accidentelles. Ce marquage de réplication est interne à StorageGRID et ne vous empêche pas d'utiliser AWS CRR lorsque vous utilisez un compartiment Amazon S3 comme destination.

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

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

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

Description des notifications pour les compartiments

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

C'est possible configurer les notifications d'événements En associant XML de configuration de notification à un compartiment source. Le XML de configuration de notification respecte les conventions S3 pour la configuration des notifications de compartiment, avec la rubrique SNS de destination spécifiée comme URN d'un terminal.

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

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

Notifications et messages pris en charge

La notification d'événements StorageGRID suit l'API Amazon S3 avec les limites suivantes :

- Vous ne pouvez pas configurer une notification pour les types d'événements suivants. Ces types d'événements sont **non** pris en charge.
  - `s3:ReducedRedundancyLostObject`
  - `s3:ObjectRestore:Completed`
- Les notifications d'événements envoyées par StorageGRID utilisent le format JSON standard, sauf qu'elles n'incluent pas certaines clés et utilisent des valeurs spécifiques pour les autres, comme illustré dans le tableau :

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

Comprendre le service d'intégration de la recherche

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

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

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

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

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

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

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

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

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

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

Informations associées

XML de configuration pour l'intégration de la recherche

Métadonnées d'objet incluses dans les notifications de métadonnées

JSON généré par le service d'intégration de la recherche

Configurez le service d'intégration de la recherche

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

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

Pour plus d'informations sur S3, reportez-vous à la section Utilisation de S3.

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

Réflexion	Détails
Surveillance des terminaux de destination	Vous devez surveiller la disponibilité de chaque point final de destination. Si la connexion au point final de destination est perdue pendant une période prolongée et qu'il existe un important retard de requêtes, les demandes client supplémentaires (telles QUE LES requêtes ENVOYÉES) à StorageGRID échoueront. Vous devez réessayer ces demandes ayant échoué lorsque le noeud final devient accessible.
Limitation du terminal de destination	Le logiciel StorageGRID peut canaliser les demandes S3 entrantes pour un compartiment si le taux d'envoi des demandes dépasse le taux à partir duquel le terminal de destination peut recevoir les demandes. La restriction ne se produit que lorsqu'il existe un arriéré de demandes en attente d'envoi vers le noeud final de destination. Le seul effet visible est que les requêtes S3 entrantes prennent plus de temps à s'exécuter. Si vous commencez à détecter les performances beaucoup plus lentes, vous devez réduire le taux d'entrée ou utiliser un terminal avec une capacité plus élevée. Si l'carnet de commandes des requêtes continue d'augmenter, les opérations S3 des clients (par EXEMPLE, LES requêtes PUT) finiront par échouer. Les demandes CloudMirror sont plus susceptibles d'être affectées par les performances du terminal de destination, car ces demandes impliquent généralement plus de transfert de données que les demandes d'intégration de recherche ou de notification d'événements.
Garanties de commande	StorageGRID garantit l'ordre des opérations sur un objet d'un site. Tant que toutes les opérations relatives à un objet se trouvent sur le même site, l'état final de l'objet (pour la réplication) sera toujours égal à l'état dans StorageGRID. StorageGRID tente également de commander des demandes lorsque des opérations sont effectuées sur des sites StorageGRID. Par exemple, si vous écrivez un objet initialement sur le site A, puis que vous le remplacez par un autre objet au niveau du site B, le dernier objet répliqué par CloudMirror vers le compartiment de destination n'est pas garanti que ce nouvel objet soit.
Suppressions d'objets basées sur des règles ILM	Pour faire correspondre le comportement de suppression des services CRR et SNS d'AWS, 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 ILM d'StorageGRID. Par exemple, aucune demande de notification de CloudMirror ou d'événement n'est envoyée si une règle ILM supprime un objet au bout de 14 jours. Au contraire, les demandes d'intégration de la recherche sont envoyées lorsque les objets sont supprimés du fait de ILM.

Considérations relatives à l'utilisation du service de réplication CloudMirror

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

Configurer les terminaux des services de plateforme

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

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

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

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

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

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

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

Terminaux pour la réplication CloudMirror

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

Terminaux pour les notifications

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

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

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

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

Informations associées

Administrer StorageGRID

Spécifiez l'URN du terminal des services de plateforme

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

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

Éléments DE RETOUR

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

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

Par exemple, si vous spécifiez l'URN pour un terminal CloudMirror hébergé sur StorageGRID, il peut commencer par l'URN `urn:sgws`.

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

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

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

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

Service	Ressource spécifique
Réplication CloudMirror	nom du compartiment
Notifications	nom-rubrique-sns

Service	Ressource spécifique
Intégration de la recherche	`domain-name/index-name/type-name` **Remarque :** si le cluster Elasticsearch est **NOT** configuré pour créer automatiquement des index, vous devez créer l'index manuellement avant de créer le noeud final.

Urns pour les services hébergés sur AWS et GCP

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

- Réplication CloudMirror :

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

- Notifications :

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

- Intégration de la recherche :

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

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

Urnes pour des services hébergés localement

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

- Réplication CloudMirror :

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

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

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

- Notifications :

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

- Intégration de la recherche :

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

> Pour les points de terminaison d'intégration de recherche hébergés localement, le `domain-name` L'élément peut être n'importe quelle chaîne tant que l'URN du terminal est unique.

Créer un terminal de services de plate-forme

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

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Les services de plateforme doivent être activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous devez appartenir à un groupe d'utilisateurs possédant l'autorisation gérer les noeuds finaux.
- La ressource référencée par le point final des services de plate-forme doit avoir été créée :
  - Réplication CloudMirror : compartiment S3
  - Notification d'événement : rubrique SNS
  - Notification de recherche : index Elasticsearch, si le cluster de destination n'est pas configuré pour créer automatiquement des index.
- Vous devez disposer des informations relatives à la ressource de destination :
  - Hôte et port pour l'URI (Uniform Resource identifier)

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

  - Nom de ressource unique (URN)

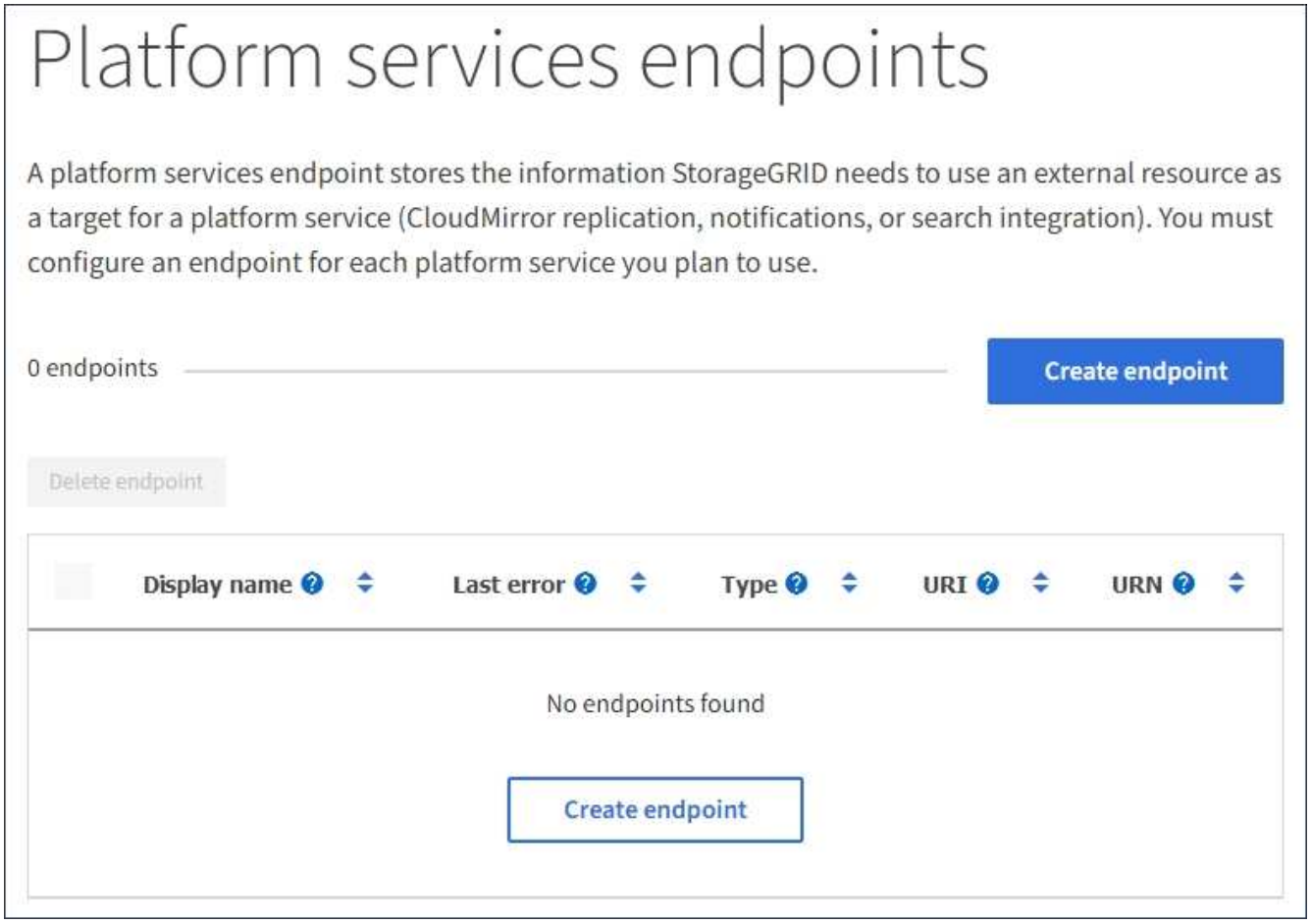
    Spécifiez l'URN du terminal des services de plateforme

