Administrer StorageGRID

StorageGRID software

NetApp
December 03, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/storagegrid-119/admin/index.html on December 03, 2025. Always check docs.netapp.com for the latest.

Sommaire

Administrer StorageGRID . . . 1
- Administrer StorageGRID . . . 1
  - À propos de ces instructions . . . 1
  - Avant de commencer . . . 1
- Démarrer avec Grid Manager . . . 1
  - Configuration requise pour le navigateur Web . . . 1
  - Sign in au gestionnaire de grille . . . 2
  - Déconnectez-vous du gestionnaire de grille . . . 8
  - Changez votre mot de passe . . . 8
  - Afficher les informations de licence StorageGRID . . . 9
  - Mettre à jour les informations de licence StorageGRID . . . 10
  - Utiliser la API . . . 10
- Contrôler l’accès à StorageGRID . . . 33
  - Contrôler l’accès à StorageGRID . . . 33
  - Modifier la phrase secrète de provisionnement . . . 34
  - Modifier les mots de passe de la console du nœud . . . 35
  - Modifier les mots de passe d’accès SSH pour les nœuds d’administration . . . 37
  - Utiliser la fédération d’identité . . . 39
  - Gérer les groupes d’administrateurs . . . 44
  - Autorisations du groupe d’administrateurs . . . 47
  - Gérer les utilisateurs . . . 51
  - Utiliser l’authentification unique (SSO) . . . 54
- Utiliser la fédération de grille . . . 85
  - Qu’est-ce que la fédération de réseau ? . . . 85
  - Qu’est-ce que le clonage de compte ? . . . 88
  - Qu’est-ce que la réplication inter-réseau ? . . . 91
  - Comparer la réplication inter-grille et la réplication CloudMirror . . . 97
  - Créer des connexions de fédération de grille . . . 99
  - Gérer les connexions de la fédération de réseau . . . 103
  - Gérer les locataires autorisés pour la fédération de réseau . . . 108
  - Résoudre les erreurs de fédération de grille . . . 114
  - Identifier et réessayer les opérations de réplication ayant échoué . . . 119
- Gérer la sécurité . . . 123
  - Gérer la sécurité . . . 123
  - Examiner les méthodes de chiffrement StorageGRID . . . 124
  - Gérer les certificats . . . 127
  - Configurer les paramètres de sécurité . . . 160
  - Configurer les serveurs de gestion de clés . . . 165
  - Gérer les paramètres de proxy . . . 183
  - Contrôler les pare-feu . . . 185
- Gérer les locataires . . . 192
  - Que sont les comptes locataires ? . . . 192
  - Créer un compte locataire . . . 194

Modifier le compte locataire . . . 199
Modifier le mot de passe de l'utilisateur root local du locataire . . . 201
Supprimer le compte locataire . . . 201
Gérer les services de la plateforme . . . 202
Gérer S3 Select pour les comptes locataires . . . 211
Configurer les connexions client . . . 212
Configurer les connexions client S3 . . . 212
Sécurité pour les clients S3 . . . 215
Utiliser l'assistant de configuration S3 . . . 216
Gérer les groupes HA . . . 226
Gérer l'équilibrage de charge . . . 237
Configurer les noms de domaine des points de terminaison S3 . . . 251
Résumé : Adresses IP et ports pour les connexions client . . . 254
Gérer les réseaux et les connexions . . . 255
Configurer les paramètres réseau . . . 255
Lignes directrices pour les réseaux StorageGRID . . . 256
Afficher les adresses IP . . . 257
Configurer les interfaces VLAN . . . 258
Gérer les politiques de classification du trafic . . . 263
Chiffres pris en charge pour les connexions TLS sortantes . . . 270
Avantages des connexions HTTP actives, inactives et simultanées . . . 270
Gérer les coûts de liaison . . . 273
Utiliser AutoSupport . . . 275
Qu'est-ce AutoSupport? . . . 275
Configurer AutoSupport . . . 280
Déclencher manuellement un package AutoSupport . . . 284
Dépannage des packages AutoSupport . . . 285
Envoyer des packages AutoSupport de la série E via StorageGRID . . . 286
Gérer les nœuds de stockage . . . 290
Gérer les nœuds de stockage . . . 290
Utiliser les options de stockage . . . 290
Gérer le stockage des métadonnées des objets . . . 294
Augmenter le paramètre d'espace réservé aux métadonnées . . . 301
Compresser les objets stockés . . . 303
Gérer des nœuds de stockage complets . . . 304
Gérer les nœuds d'administration . . . 305
Utiliser plusieurs nœuds d'administration . . . 305
Identifier le nœud d'administration principal . . . 306
Afficher l'état des notifications et les files d'attente . . . 306

Administrer StorageGRID

Administrer StorageGRID

Utilisez ces instructions pour configurer et administrer un système StorageGRID .

À propos de ces instructions

Les principales tâches de configuration et d'administration de StorageGRID vous permettent de :

- Utilisez le gestionnaire de grille pour configurer des groupes et des utilisateurs
- Créer des comptes locataires pour permettre aux applications clientes S3 de stocker et de récupérer des objets
- Configurer et gérer les réseaux StorageGRID
- Configurer AutoSupport
- Gérer les paramètres des nœuds

Avant de commencer

- Vous avez une compréhension générale du système StorageGRID .
- Vous avez une connaissance assez détaillée des shells de commande Linux, de la mise en réseau et de la configuration du matériel du serveur.

Démarrer avec Grid Manager

Configuration requise pour le navigateur Web

Vous devez utiliser un navigateur Web pris en charge.

navigateur Web	Version minimale prise en charge
Google Chrome	119
Microsoft Edge	119
Mozilla Firefox	119

Vous devez définir la fenêtre du navigateur à une largeur recommandée.

Largeur du navigateur	Pixels
Minimum	1024
Optimum	1280

Sign in au gestionnaire de grille

Vous accédez à la page de connexion de Grid Manager en saisissant le nom de domaine complet (FQDN) ou l'adresse IP d'un nœud d'administration dans la barre d'adresse d'un navigateur Web pris en charge.

Chaque système StorageGRID comprend un nœud d'administration principal et un nombre quelconque de nœuds d'administration non principaux. Vous pouvez vous connecter au Grid Manager sur n'importe quel nœud d'administration pour gérer le système StorageGRID . Cependant, certaines procédures de maintenance ne peuvent être effectuées qu'à partir du nœud d'administration principal.

Se connecter au groupe HA

Si les nœuds d'administration sont inclus dans un groupe haute disponibilité (HA), vous vous connectez à l'aide de l'adresse IP virtuelle du groupe HA ou d'un nom de domaine complet mappé à l'adresse IP virtuelle. Le nœud d'administration principal doit être sélectionné comme interface principale du groupe, de sorte que lorsque vous accédez au gestionnaire de grille, vous y accédez sur le nœud d'administration principal, sauf si le nœud d'administration principal n'est pas disponible. Voir "Gérer les groupes de haute disponibilité" .

Utiliser SSO

Les étapes de connexion sont légèrement différentes si"l'authentification unique (SSO) a été configurée" .

Sign in à Grid Manager sur le premier nœud d'administration

Avant de commencer

- Vous avez vos identifiants de connexion.
- Vous utilisez un"navigateur Web pris en charge" .
- Les cookies sont activés dans votre navigateur Web.
- Vous appartenez à un groupe d'utilisateurs qui dispose d'au moins une autorisation.
- Vous avez l'URL du Grid Manager :

  `https://FQDN_or_Admin_Node_IP/`

  Vous pouvez utiliser le nom de domaine complet, l'adresse IP d'un nœud d'administration ou l'adresse IP virtuelle d'un groupe HA de nœuds d'administration.

  Pour accéder au Grid Manager sur un port autre que le port par défaut pour HTTPS (443), incluez le numéro de port dans l'URL :

  `https://FQDN_or_Admin_Node_IP:port/`

  > SSO n'est pas disponible sur le port restreint du Grid Manager. Vous devez utiliser le port 443.

Étapes

1. Lancez un navigateur Web pris en charge.
2. Dans la barre d'adresse du navigateur, saisissez l'URL du gestionnaire de grille.
3. Si une alerte de sécurité s'affiche, installez le certificat à l'aide de l'assistant d'installation du navigateur. Voir "Gérer les certificats de sécurité" .

4. Sign in au gestionnaire de grille.

   L’écran de connexion qui s’affiche dépend de la configuration de l’authentification unique (SSO) pour StorageGRID.

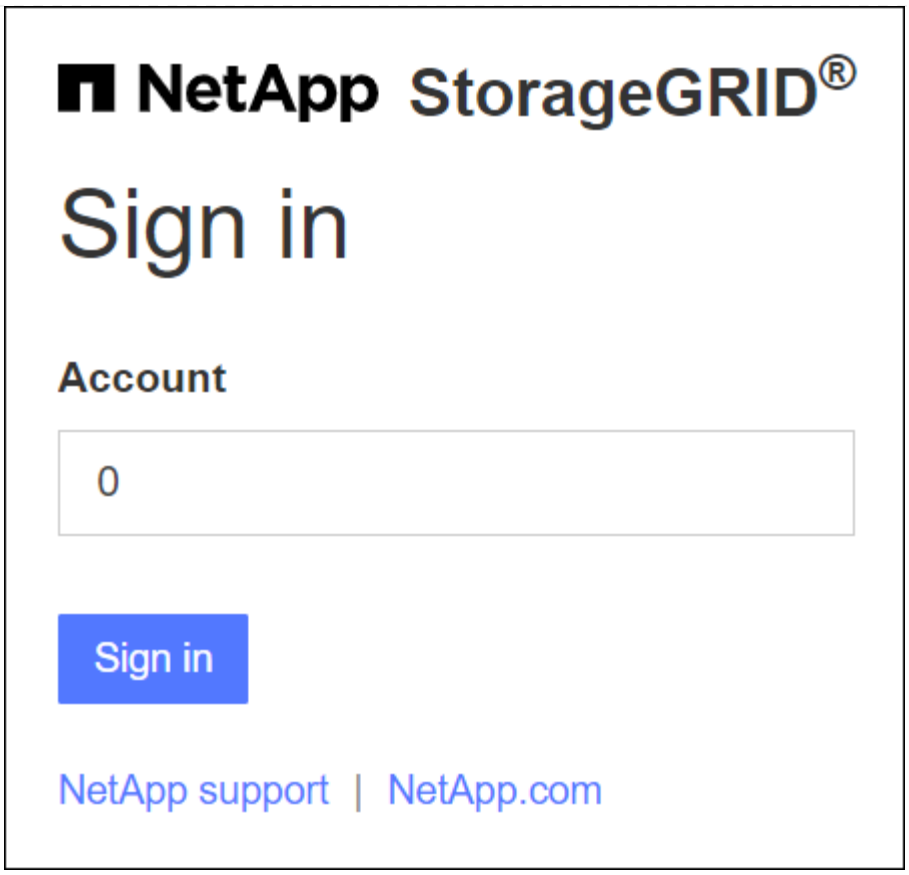
Ne pas utiliser SSO

a. Entrez votre nom d'utilisateur et votre mot de passe pour le Grid Manager.

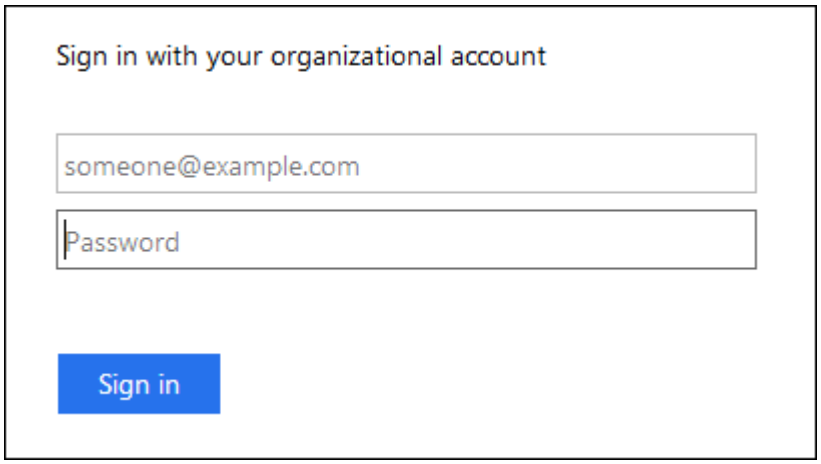
b. Sélectionnez **Connexion**.

Utilisation de SSO

- Si StorageGRID utilise SSO et que c'est la première fois que vous accédez à l'URL sur ce navigateur :
  i. Sélectionnez * Sign in*. Vous pouvez laisser le 0 dans le champ Compte.



ii. Saisissez vos informations d'identification SSO standard sur la page de connexion SSO de votre organisation. Par exemple:



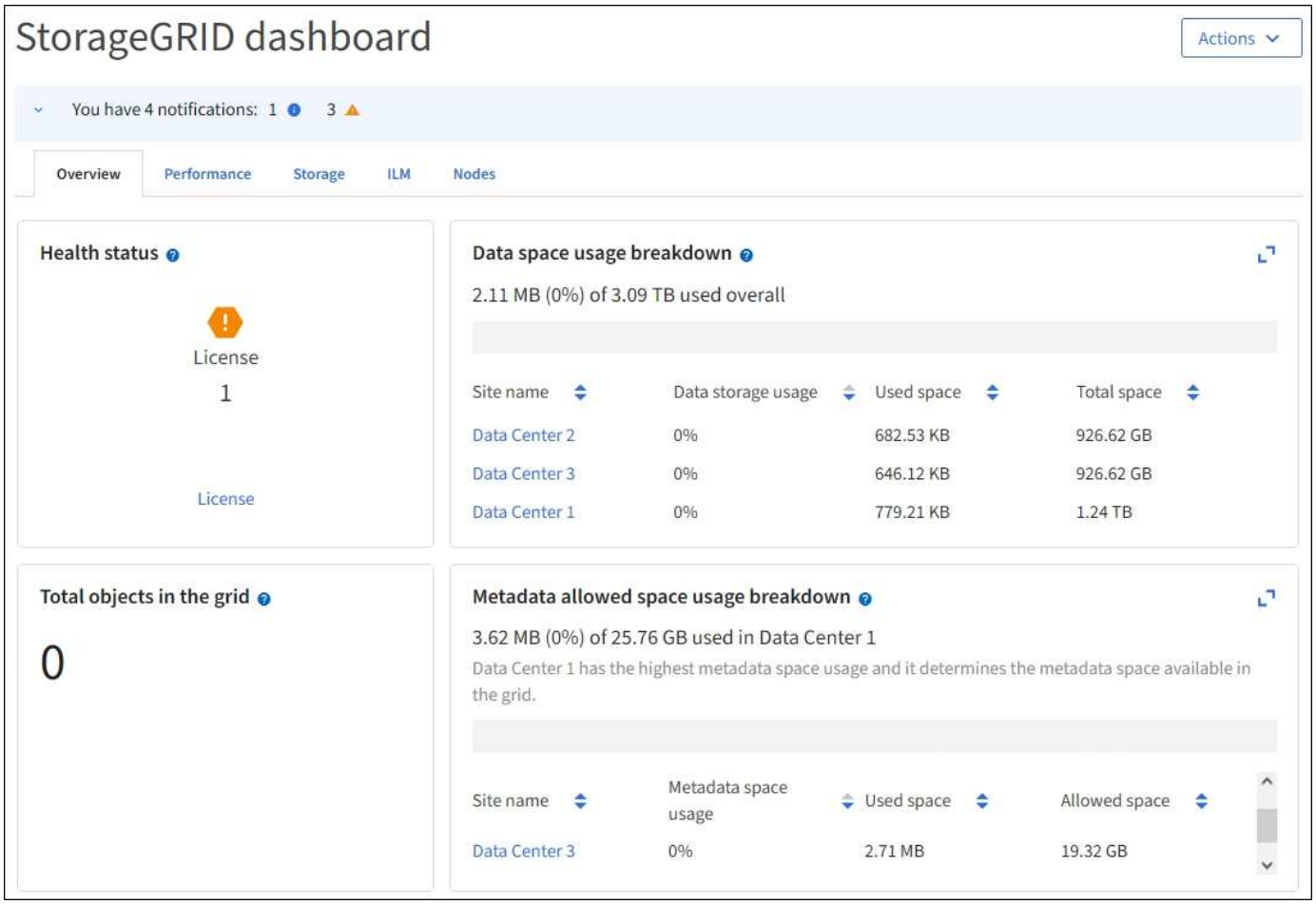
- Si StorageGRID utilise SSO et que vous avez déjà accédé au Grid Manager ou à un compte locataire :

  i. Saisissez **0** (l'ID de compte pour le gestionnaire de grille) ou sélectionnez **Gestionnaire de grille** s'il apparaît dans la liste des comptes récents.

ii. Sélectionnez * Sign in*.

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

Lorsque vous êtes connecté, la page d'accueil du Grid Manager apparaît, qui comprend le tableau de bord. Pour savoir quelles informations sont fournies, consultez"Afficher et gérer le tableau de bord" .



Connectez-vous à un autre nœud d'administration

Suivez ces étapes pour vous connecter à un autre nœud d'administration.

Ne pas utiliser SSO

Étapes

1. Dans la barre d'adresse du navigateur, saisissez le nom de domaine complet ou l'adresse IP de l'autre nœud d'administration. Incluez le numéro de port si nécessaire.
2. Entrez votre nom d'utilisateur et votre mot de passe pour le Grid Manager.
3. Sélectionnez **Connexion**.

Utilisation de SSO

Si StorageGRID utilise SSO et que vous êtes connecté à un nœud d'administration, vous pouvez accéder aux autres nœuds d'administration sans avoir à vous reconnecter.

Étapes

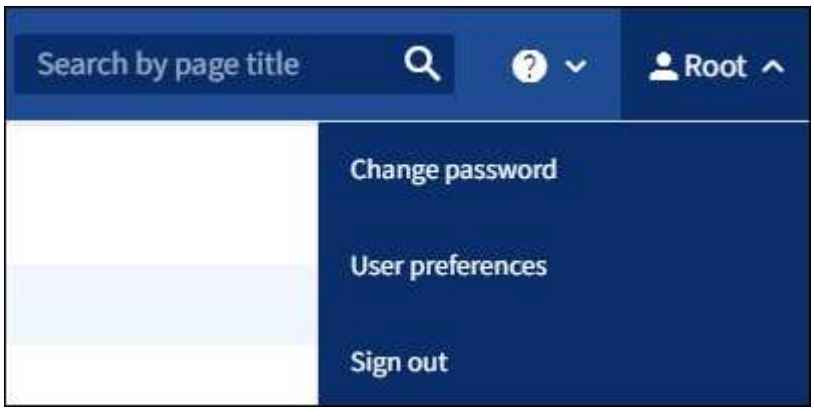
1. Saisissez le nom de domaine complet ou l'adresse IP de l'autre nœud d'administration dans la barre d'adresse du navigateur.
2. Si votre session SSO a expiré, saisissez à nouveau vos informations d'identification.