  - Informations d'authentification (si nécessaire) :
    - Clé d'accès : ID de clé d'accès et clé d'accès secrète
    - HTTP de base : nom d'utilisateur et mot de passe
    - CAP (C2S Access Portal) : URL d'informations d'identification temporaires, certificats de serveur et de client, clés client et phrase de passe de clé privée de client facultative.
  - Certificat de sécurité (en cas d'utilisation d'un certificat d'autorité de certification personnalisé)

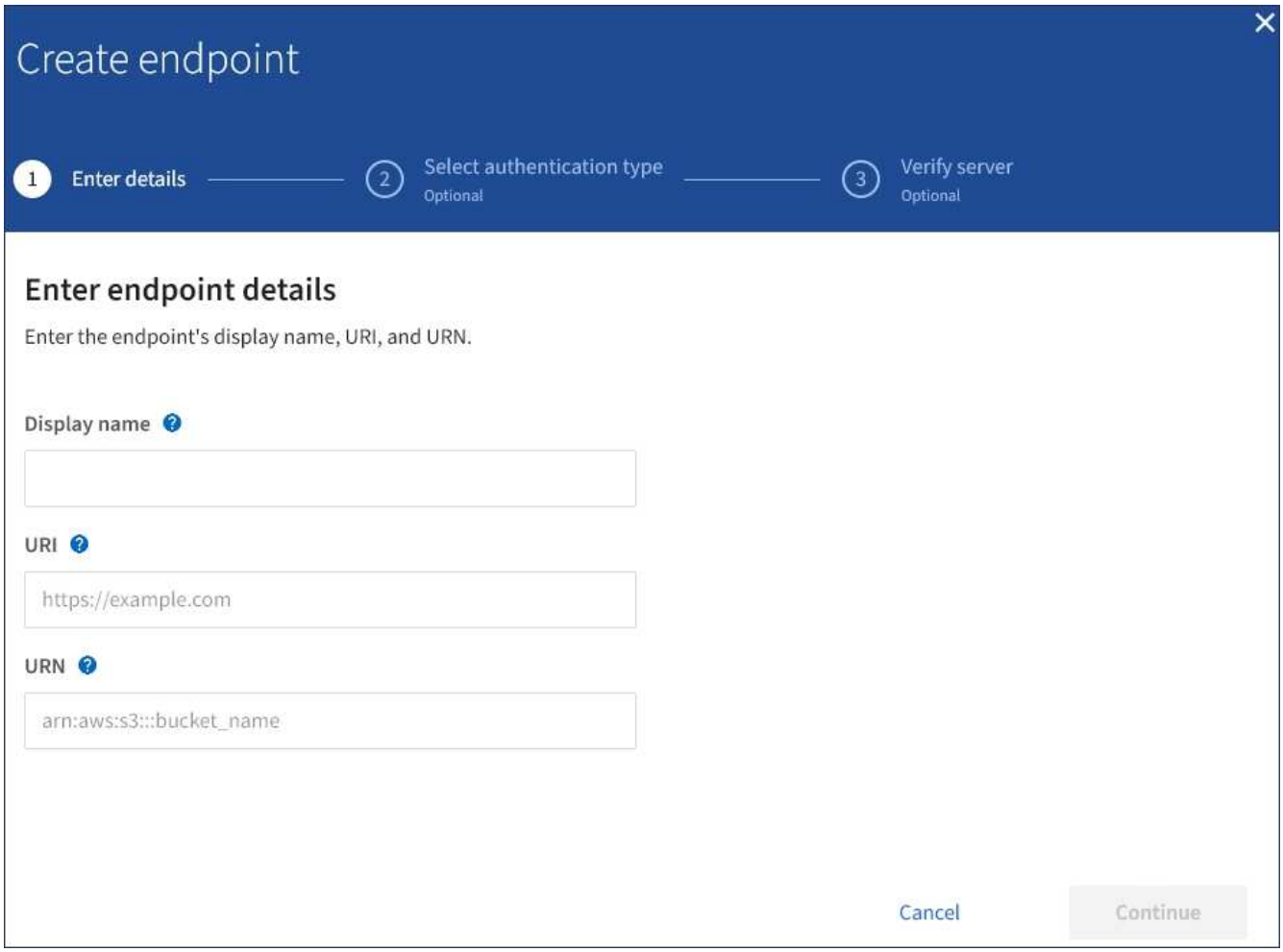
Étapes

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

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



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



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

   Le type de service de plate-forme pris en charge par le noeud final s'affiche en regard du nom du noeud final lorsqu'il est répertorié sur la page noeuds finaux. Vous n'avez donc pas besoin d'inclure ces informations dans le nom.

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

   Utilisez l'un des formats suivants :

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

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

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

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

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

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

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

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

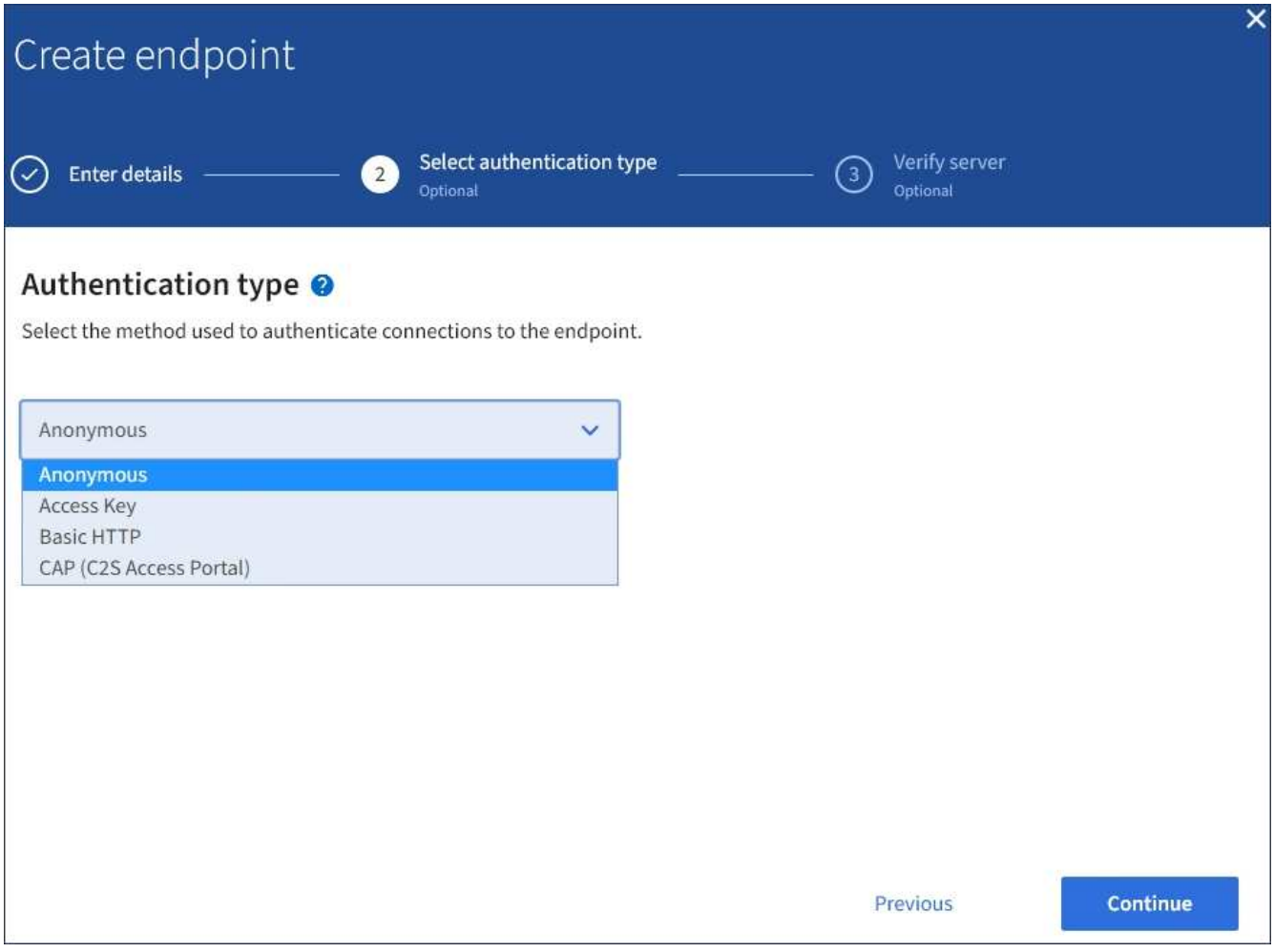
```
https://s3-aws-region.amazonaws.com
```

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

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

> Vous ne pouvez pas modifier l'URN d'un terminal après sa création.

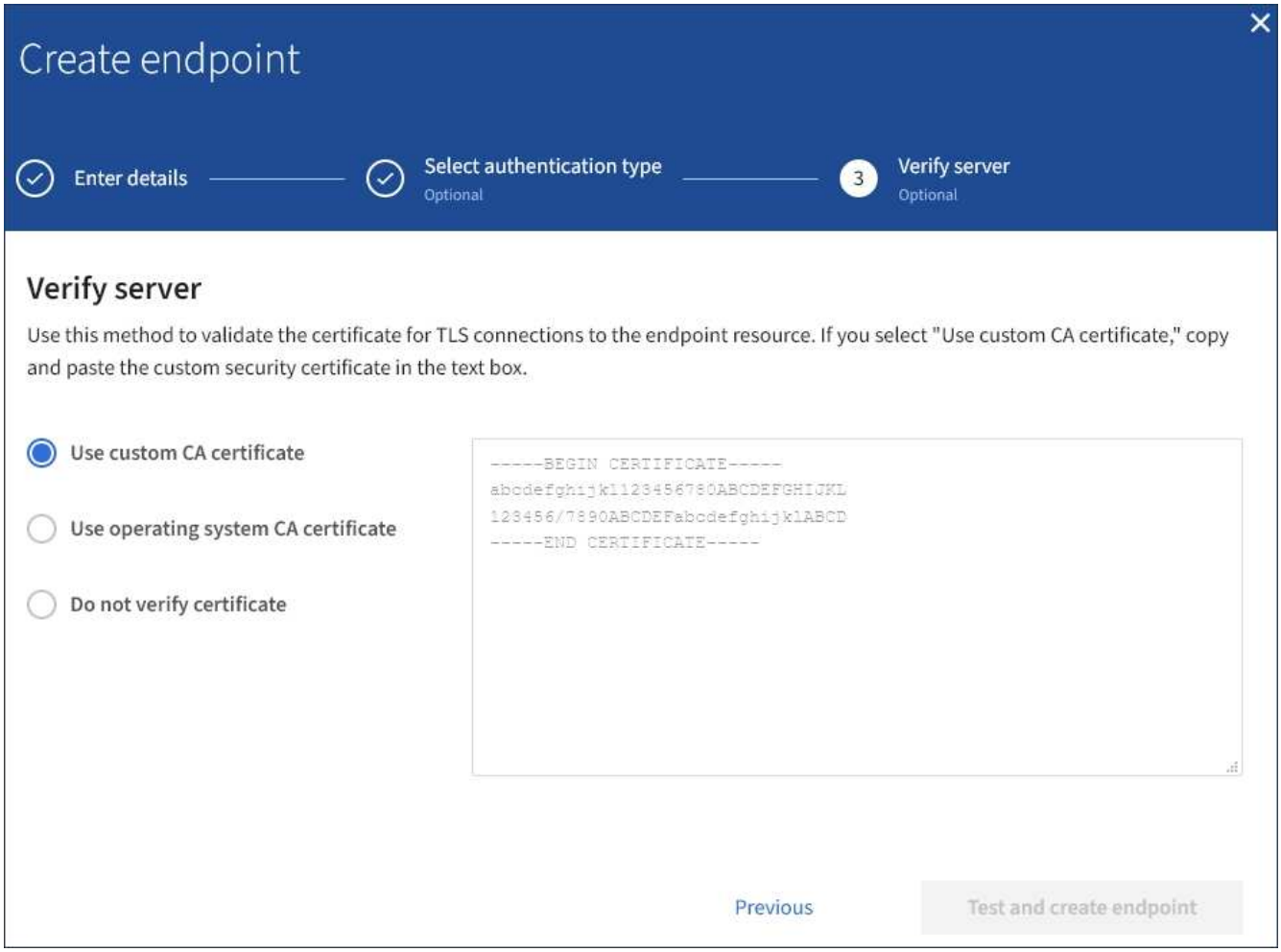
6. Sélectionnez **Continuer**.
7. Sélectionnez une valeur pour **Type d'authentification**, puis saisissez ou téléchargez les informations d'identification requises.



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

Type d'authentification	Description	Informations d'identification
Anonyme	Fournit un accès anonyme à la destination. Fonctionne uniquement pour les terminaux dont la sécurité est désactivée.	Pas d'authentification.
Clé d'accès	Utilise des identifiants de style AWS pour authentifier les connexions avec la destination.	• ID de clé d'accès • Clé d'accès secrète
HTTP de base	Utilise un nom d'utilisateur et un mot de passe pour authentifier les connexions à la destination.	• Nom d'utilisateur • Mot de passe
CAP (portail d'accès C2S)	Utilise des certificats et des clés pour authentifier les connexions à la destination.	• URL des informations d'identification temporaires • Certificat autorité de certification du serveur (téléchargement de fichiers PEM) • Certificat client (téléchargement de fichier PEM) • Clé privée client (téléchargement de fichiers PEM, format crypté OpenSSL ou format de clé privée non crypté) • Phrase de passe de clé privée du client (facultatif)

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



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

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

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

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

Informations associées

Spécifiez l'URN du terminal des services de plateforme

Configurez la réplication CloudMirror

Configurer les notifications d'événements

Configurez le service d'intégration de la recherche

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

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

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs possédant l'autorisation gérer les noeuds finaux.