Déconnectez-vous du gestionnaire de grille

Lorsque vous avez terminé d'utiliser Grid Manager, vous devez vous déconnecter pour garantir que les utilisateurs non autorisés ne peuvent pas accéder au système StorageGRID . La fermeture de votre navigateur peut ne pas vous déconnecter du système, en fonction des paramètres de cookies du navigateur.

Étapes

1. Sélectionnez votre nom d'utilisateur dans le coin supérieur droit.



2. Sélectionnez **Déconnexion**.

Option	Description
SSO non utilisé	Vous êtes déconnecté du nœud d'administration. La page de connexion de Grid Manager s'affiche. **Remarque :** si vous vous êtes connecté à plusieurs nœuds d'administration, vous devez vous déconnecter de chaque nœud.
SSO activé	Vous êtes déconnecté de tous les nœuds d'administration auxquels vous accédiez. La page de connexion StorageGRID s'affiche. **Grid Manager** est répertorié par défaut dans la liste déroulante **Comptes récents** et le champ **ID de compte** affiche 0. **Remarque :** si l'authentification unique est activée et que vous êtes également connecté au gestionnaire de locataires, vous devez également"se déconnecter du compte locataire" à"se déconnecter de SSO" .

Changez votre mot de passe

Si vous êtes un utilisateur local du Grid Manager, vous pouvez modifier votre propre mot de passe.

Avant de commencer

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

À propos de cette tâche

Si vous vous connectez à StorageGRID en tant qu'utilisateur fédéré ou si l'authentification unique (SSO) est activée, vous ne pouvez pas modifier votre mot de passe dans Grid Manager. Au lieu de cela, vous devez modifier votre mot de passe dans la source d'identité externe, par exemple, Active Directory ou OpenLDAP.

Étapes

1. Dans l'en-tête du Gestionnaire de grille, sélectionnez ***votre nom*** > **Modifier le mot de passe**.
2. Entrez votre mot de passe actuel.
3. Tapez un nouveau mot de passe.

   Votre mot de passe doit contenir au moins 8 et pas plus de 32 caractères. Les mots de passe sont sensibles à la casse.

4. Entrez à nouveau le nouveau mot de passe.
5. Sélectionnez **Enregistrer**.

Afficher les informations de licence StorageGRID

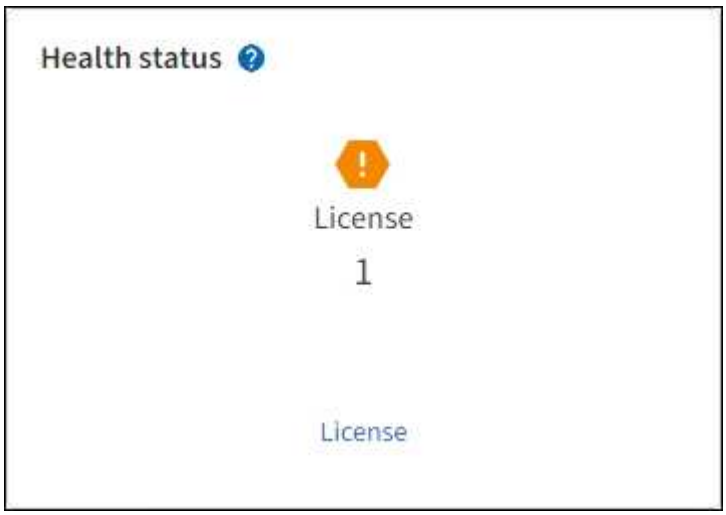
Vous pouvez afficher les informations de licence de votre système StorageGRID , telles que la capacité de stockage maximale de votre grille, chaque fois que nécessaire.

Avant de commencer

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

À propos de cette tâche

S'il y a un problème avec la licence du logiciel pour ce système StorageGRID , la carte d'état de santé sur le tableau de bord comprend une icône d'état de licence et un lien **Licence**. Le nombre indique le nombre de problèmes liés aux licences.



Étapes

1. Accédez à la page Licence en effectuant l'une des opérations suivantes :
   - Sélectionnez **MAINTENANCE** > **Système** > **Licence**.
   - À partir de la carte d'état de santé du tableau de bord, sélectionnez l'icône d'état de la licence ou le lien **Licence**.

Ce lien apparaît uniquement s'il y a un problème avec la licence.

2. Afficher les détails en lecture seule de la licence actuelle :
   - ID système StorageGRID , qui est le numéro d'identification unique de cette installation StorageGRID
   - Numéro de série de la licence
   - Type de licence, soit **Perpétuelle** soit **Abonnement**
   - Capacité de stockage sous licence du réseau
   - Capacité de stockage prise en charge
   - Date de fin de licence. **N/A** apparaît pour une licence perpétuelle.
   - Date de fin du support

     Cette date est lue à partir du fichier de licence actuel et peut être obsolète si vous avez prolongé ou renouvelé le contrat de service d'assistance après avoir obtenu le fichier de licence. Pour mettre à jour cette valeur, voir"Mettre à jour les informations de licence StorageGRID" . Vous pouvez également consulter la date de fin réelle du contrat à l'aide d' Active IQ.

   - Contenu du fichier texte de licence

Mettre à jour les informations de licence StorageGRID

Vous devez mettre à jour les informations de licence de votre système StorageGRID chaque fois que les termes de votre licence changent. Par exemple, vous devez mettre à jour les informations de licence si vous achetez une capacité de stockage supplémentaire pour votre réseau.

Avant de commencer

- Vous disposez d'un nouveau fichier de licence à appliquer à votre système StorageGRID .
- Tu as"autorisations d'accès spécifiques" .
- Vous disposez de la phrase secrète de provisionnement.

Étapes

1. Sélectionnez **MAINTENANCE** > **Système** > **Licence**.
2. Dans la section Mettre à jour la licence, sélectionnez **Parcourir**.
3. Localisez et sélectionnez le nouveau fichier de licence(`.txt`).

   Le nouveau fichier de licence est validé et affiché.

4. Saisissez la phrase secrète d'approvisionnement.
5. Sélectionnez **Enregistrer**.

Utiliser la API

Utiliser l'API de gestion de grille

Vous pouvez effectuer des tâches de gestion du système à l'aide de l'API REST Grid Management au lieu de l'interface utilisateur Grid Manager. Par exemple, vous souhaiterez peut-être utiliser l'API pour automatiser des opérations ou créer plusieurs

entités, telles que des utilisateurs, plus rapidement.

Ressources de haut niveau

L'API de gestion de grille fournit les ressources de niveau supérieur suivantes :

- `/grid`:L'accès est limité aux utilisateurs de Grid Manager et est basé sur les autorisations de groupe configurées.
- `/org`:L'accès est limité aux utilisateurs qui appartiennent à un groupe LDAP local ou fédéré pour un compte locataire. Pour plus de détails, consultez la section "Utiliser un compte locataire" .
- `/private`:L'accès est limité aux utilisateurs de Grid Manager et est basé sur les autorisations de groupe configurées. Les API privées sont susceptibles d'être modifiées sans préavis. Les points de terminaison privés StorageGRID ignorent également la version API de la demande.

Émettre des requêtes API

L'API de gestion de grille utilise la plate-forme API open source Swagger. Swagger fournit une interface utilisateur intuitive qui permet aux développeurs et aux non-développeurs d'effectuer des opérations en temps réel dans StorageGRID avec l'API.

L'interface utilisateur de Swagger fournit des détails complets et une documentation pour chaque opération API.

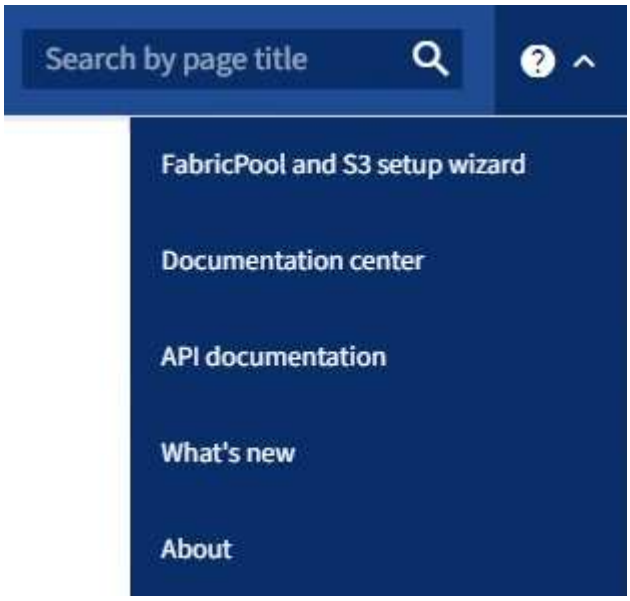
Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .

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

Étapes

1. Depuis l'en-tête du gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **Documentation API**.



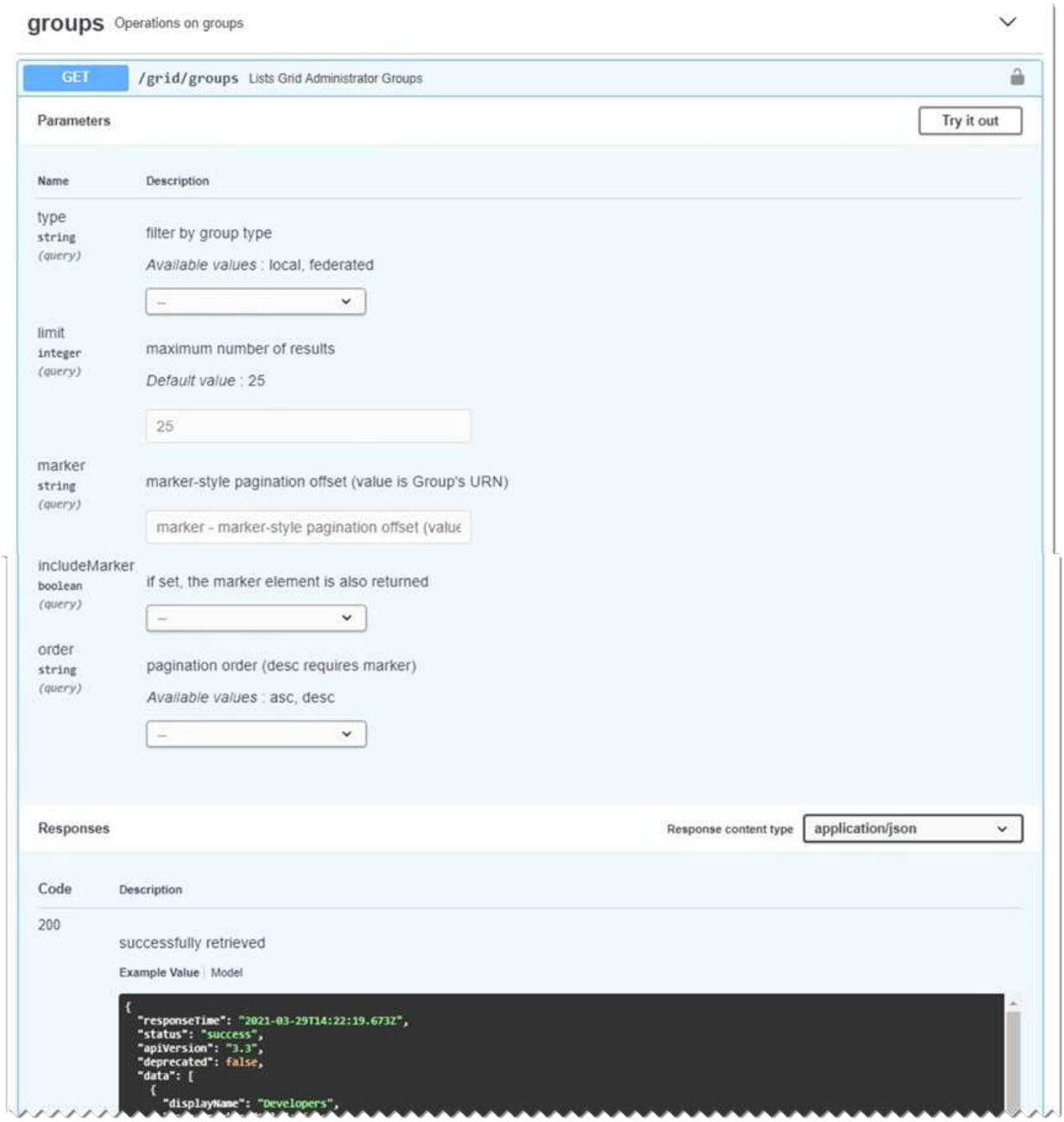
2. Pour effectuer une opération avec l'API privée, sélectionnez **Accéder à la documentation de l'API privée** sur la page API de gestion StorageGRID .

   Les API privées sont susceptibles d'être modifiées sans préavis. Les points de terminaison privés StorageGRID ignorent également la version API de la demande.

3. Sélectionnez l'opération souhaitée.

   Lorsque vous développez une opération API, vous pouvez voir les actions HTTP disponibles, telles que GET, PUT, UPDATE et DELETE.

4. Sélectionnez une action HTTP pour afficher les détails de la demande, y compris l'URL du point de terminaison, une liste de tous les paramètres obligatoires ou facultatifs, un exemple du corps de la demande (si nécessaire) et les réponses possibles.



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

Opérations de l'API de gestion de grille

L'API de gestion de grille organise les opérations disponibles dans les sections suivantes.

Cette liste inclut uniquement les opérations disponibles dans l'API publique.

- **comptes** : opérations de gestion des comptes de locataires de stockage, y compris la création de nouveaux comptes et la récupération de l'utilisation du stockage pour un compte donné.
- **alert-history** : Opérations sur les alertes résolues.
- **alert-receivers** : Opérations sur les récepteurs de notifications d'alerte (e-mail).
- **alert-rules** : Opérations sur les règles d'alerte.
- **alert-silences** : Opérations sur les silences d'alerte.
- **alertes** : Opérations sur les alertes.
- **audit** : opérations permettant de répertorier et de mettre à jour la configuration de l'audit.
- **auth** : opérations permettant d'effectuer l'authentification de la session utilisateur.

  L'API de gestion de grille prend en charge le schéma d'authentification du jeton porteur. Pour vous connecter, vous fournissez un nom d'utilisateur et un mot de passe dans le corps JSON de la demande d'authentification (c'est-à-dire, `POST /api/v3/authorize`). Si l'utilisateur est authentifié avec succès, un jeton de sécurité est renvoyé. Ce jeton doit être fourni dans l'en-tête des requêtes API ultérieures (« Authorization : Bearer *token* »). Le jeton expire après 16 heures.

  Si l'authentification unique est activée pour le système StorageGRID , vous devez effectuer différentes étapes pour vous authentifier. Voir « Authentification auprès de l'API si l'authentification unique est activée ».

  Consultez « Protection contre la falsification de requêtes intersites » pour obtenir des informations sur l'amélioration de la sécurité de l'authentification.

- **client-certificates** : opérations de configuration des certificats clients afin que StorageGRID soit accessible en toute sécurité à l'aide d'outils de surveillance externes.
- **config** : opérations liées à la version du produit et aux versions de l'API Grid Management. Vous pouvez répertorier la version du produit et les versions principales de l'API Grid Management prises en charge par cette version, et vous pouvez désactiver les versions obsolètes de l'API.
- **fonctionnalités désactivées** : opérations permettant d'afficher les fonctionnalités qui pourraient avoir été désactivées.
- **dns-servers** : opérations permettant de lister et de modifier les serveurs DNS externes configurés.
- **drive-details** : opérations sur les lecteurs pour des modèles d'appareils de stockage spécifiques.
- **endpoint-domain-names** : opérations permettant de répertorier et de modifier les noms de domaine de point de terminaison S3.
- **erasure-coding** : Opérations sur les profils d'effacement-codage.
- **expansion** : Opérations sur l'expansion (niveau procédure).
- **expansion-nodes** : opérations sur l'expansion (au niveau du nœud).
- **expansion-sites** : Opérations sur l'extension (au niveau du site).
- **grid-networks** : Opérations permettant de lister et de modifier la liste des réseaux de grille.

- **grid-passwords** : Opérations pour la gestion des mots de passe de la grille.
- **groupes** : opérations de gestion des groupes d'administrateurs de grille locaux et de récupération des groupes d'administrateurs de grille fédérés à partir d'un serveur LDAP externe.
- **identity-source** : opérations permettant de configurer une source d'identité externe et de synchroniser manuellement les informations des groupes fédérés et des utilisateurs.
- **ilm** : Opérations sur la gestion du cycle de vie de l'information (ILM).
- **in-progress-procedures**: Récupère les procédures de maintenance actuellement en cours.
- **licence** : opérations permettant de récupérer et de mettre à jour la licence StorageGRID .
- **logs** : opérations de collecte et de téléchargement des fichiers journaux.v
- **métriques** : opérations sur les métriques StorageGRID , y compris les requêtes de métriques instantanées à un moment donné et les requêtes de métriques de plage sur une plage de temps. L'API Grid Management utilise l'outil de surveillance des systèmes Prometheus comme source de données back-end. Pour plus d'informations sur la construction de requêtes Prometheus, consultez le site Web Prometheus.

> Les mesures qui incluent`private` dans leurs noms sont destinés à un usage interne uniquement. Ces mesures sont susceptibles d'être modifiées entre les versions de StorageGRID sans préavis.

- **node-details** : Opérations sur les détails du nœud.
- **node-health** : opérations sur l'état de santé du nœud.
- **node-storage-state** : opérations sur l'état de stockage des nœuds.
- **ntp-servers** : opérations permettant de répertorier ou de mettre à jour les serveurs NTP (Network Time Protocol) externes.
- **objets** : opérations sur les objets et les métadonnées des objets.
- **récupération** : opérations pour la procédure de récupération.
- **recovery-package** : opérations de téléchargement du package de récupération.
- **régions** : opérations permettant d'afficher et de créer des régions.
- **s3-object-lock** : opérations sur les paramètres globaux de verrouillage d'objet S3.
- **server-certificate** : opérations permettant d'afficher et de mettre à jour les certificats du serveur Grid Manager.
- **snmp** : opérations sur la configuration SNMP actuelle.
- **storage-watermarks** : Filigranes des nœuds de stockage.
- **traffic-classes** : opérations pour les politiques de classification du trafic.
- **untrusted-client-network** : opérations sur la configuration du réseau client non approuvé.
- **utilisateurs** : opérations permettant d'afficher et de gérer les utilisateurs de Grid Manager.