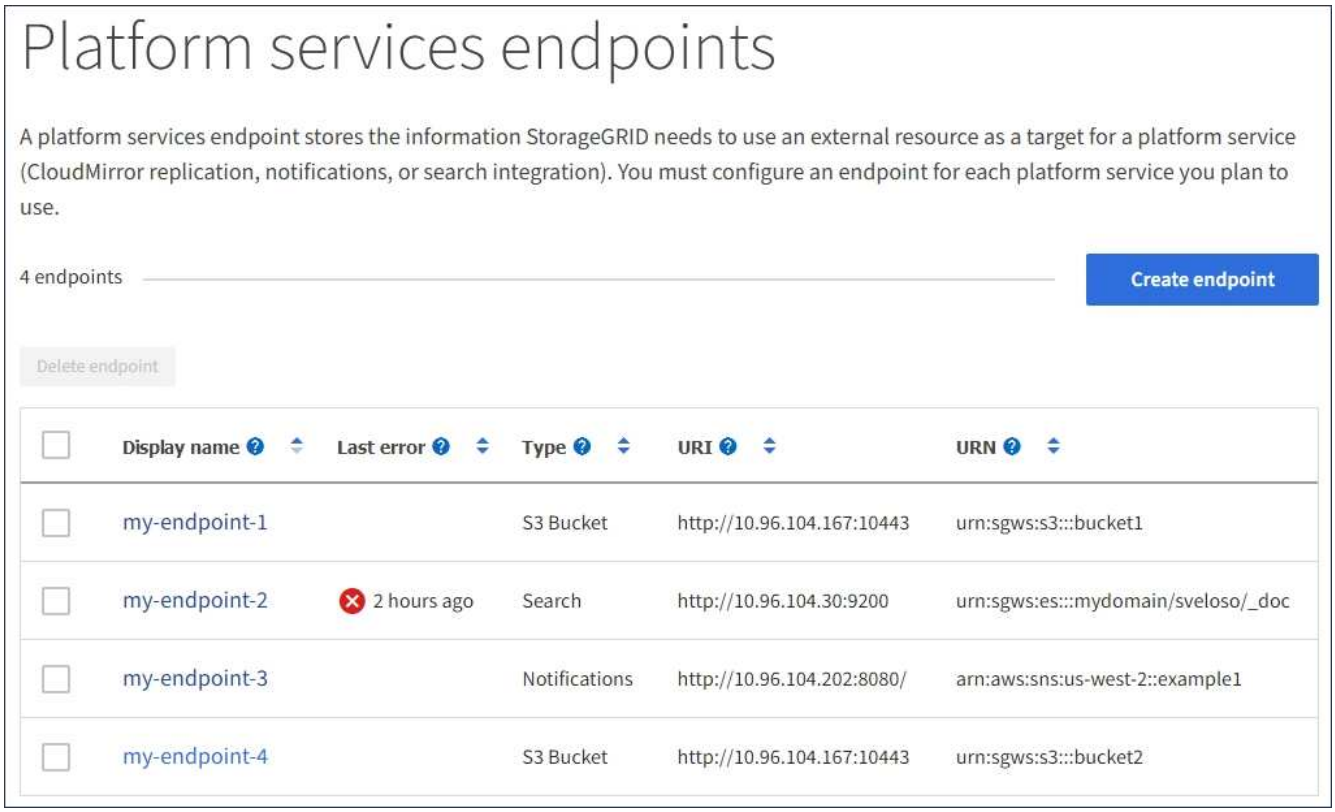
Description de la tâche

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

Étapes

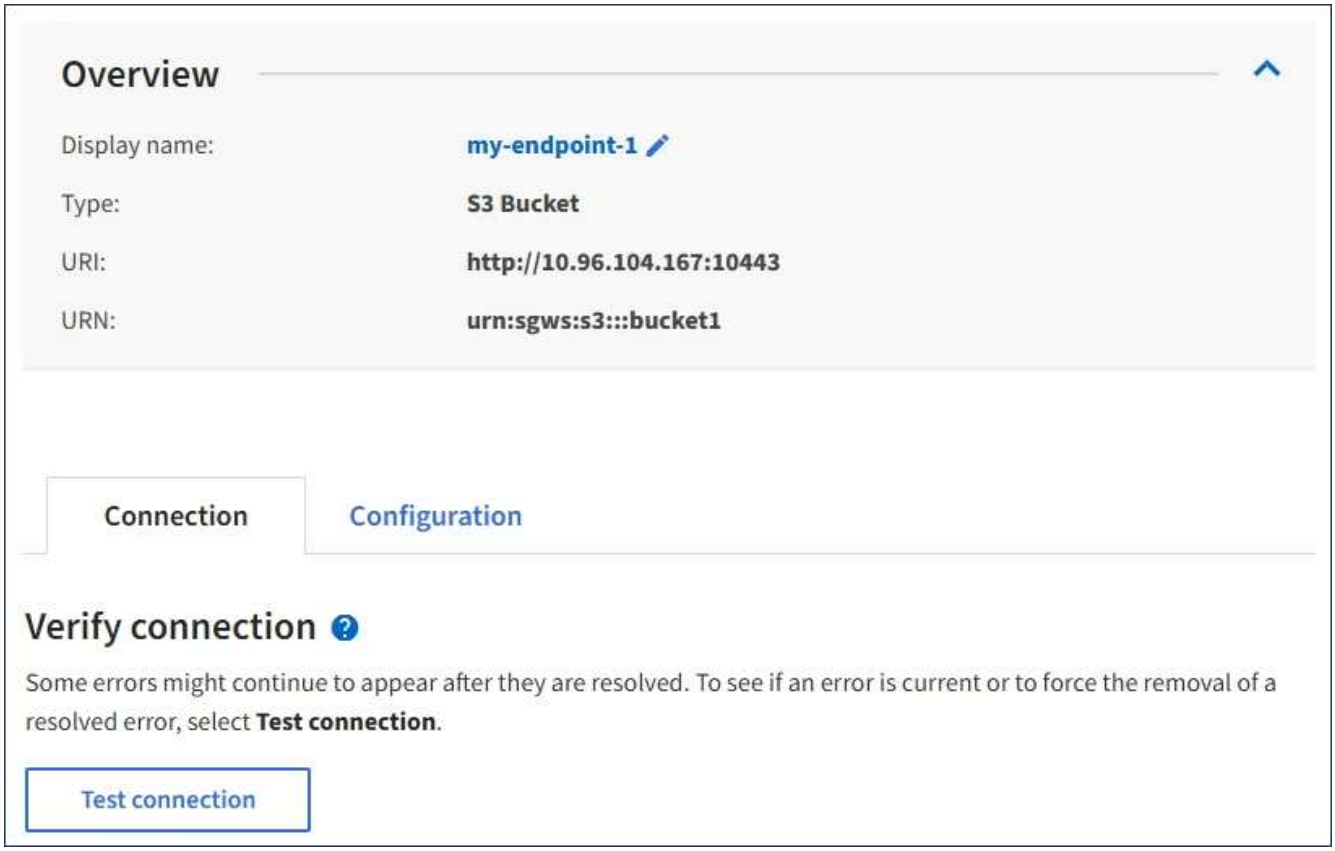
1. Sélectionnez **STORAGE (S3) Platform services Endpoints**.

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



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

   La page des détails du point final s'affiche.



3. Sélectionnez **Tester la connexion**.

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

Modifier le point final des services de plate-forme

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

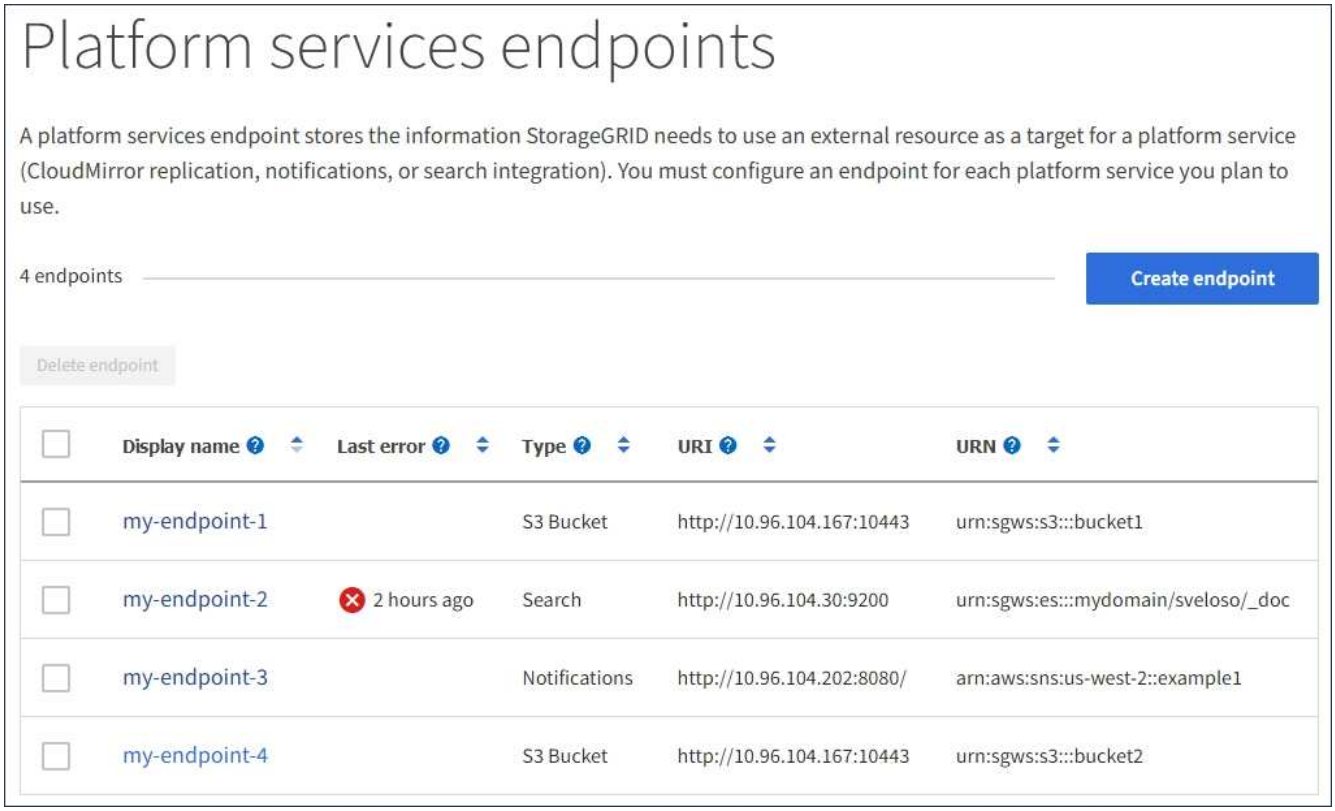
Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs possédant l'autorisation gérer les noeuds finaux. Voir Autorisations de gestion des locataires.

Étapes

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

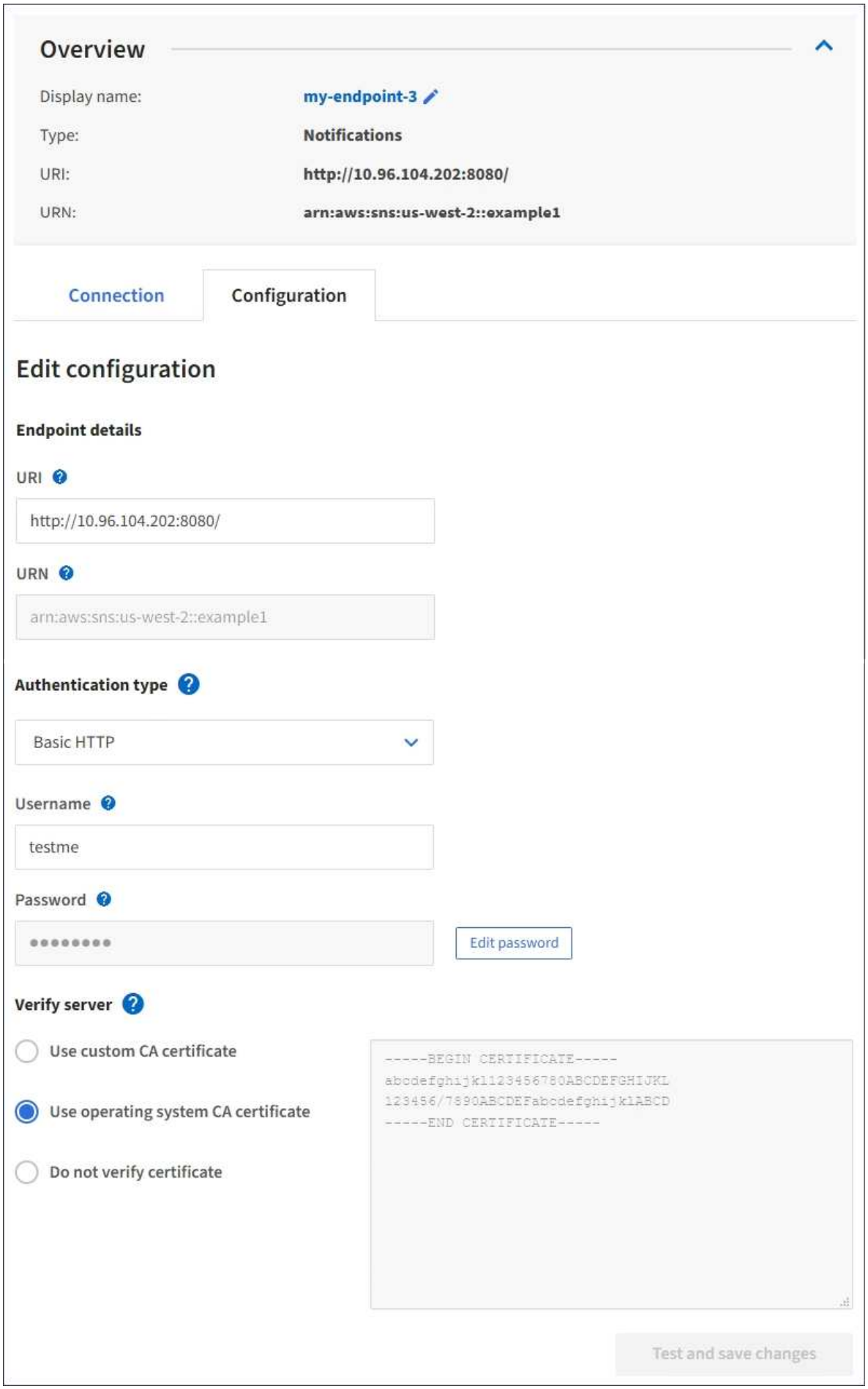
   La page noeuds finaux des services de plate-forme s'affiche et affiche la liste des noeuds finaux des services de plate-forme déjà configurés.



2. Sélectionnez le point final que vous souhaitez modifier.

   La page des détails du point final s'affiche.

3. Sélectionnez **Configuration**.


Overview
Display name:
my-endpoint-3
Type:
Notifications
URI:
http://10.96.104.202:8080/
URN:
arn:aws:sns:us-west-2::example1
Connection
Configuration
Edit configuration
Endpoint details
URI
http://10.96.104.202:8080/
URN
arn:aws:sns:us-west-2::example1
Authentication type
Basic HTTP
Username
testme
Password
Edit password
Verify server
Use custom CA certificate
Use operating system CA certificate
Do not verify certificate
-----BEGIN CERTIFICATE-----
abcdefghijkl123456780ABCDEFGHIJKL
123456/7890ABCDEFabcdefghijklABCD
-----END CERTIFICATE-----
Test and save changes

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

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

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

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

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

Supprimer le noeud final des services de plate-forme

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

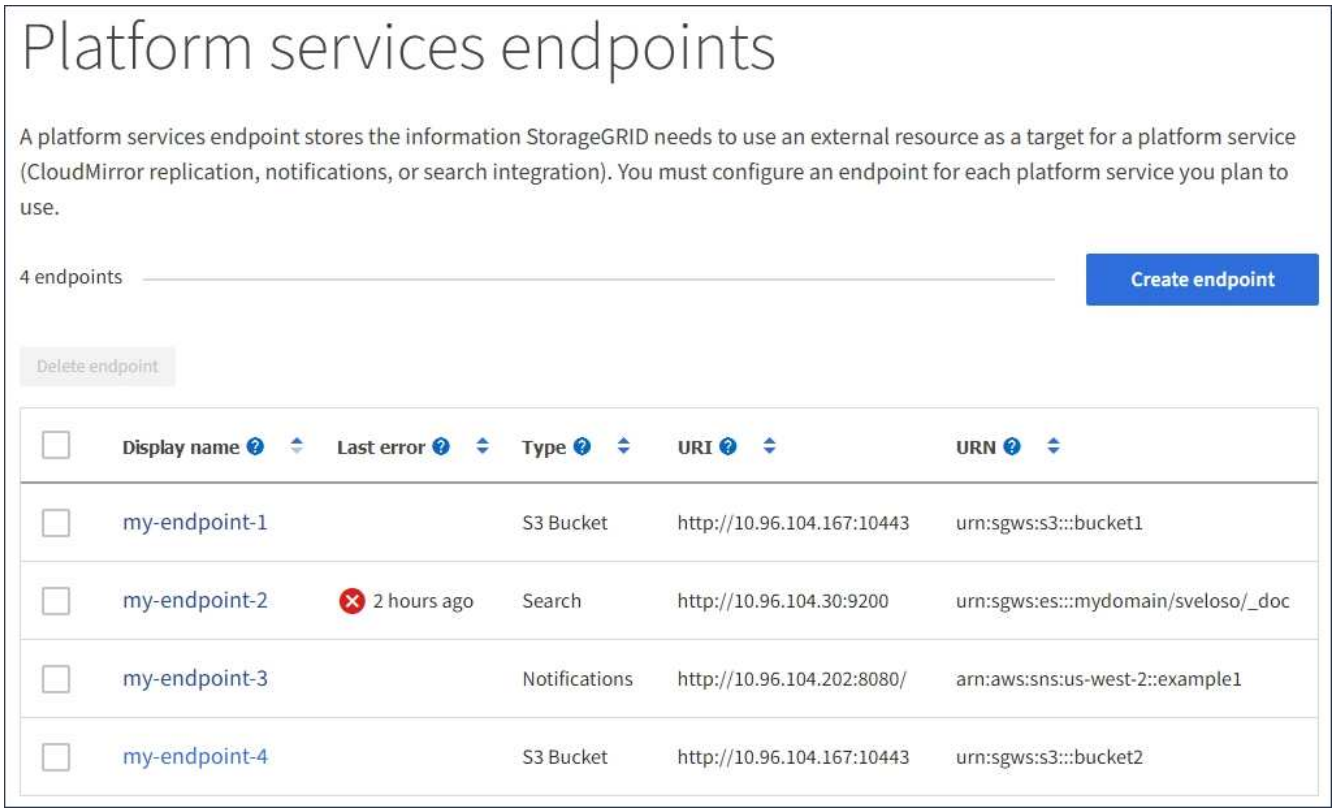
Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs qui dispose de l'autorisation **gérer les noeuds finaux** . Voir Autorisations de gestion des locataires.

Étapes

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

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

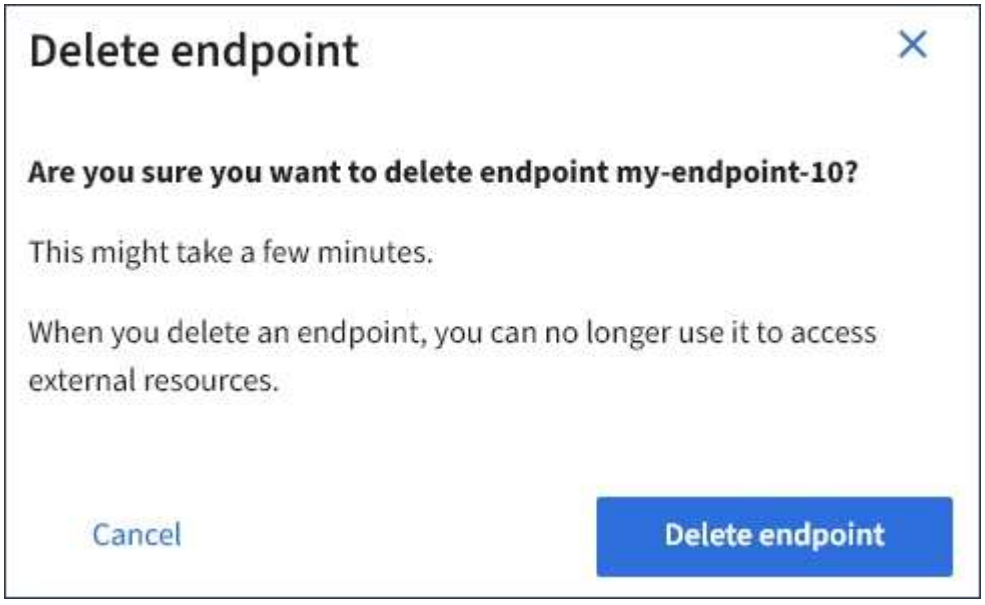


2. Cochez la case correspondant à chaque noeud final que vous souhaitez supprimer.

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

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

   Un message de confirmation s'affiche.



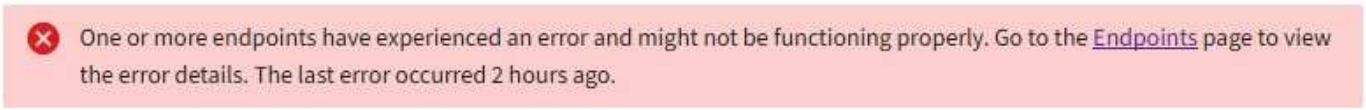
4. Sélectionnez **Supprimer le point final**.