Gestion des versions de l'API de gestion de grille

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

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

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

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

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

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

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

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

Les demandes obsolètes sont marquées comme obsolètes des manières suivantes :

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

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

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

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

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

Spécifier une version d'API pour une requête

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

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

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

Protection contre la falsification de requêtes intersites (CSRF)

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

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

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

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

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

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

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

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

Consultez la documentation de l'API en ligne pour des exemples et des détails supplémentaires.

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

Utiliser l'API si l'authentification unique est activée

Utiliser l'API si l'authentification unique est activée (Active Directory)

Si vous avez"configuré et activé l'authentification unique (SSO)" et que vous utilisez Active Directory comme fournisseur SSO, vous devez émettre une série de requêtes API pour obtenir un jeton d'authentification valide pour l'API Grid Management ou l'API Tenant Management.

Sign in à l'API si l'authentification unique est activée

Ces instructions s'appliquent si vous utilisez Active Directory comme fournisseur d'identité SSO.

Avant de commencer

- Vous connaissez le nom d'utilisateur et le mot de passe SSO d'un utilisateur fédéré qui appartient à un groupe d'utilisateurs StorageGRID .
- Si vous souhaitez accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

À propos de cette tâche

Pour obtenir un jeton d'authentification, vous pouvez utiliser l'un des exemples suivants :

- Le `storagegrid-ssoauth.py` Script Python, situé dans le répertoire des fichiers d'installation de StorageGRID(`./rpms` pour Red Hat Enterprise Linux, `./debs` pour Ubuntu ou Debian, et `./vsphere`

pour VMware).

- Un exemple de flux de travail de requêtes curl.

  Le flux de travail curl peut expirer si vous l'exécutez trop lentement. Vous pourriez voir l'erreur : `A valid SubjectConfirmation was not found on this Response`.

  > L'exemple de workflow curl ne protège pas le mot de passe contre toute visualisation par d'autres utilisateurs.

Si vous avez un problème d'encodage d'URL, vous pourriez voir l'erreur : `Unsupported SAML version`.

Étapes

1. Sélectionnez l'une des méthodes suivantes pour obtenir un jeton d'authentification :
   - Utilisez le `storagegrid-ssoauth.py` Script Python. Passez à l'étape 2.
   - Utilisez les requêtes curl. Passez à l'étape 3.
2. Si vous souhaitez utiliser le `storagegrid-ssoauth.py` script, transmettez le script à l'interpréteur Python et exécutez le script.

   Lorsque vous y êtes invité, saisissez des valeurs pour les arguments suivants :

   - La méthode SSO. Entrez ADFS ou adfs.
   - Le nom d'utilisateur SSO
   - Le domaine où StorageGRID est installé
   - L'adresse de StorageGRID
   - L'ID du compte locataire, si vous souhaitez accéder à l'API de gestion des locataires.

   ```
   python3 storagegrid-ssoauth.py
   sso_method: adfs
   saml_user: my-sso-username
   saml_domain: my-domain
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   Le jeton d'autorisation StorageGRID est fourni dans la sortie. Vous pouvez désormais utiliser le jeton pour d'autres requêtes, de la même manière que vous utiliseriez l'API si SSO n'était pas utilisé.

3. Si vous souhaitez utiliser des requêtes curl, utilisez la procédure suivante.

   a. Déclarez les variables nécessaires à la connexion.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```

Pour accéder à l'API de gestion de grille, utilisez 0 comme `TENANTACCOUNTID` .

b. Pour recevoir une URL d'authentification signée, émettez une requête POST à `/api/v3/authorize-saml` et supprimez l'encodage JSON supplémentaire de la réponse.

Cet exemple montre une requête POST pour une URL d'authentification signée pour `TENANTACCOUNTID` . Les résultats seront transmis à `python -m json.tool` pour supprimer l'encodage JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

La réponse pour cet exemple inclut une URL signée qui est codée en URL, mais elle n'inclut pas la couche de codage JSON supplémentaire.

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Sauver le `SAMLRequest` à partir de la réponse à utiliser dans les commandes suivantes.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. Obtenez une URL complète qui inclut l'ID de demande client d'AD FS.

Une option consiste à demander le formulaire de connexion en utilisant l'URL de la réponse précédente.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post"
id="loginForm"'
```

La réponse inclut l'ID de la demande du client :

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Enregistrez l'ID de demande du client à partir de la réponse.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. Envoyez vos informations d'identification à l'action du formulaire de la réponse précédente.

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client
-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=
$SAMLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS renvoie une redirection 302, avec des informations supplémentaires dans les en-têtes.

> Si l'authentification multifacteur (MFA) est activée pour votre système SSO, le formulaire de publication contiendra également le deuxième mot de passe ou d'autres informations d'identification.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. Sauver le `MSISAuth` cookie de la réponse.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. Envoyez une requête GET à l'emplacement spécifié avec les cookies du POST d'authentification.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-
id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

Les en-têtes de réponse contiendront des informations de session AD FS pour une utilisation ultérieure lors de la déconnexion, et le corps de la réponse contient la réponse SAML dans un champ de formulaire masqué.

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. Sauver le `SAMLResponse` du champ caché :

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Utilisation de la sauvegarde `SAMLResponse` , créer un StorageGRID`/api/saml-response` demande de génération d'un jeton d'authentification StorageGRID .

Pour `RelayState` , utilisez l'ID de compte locataire ou utilisez 0 si vous souhaitez vous connecter à l'API Grid Management.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

La réponse inclut le jeton d'authentification.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. Enregistrez le jeton d'authentification dans la réponse sous `MYTOKEN` .

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Vous pouvez désormais utiliser `MYTOKEN` pour d'autres demandes, de la même manière que vous utiliseriez l'API si SSO n'était pas utilisé.

Déconnectez-vous de l'API si l'authentification unique est activée

Si l'authentification unique (SSO) a été activée, vous devez émettre une série de requêtes API pour vous déconnecter de l'API Grid Management ou de l'API Tenant Management. Ces instructions s'appliquent si vous utilisez Active Directory comme fournisseur d'identité SSO

À propos de cette tâche

Si nécessaire, vous pouvez vous déconnecter de l'API StorageGRID en vous déconnectant de la page de déconnexion unique de votre organisation. Vous pouvez également déclencher une déconnexion unique (SLO) à partir de StorageGRID, ce qui nécessite un jeton porteur StorageGRID valide.

Étapes

1. Pour générer une demande de déconnexion signée, transmettez `cookie "sso=true" à l'API SLO :

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Une URL de déconnexion est renvoyée :

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. Enregistrez l'URL de déconnexion.

```
export LOGOUT_REQUEST
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%
3D'
```

3. Envoyez une demande à l'URL de déconnexion pour déclencher SLO et rediriger vers StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

La réponse 302 est renvoyée. L'emplacement de redirection ne s'applique pas à la déconnexion de l'API uniquement.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. Supprimez le jeton porteur StorageGRID .

La suppression du jeton porteur StorageGRID fonctionne de la même manière que sans SSO. Si `cookie "sso=true" n'est pas fourni, l'utilisateur est déconnecté de StorageGRID sans affecter l'état SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

UN `204 No Content` la réponse indique que l'utilisateur est maintenant déconnecté.

```
HTTP/1.1 204 No Content
```

Utiliser l'API si l'authentification unique est activée (Azure)

Si vous avez"configuré et activé l'authentification unique (SSO)" et vous utilisez Azure comme fournisseur SSO, vous pouvez utiliser deux exemples de scripts pour obtenir un jeton d'authentification valide pour l'API Grid Management ou l'API Tenant Management.

Sign in à l'API si l'authentification unique Azure est activée

Ces instructions s'appliquent si vous utilisez Azure comme fournisseur d'identité SSO

Avant de commencer

- Vous connaissez l'adresse e-mail et le mot de passe SSO d'un utilisateur fédéré qui appartient à un groupe d'utilisateurs StorageGRID .
- Si vous souhaitez accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

À propos de cette tâche

Pour obtenir un jeton d'authentification, vous pouvez utiliser les exemples de scripts suivants :

- Le `storagegrid-ssoauth-azure.py` Script Python
- Le `storagegrid-ssoauth-azure.js` Script Node.js

Les deux scripts se trouvent dans le répertoire des fichiers d'installation de StorageGRID(`./rpms` pour Red Hat Enterprise Linux, `./debs` pour Ubuntu ou Debian, et `./vsphere` pour VMware).

Pour écrire votre propre intégration d'API avec Azure, consultez le `storagegrid-ssoauth-azure.py` scénario. Le script Python envoie deux requêtes directement à StorageGRID (d'abord pour obtenir le SAMLRequest, puis pour obtenir le jeton d'autorisation) et appelle également le script Node.js pour interagir avec Azure afin d'effectuer les opérations SSO.

Les opérations SSO peuvent être exécutées à l'aide d'une série de requêtes API, mais cela n'est pas simple. Le module Puppeteer Node.js est utilisé pour récupérer l'interface Azure SSO.

Si vous avez un problème d'encodage d'URL, vous pourriez voir l'erreur : `Unsupported SAML version`.

Étapes

1. Installez les dépendances requises, comme suit :
   a. Installez Node.js (voir "https://nodejs.org/en/download/").

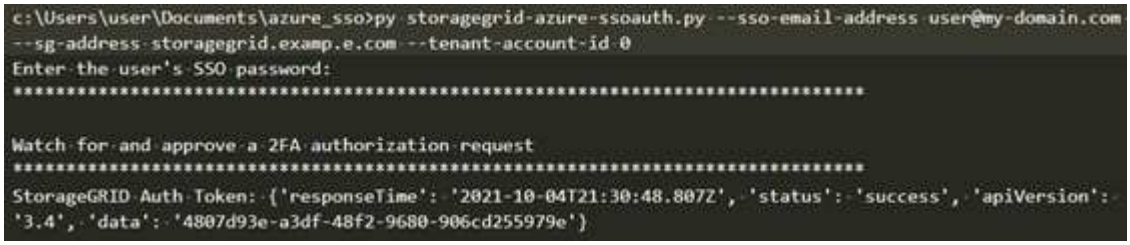
b. Installez les modules Node.js requis (puppeteer et jsdom) :

```
npm install -g <module>
```

2. Transmettez le script Python à l'interpréteur Python pour exécuter le script.

   Le script Python appellera ensuite le script Node.js correspondant pour effectuer les interactions Azure SSO.

3. Lorsque vous y êtes invité, saisissez des valeurs pour les arguments suivants (ou transmettez-les à l'aide de paramètres) :
   - L'adresse e-mail SSO utilisée pour se connecter à Azure
   - L'adresse de StorageGRID
   - L'ID du compte locataire, si vous souhaitez accéder à l'API de gestion des locataires
4. Lorsque vous y êtes invité, saisissez le mot de passe et soyez prêt à fournir une autorisation MFA à Azure si nécessaire.



> Le script suppose que l'authentification multifacteur est effectuée à l'aide de Microsoft Authenticator. Vous devrez peut-être modifier le script pour prendre en charge d'autres formes d'authentification multifacteur (comme la saisie d'un code reçu dans un message texte).

Le jeton d'autorisation StorageGRID est fourni dans la sortie. Vous pouvez désormais utiliser le jeton pour d'autres requêtes, de la même manière que vous utiliseriez l'API si SSO n'était pas utilisé.

Utiliser l'API si l'authentification unique est activée (PingFederate)

Si vous avez"configuré et activé l'authentification unique (SSO)" et que vous utilisez PingFederate comme fournisseur SSO, vous devez émettre une série de requêtes API pour obtenir un jeton d'authentification valide pour l'API de gestion de grille ou l'API de gestion des locataires.

Sign in à l'API si l'authentification unique est activée

Ces instructions s'appliquent si vous utilisez PingFederate comme fournisseur d'identité SSO

Avant de commencer

- Vous connaissez le nom d'utilisateur et le mot de passe SSO d'un utilisateur fédéré qui appartient à un groupe d'utilisateurs StorageGRID .
- Si vous souhaitez accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

À propos de cette tâche

Pour obtenir un jeton d'authentification, vous pouvez utiliser l'un des exemples suivants :

- Le `storagegrid-ssoauth.py` Script Python, situé dans le répertoire des fichiers d'installation de StorageGRID(`./rpms` pour Red Hat Enterprise Linux, `./debs` pour Ubuntu ou Debian, et `./vsphere` pour VMware).
- Un exemple de flux de travail de requêtes curl.

  Le flux de travail curl peut expirer si vous l'exécutez trop lentement. Vous pourriez voir l'erreur : `A valid SubjectConfirmation was not found on this Response`.

  > L'exemple de workflow curl ne protège pas le mot de passe contre toute visualisation par d'autres utilisateurs.

  Si vous avez un problème d'encodage d'URL, vous pourriez voir l'erreur : `Unsupported SAML version`.

Étapes

1. Sélectionnez l'une des méthodes suivantes pour obtenir un jeton d'authentification :
   - Utilisez le `storagegrid-ssoauth.py` Script Python. Passez à l'étape 2.
   - Utilisez les requêtes curl. Passez à l'étape 3.
2. Si vous souhaitez utiliser le `storagegrid-ssoauth.py` script, transmettez le script à l'interpréteur Python et exécutez le script.

   Lorsque vous y êtes invité, saisissez des valeurs pour les arguments suivants :

   - La méthode SSO. Vous pouvez saisir n'importe quelle variante de « pingfederate » (PINGFEDERATE, pingfederate, etc.).
   - Le nom d'utilisateur SSO
   - Le domaine où StorageGRID est installé. Ce champ n'est pas utilisé pour PingFederate. Vous pouvez le laisser vide ou saisir n'importe quelle valeur.
   - L'adresse de StorageGRID
   - L'ID du compte locataire, si vous souhaitez accéder à l'API de gestion des locataires.

   ```
   python3 storagegrid-ssoauth.py
   sso_method: pingfederate
   saml_user: my-sso-username
   saml_domain:
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   Le jeton d'autorisation StorageGRID est fourni dans la sortie. Vous pouvez désormais utiliser le jeton pour d'autres requêtes, de la même manière que vous utiliseriez l'API si SSO n'était pas utilisé.
3. Si vous souhaitez utiliser des requêtes curl, utilisez la procédure suivante.

a. Déclarez les variables nécessaires à la connexion.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```

Pour accéder à l'API de gestion de grille, utilisez 0 comme `TENANTACCOUNTID` .

b. Pour recevoir une URL d'authentification signée, émettez une requête POST à `/api/v3/authorize-saml` et supprimez l'encodage JSON supplémentaire de la réponse.

Cet exemple montre une requête POST pour une URL d'authentification signée pour TENANTACCOUNTID. Les résultats seront transmis à python -m json.tool pour supprimer l'encodage JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

La réponse pour cet exemple inclut une URL signée qui est codée en URL, mais elle n'inclut pas la couche de codage JSON supplémentaire.

```
{
    "apiVersion": "3.0",
    "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Sauver le `SAMLRequest` à partir de la réponse à utiliser dans les commandes suivantes.

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

d. Exportez la réponse et le cookie, et faites écho à la réponse :

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. Exportez la valeur « pf.adapterId » et renvoyez la réponse :

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. Exportez la valeur « href » (supprimez la barre oblique /) et affichez la réponse :

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. Exporter la valeur « action » :

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. Envoyer des cookies avec les informations d'identification :

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. Sauver le `SAMLResponse` du champ caché :

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Utilisation de la sauvegarde `SAMLResponse` , créer un StorageGRID`/api/saml-response` demande de génération d'un jeton d'authentification StorageGRID .

   Pour `RelayState` , utilisez l'ID de compte locataire ou utilisez 0 si vous souhaitez vous connecter à l'API Grid Management.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

La réponse inclut le jeton d'authentification.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. Enregistrez le jeton d'authentification dans la réponse sous `MYTOKEN` .

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Vous pouvez désormais utiliser `MYTOKEN` pour d'autres demandes, de la même manière que vous utiliseriez l'API si SSO n'était pas utilisé.

Déconnectez-vous de l'API si l'authentification unique est activée

Si l'authentification unique (SSO) a été activée, vous devez émettre une série de requêtes API pour vous déconnecter de l'API Grid Management ou de l'API Tenant Management. Ces instructions s'appliquent si vous utilisez PingFederate comme fournisseur d'identité SSO

À propos de cette tâche

Si nécessaire, vous pouvez vous déconnecter de l'API StorageGRID en vous déconnectant de la page de déconnexion unique de votre organisation. Vous pouvez également déclencher une déconnexion unique (SLO) à partir de StorageGRID, ce qui nécessite un jeton porteur StorageGRID valide.

Étapes

1. Pour générer une demande de déconnexion signée, transmettez `cookie "sso=true" à l'API SLO :

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Une URL de déconnexion est renvoyée :

```
{
    "apiVersion": "3.0",
    "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2021-10-12T22:20:30.839Z",
    "status": "success"
}
```

2. Enregistrez l'URL de déconnexion.

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Envoyez une demande à l'URL de déconnexion pour déclencher SLO et rediriger vers StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

La réponse 302 est renvoyée. L'emplacement de redirection ne s'applique pas à la déconnexion de l'API uniquement.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. Supprimez le jeton porteur StorageGRID .

La suppression du jeton porteur StorageGRID fonctionne de la même manière que sans SSO. Si `cookie "sso=true" n'est pas fourni, l'utilisateur est déconnecté de StorageGRID sans affecter l'état SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

UN `204 No Content` la réponse indique que l'utilisateur est maintenant déconnecté.

```
HTTP/1.1 204 No Content
```

Désactiver les fonctionnalités avec l'API

Vous pouvez utiliser l'API Grid Management pour désactiver complètement certaines fonctionnalités du système StorageGRID . Lorsqu'une fonctionnalité est désactivée, personne ne peut se voir attribuer d'autorisations pour effectuer les tâches liées à cette fonctionnalité.