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

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

Déterminez si l'erreur s'est produite

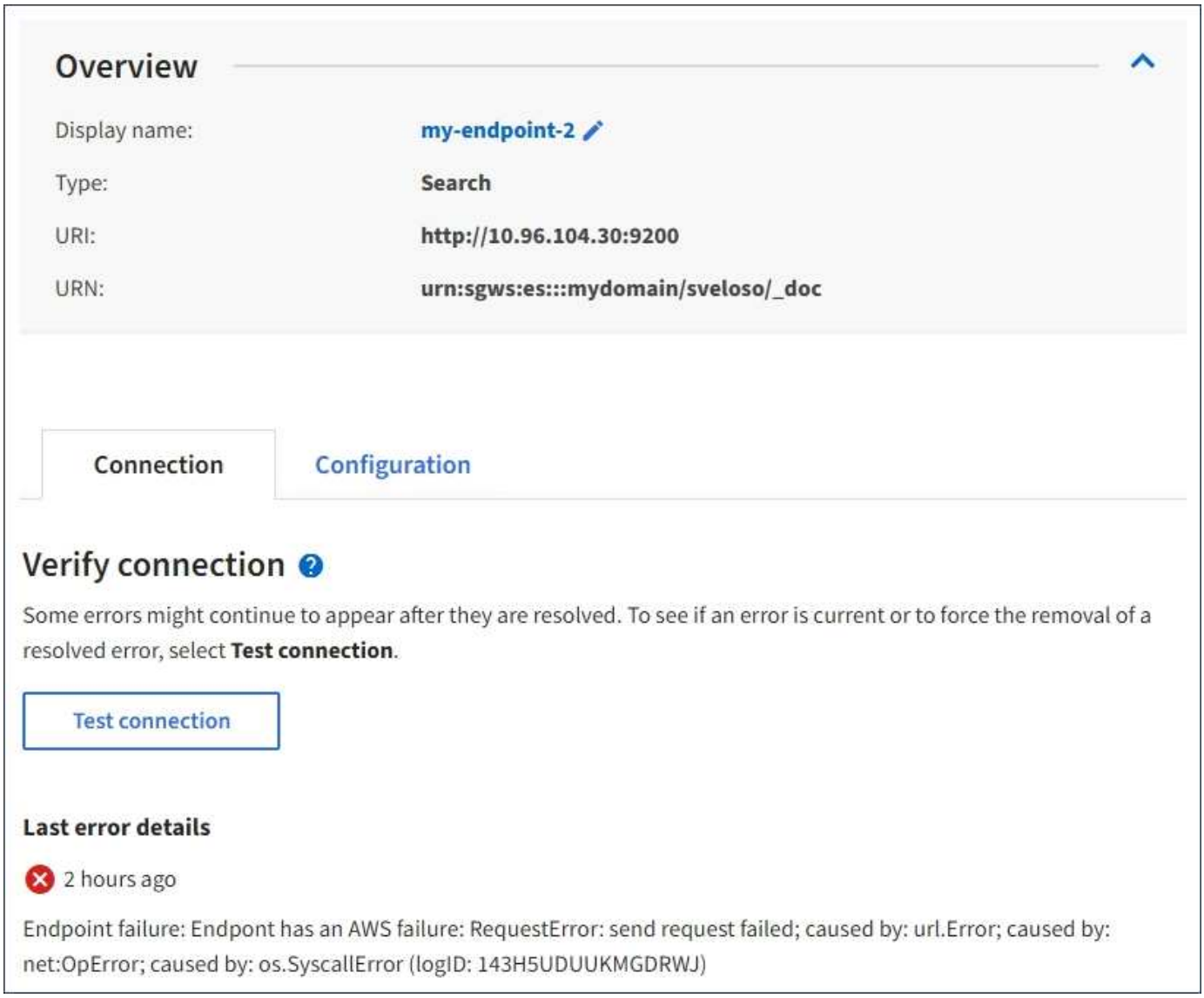
Si des erreurs de point de terminaison des services de plateforme se sont produites au cours des 7 derniers jours, le tableau de bord du gestionnaire des locataires affiche un message d'alerte. Vous pouvez accéder à la page noeuds finaux des services de plate-forme pour obtenir plus de détails sur l'erreur.



La même erreur qui s'affiche sur le tableau de bord s'affiche également en haut de la page noeuds finaux des services de plate-forme. Pour afficher un message d'erreur plus détaillé :

Étapes

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



Vérifiez si l'erreur est toujours à jour

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

Étapes

1. Sélectionnez l'extrémité.

   La page des détails du point final s'affiche.

2. Sélectionnez **connexion Test connexion**.

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

Résoudre les erreurs de point final

Vous pouvez utiliser le message **dernière erreur** sur la page des détails du noeud final pour déterminer ce qui est à l'origine de l'erreur. Certaines erreurs peuvent vous obliger à modifier le noeud final pour résoudre le problème. Par exemple, une erreur CloudMirroring peut se produire si StorageGRID ne parvient pas à accéder

au compartiment S3 de destination, car il ne dispose pas des autorisations d'accès correctes ou si la clé d'accès a expiré. Le message est ""les identifiants de point de terminaison ou l'accès de destination doivent être mis à jour", et les détails sont "AccessDenied" ou "InvalidAccessKeyId."".

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

Étapes

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

Identifiants de point de terminaison avec autorisations insuffisantes

Lorsque StorageGRID valide un terminal de services de plateforme, il confirme que les identifiants du terminal peuvent être utilisés pour contacter la ressource de destination et il vérifie les autorisations de base. Cependant, StorageGRID ne valide pas toutes les autorisations requises pour certaines opérations de services de plateforme. Pour cette raison, si vous recevez une erreur lors de la tentative d'utilisation d'un service de plate-forme (par exemple « 403 interdit »), vérifiez les autorisations associées aux identifiants du noeud final.

Dépannage des services de plateforme supplémentaires

Pour plus d'informations sur le dépannage des services de plate-forme, reportez-vous aux instructions d'administration de StorageGRID.

Administrer StorageGRID

Informations associées

Créer un terminal de services de plate-forme

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

Modifier le point final des services de plate-forme

Configurez la réplication CloudMirror

Le Service de réplication CloudMirror Est l'un des trois services de plateforme StorageGRID. Vous pouvez utiliser la réplication CloudMirror pour répliquer automatiquement les objets dans un compartiment S3 externe.

Ce dont vous avez besoin

- Les services de plateforme doivent être activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous devez avoir déjà créé un compartiment pour agir en tant que source de réplication.
- Le terminal que vous prévoyez d'utiliser comme destination pour la réplication CloudMirror doit déjà exister, et vous devez disposer de son URN.
- Vous devez appartenir à un groupe d'utilisateurs disposant de l'autorisation gérer toutes les rubriques ou accès racine, ce qui vous permet de gérer les paramètres de tous les compartiments S3 de votre compte

locataire. Ces autorisations remplacent les paramètres d'autorisation des stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Gestionnaire de locataires.

Description de la tâche

La réplication CloudMirror copie les objets à partir d'un compartiment source vers un compartiment de destination spécifié dans un terminal. Pour activer la réplication CloudMirror pour un compartiment, vous devez créer et appliquer un fichier XML de configuration de réplication de compartiment valide. Le XML de configuration de réplication doit utiliser l'URN d'un terminal de compartiment S3 pour chaque destination.

> La réplication n'est pas prise en charge pour les compartiments source ou de destination lorsque le verrouillage d'objet S3 est activé.

Pour des informations générales sur la réplication des compartiments et sur la configuration de cette réplication, consultez la documentation Amazon simple Storage Service (S3) sur la réplication inter-région (CRR). Pour plus d'informations sur la StorageGRID mise en œuvre de l'API de configuration de réplication des compartiments S3, consultez le Instructions d'implémentation des applications client S3.

Si vous activez la réplication CloudMirror sur un compartiment qui contient des objets, les nouveaux objets ajoutés au compartiment sont répliqués, mais les objets existants dans le compartiment ne le sont pas. Vous devez mettre à jour des objets existants pour déclencher la réplication.

Si vous spécifiez une classe de stockage dans le fichier XML de configuration de réplication, StorageGRID utilise cette classe lors des opérations sur le terminal S3 de destination. Le noeud final de destination doit également prendre en charge la classe de stockage spécifiée. Veillez à suivre les recommandations fournies par le fournisseur du système de destination.

Étapes

1. Activer la réplication pour le compartiment source :

   Utilisez un éditeur de texte pour créer le XML de configuration de réplication requis pour activer la réplication, comme spécifié dans l'API de réplication S3. Lors de la configuration du XML :

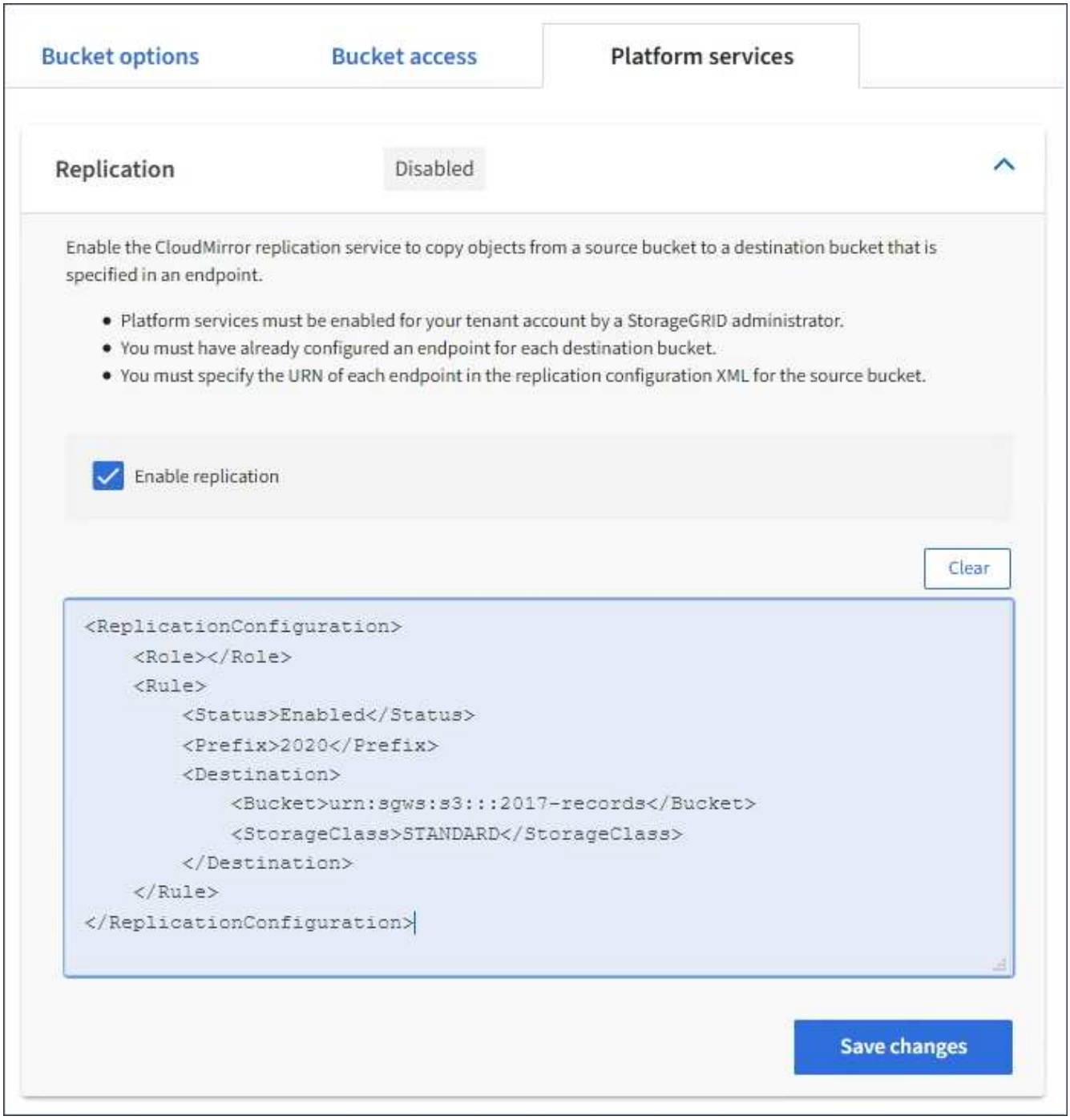
   - Notez que StorageGRID ne prend en charge que le V1 de la configuration de la réplication. Cela signifie que StorageGRID ne prend pas en charge l'utilisation de `Filter` Elément pour les règles, et suit les conventions V1 pour la suppression des versions d'objet. Pour plus d'informations, reportez-vous à la documentation Amazon sur la configuration de la réplication.
   - Utiliser l'URN d'un terminal du compartiment S3 comme destination.
   - Vous pouvez éventuellement ajouter le `<StorageClass>` et spécifiez l'un des éléments suivants :
     - `STANDARD`: La classe de stockage par défaut. Si vous ne spécifiez pas de classe de stockage lors du chargement d'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 vous accédez moins fréquemment, mais qui exige toujours un accès rapide lorsque cela est nécessaire.
     - `REDUCED_REDUNDANCY`: Utilisez cette classe de stockage pour les données non stratégiques reproductibles qui peuvent être stockées avec moins de redondance que le `STANDARD` classe de stockage.
   - Si vous spécifiez un `Role` Dans le XML de configuration, il sera ignoré. Cette valeur n'est pas utilisée par StorageGRID.

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

2. Dans le Gestionnaire de locataires, sélectionnez **STORAGE (S3) seaux**.
3. Sélectionnez le nom du compartiment source.

   La page des détails du compartiment s'affiche.

4. Sélectionnez **Platform Services Replication**.
5. Cochez la case **Activer la réplication**.
6. Collez le XML de configuration de réplication dans la zone de texte et sélectionnez **Enregistrer les modifications**.



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

7. Vérifiez que la réplication est configurée correctement :
   a. Ajoutez un objet au compartiment source qui répond aux exigences de réplication telles que spécifiées dans la configuration de la réplication.

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

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

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

Informations associées

Utilisation de S3

Créer un terminal de services de plate-forme

Configurer les notifications d'événements

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

Ce dont vous avez besoin

- Les services de plateforme doivent être activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous devez avoir déjà créé un compartiment pour faire office de source de notifications.
- Le terminal que vous prévoyez d'utiliser comme destination pour les notifications d'événements doit déjà exister et vous devez disposer de son URN.
- Vous devez appartenir à un groupe d'utilisateurs disposant de l'autorisation gérer toutes les rubriques ou accès racine, ce qui vous permet de gérer les paramètres de tous les compartiments S3 de votre compte locataire. Ces autorisations remplacent les paramètres d'autorisation des stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Gestionnaire de locataires.

Description de la tâche

Après avoir configuré les notifications d'événements, chaque fois qu'un événement spécifié se produit pour un objet dans le compartiment source, une notification est générée et envoyée à la rubrique SNS (simple notification Service) utilisée comme point final de destination. Pour activer les notifications pour un compartiment, vous devez créer et appliquer un XML de configuration de notification valide. Le XML de configuration de notification doit utiliser l'URN d'un terminal de notification d'événement pour chaque destination.

Pour obtenir des informations générales sur les notifications d'événements et leur configuration, consultez la documentation Amazon. Pour plus d'informations sur la façon dont StorageGRID implémente l'API de notification des compartiments S3, consultez les instructions pour l'implémentation des applications client S3.

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

Étapes

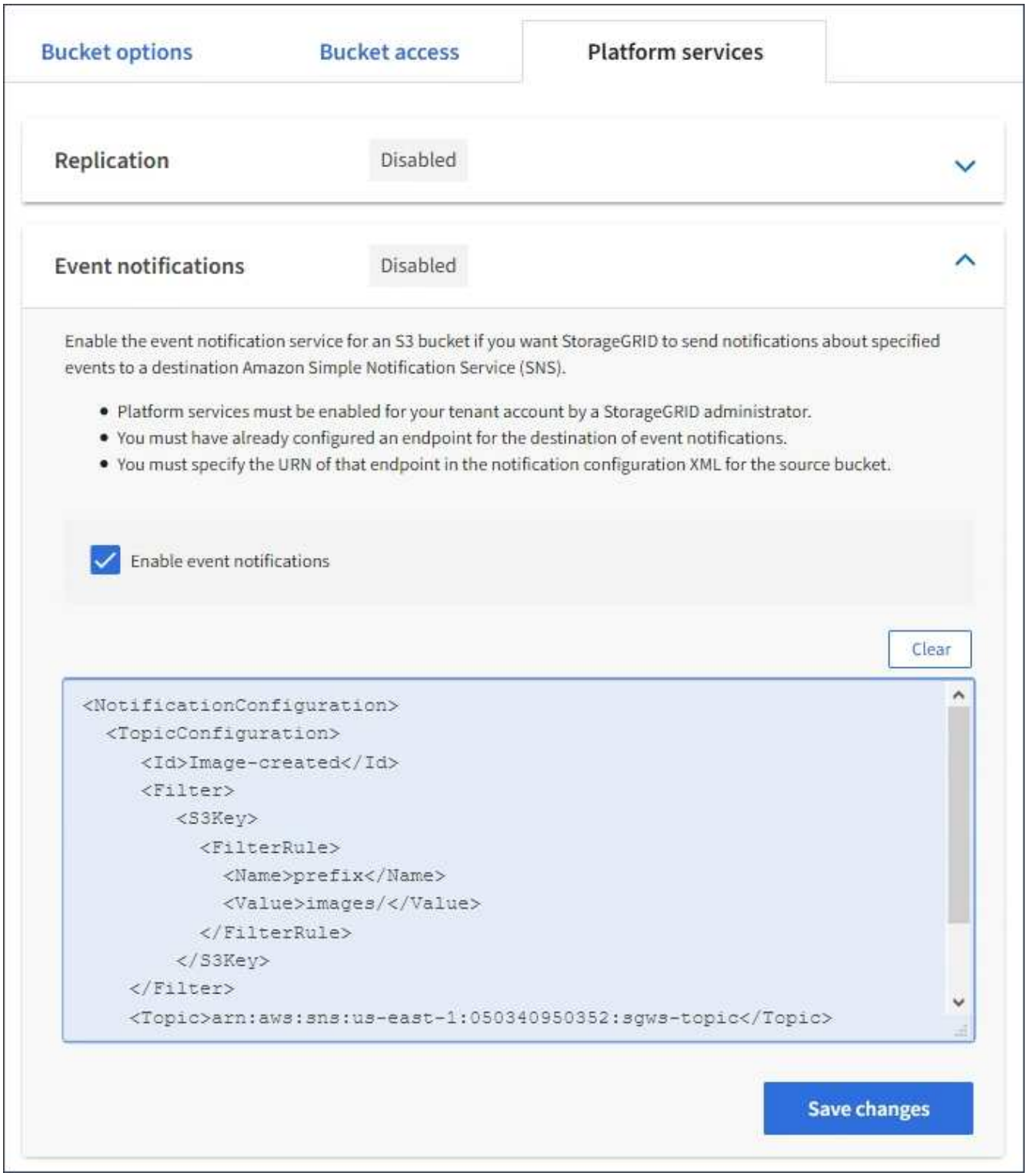
1. Activer les notifications pour le compartiment source :
   - Utilisez un éditeur de texte pour créer le XML de configuration de notification requis pour activer les notifications d'événement, comme spécifié dans l'API de notification S3.
   - Lors de la configuration du XML, utilisez l'URN d'un terminal de notification d'événements comme sujet de destination.

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. Dans le Gestionnaire de locataires, sélectionnez **STORAGE (S3) seaux**.
3. Sélectionnez le nom du compartiment source.

   La page des détails du compartiment s'affiche.

4. Sélectionnez **Platform Services Event Notifications**.
5. Cochez la case **Activer les notifications d'événement**.
6. Collez le XML de configuration de notification dans la zone de texte, puis sélectionnez **Enregistrer les modifications**.



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

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

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

Dans l'exemple, une notification d'événement est envoyée chaque fois qu'un objet est créé avec le `images/` préfixe.

b. Confirmez qu'une notification a été envoyée à la rubrique SNS de destination.

Par exemple, si le sujet de votre destination est hébergé sur le service SNS (simple notification Service) d'AWS, vous pouvez configurer le service pour vous envoyer un e-mail une fois la notification envoyée.


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

Si la notification est reçue dans la rubrique de destination, vous avez configuré votre compartiment source pour les notifications StorageGRID.