À propos de cette tâche

Le système de fonctionnalités désactivées vous permet d'empêcher l'accès à certaines fonctionnalités du système StorageGRID . La désactivation d'une fonctionnalité est le seul moyen d'empêcher l'utilisateur root ou les utilisateurs appartenant à des groupes d'administrateurs avec l'autorisation **Accès root** de pouvoir utiliser cette fonctionnalité.

Pour comprendre comment cette fonctionnalité pourrait être utile, considérez le scénario suivant :

_La société A est un fournisseur de services qui loue la capacité de stockage de son système StorageGRID en créant des comptes locataires. Pour protéger la sécurité des objets de ses locataires, la société A souhaite s'assurer que ses propres employés ne pourront jamais accéder à un compte locataire après le déploiement du compte.

_L'entreprise A peut atteindre cet objectif en utilisant le système de désactivation des fonctionnalités dans l'API de gestion de la grille. En désactivant complètement la fonctionnalité **Modifier le mot de passe root du locataire** dans le gestionnaire de grille (à la fois l'interface utilisateur et l'API), la société A garantit que les utilisateurs administrateurs, y compris l'utilisateur root et les utilisateurs appartenant à des groupes disposant de l'autorisation **Accès root**, ne peuvent pas modifier le mot de passe de l'utilisateur root d'un compte locataire.

Étapes

1. Accédez à la documentation Swagger pour l'API de gestion de grille. Voir "Utiliser l'API de gestion de grille" .
2. Localisez le point de terminaison Désactiver les fonctionnalités.
3. Pour désactiver une fonctionnalité, telle que Modifier le mot de passe racine du locataire, envoyez un corps à l'API comme ceci :

   ```
   { "grid": {"changeTenantRootPassword": true} }
   ```

   Une fois la demande terminée, la fonctionnalité Modifier le mot de passe racine du locataire est désactivée. L'autorisation de gestion **Modifier le mot de passe racine du locataire** n'apparaît plus dans l'interface utilisateur et toute demande d'API qui tente de modifier le mot de passe racine d'un locataire échouera avec le message « 403 Forbidden ».

Réactiver les fonctionnalités désactivées

Par défaut, vous pouvez utiliser l'API de gestion de grille pour réactiver une fonctionnalité qui a été désactivée. Cependant, si vous souhaitez empêcher que les fonctionnalités désactivées ne soient réactivées, vous pouvez désactiver la fonctionnalité **activateFeatures** elle-même.

> La fonctionnalité **activateFeatures** ne peut pas être réactivée. Si vous décidez de désactiver cette fonctionnalité, sachez que vous perdrez définitivement la possibilité de réactiver toute autre fonctionnalité désactivée. Vous devez contacter le support technique pour restaurer toute fonctionnalité perdue.

Étapes

1. Accédez à la documentation Swagger pour l'API de gestion de grille.
2. Localisez le point de terminaison Désactiver les fonctionnalités.
3. Pour réactiver toutes les fonctionnalités, envoyez un corps à l'API comme ceci :

```
{ "grid": null }
```

Une fois cette demande terminée, toutes les fonctionnalités, y compris la fonctionnalité Modifier le mot de passe racine du locataire, sont réactivées. L'autorisation de gestion **Modifier le mot de passe racine du locataire** apparaît désormais dans l'interface utilisateur, et toute demande d'API qui tente de modifier le mot de passe racine d'un locataire réussira, en supposant que l'utilisateur dispose de l'autorisation de gestion **Accès racine** ou **Modifier le mot de passe racine du locataire**.

L'exemple précédent provoque la réactivation de *toutes* les fonctionnalités désactivées. Si d'autres fonctionnalités ont été désactivées et doivent rester désactivées, vous devez les spécifier explicitement dans la requête PUT. Par exemple, pour réactiver la fonctionnalité Modifier le mot de passe root du locataire et continuer à désactiver l'autorisation de gestion storageAdmin, envoyez cette requête PUT :

```
{ "grid": {"storageAdmin": true} }
```

Contrôler l'accès à StorageGRID

Contrôler l'accès à StorageGRID

Vous contrôlez qui peut accéder à StorageGRID et quelles tâches les utilisateurs peuvent effectuer en créant ou en important des groupes et des utilisateurs et en attribuant des autorisations à chaque groupe. En option, vous pouvez activer l'authentification unique (SSO), créer des certificats clients et modifier les mots de passe de la grille.

Contrôler l'accès au Grid Manager

Vous déterminez qui peut accéder au Grid Manager et à l'API Grid Management en important des groupes et des utilisateurs à partir d'un service de fédération d'identité ou en configurant des groupes et des utilisateurs locaux.

En utilisant"fédération d'identité" facilite la mise en place"groupes" et"utilisateurs" plus rapide et permet aux utilisateurs de se connecter à StorageGRID à l'aide d'informations d'identification familières. Vous pouvez configurer la fédération d'identité si vous utilisez Active Directory, OpenLDAP ou Oracle Directory Server.

Contactez le support technique si vous souhaitez utiliser un autre service LDAP v3.

Vous déterminez les tâches que chaque utilisateur peut effectuer en attribuant des rôles différents."autorisations" à chaque groupe. Par exemple, vous souhaiterez peut-être que les utilisateurs d'un groupe puissent gérer les règles ILM et que les utilisateurs d'un autre groupe puissent effectuer des tâches de maintenance. Un utilisateur doit appartenir à au moins un groupe pour accéder au système.

En option, vous pouvez configurer un groupe pour qu'il soit en lecture seule. Les utilisateurs d'un groupe en lecture seule peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent apporter aucune modification ni effectuer aucune opération dans Grid Manager ou l'API Grid Management.

Activer l’authentification unique

Le système StorageGRID prend en charge l’authentification unique (SSO) à l’aide de la norme Security Assertion Markup Language 2.0 (SAML 2.0). Après vous"configurer et activer SSO" , tous les utilisateurs doivent être authentifiés par un fournisseur d’identité externe avant de pouvoir accéder au Grid Manager, au Tenant Manager, à l’API Grid Management ou à l’API Tenant Management. Les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

Modifier la phrase secrète d’approvisionnement

La phrase secrète de provisionnement est requise pour de nombreuses procédures d’installation et de maintenance, ainsi que pour le téléchargement du package de récupération StorageGRID . La phrase secrète est également requise pour télécharger les sauvegardes des informations de topologie de grille et des clés de chiffrement pour le système StorageGRID . Tu peux"changer la phrase secrète" selon les besoins.

Modifier les mots de passe de la console du nœud

Chaque nœud de votre grille possède un mot de passe de console de nœud unique, dont vous avez besoin pour vous connecter au nœud en tant qu'« admin » via SSH, ou en tant qu’utilisateur root sur une connexion VM/console physique. Au besoin, vous pouvez"modifier le mot de passe de la console du nœud" pour chaque nœud.

Modifier la phrase secrète de provisionnement

Utilisez cette procédure pour modifier la phrase secrète de provisionnement StorageGRID . La phrase secrète est requise pour les procédures de récupération, d’extension et de maintenance. La phrase secrète est également requise pour télécharger les sauvegardes du package de récupération qui incluent les informations de topologie de grille, les mots de passe de la console du nœud de grille et les clés de chiffrement du système StorageGRID .

Avant de commencer

- Vous êtes connecté au Grid Manager à l’aide d’un"navigateur Web pris en charge" .
- Vous disposez des autorisations d’accès Maintenance ou Root.
- Vous disposez de la phrase secrète de provisionnement actuelle.

À propos de cette tâche

La phrase secrète de provisionnement est requise pour de nombreuses procédures d’installation et de maintenance, ainsi que pour"téléchargement du package de récupération" . La phrase secrète de provisionnement n’est pas répertoriée dans le `Passwords.txt` déposer. Assurez-vous de documenter la phrase secrète de provisionnement et de la conserver dans un endroit sûr et sécurisé.

Étapes

1. Sélectionnez **CONFIGURATION** > **Contrôle d’accès**> **Mots de passe de la grille**.
2. Sous **Modifier la phrase secrète d’approvisionnement**, sélectionnez **Effectuer une modification**
3. Saisissez votre mot de passe de provisionnement actuel.
4. Entrez la nouvelle phrase secrète. La phrase secrète doit contenir au moins 8 et pas plus de 32 caractères. Les phrases secrètes sont sensibles à la casse.
5. Stockez la nouvelle phrase secrète de provisionnement dans un endroit sûr. Il est nécessaire pour les procédures d’installation, d’extension et de maintenance.

6. Saisissez à nouveau la nouvelle phrase secrète et sélectionnez **Enregistrer**.

   Le système affiche une bannière de réussite verte lorsque la modification de la phrase secrète de provisionnement est terminée.

7. Sélectionnez **Pack de récupération**.
8. Saisissez la nouvelle phrase secrète de provisionnement pour télécharger le nouveau package de récupération.

> Après avoir modifié la phrase secrète de provisionnement, vous devez immédiatement télécharger un nouveau package de récupération. Le fichier Recovery Package vous permet de restaurer le système en cas de panne.

Modifier les mots de passe de la console du nœud

Chaque nœud de votre grille possède un mot de passe de console de nœud unique, dont vous avez besoin pour vous connecter au nœud. Suivez ces étapes pour modifier chaque mot de passe de console de nœud unique pour chaque nœud de votre grille.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès de maintenance ou root" .
- Vous disposez de la phrase secrète de provisionnement actuelle.

À propos de cette tâche

Utilisez le mot de passe de la console du nœud pour vous connecter à un nœud en tant qu'« administrateur » à l'aide de SSH ou en tant qu'utilisateur root sur une connexion VM/console physique. Le processus de changement de mot de passe de la console du nœud crée de nouveaux mots de passe pour chaque nœud de votre grille et stocke les mots de passe dans un fichier mis à jour. `Passwords.txt` fichier dans le package de récupération. Les mots de passe sont répertoriés dans la colonne Mot de passe du fichier Passwords.txt.

> Il existe des mots de passe d'accès SSH distincts pour les clés SSH utilisées pour la communication entre les nœuds. Les mots de passe d'accès SSH ne sont pas modifiés par cette procédure.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Mots de passe de la grille**.
2. Sous **Modifier les mots de passe de la console du nœud**, sélectionnez **Effectuer une modification**.

Saisissez la phrase secrète de provisionnement

Étapes

1. Saisissez la phrase secrète de provisionnement de votre grille.
2. Sélectionnez **Continuer**.

Télécharger le package de récupération actuel

Avant de modifier les mots de passe de la console du nœud, téléchargez le package de récupération actuel. Vous pouvez utiliser les mots de passe de ce fichier si le processus de changement de mot de passe échoue pour un nœud.

Étapes

1. Sélectionnez **Télécharger le package de récupération**.
2. Copier le fichier du package de récupération(`.zip`) vers deux endroits sûrs, sécurisés et séparés.

   Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID .

3. Sélectionnez **Continuer**.
4. Lorsque la boîte de dialogue de confirmation s'affiche, sélectionnez **Oui** si vous êtes prêt à commencer à modifier les mots de passe de la console du nœud.

   Vous ne pouvez pas annuler ce processus une fois qu'il a commencé.

Modifier les mots de passe de la console du nœud

Lorsque le processus de mot de passe de la console du nœud démarre, un nouveau package de récupération est généré qui inclut les nouveaux mots de passe. Ensuite, les mots de passe sont mis à jour sur chaque nœud.

Étapes

1. Attendez que le nouveau package de récupération soit généré, ce qui peut prendre quelques minutes.
2. Sélectionnez **Télécharger un nouveau package de récupération**.
3. Une fois le téléchargement terminé :

   a. Ouvrez le `.zip` déposer.

   b. Confirmez que vous pouvez accéder au contenu, y compris le `Passwords.txt` fichier, qui contient les nouveaux mots de passe de la console du nœud.

   c. Copiez le nouveau fichier du package de récupération(`.zip`) vers deux endroits sûrs, sécurisés et séparés.

      N'écrasez pas l'ancien package de récupération.

   Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID .

4. Cochez la case pour indiquer que vous avez téléchargé le nouveau package de récupération et vérifié le contenu.
5. Sélectionnez **Modifier les mots de passe de la console du nœud** et attendez que tous les nœuds soient mis à jour avec les nouveaux mots de passe. Cela peut prendre quelques minutes.

   Si les mots de passe sont modifiés pour tous les nœuds, une bannière de réussite verte apparaît. Passez à l'étape suivante.

S'il y a une erreur pendant le processus de mise à jour, un message de bannière répertorie le nombre de nœuds dont le mot de passe n'a pas pu être modifié. Le système réessaiera automatiquement le processus sur tout nœud dont le mot de passe n'a pas été modifié. Si le processus se termine et que certains nœuds n'ont toujours pas de mot de passe modifié, le bouton **Réessayer** apparaît.

Si la mise à jour du mot de passe a échoué pour un ou plusieurs nœuds :

a. Consultez les messages d'erreur répertoriés dans le tableau.

b. Résoudre les problèmes.

c. Sélectionnez **Réessayer**.

> La nouvelle tentative modifie uniquement les mots de passe de la console du nœud sur les nœuds qui ont échoué lors des tentatives de modification de mot de passe précédentes.

6. Une fois les mots de passe de la console de nœud modifiés pour tous les nœuds, supprimez lepremier package de récupération que vous avez téléchargé .
7. Vous pouvez également utiliser le lien **Pack de récupération** pour télécharger une copie supplémentaire du nouveau package de récupération.

Modifier les mots de passe d'accès SSH pour les nœuds d'administration

La modification des mots de passe d'accès SSH pour les nœuds d'administration met également à jour les ensembles uniques de clés SSH internes pour chaque nœud de la grille. Le nœud d'administration principal utilise ces clés SSH pour accéder aux nœuds à l'aide d'une authentification sécurisée et sans mot de passe.

Utilisez une clé SSH pour vous connecter à un nœud en tant que `admin` ou à l'utilisateur root sur une connexion VM ou console physique.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès de maintenance ou root" .
- Vous disposez de la phrase secrète de provisionnement actuelle.

À propos de cette tâche

Les nouveaux mots de passe d'accès pour les nœuds d'administration et les nouvelles clés internes pour chaque nœud sont stockés dans le `Passwords.txt` fichier dans le package de récupération. Les clés sont répertoriées dans la colonne Mot de passe de ce fichier.

Il existe des mots de passe d'accès SSH distincts pour les clés SSH utilisées pour la communication entre les nœuds. Ceux-ci ne sont pas modifiés par cette procédure.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Mots de passe de la grille**.
2. Sous **Modifier les clés SSH**, sélectionnez **Effectuer une modification**.

Télécharger le package de récupération actuel

Avant de modifier les clés d'accès SSH, téléchargez le package de récupération actuel. Vous pouvez utiliser les clés de ce fichier si le processus de changement de clé échoue pour un nœud.

Étapes

1. Saisissez la phrase secrète de provisionnement de votre grille.
2. Sélectionnez **Télécharger le package de récupération**.
3. Copier le fichier du package de récupération(`.zip`) vers deux endroits sûrs, sécurisés et séparés.

   > Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID .

4. Sélectionnez **Continuer**.
5. Lorsque la boîte de dialogue de confirmation apparaît, sélectionnez **Oui** si vous êtes prêt à commencer à modifier les clés d'accès SSH.

   > Vous ne pouvez pas annuler ce processus une fois qu'il a commencé.

Modifier les clés d'accès SSH

Lorsque le processus de modification des clés d'accès SSH démarre, un nouveau package de récupération est généré qui inclut les nouvelles clés. Ensuite, les clés sont mises à jour sur chaque nœud.

Étapes

1. Attendez que le nouveau package de récupération soit généré, ce qui peut prendre quelques minutes.
2. Lorsque le bouton Télécharger un nouveau package de récupération est activé, sélectionnez **Télécharger un nouveau package de récupération** et enregistrez le nouveau fichier de package de récupération(`.zip`) vers deux endroits sûrs, sécurisés et séparés.
3. Une fois le téléchargement terminé :

   a. Ouvrez le `.zip` déposer.

   b. Confirmez que vous pouvez accéder au contenu, y compris le `Passwords.txt` fichier, qui contient les nouvelles clés d'accès SSH.

   c. Copiez le nouveau fichier du package de récupération(`.zip`) vers deux endroits sûrs, sécurisés et séparés.

      > N'écrasez pas l'ancien package de récupération.

   Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID .

4. Attendez que les clés soient mises à jour sur chaque nœud, ce qui peut prendre quelques minutes.

   Si les clés sont modifiées pour tous les nœuds, une bannière de réussite verte apparaît.

   En cas d'erreur lors du processus de mise à jour, un message de bannière répertorie le nombre de nœuds dont les clés n'ont pas pu être modifiées. Le système réessaiera automatiquement le processus sur tout

nœud dont la clé n'a pas été modifiée. Si le processus se termine avec certains nœuds n'ayant toujours pas de clé modifiée, le bouton **Réessayer** apparaît.

Si la mise à jour de la clé a échoué pour un ou plusieurs nœuds :

a. Consultez les messages d'erreur répertoriés dans le tableau.
b. Résoudre les problèmes.
c. Sélectionnez **Réessayer**.

La nouvelle tentative modifie uniquement les clés d'accès SSH sur les nœuds qui ont échoué lors des tentatives de modification de clé précédentes.

5. Une fois les clés d'accès SSH modifiées pour tous les nœuds, supprimez lepremier package de récupération que vous avez téléchargé .
6. Vous pouvez également sélectionner **MAINTENANCE** > **Système** > **Pack de récupération** pour télécharger une copie supplémentaire du nouveau package de récupération.

Utiliser la fédération d'identité

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

Configurer la fédération d'identité pour Grid Manager

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

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"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 qui n'est pas répertorié, contactez le support technique.

- Si vous prévoyez d'utiliser OpenLDAP, vous devez configurer le serveur OpenLDAP. Voir Directives pour la configuration d'un serveur OpenLDAP .
- Si vous envisagez d'activer l'authentification unique (SSO), vous avez examiné les"exigences et considérations relatives à l'authentification unique" .
- Si vous prévoyez d'utiliser Transport Layer Security (TLS) pour les communications avec le serveur LDAP, le fournisseur d'identité utilise TLS 1.2 ou 1.3. Voir "Chiffres pris en charge pour les connexions TLS sortantes" .

À propos de cette tâche

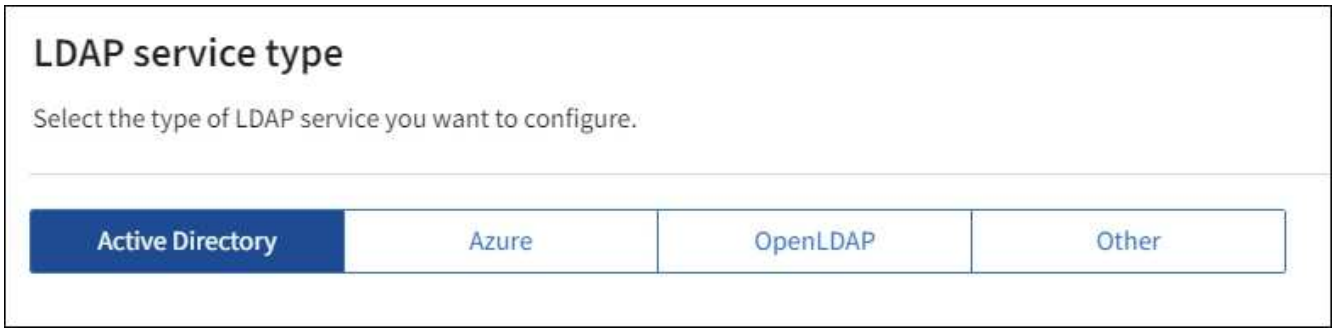
Vous pouvez configurer une source d'identité pour Grid Manager si vous souhaitez importer des groupes à partir d'un autre système tel qu'Active Directory, Azure AD, OpenLDAP ou Oracle Directory Server. Vous pouvez importer les types de groupes suivants :

- Groupes d'administrateurs. Les utilisateurs des groupes d'administrateurs peuvent se connecter au gestionnaire de grille et effectuer des tâches, en fonction des autorisations de gestion attribuées au groupe.
- Groupes d'utilisateurs locataires pour les locataires qui n'utilisent pas leur propre source d'identité. Les utilisateurs des groupes de locataires peuvent se connecter au gestionnaire de locataires et effectuer des tâches, en fonction des autorisations attribuées au groupe dans le gestionnaire de locataires. Voir"Créer un compte locataire" et"Utiliser un compte locataire" pour plus de détails.

Entrer la configuration

Étapes

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



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

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

- **Port** : Le port utilisé pour se connecter au serveur LDAP.

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

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

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

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

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

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

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

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

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

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

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

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

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

  Saisissez l'un de ces modèles :

  - **Modèle UserPrincipalName (Active Directory et Azure)**: `[USERNAME]@*example*.com`

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

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

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

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

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

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

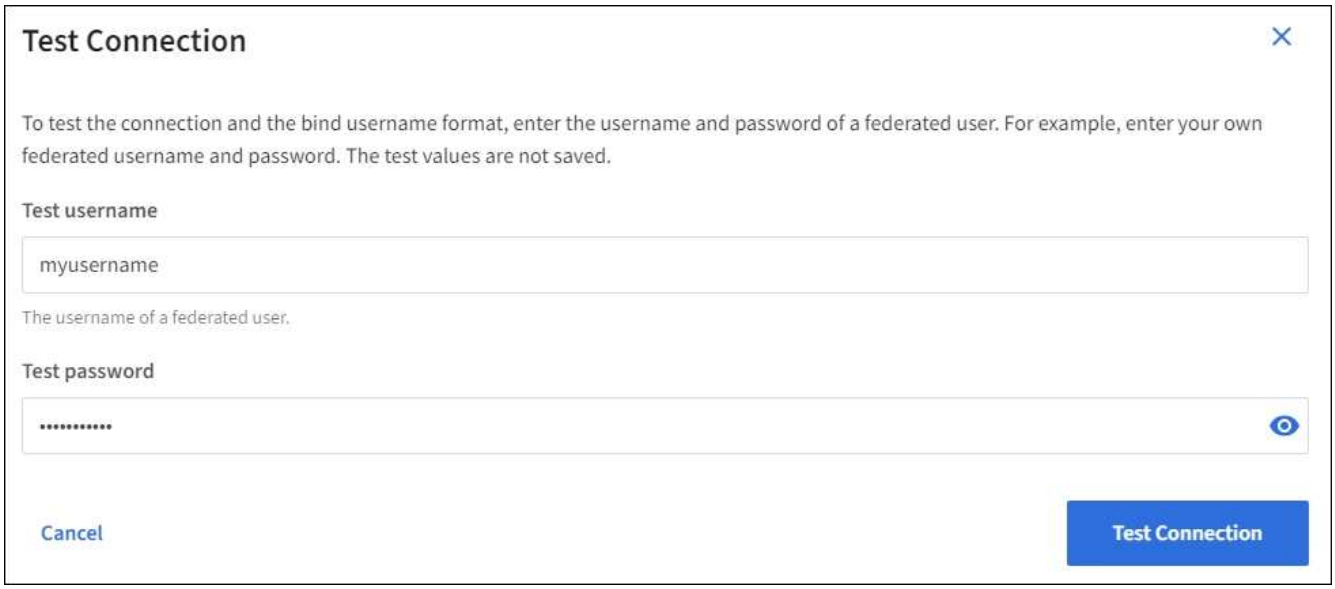
Tester la connexion et enregistrer la configuration

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

Étapes

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

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



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

Forcer la synchronisation avec la source d'identité

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

Étapes

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

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

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

Désactiver la fédération d'identité

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

À propos de cette tâche

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

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

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

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

Étapes

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

Directives pour la configuration d'un serveur OpenLDAP

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

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

Superpositions Memberof et refint

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

Indexage

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

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

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

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

Gérer les groupes d'administrateurs

Vous pouvez créer des groupes d'administrateurs pour gérer les autorisations de sécurité d'un ou plusieurs utilisateurs administrateurs. Les utilisateurs doivent appartenir à un groupe pour avoir accès au système StorageGRID .

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .
- Si vous prévoyez d'importer un groupe fédéré, vous avez configuré la fédération d'identité et le groupe fédéré existe déjà dans la source d'identité configurée.

Créer un groupe d'administrateurs

Les groupes d'administrateurs vous permettent de déterminer quels utilisateurs peuvent accéder à quelles fonctionnalités et opérations dans Grid Manager et l'API Grid Management.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Groupes d'administrateurs**.
2. Sélectionnez **Créer un groupe**.

Choisissez un type de groupe

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

- Créez un groupe local si vous souhaitez attribuer des autorisations aux utilisateurs locaux.
- Créez un groupe fédéré pour importer des utilisateurs à partir de la source d'identité.

Groupe local

Étapes

1. Sélectionnez **Groupe local**.
2. Saisissez un nom d'affichage pour le groupe, que vous pourrez mettre à jour ultérieurement si nécessaire. Par exemple, « Utilisateurs de maintenance » ou « Administrateurs ILM ».
3. Saisissez un nom unique pour le groupe, que vous ne pourrez pas mettre à jour ultérieurement.
4. Sélectionnez **Continuer**.

Groupe fédéré

Étapes

1. Sélectionnez **Groupe fédéré**.
2. Saisissez le nom du groupe que vous souhaitez importer, exactement tel qu'il apparaît dans la source d'identité configurée.
   - Pour Active Directory et Azure, utilisez sAMAccountName.
   - Pour OpenLDAP, utilisez le CN (Common Name).
   - Pour un autre LDAP, utilisez le nom unique approprié pour le serveur LDAP.
3. Sélectionnez **Continuer**.

Gérer les autorisations de groupe

Étapes

1. Pour le **Mode d'accès**, sélectionnez si les utilisateurs du groupe peuvent modifier les paramètres et effectuer des opérations dans le gestionnaire de grille et l'API de gestion de grille ou s'ils peuvent

uniquement afficher les paramètres et les fonctionnalités.

- **Lecture-écriture** (par défaut) : les utilisateurs peuvent modifier les paramètres et effectuer les opérations autorisées par leurs autorisations de gestion.
- **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent apporter aucune modification ni effectuer aucune opération dans Grid Manager ou l'API Grid Management. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.

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

2. Sélectionnez un ou plusieurs"autorisations du groupe administrateur" .

   Vous devez attribuer au moins une autorisation à chaque groupe ; sinon, les utilisateurs appartenant au groupe ne pourront pas se connecter à StorageGRID.

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

Ajouter des utilisateurs (groupes locaux uniquement)

Étapes

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

   Si vous n'avez pas encore créé d'utilisateurs locaux, vous pouvez enregistrer le groupe sans ajouter d'utilisateurs. Vous pouvez ajouter ce groupe à l'utilisateur sur la page Utilisateurs. Voir"Gérer les utilisateurs" pour plus de détails.

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

Afficher et modifier les groupes d'administrateurs

Vous pouvez afficher les détails des groupes existants, modifier un groupe ou dupliquer un groupe.

- Pour afficher les informations de base de tous les groupes, consultez le tableau sur la page Groupes.
- Pour afficher tous les détails d'un groupe spécifique ou pour modifier un groupe, utilisez le menu **Actions** ou la page de détails.

Tâche	Menu Actions	Page de détails
Afficher les détails du groupe	a. Cochez la case correspondant au groupe. b. Sélectionnez **Actions** > **Afficher les détails du groupe**.	Sélectionnez le nom du groupe dans le tableau.

Tâche	Menu Actions	Page de détails
Modifier le nom d'affichage (groupes locaux uniquement)	a. Cochez la case correspondant au groupe. b. Sélectionnez **Actions** > **Modifier le nom du groupe**. c. Entrez le nouveau nom. d. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom du groupe pour afficher les détails. b. Sélectionnez l'icône d'édition . c. Entrez le nouveau nom. d. Sélectionnez **Enregistrer les modifications**.
Modifier le mode d'accès ou les autorisations	a. Cochez la case correspondant au groupe. b. Sélectionnez **Actions** > **Afficher les détails du groupe**. c. Vous pouvez également modifier le mode d'accès du groupe. d. En option, sélectionnez ou désélectionnez"autorisations du groupe administrateur" . e. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom du groupe pour afficher les détails. b. Vous pouvez également modifier le mode d'accès du groupe. c. En option, sélectionnez ou désélectionnez"autorisations du groupe administrateur" . d. Sélectionnez **Enregistrer les modifications**.

Dupliquer un groupe

Étapes

1. Cochez la case correspondant au groupe.
2. Sélectionnez **Actions** > **Dupliquer le groupe**.
3. Complétez l'assistant de duplication de groupe.

Supprimer un groupe

Vous pouvez supprimer un groupe d'administrateurs lorsque vous souhaitez supprimer le groupe du système et supprimer toutes les autorisations associées au groupe. La suppression d'un groupe d'administrateurs supprime tous les utilisateurs du groupe, mais ne supprime pas les utilisateurs.

Étapes

1. Depuis la page Groupes, cochez la case correspondant à chaque groupe que vous souhaitez supprimer.
2. Sélectionnez **Actions** > **Supprimer le groupe**.
3. Sélectionnez **Supprimer les groupes**.

Autorisations du groupe d'administrateurs

Lors de la création de groupes d'utilisateurs administrateurs, vous sélectionnez une ou plusieurs autorisations pour contrôler l'accès à des fonctionnalités spécifiques du gestionnaire de grille. Vous pouvez ensuite affecter chaque utilisateur à un ou plusieurs de ces groupes d'administrateurs pour déterminer les tâches que cet utilisateur peut

effectuer.

Vous devez attribuer au moins une autorisation à chaque groupe ; sinon, les utilisateurs appartenant à ce groupe ne pourront pas se connecter au gestionnaire de grille ou à l'API de gestion de grille.

Par défaut, tout utilisateur appartenant à un groupe disposant d'au moins une autorisation peut effectuer les tâches suivantes :

- Sign in au gestionnaire de grille
- Afficher le tableau de bord
- Afficher les pages Nœuds
- Afficher les alertes actuelles et résolues
- Modifier leur propre mot de passe (utilisateurs locaux uniquement)
- Consultez certaines informations fournies sur les pages Configuration et Maintenance

Interaction entre les autorisations et le mode d'accès

Pour toutes les autorisations, le paramètre **Mode d'accès** du groupe détermine si les utilisateurs peuvent modifier les paramètres et effectuer des opérations ou s'ils peuvent uniquement afficher les paramètres et fonctionnalités associés. Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur **Lecture seule**, l'utilisateur aura un accès en lecture seule à tous les paramètres et fonctionnalités sélectionnés.

Les sections suivantes décrivent les autorisations que vous pouvez attribuer lors de la création ou de la modification d'un groupe d'administrateurs. Toute fonctionnalité non explicitement mentionnée nécessite l'autorisation **Accès root**.

Accès root

Cette autorisation donne accès à toutes les fonctionnalités d'administration du réseau.

Modifier le mot de passe root du locataire

Cette autorisation donne accès à l'option **Modifier le mot de passe root** sur la page Locataires, vous permettant de contrôler qui peut modifier le mot de passe de l'utilisateur root local du locataire. Cette autorisation est également utilisée pour migrer les clés S3 lorsque la fonctionnalité d'importation de clés S3 est activée. Les utilisateurs qui ne disposent pas de cette autorisation ne peuvent pas voir l'option **Modifier le mot de passe root**.

> Pour accorder l'accès à la page Locataires, qui contient l'option **Modifier le mot de passe root**, attribuez également l'autorisation **Comptes locataires**.

Configuration de la page de topologie de grille

Cette autorisation donne accès aux onglets de configuration sur la page **SUPPORT** > **Outils** > **Topologie de grille**.

> La page Topologie de grille est obsolète et sera supprimée dans une prochaine version.

ILM

Cette autorisation donne accès aux options de menu **ILM** suivantes :

- Règles
- Politiques
- Balises de politique
- Piscines de stockage
- Niveaux de stockage
- Régions
- Recherche de métadonnées d'objet

> Les utilisateurs doivent disposer des autorisations **Autre configuration de grille** et **Configuration de la page de topologie de grille** pour gérer les niveaux de stockage.

Entretien

Les utilisateurs doivent disposer de l'autorisation Maintenance pour utiliser ces options :

- **CONFIGURATION** > **Contrôle d'accès**:
  - Mots de passe de la grille
- **CONFIGURATION** > **Réseau**:
  - Noms de domaine de point de terminaison S3
- **ENTRETIEN** > **Tâches**:
  - Déclassement
  - Expansion
  - Vérification de l'existence de l'objet
  - Récupération
- **ENTRETIEN** > **Système** :
  - Paquet de relance
  - Mise à jour du logiciel
- **SUPPORT** > **Outils**:
  - Journaux

Les utilisateurs qui ne disposent pas de l'autorisation Maintenance peuvent afficher, mais pas modifier, ces pages :

- **ENTRETIEN** > **Réseau** :
  - serveurs DNS
  - Réseau de grille
  - Serveurs NTP
- **ENTRETIEN** > **Système** :
  - Licence
- **CONFIGURATION** > **Réseau**:
  - Noms de domaine de point de terminaison S3

- **CONFIGURATION** > **Sécurité**:
  - Certificats
- **CONFIGURATION** > **Surveillance**:
  - Serveur d'audit et syslog

Gérer les alertes

Cette autorisation donne accès aux options de gestion des alertes. Les utilisateurs doivent disposer de cette autorisation pour gérer les silences, les notifications d'alerte et les règles d'alerte.

Requête de métriques

Cette autorisation donne accès à :

- **SUPPORT** > **Outils** > Page **Métriques**
- Requêtes de métriques Prometheus personnalisées à l'aide de la section **Metrics** de l'API Grid Management
- Cartes de tableau de bord Grid Manager contenant des métriques

Recherche de métadonnées d'objet

Cette autorisation donne accès à la page **ILM** > **Recherche de métadonnées d'objet**.

Autre configuration de grille

Cette autorisation donne accès à des options de configuration de grille supplémentaires.

Pour voir ces options supplémentaires, les utilisateurs doivent également disposer de l'autorisation **Configuration de la page de topologie de grille**.

- **ILM**:
  - Niveaux de stockage
- **CONFIGURATION** > **Système**:
- **SOUTIEN** > **Autre** :
  - Coût du lien

Administrateur d'appareils de stockage

Cette autorisation prévoit :

- Accès au gestionnaire de système SANtricity E-Series sur les appliances de stockage via Grid Manager.
- La possibilité d'effectuer des tâches de dépannage et de maintenance sur l'onglet Gérer les lecteurs pour les appareils qui prennent en charge ces opérations.

Comptes locataires

Cette autorisation donne la possibilité de :

- Accédez à la page Locataires, où vous pouvez créer, modifier et supprimer des comptes locataires

- Afficher les politiques de classification du trafic existantes
- Afficher les cartes du tableau de bord Grid Manager qui contiennent les détails du locataire

Gérer les utilisateurs

Vous pouvez afficher les utilisateurs locaux et fédérés. Vous pouvez également créer des utilisateurs locaux et les affecter à des groupes d'administrateurs locaux pour déterminer les fonctionnalités de Grid Manager auxquelles ces utilisateurs peuvent accéder.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .

Créer un utilisateur local

Vous pouvez créer un ou plusieurs utilisateurs locaux et affecter chaque utilisateur à un ou plusieurs groupes locaux. Les autorisations du groupe contrôlent les fonctionnalités de Grid Manager et de l'API Grid Management auxquelles l'utilisateur peut accéder.

Vous ne pouvez créer que des utilisateurs locaux. Utilisez la source d'identité externe pour gérer les utilisateurs et les groupes fédérés.

Le gestionnaire de grille comprend un utilisateur local prédéfini, nommé « root ». Vous ne pouvez pas supprimer l'utilisateur root.

> Si l'authentification unique (SSO) est activée, les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Utilisateurs administrateurs**.
2. Sélectionnez **Créer un utilisateur**.

Entrez les informations d'identification de l'utilisateur

Étapes

1. Saisissez le nom complet de l'utilisateur, un nom d'utilisateur unique et un mot de passe.
2. Si vous le souhaitez, sélectionnez **Oui** si cet utilisateur ne doit pas avoir accès au Grid Manager ou à l'API Grid Management.
3. Sélectionnez **Continuer**.

Affecter à des groupes

Étapes

1. Vous pouvez également affecter l'utilisateur à un ou plusieurs groupes pour déterminer les autorisations de l'utilisateur.

   Si vous n'avez pas encore créé de groupes, vous pouvez enregistrer l'utilisateur sans sélectionner de groupes. Vous pouvez ajouter cet utilisateur à un groupe sur la page Groupes.

Si un utilisateur appartient à plusieurs groupes, les autorisations sont cumulatives. Voir"Gérer les groupes d'administrateurs" pour plus de détails.