Informations associées

Description des notifications pour les compartiments

Utilisation de S3

Créer un terminal de services de plate-forme

Utilisez le service d'intégration de la recherche

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

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

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

Voir la Instructions d'implémentation des applications client S3 Pour plus d'informations sur les opérations d'API REST personnalisées suivantes de StorageGRID S3 :

- SUPPRIME la demande de configuration de notification des métadonnées de compartiment
- LIRE la demande de configuration de notification des métadonnées de compartiment
- PUT Bucket metadata notification configuration

Informations associées

XML de configuration pour l'intégration de la recherche

Métadonnées d'objet incluses dans les notifications de métadonnées

JSON généré par le service d'intégration de la recherche

Configurez le service d'intégration de la recherche

Utilisation de S3

XML de configuration pour l'intégration de la recherche

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

Les objets peuvent être filtrés sur le préfixe du nom de l'objet. Par exemple, vous pouvez envoyer les métadonnées pour les objets avec le préfixe `images` à une destination et aux métadonnées pour les objets avec le préfixe `videos` à un autre. Les configurations dont les préfixes se chevauchent ne sont pas valides et sont rejetées lors de leur envoi. Par exemple, une configuration qui inclut une règle pour les objets avec le préfixe `test` et une seconde règle pour les objets avec le préfixe `test2` n'est pas autorisé.

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

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

Le tableau décrit les éléments du XML de configuration de notification des métadonnées.

Nom	Description	Obligatoire
Configuration de la MetadaNotificationConfiguration	Balise de conteneur pour les règles utilisées pour spécifier les objets et la destination des notifications de métadonnées. Contient un ou plusieurs éléments de règle.	Oui.
Règle	Balise de conteneur d'une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié. Les règles avec des préfixes qui se chevauchent sont rejetées. Inclus dans l'élément MetadaNotificationConfiguration.	Oui.

Nom	Description	Obligatoire
ID	Identifiant unique de la règle. Inclus dans l'élément règle.	Non
État	L'état peut être « activé » ou « désactivé ». Aucune action n'est prise pour les règles désactivées. Inclus dans l'élément règle.	Oui.
Préfixe	Les objets qui correspondent au préfixe sont affectés par la règle et leurs métadonnées sont envoyées à la destination spécifiée. Pour faire correspondre tous les objets, spécifiez un préfixe vide. Inclus dans l'élément règle.	Oui.
Destination	Balise de conteneur pour la destination d'une règle. Inclus dans l'élément règle.	Oui.
Urne	URN de la destination où les métadonnées d'objet sont envoyées. Doit être l'URN d'un terminal StorageGRID avec les propriétés suivantes : • `es` doit être le troisième élément. • L'URN doit se terminer par l'index et le type où les métadonnées sont stockées, sous la forme `domain-name/myindex/mytype`. Les terminaux sont configurés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Ils se présentent sous la forme suivante : • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` Le noeud final doit être configuré avant la soumission du XML de configuration, ou la configuration échouera avec une erreur 404. L'URNE est incluse dans l'élément destination.	Oui.

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

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

Dans cet exemple, les métadonnées d'objet de tous les objets sont envoyées vers la même destination.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Configuration des notifications de métadonnées avec deux règles

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

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Informations associées

Utilisation de S3

Métadonnées d'objet incluses dans les notifications de métadonnées

JSON généré par le service d'intégration de la recherche

Configurez le service d'intégration de la recherche

Configurer le service d'intégration de la recherche

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

Ce dont vous avez besoin

- Les services de plateforme doivent être activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous devez avoir déjà créé un compartiment S3 dont vous souhaitez indexer le contenu.
- Le terminal que vous prévoyez d'utiliser comme destination pour le service d'intégration de la recherche doit déjà exister et vous devez disposer de son URN.
- Vous devez appartenir à un groupe d'utilisateurs disposant de l'autorisation gérer toutes les rubriques ou accès racine, ce qui vous permet de gérer les paramètres de tous les compartiments S3 de votre compte locataire. Ces autorisations remplacent les paramètres d'autorisation des stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Gestionnaire de locataires.

Description de la tâche

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

Étapes

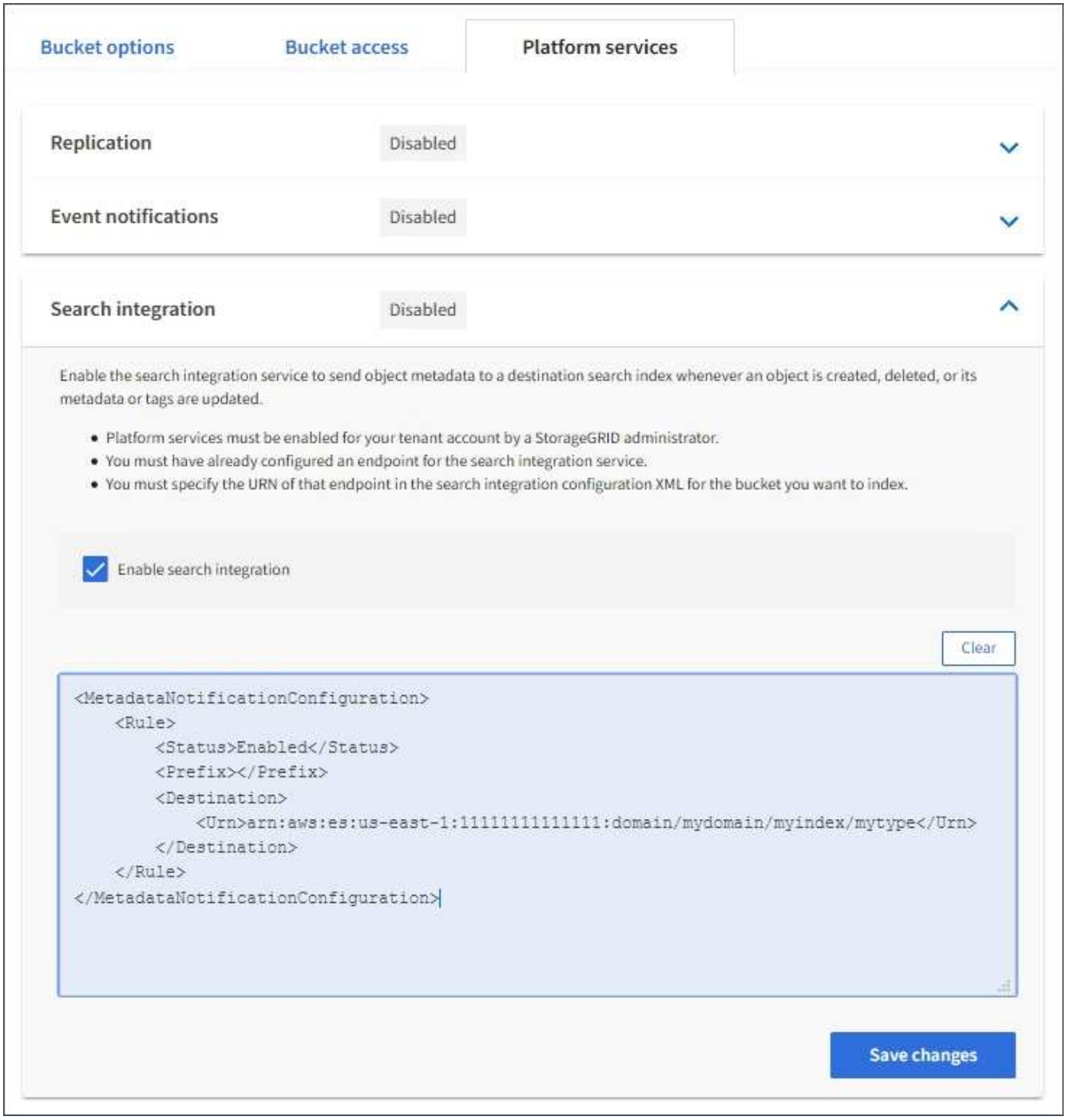
1. Utilisez un éditeur de texte pour créer le XML de notification de métadonnées requis pour activer l'intégration de la recherche.
   - Voir les informations sur le XML de configuration pour l'intégration de la recherche.
   - Lors de la configuration du XML, utilisez l'URN d'un noeud final d'intégration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

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>arn:aws:es:us-east-
1:11111111111111:domain/mydomain/myindex/mytype</Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

2. Dans le Gestionnaire de locataires, sélectionnez **STORAGE (S3) seaux**.
3. Sélectionnez le nom du compartiment source.

   La page des détails du compartiment s'affiche.

4. Sélectionnez **Platform Services Search Integration**
5. Cochez la case **Activer l'intégration de la recherche**.
6. Collez la configuration de notification de métadonnées dans la zone de texte, puis sélectionnez **Enregistrer les modifications**.



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

7. Vérifiez que le service d'intégration de la recherche est configuré correctement :
   a. Ajoutez un objet au compartiment source qui répond aux exigences relatives au déclenchement d'une notification de métadonnées comme spécifié dans le XML de configuration.

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

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

Une fois que vous avez terminé

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

- Sélectionner **STORAGE (S3) seaux** et désélectionner la case à cocher **Activer l'intégration de recherche**.
- Si vous utilisez directement l'API S3, utilisez une demande de notification DE suppression des métadonnées du compartiment. Pour plus d'informations sur l'implémentation des applications client S3, reportez-vous aux instructions.

Informations associées

Comprendre le service d'intégration de la recherche

XML de configuration pour l'intégration de la recherche

Utilisation de S3

Créer un terminal de services de plate-forme

JSON généré par le service d'intégration de la recherche

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

Cet exemple montre un exemple de fichier JSON qui peut être généré lorsqu'un objet doté de la clé est associé `SGWS/Tagging.txt` est créé dans un compartiment nommé `test`. Le `test` le compartiment n'est pas multiversion `versionId` l'étiquette est vide.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1"
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Métadonnées d'objet incluses dans les notifications de métadonnées

Le tableau répertorie tous les champs inclus dans le document JSON qui est envoyé au noeud final de destination lorsque l'intégration de la recherche est activée.

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

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

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