2. Sélectionnez **Créer un utilisateur** et sélectionnez **Terminer**.

Afficher et modifier les utilisateurs locaux

Vous pouvez afficher les détails des utilisateurs locaux et fédérés existants. Vous pouvez modifier un utilisateur local pour modifier son nom complet, son mot de passe ou son appartenance à un groupe. Vous pouvez également empêcher temporairement un utilisateur d'accéder au Grid Manager et à l'API Grid Management.

Vous ne pouvez modifier que les utilisateurs locaux. Utilisez la source d'identité externe pour gérer les utilisateurs fédérés.

- Pour afficher les informations de base de tous les utilisateurs locaux et fédérés, consultez le tableau sur la page Utilisateurs.
- Pour afficher tous les détails d'un utilisateur spécifique, modifier un utilisateur local ou changer le mot de passe d'un utilisateur local, utilisez le menu **Actions** ou la page de détails.

  Toutes les modifications sont appliquées la prochaine fois que l'utilisateur se déconnecte, puis se reconnecte au gestionnaire de grille.

> Les utilisateurs locaux peuvent modifier leurs propres mots de passe à l'aide de l'option **Modifier le mot de passe** dans la bannière du gestionnaire de grille.

Tâche	Menu Actions	Page de détails
Afficher les détails de l'utilisateur	a. Cochez la case correspondant à l'utilisateur. b. Sélectionnez **Actions** > **Afficher les détails de l'utilisateur**.	Sélectionnez le nom de l'utilisateur dans le tableau.
Modifier le nom complet (utilisateurs locaux uniquement)	a. Cochez la case correspondant à l'utilisateur. b. Sélectionnez **Actions** > **Modifier le nom complet**. c. Entrez le nouveau nom. d. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'icône d'édition . c. Entrez le nouveau nom. d. Sélectionnez **Enregistrer les modifications**.

Tâche	Menu Actions	Page de détails
Refuser ou autoriser l'accès à StorageGRID	a. Cochez la case correspondant à l'utilisateur. b. Sélectionnez **Actions** > **Afficher les détails de l'utilisateur**. c. Sélectionnez l'onglet Accès. d. Sélectionnez **Oui** pour empêcher l'utilisateur de se connecter au gestionnaire de grille ou à l'API de gestion de grille, ou sélectionnez **Non** pour autoriser l'utilisateur à se connecter. e. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'onglet Accès. c. Sélectionnez **Oui** pour empêcher l'utilisateur de se connecter au gestionnaire de grille ou à l'API de gestion de grille, ou sélectionnez **Non** pour autoriser l'utilisateur à se connecter. d. Sélectionnez **Enregistrer les modifications**.
Changer le mot de passe (utilisateurs locaux uniquement)	a. Cochez la case correspondant à l'utilisateur. b. Sélectionnez **Actions** > **Afficher les détails de l'utilisateur**. c. Sélectionnez l'onglet Mot de passe. d. Entrez un nouveau mot de passe. e. Sélectionnez **Modifier le mot de passe**.	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'onglet Mot de passe. c. Entrez un nouveau mot de passe. d. Sélectionnez **Modifier le mot de passe**.
Changer de groupe (utilisateurs locaux uniquement)	a. Cochez la case correspondant à l'utilisateur. b. Sélectionnez **Actions** > **Afficher les détails de l'utilisateur**. c. Sélectionnez l'onglet Groupes. d. Vous pouvez également sélectionner le lien après le nom d'un groupe pour afficher les détails du groupe dans un nouvel onglet du navigateur. e. Sélectionnez **Modifier les groupes** pour sélectionner différents groupes. f. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'onglet Groupes. c. Vous pouvez également sélectionner le lien après le nom d'un groupe pour afficher les détails du groupe dans un nouvel onglet du navigateur. d. Sélectionnez **Modifier les groupes** pour sélectionner différents groupes. e. Sélectionnez **Enregistrer les modifications**.

Dupliquer un utilisateur

Vous pouvez dupliquer un utilisateur existant pour créer un nouvel utilisateur avec les mêmes autorisations.

Étapes

1. Cochez la case correspondant à l'utilisateur.

2. Sélectionnez **Actions** > **Dupliquer l'utilisateur**.
3. Complétez l'assistant de duplication d'utilisateur.

Supprimer un utilisateur

Vous pouvez supprimer un utilisateur local pour supprimer définitivement cet utilisateur du système.

> Vous ne pouvez pas supprimer l'utilisateur root.

Étapes

1. Depuis la page Utilisateurs, cochez la case correspondant à chaque utilisateur que vous souhaitez supprimer.
2. Sélectionnez **Actions** > **Supprimer l'utilisateur**.
3. Sélectionnez **Supprimer l'utilisateur**.

Utiliser l'authentification unique (SSO)

Configurer l'authentification unique

Lorsque l'authentification unique (SSO) est activée, les utilisateurs ne peuvent accéder au gestionnaire de grille, au gestionnaire de locataires, à l'API de gestion de grille ou à l'API de gestion de locataires que si leurs informations d'identification sont autorisées à l'aide du processus de connexion SSO mis en œuvre par votre organisation. Les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

Comment fonctionne l'authentification unique

Le système StorageGRID prend en charge l'authentification unique (SSO) à l'aide de la norme Security Assertion Markup Language 2.0 (SAML 2.0).

Avant d'activer l'authentification unique (SSO), vérifiez comment les processus de connexion et de déconnexion StorageGRID sont affectés lorsque SSO est activé.

Sign in lorsque SSO est activé

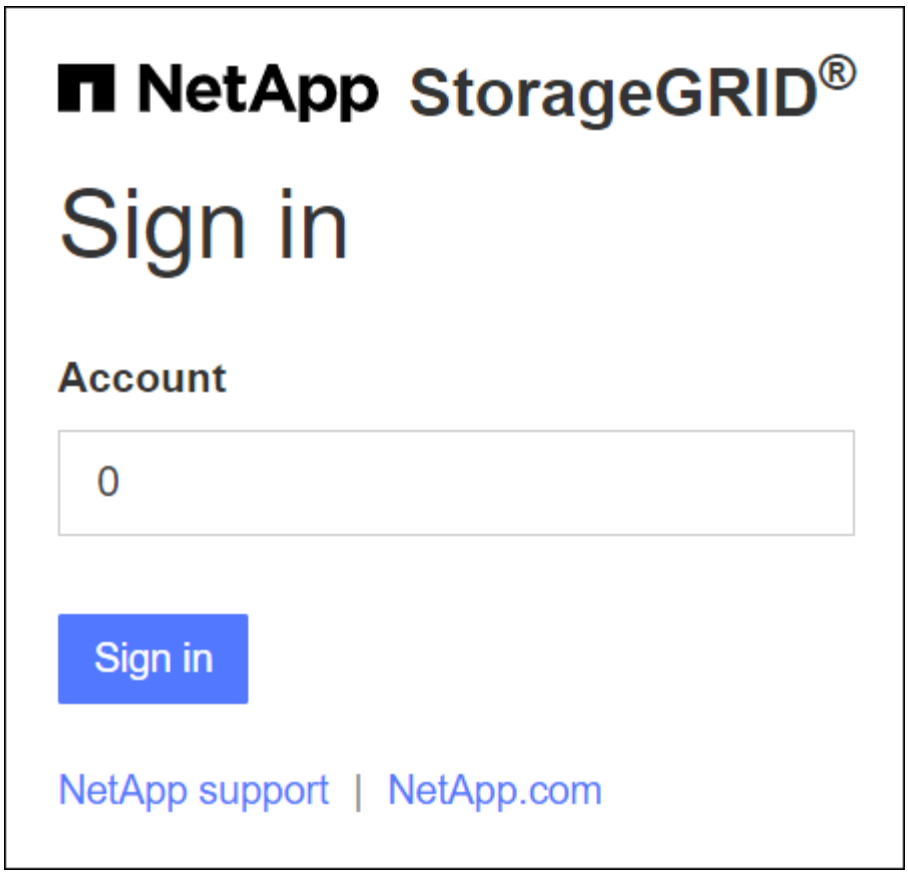
Lorsque SSO est activé et que vous vous connectez à StorageGRID, vous êtes redirigé vers la page SSO de votre organisation pour valider vos informations d'identification.

Étapes

1. Saisissez le nom de domaine complet ou l'adresse IP de n'importe quel nœud d'administration StorageGRID dans un navigateur Web.

   La page de Sign in StorageGRID s'affiche.

   - Si c'est la première fois que vous accédez à l'URL sur ce navigateur, vous êtes invité à saisir un identifiant de compte :

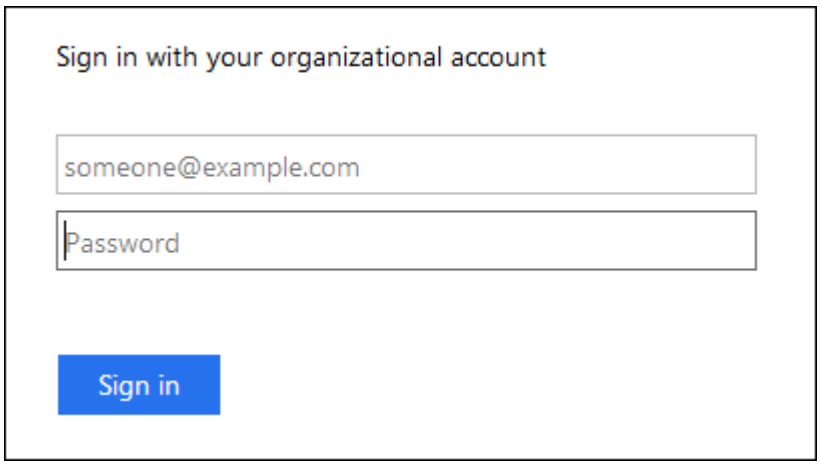


- Si vous avez déjà accédé au Grid Manager ou au Tenant Manager, vous êtes invité à sélectionner un compte récent ou à saisir un ID de compte :

La page de Sign in StorageGRID ne s'affiche pas lorsque vous saisissez l'URL complète d'un compte locataire (c'est-à-dire un nom de domaine complet ou une adresse IP suivi de `/?accountId=20-digit-account-id`). Au lieu de cela, vous êtes immédiatement redirigé vers la page de connexion SSO de votre organisation, où vous pouvezconnectez-vous avec vos identifiants SSO .

2. Indiquez si vous souhaitez accéder au Grid Manager ou au Tenant Manager :
   - Pour accéder au Gestionnaire de grille, laissez le champ **ID de compte** vide, saisissez **0** comme ID de compte ou sélectionnez **Gestionnaire de grille** s'il apparaît dans la liste des comptes récents.
   - Pour accéder au gestionnaire de locataires, saisissez l'ID de compte locataire à 20 chiffres ou sélectionnez un locataire par son nom s'il apparaît dans la liste des comptes récents.
3. Sélectionner * Sign in*

   StorageGRID vous redirige vers la page de connexion SSO de votre organisation. Par exemple:



4. Sign in avec vos identifiants SSO.

   Si vos informations d'identification SSO sont correctes :

   a. Le fournisseur d'identité (IdP) fournit une réponse d'authentification à StorageGRID.
   b. StorageGRID valide la réponse d'authentification.
   c. Si la réponse est valide et que vous appartenez à un groupe fédéré avec des autorisations d'accès StorageGRID , vous êtes connecté au Grid Manager ou au Tenant Manager, selon le compte que vous avez sélectionné.

   Si le compte de service est inaccessible, vous pouvez toujours vous connecter, à condition que vous soyez un utilisateur existant appartenant à un groupe fédéré avec des autorisations d'accès StorageGRID .

5. Vous pouvez également accéder à d'autres nœuds d'administration ou accéder au gestionnaire de grille ou au gestionnaire de locataires, si vous disposez des autorisations adéquates.

   Vous n'avez pas besoin de ressaisir vos identifiants SSO.

Déconnectez-vous lorsque SSO est activé

Lorsque SSO est activé pour StorageGRID, ce qui se passe lorsque vous vous déconnectez dépend de ce à quoi vous êtes connecté et de l'endroit d'où vous vous déconnectez.

Étapes

1. Localisez le lien **Déconnexion** dans le coin supérieur droit de l'interface utilisateur.
2. Sélectionnez **Déconnexion**.

   La page de Sign in StorageGRID s'affiche. La liste déroulante **Comptes récents** est mise à jour pour inclure **Grid Manager** ou le nom du locataire, afin que vous puissiez accéder à ces interfaces utilisateur plus rapidement à l'avenir.

Si vous êtes connecté à…	Et vous vous déconnectez de…	Vous êtes déconnecté de…
Gestionnaire de grille sur un ou plusieurs nœuds d'administration	Gestionnaire de grille sur n'importe quel nœud d'administration	Gestionnaire de grille sur tous les nœuds d'administration **Remarque :** si vous utilisez Azure pour l'authentification unique, la déconnexion de tous les nœuds d'administration peut prendre quelques minutes.
Gestionnaire de locataires sur un ou plusieurs nœuds d'administration	Gestionnaire de locataires sur n'importe quel nœud d'administration	Gestionnaire de locataires sur tous les nœuds d'administration
Gestionnaire de réseau et gestionnaire de locataires	Gestionnaire de grille	Le gestionnaire de grille uniquement. Vous devez également vous déconnecter du gestionnaire de locataires pour vous déconnecter de SSO.

Le tableau résume ce qui se passe lorsque vous vous déconnectez si vous utilisez une seule session de navigateur. Si vous êtes connecté à StorageGRID sur plusieurs sessions de navigateur, vous devez vous déconnecter de toutes les sessions de navigateur séparément.

Exigences et considérations relatives à l'authentification unique

Avant d'activer l'authentification unique (SSO) pour un système StorageGRID , examinez les exigences et les considérations.

Exigences relatives aux fournisseurs d'identité

StorageGRID prend en charge les fournisseurs d'identité SSO (IdP) suivants :

- Service de fédération Active Directory (AD FS)
- Azure Active Directory (Azure AD)
- PingFédéré

Vous devez configurer la fédération d'identité pour votre système StorageGRID avant de pouvoir configurer un fournisseur d'identité SSO. Le type de service LDAP que vous utilisez pour la fédération d'identité contrôle le type de SSO que vous pouvez implémenter.

Type de service LDAP configuré	Options pour le fournisseur d'identité SSO
Active Directory	• Active Directory • Azuré • PingFédéré
Azuré	Azuré

Exigences AD FS

Vous pouvez utiliser l'une des versions suivantes d'AD FS :

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS

> Windows Server 2016 devrait utiliser le "Mise à jour KB3201845" , ou supérieur.

Exigences supplémentaires

- Sécurité de la couche transport (TLS) 1.2 ou 1.3
- Microsoft .NET Framework, version 3.5.1 ou supérieure

Considérations pour Azure

Si vous utilisez Azure comme type SSO et que les utilisateurs ont des noms d'utilisateur principaux qui n'utilisent pas sAMAccountName comme préfixe, des problèmes de connexion peuvent survenir si StorageGRID perd sa connexion avec le serveur LDAP. Pour permettre aux utilisateurs de se connecter, vous devez restaurer la connexion au serveur LDAP.

Exigences relatives aux certificats de serveur

Par défaut, StorageGRID utilise un certificat d'interface de gestion sur chaque nœud d'administration pour sécuriser l'accès au gestionnaire de grille, au gestionnaire de locataires, à l'API de gestion de grille et à l'API de gestion de locataires. Lorsque vous configurez des approbations de parties de confiance (AD FS), des applications d'entreprise (Azure) ou des connexions de fournisseurs de services (PingFederate) pour StorageGRID, vous utilisez le certificat du serveur comme certificat de signature pour les demandes StorageGRID .

Si vous ne l'avez pas déjà fait"configuré un certificat personnalisé pour l'interface de gestion" , tu devrais le faire maintenant. Lorsque vous installez un certificat de serveur personnalisé, il est utilisé pour tous les nœuds d'administration et vous pouvez l'utiliser dans toutes les approbations de parties de confiance StorageGRID , les applications d'entreprise ou les connexions SP .

L'utilisation du certificat de serveur par défaut d'un nœud d'administration dans une connexion de confiance, une application d'entreprise ou un SP n'est pas recommandée. Si le nœud échoue et que vous le récupérez, un nouveau certificat de serveur par défaut est généré. Avant de pouvoir vous connecter au nœud récupéré, vous devez mettre à jour l'approbation de la partie de confiance, l'application d'entreprise ou la connexion SP avec le nouveau certificat.

Vous pouvez accéder au certificat du serveur d'un nœud d'administration en vous connectant à l'interpréteur de commandes du nœud et en accédant à l' `/var/local/mgmt-api` annuaire. Un certificat de serveur personnalisé est nommé `custom-server.crt` . Le certificat de serveur par défaut du nœud est nommé `server.crt` .

Exigences portuaires

L'authentification unique (SSO) n'est pas disponible sur les ports restreints Grid Manager ou Tenant Manager. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec l'authentification unique. Voir "Contrôler l'accès au pare-feu externe" .

Confirmer que les utilisateurs fédérés peuvent se connecter

Avant d'activer l'authentification unique (SSO), vous devez confirmer qu'au moins un utilisateur fédéré peut se connecter au gestionnaire de grille et au gestionnaire de locataires pour tous les comptes de locataires existants.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .
- Vous avez déjà configuré la fédération d'identité.

Étapes

1. S'il existe des comptes locataires existants, confirmez qu'aucun des locataires n'utilise sa propre source d'identité.

   Lorsque vous activez SSO, une source d'identité configurée dans le gestionnaire de locataires est remplacée par la source d'identité configurée dans le gestionnaire de grille. Les utilisateurs appartenant à la source d'identité du locataire ne pourront plus se connecter à moins qu'ils ne disposent d'un compte auprès de la source d'identité Grid Manager.

   a. Sign in au gestionnaire de locataires pour chaque compte locataire.
   b. Sélectionnez **GESTION DES ACCÈS** > **Fédération d'identité**.
   c. Vérifiez que la case à cocher **Activer la fédération d'identité** n'est pas sélectionnée.
   d. Si tel est le cas, confirmez que tous les groupes fédérés susceptibles d'être utilisés pour ce compte locataire ne sont plus nécessaires, décochez la case et sélectionnez **Enregistrer**.

2. Confirmer qu'un utilisateur fédéré peut accéder au gestionnaire de grille :
   a. Depuis le Gestionnaire de grille, sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Groupes d'administrateurs**.
   b. Assurez-vous qu'au moins un groupe fédéré a été importé à partir de la source d'identité Active Directory et que l'autorisation d'accès racine lui a été attribuée.
   c. Se déconnecter.

d. Confirmez que vous pouvez vous reconnecter au gestionnaire de grille en tant qu'utilisateur du groupe fédéré.

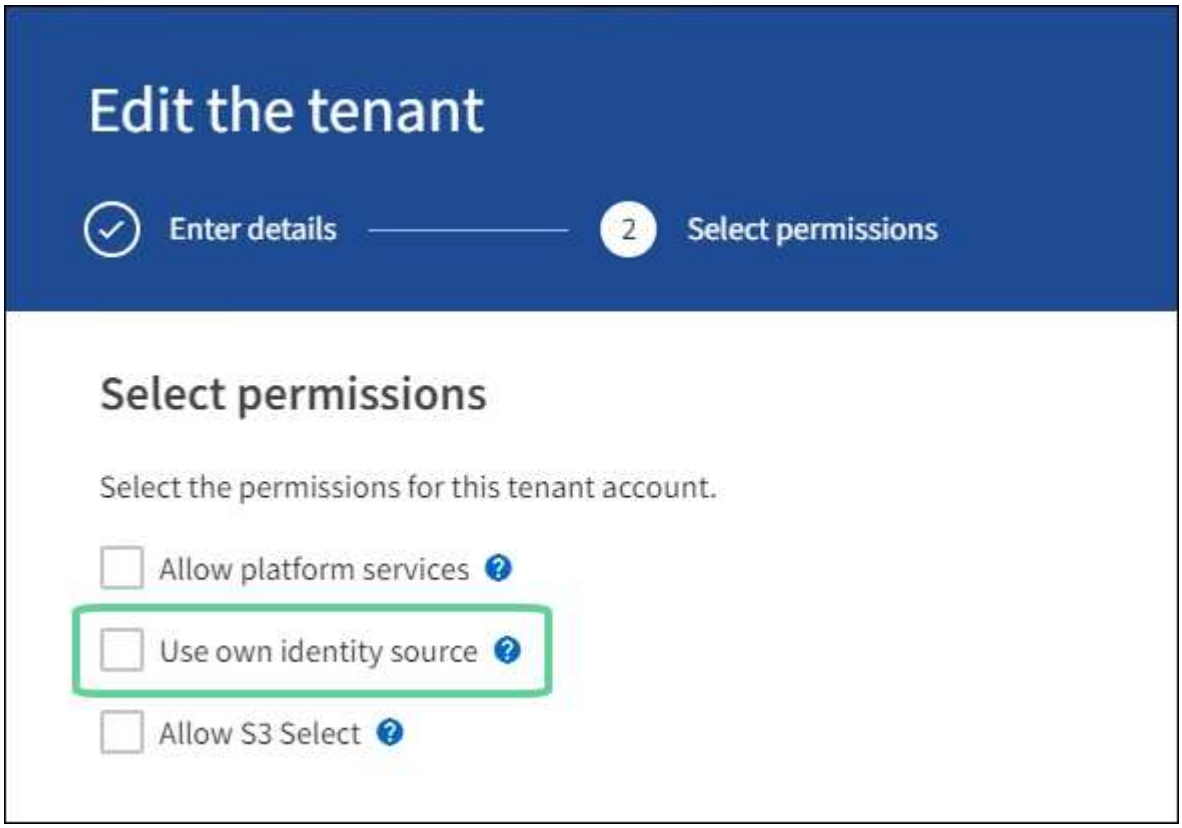
3. S'il existe des comptes locataires existants, confirmez qu'un utilisateur fédéré disposant d'une autorisation d'accès root peut se connecter :

   a. Depuis le gestionnaire de grille, sélectionnez **LOCATAIRES**.

   b. Sélectionnez le compte locataire, puis sélectionnez **Actions** > **Modifier**.

   c. Dans l'onglet Entrer les détails, sélectionnez **Continuer**.

   d. Si la case à cocher **Utiliser sa propre source d'identité** est sélectionnée, décochez la case et sélectionnez **Enregistrer**.



   La page Locataire apparaît.

   a. Sélectionnez le compte locataire, sélectionnez * Sign in* et connectez-vous au compte locataire en tant qu'utilisateur root local.

   b. Depuis le gestionnaire de locataires, sélectionnez **GESTION DES ACCÈS** > **Groupes**.

   c. Assurez-vous qu'au moins un groupe fédéré du gestionnaire de grille s'est vu attribuer l'autorisation d'accès racine pour ce locataire.

   d. Se déconnecter.

   e. Confirmez que vous pouvez vous reconnecter au locataire en tant qu'utilisateur du groupe fédéré.

Informations connexes

- "Exigences et considérations relatives à l'authentification unique"
- "Gérer les groupes d'administrateurs"
- "Utiliser un compte locataire"

Utiliser le mode sandbox

Vous pouvez utiliser le mode sandbox pour configurer et tester l'authentification unique (SSO) avant de l'activer pour tous les utilisateurs StorageGRID . Une fois l'authentification unique activée, vous pouvez revenir au mode sandbox chaque fois que vous devez modifier ou retester la configuration.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès root" .
- Vous avez configuré la fédération d'identité pour votre système StorageGRID .
- Pour le type de service LDAP de fédération d'identité, vous avez sélectionné Active Directory ou Azure, en fonction du fournisseur d'identité SSO que vous prévoyez d'utiliser.

Type de service LDAP configuré	Options pour le fournisseur d'identité SSO
Active Directory	• Active Directory • Azuré • PingFédéré
Azuré	Azuré

À propos de cette tâche

Lorsque SSO est activé et qu'un utilisateur tente de se connecter à un nœud d'administration, StorageGRID envoie une demande d'authentification au fournisseur d'identité SSO. À son tour, le fournisseur d'identité SSO renvoie une réponse d'authentification à StorageGRID, indiquant si la demande d'authentification a réussi. Pour des demandes réussies :

- La réponse d'Active Directory ou de PingFederate inclut un identifiant unique universel (UUID) pour l'utilisateur.
- La réponse d'Azure inclut un nom d'utilisateur principal (UPN).

Pour permettre à StorageGRID (le fournisseur de services) et au fournisseur d'identité SSO de communiquer en toute sécurité sur les demandes d'authentification des utilisateurs, vous devez configurer certains paramètres dans StorageGRID. Ensuite, vous devez utiliser le logiciel du fournisseur d'identité SSO pour créer une approbation de partie de confiance (AD FS), une application d'entreprise (Azure) ou un fournisseur de services (PingFederate) pour chaque nœud d'administration. Enfin, vous devez revenir à StorageGRID pour activer SSO.

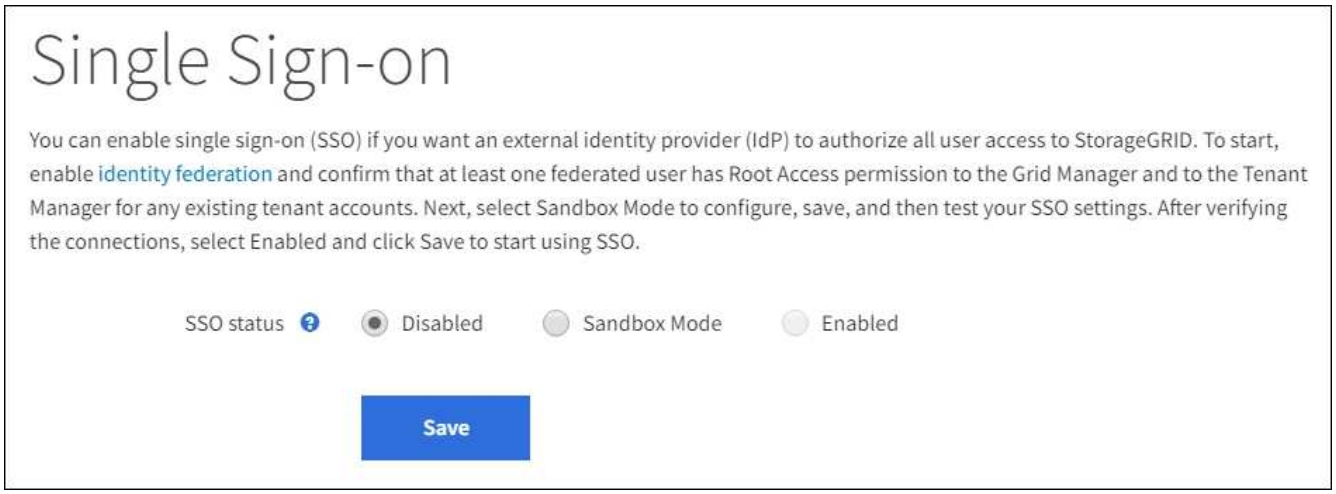
Le mode Sandbox facilite l'exécution de cette configuration aller-retour et permet de tester tous vos paramètres avant d'activer SSO. Lorsque vous utilisez le mode sandbox, les utilisateurs ne peuvent pas se connecter à l'aide de SSO.

Accéder au mode sandbox

Étapes

1. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**.

   La page d'authentification unique s'affiche, avec l'option **Désactivé** sélectionnée.



Si les options d'état SSO n'apparaissent pas, confirmez que vous avez configuré le fournisseur d'identité comme source d'identité fédérée. Voir "Exigences et considérations relatives à l'authentification unique" .

2. Sélectionnez **Mode Sandbox**.

   La section Fournisseur d'identité apparaît.

Entrez les détails du fournisseur d'identité

Étapes

1. Sélectionnez le **type SSO** dans la liste déroulante.
2. Remplissez les champs de la section Fournisseur d'identité en fonction du type SSO que vous avez sélectionné.

Active Directory

a. Saisissez le **Nom du service de fédération** pour le fournisseur d'identité, exactement tel qu'il apparaît dans Active Directory Federation Service (AD FS).

> Pour localiser le nom du service de fédération, accédez au Gestionnaire de serveur Windows. Sélectionnez **Outils** > **Gestion AD FS**. Dans le menu Action, sélectionnez **Modifier les propriétés du service de fédération**. Le nom du service de fédération est affiché dans le deuxième champ.

b. Spécifiez quel certificat TLS sera utilisé pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux demandes StorageGRID .

- **Utiliser le certificat CA du système d'exploitation** : utilisez le certificat CA par défaut installé sur le système d'exploitation pour sécuriser la connexion.
- **Utiliser un certificat CA personnalisé** : utilisez un certificat CA personnalisé pour sécuriser la connexion.

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

- **Ne pas utiliser TLS** : N'utilisez pas de certificat TLS pour sécuriser la connexion.

> Si vous modifiez le certificat CA, immédiatement"redémarrer le service mgmt-api sur les nœuds d'administration" et tester une connexion SSO réussie dans le Grid Manager.

c. Dans la section Partie de confiance, spécifiez l'**identifiant de la partie de confiance** pour StorageGRID. Cette valeur contrôle le nom que vous utilisez pour chaque approbation de partie de confiance dans AD FS.

- Par exemple, si votre grille ne comporte qu'un seul nœud d'administration et que vous ne prévoyez pas d'ajouter d'autres nœuds d'administration à l'avenir, entrez `SG` ou `StorageGRID` .
- Si votre grille comprend plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identifiant. Par exemple : `SG-[HOSTNAME]` . Cela génère un tableau qui affiche l'identifiant de la partie de confiance pour chaque nœud d'administration de votre système, en fonction du nom d'hôte du nœud.

> Vous devez créer une approbation de partie de confiance pour chaque nœud d'administration de votre système StorageGRID . Le fait de disposer d'une partie de confiance pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration.

d. Sélectionnez **Enregistrer**.

Une coche verte apparaît sur le bouton **Enregistrer** pendant quelques secondes.

Azuré

a. Spécifiez quel certificat TLS sera utilisé pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux demandes StorageGRID .

   - **Utiliser le certificat CA du système d'exploitation** : utilisez le certificat CA par défaut installé sur le système d'exploitation pour sécuriser la connexion.
   - **Utiliser un certificat CA personnalisé** : utilisez un certificat CA personnalisé pour sécuriser la connexion.

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

   - **Ne pas utiliser TLS** : N'utilisez pas de certificat TLS pour sécuriser la connexion.

   > Si vous modifiez le certificat CA, immédiatement"redémarrer le service mgmt-api sur les nœuds d'administration" et tester une connexion SSO réussie dans le Grid Manager.

b. Dans la section Application d'entreprise, spécifiez le **Nom de l'application d'entreprise** pour StorageGRID. Cette valeur contrôle le nom que vous utilisez pour chaque application d'entreprise dans Azure AD.

   - Par exemple, si votre grille ne comporte qu'un seul nœud d'administration et que vous ne prévoyez pas d'ajouter d'autres nœuds d'administration à l'avenir, entrez `SG` ou `StorageGRID` .
   - Si votre grille comprend plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identifiant. Par exemple : `SG-[HOSTNAME]` . Cela génère un tableau qui affiche un nom d'application d'entreprise pour chaque nœud d'administration de votre système, en fonction du nom d'hôte du nœud.

   > Vous devez créer une application d'entreprise pour chaque nœud d'administration de votre système StorageGRID . Disposer d'une application d'entreprise pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration.

c. Suivez les étapes dans"Créer des applications d'entreprise dans Azure AD" pour créer une application d'entreprise pour chaque nœud d'administration répertorié dans le tableau.

d. Depuis Azure AD, copiez l'URL des métadonnées de fédération pour chaque application d'entreprise. Ensuite, collez cette URL dans le champ **URL des métadonnées de la fédération** correspondant dans StorageGRID.

e. Après avoir copié et collé une URL de métadonnées de fédération pour tous les nœuds d'administration, sélectionnez **Enregistrer**.

   Une coche verte apparaît sur le bouton **Enregistrer** pendant quelques secondes.

PingFédéré

a. Spécifiez quel certificat TLS sera utilisé pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux demandes StorageGRID .

   - **Utiliser le certificat CA du système d'exploitation** : utilisez le certificat CA par défaut installé sur le système d'exploitation pour sécuriser la connexion.
   - **Utiliser un certificat CA personnalisé** : utilisez un certificat CA personnalisé pour sécuriser la connexion.

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

   - **Ne pas utiliser TLS** : N'utilisez pas de certificat TLS pour sécuriser la connexion.

   > Si vous modifiez le certificat CA, immédiatement"redémarrer le service mgmt-api sur les nœuds d'administration" et tester une connexion SSO réussie dans le Grid Manager.

b. Dans la section Fournisseur de services (SP), spécifiez l'*ID de connexion SP * pour StorageGRID. Cette valeur contrôle le nom que vous utilisez pour chaque connexion SP dans PingFederate.

   - Par exemple, si votre grille ne comporte qu'un seul nœud d'administration et que vous ne prévoyez pas d'ajouter d'autres nœuds d'administration à l'avenir, entrez `SG` ou `StorageGRID` .
   - Si votre grille comprend plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identifiant. Par exemple : `SG-[HOSTNAME]` . Cela génère un tableau qui affiche l'ID de connexion SP pour chaque nœud d'administration de votre système, en fonction du nom d'hôte du nœud.

   > Vous devez créer une connexion SP pour chaque nœud d'administration de votre système StorageGRID . Disposer d'une connexion SP pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration.

c. Spécifiez l'URL des métadonnées de la fédération pour chaque nœud d'administration dans le champ **URL des métadonnées de la fédération**.

   Utilisez le format suivant :

   ```
   https://<Federation Service
   Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP
   Connection ID>
   ```

d. Sélectionnez **Enregistrer**.

   Une coche verte apparaît sur le bouton **Enregistrer** pendant quelques secondes.

Configurer les approbations des parties de confiance, les applications d'entreprise ou les connexions SP

Lorsque la configuration est enregistrée, l'avis de confirmation du mode Sandbox apparaît. Cet avis confirme que le mode sandbox est désormais activé et fournit des instructions générales.

StorageGRID peut rester en mode sandbox aussi longtemps que nécessaire. Cependant, lorsque le **Mode Sandbox** est sélectionné sur la page d'authentification unique, l'authentification unique est désactivée pour tous les utilisateurs de StorageGRID . Seuls les utilisateurs locaux peuvent se connecter.

Suivez ces étapes pour configurer les approbations des parties de confiance (Active Directory), compléter les applications d'entreprise (Azure) ou configurer les connexions SP (PingFederate).

Active Directory

Étapes

1. Accédez aux services de fédération Active Directory (AD FS).
2. Créez une ou plusieurs approbations de partie de confiance pour StorageGRID, en utilisant chaque identifiant de partie de confiance indiqué dans le tableau de la page d'authentification unique StorageGRID .

   Vous devez créer une approbation pour chaque nœud d'administration affiché dans le tableau.

   Pour obtenir des instructions, rendez-vous sur"Créer des approbations de parties de confiance dans AD FS" .

Azuré

Étapes

1. Depuis la page d'authentification unique du nœud d'administration auquel vous êtes actuellement connecté, sélectionnez le bouton pour télécharger et enregistrer les métadonnées SAML.
2. Ensuite, pour tous les autres nœuds d'administration de votre grille, répétez ces étapes :
   a. Sign in au nœud.
   b. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**.
   c. Téléchargez et enregistrez les métadonnées SAML pour ce nœud.
3. Accédez au portail Azure.
4. Suivez les étapes dans"Créer des applications d'entreprise dans Azure AD" pour télécharger le fichier de métadonnées SAML pour chaque nœud d'administration dans son application d'entreprise Azure correspondante.

PingFédéré

Étapes

1. Depuis la page d'authentification unique du nœud d'administration auquel vous êtes actuellement connecté, sélectionnez le bouton pour télécharger et enregistrer les métadonnées SAML.
2. Ensuite, pour tous les autres nœuds d'administration de votre grille, répétez ces étapes :
   a. Sign in au nœud.
   b. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**.
   c. Téléchargez et enregistrez les métadonnées SAML pour ce nœud.
3. Accédez à PingFederate.
4. "Créer une ou plusieurs connexions de fournisseur de services (SP) pour StorageGRID" . Utilisez l'ID de connexion SP pour chaque nœud d'administration (affiché dans le tableau de la page d'authentification unique StorageGRID) et les métadonnées SAML que vous avez téléchargées pour ce nœud d'administration.

   Vous devez créer une connexion SP pour chaque nœud d'administration indiqué dans le tableau.

Tester les connexions SSO

Avant d'appliquer l'utilisation de l'authentification unique pour l'ensemble de votre système StorageGRID ,

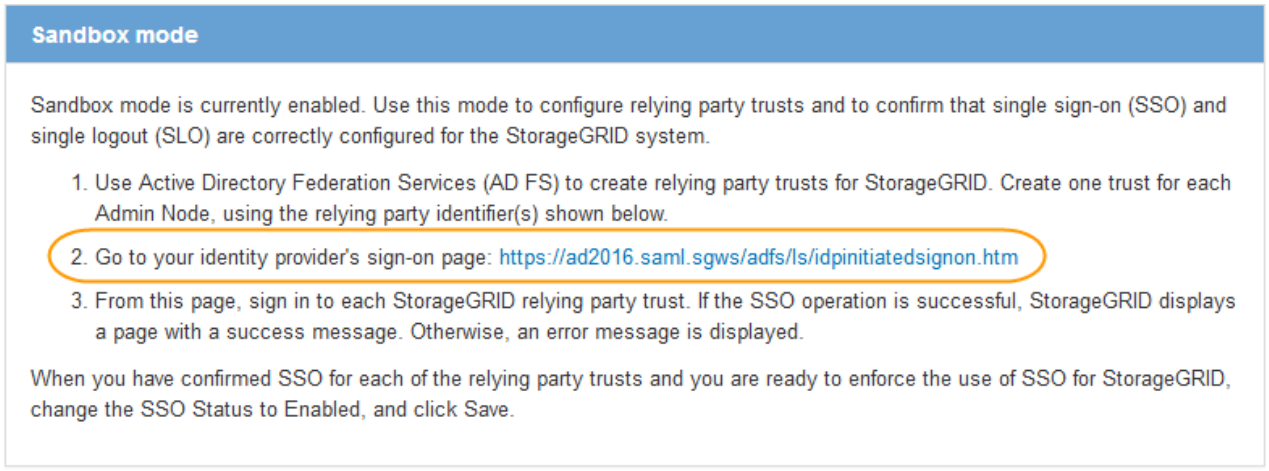
vous devez confirmer que l’authentification unique et la déconnexion unique sont correctement configurées pour chaque nœud d’administration.

Active Directory

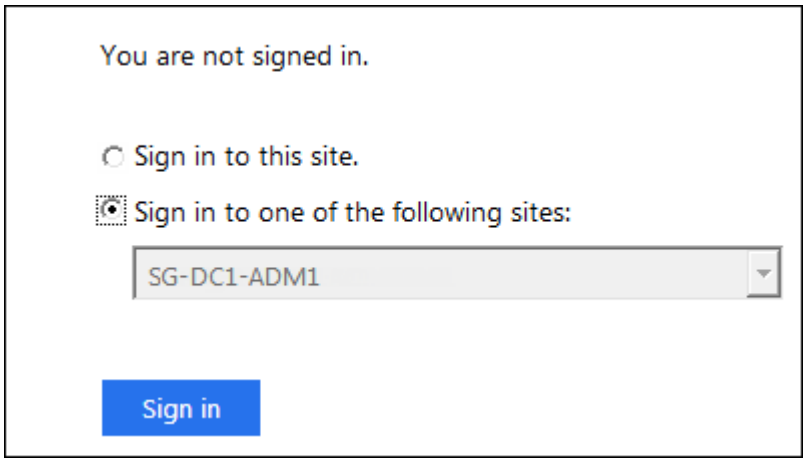
Étapes

1. À partir de la page d'authentification unique StorageGRID , recherchez le lien dans le message du mode Sandbox.

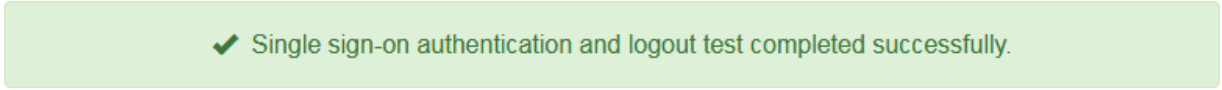
   L'URL est dérivée de la valeur que vous avez saisie dans le champ **Nom du service de fédération**.

2. Sélectionnez le lien ou copiez et collez l'URL dans un navigateur pour accéder à la page de connexion de votre fournisseur d'identité.
3. Pour confirmer que vous pouvez utiliser SSO pour vous connecter à StorageGRID, sélectionnez * Sign in à l'un des sites suivants*, sélectionnez l'identifiant de la partie de confiance pour votre nœud d'administration principal et sélectionnez * Sign in*.

4. Entrez votre nom d'utilisateur et votre mot de passe fédérés.
   - Si les opérations de connexion et de déconnexion SSO réussissent, un message de réussite s'affiche.

   - Si l'opération SSO échoue, un message d'erreur s'affiche. Résolvez le problème, effacez les cookies du navigateur et réessayez.
5. Répétez ces étapes pour vérifier la connexion SSO pour chaque nœud d'administration de votre

grille.

Azuré

Étapes

1. Accédez à la page d'authentification unique dans le portail Azure.
2. Sélectionnez **Tester cette application**.
3. Saisissez les informations d'identification d'un utilisateur fédéré.
   - Si les opérations de connexion et de déconnexion SSO réussissent, un message de réussite s'affiche.

     ✔ Single sign-on authentication and logout test completed successfully.

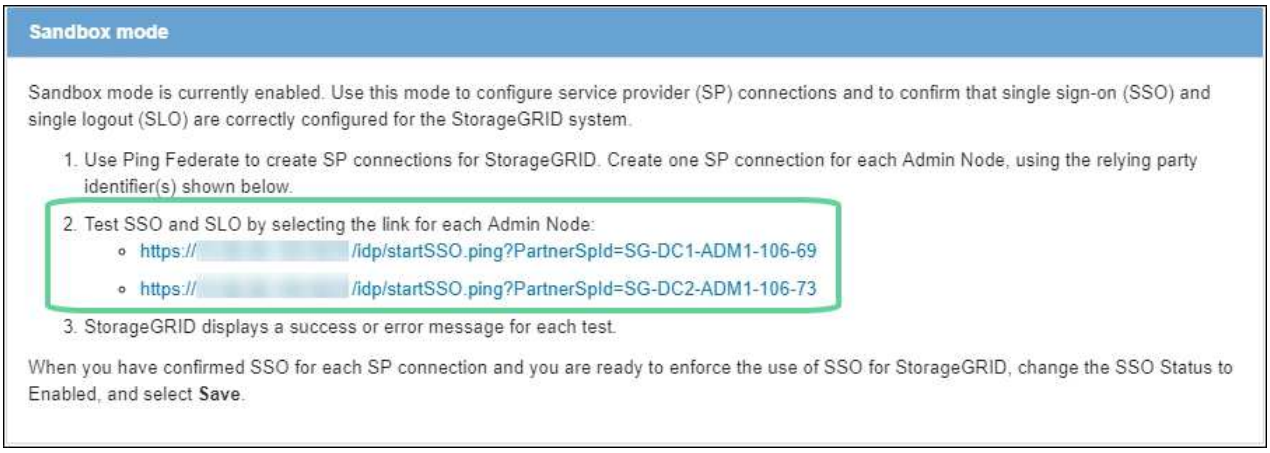
   - Si l'opération SSO échoue, un message d'erreur s'affiche. Résolvez le problème, effacez les cookies du navigateur et réessayez.
4. Répétez ces étapes pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

PingFédéré

Étapes

1. À partir de la page d'authentification unique StorageGRID , sélectionnez le premier lien dans le message du mode Sandbox.

   Sélectionnez et testez un lien à la fois.



2. Saisissez les informations d'identification d'un utilisateur fédéré.
   - Si les opérations de connexion et de déconnexion SSO réussissent, un message de réussite s'affiche.

     ✔ Single sign-on authentication and logout test completed successfully.

   - Si l'opération SSO échoue, un message d'erreur s'affiche. Résolvez le problème, effacez les cookies du navigateur et réessayez.
3. Sélectionnez le lien suivant pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

Si vous voyez un message indiquant que la page a expiré, sélectionnez le bouton **Retour** dans votre navigateur et soumettez à nouveau vos informations d'identification.

Activer l'authentification unique

Une fois que vous avez confirmé que vous pouvez utiliser SSO pour vous connecter à chaque nœud d'administration, vous pouvez activer SSO pour l'ensemble de votre système StorageGRID .

Lorsque SSO est activé, tous les utilisateurs doivent utiliser SSO pour accéder au gestionnaire de grille, au gestionnaire de locataires, à l'API de gestion de grille et à l'API de gestion de locataires. Les utilisateurs locaux ne peuvent plus accéder à StorageGRID.

Étapes

1. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**.
2. Modifiez le statut SSO sur **Activé**.
3. Sélectionnez **Enregistrer**.
4. Lisez le message d'avertissement et sélectionnez **OK**.

   L'authentification unique est désormais activée.

Si vous utilisez le portail Azure et que vous accédez à StorageGRID à partir du même ordinateur que celui que vous utilisez pour accéder à Azure, assurez-vous que l'utilisateur du portail Azure est également un utilisateur StorageGRID autorisé (un utilisateur d'un groupe fédéré qui a été importé dans StorageGRID) ou déconnectez-vous du portail Azure avant de tenter de vous connecter à StorageGRID.

Créer des approbations de parties de confiance dans AD FS

Vous devez utiliser les services de fédération Active Directory (AD FS) pour créer une approbation de partie de confiance pour chaque nœud d'administration de votre système. Vous pouvez créer des approbations de parties de confiance à l'aide de commandes PowerShell, en important des métadonnées SAML à partir de StorageGRID ou en saisissant les données manuellement.

Avant de commencer

- Vous avez configuré l'authentification unique pour StorageGRID et vous avez sélectionné **AD FS** comme type d'authentification unique.
- Le **mode Sandbox** est sélectionné sur la page d'authentification unique dans Grid Manager. Voir "Utiliser le mode sandbox" .
- Vous connaissez le nom de domaine complet (ou l'adresse IP) et l'identifiant de la partie de confiance pour chaque nœud d'administration de votre système. Vous pouvez trouver ces valeurs dans le tableau détaillé des nœuds d'administration sur la page d'authentification unique StorageGRID .

Vous devez créer une approbation de partie de confiance pour chaque nœud d'administration de votre système StorageGRID . Le fait de disposer d'une partie de confiance pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration.

- Vous avez de l'expérience dans la création d'approbations de parties de confiance dans AD FS ou vous avez accès à la documentation Microsoft AD FS.
- Vous utilisez le composant logiciel enfichable Gestion AD FS et vous appartenez au groupe Administrateurs.
- Si vous créez manuellement l'approbation de partie de confiance, vous disposez du certificat personnalisé qui a été téléchargé pour l'interface de gestion StorageGRID ou vous savez comment vous connecter à un nœud d'administration à partir de l'interpréteur de commandes.

À propos de cette tâche

Ces instructions s'appliquent à Windows Server 2016 AD FS. Si vous utilisez une version différente d'AD FS, vous remarquerez de légères différences dans la procédure. Consultez la documentation Microsoft AD FS si vous avez des questions.

Créer une approbation de partie de confiance à l'aide de Windows PowerShell

Vous pouvez utiliser Windows PowerShell pour créer rapidement une ou plusieurs approbations de parties de confiance.

Étapes

1. Dans le menu Démarrer de Windows, sélectionnez avec le bouton droit de la souris l'icône PowerShell et sélectionnez **Exécuter en tant qu'administrateur**.
2. À l'invite de commande PowerShell, entrez la commande suivante :

   ```
   Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
   "https://Admin_Node_FQDN/api/saml-metadata"
   ```

   - Pour *Admin_Node_Identifier* , saisissez l'identifiant de la partie de confiance pour le nœud d'administration, exactement tel qu'il apparaît sur la page d'authentification unique. Par exemple : `SG-DC1-ADM1` .
   - Pour *Admin_Node_FQDN* , entrez le nom de domaine complet pour le même nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Cependant, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette approbation de partie de confiance si cette adresse IP change un jour.)
3. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils** > **Gestion AD FS**.

   L'outil de gestion AD FS apparaît.

4. Sélectionnez **AD FS** > **Approbations de parties de confiance**.

   La liste des fiducies de parties utilisatrices s'affiche.

5. Ajoutez une politique de contrôle d'accès à la nouvelle approbation de partie de confiance créée :
   a. Localisez la fiducie de partie de confiance que vous venez de créer.
   b. Cliquez avec le bouton droit sur l'approbation et sélectionnez **Modifier la politique de contrôle d'accès**.
   c. Sélectionnez une politique de contrôle d'accès.
   d. Sélectionnez **Appliquer**, puis **OK**
6. Ajoutez une politique d'émission de réclamation à la fiducie de partie utilisatrice nouvellement créée :
   a. Localisez la fiducie de partie de confiance que vous venez de créer.

b. Cliquez avec le bouton droit sur la fiducie et sélectionnez **Modifier la politique d'émission de réclamation**.

c. Sélectionnez **Ajouter une règle**.

d. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer les attributs LDAP en tant que revendications** dans la liste, puis sélectionnez **Suivant**.

e. Sur la page Configurer la règle, entrez un nom d'affichage pour cette règle.

   Par exemple, **ObjectGUID vers Name ID** ou **UPN vers Name ID**.

f. Pour le magasin d'attributs, sélectionnez **Active Directory**.

g. Dans la colonne Attribut LDAP de la table de mappage, saisissez **objectGUID** ou sélectionnez **User-Principal-Name**.

h. Dans la colonne Type de réclamation sortante de la table de mappage, sélectionnez **ID de nom** dans la liste déroulante.

i. Sélectionnez **Terminer**, puis **OK**.

7. Confirmez que les métadonnées ont été importées avec succès.

   a. Cliquez avec le bouton droit sur l'approbation de la partie de confiance pour ouvrir ses propriétés.

   b. Confirmez que les champs des onglets **Points de terminaison**, **Identifiants** et **Signature** sont renseignés.

      Si les métadonnées sont manquantes, confirmez que l'adresse des métadonnées de la Fédération est correcte ou saisissez les valeurs manuellement.

8. Répétez ces étapes pour configurer une approbation de partie de confiance pour tous les nœuds d'administration de votre système StorageGRID .

9. Une fois que vous avez terminé, revenez à StorageGRID et testez toutes les approbations des parties de confiance pour confirmer qu'elles sont correctement configurées. Voir"Utiliser le mode Sandbox" pour les instructions.

Créer une approbation de partie de confiance en important des métadonnées de fédération

Vous pouvez importer les valeurs de chaque partie de confiance en accédant aux métadonnées SAML pour chaque nœud d'administration.

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis **Gestion AD FS**.
2. Sous Actions, sélectionnez **Ajouter une approbation de partie de confiance**.
3. Sur la page d'accueil, choisissez **Réclamations prises en compte**, puis sélectionnez **Démarrer**.
4. Sélectionnez **Importer des données sur la partie utilisatrice publiées en ligne ou sur un réseau local**.
5. Dans **Adresse des métadonnées de la fédération (nom d'hôte ou URL)**, saisissez l'emplacement des métadonnées SAML pour ce nœud d'administration :

   `https://Admin_Node_FQDN/api/saml-metadata`

   Pour *`Admin_Node_FQDN`* , entrez le nom de domaine complet pour le même nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Cependant, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette approbation de partie de confiance si cette adresse IP change un jour.)

6. Terminez l'assistant d'approbation de partie de confiance, enregistrez l'approbation de partie de confiance et fermez l'assistant.

> Lors de la saisie du nom d'affichage, utilisez l'identifiant de la partie de confiance pour le nœud d'administration, exactement tel qu'il apparaît sur la page d'authentification unique dans le gestionnaire de grille. Par exemple : `SG-DC1-ADM1` .

7. Ajouter une règle de revendication :
   a. Cliquez avec le bouton droit sur la fiducie et sélectionnez **Modifier la politique d'émission de réclamation**.
   b. Sélectionnez **Ajouter une règle**:
   c. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer les attributs LDAP en tant que revendications** dans la liste, puis sélectionnez **Suivant**.
   d. Sur la page Configurer la règle, entrez un nom d'affichage pour cette règle.

      Par exemple, **ObjectGUID vers Name ID** ou **UPN vers Name ID**.

   e. Pour le magasin d'attributs, sélectionnez **Active Directory**.
   f. Dans la colonne Attribut LDAP de la table de mappage, saisissez **objectGUID** ou sélectionnez **User-Principal-Name**.
   g. Dans la colonne Type de réclamation sortante de la table de mappage, sélectionnez **ID de nom** dans la liste déroulante.
   h. Sélectionnez **Terminer**, puis **OK**.
8. Confirmez que les métadonnées ont été importées avec succès.
   a. Cliquez avec le bouton droit sur l'approbation de la partie de confiance pour ouvrir ses propriétés.
   b. Confirmez que les champs des onglets **Points de terminaison**, **Identifiants** et **Signature** sont renseignés.

      Si les métadonnées sont manquantes, confirmez que l'adresse des métadonnées de la Fédération est correcte ou saisissez les valeurs manuellement.

9. Répétez ces étapes pour configurer une approbation de partie de confiance pour tous les nœuds d'administration de votre système StorageGRID .
10. Une fois que vous avez terminé, revenez à StorageGRID et testez toutes les approbations des parties de confiance pour confirmer qu'elles sont correctement configurées. Voir"Utiliser le mode Sandbox" pour les instructions.

Créer manuellement une fiducie de partie utilisatrice

Si vous choisissez de ne pas importer les données des approbations de partie de confiance, vous pouvez saisir les valeurs manuellement.

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis **Gestion AD FS**.
2. Sous Actions, sélectionnez **Ajouter une approbation de partie de confiance**.
3. Sur la page d'accueil, choisissez **Réclamations prises en compte**, puis sélectionnez **Démarrer**.
4. Sélectionnez **Saisir manuellement les données sur la partie de confiance**, puis sélectionnez **Suivant**.

5. Complétez l'assistant d'approbation de partie de confiance :

   a. Saisissez un nom d'affichage pour ce nœud d'administration.

      Par souci de cohérence, utilisez l'identifiant de partie de confiance pour le nœud d'administration, exactement tel qu'il apparaît sur la page d'authentification unique dans le gestionnaire de grille. Par exemple : `SG-DC1-ADM1` .

   b. Ignorez l'étape pour configurer un certificat de chiffrement de jeton facultatif.

   c. Sur la page Configurer l'URL, cochez la case **Activer la prise en charge du protocole SAML 2.0 WebSSO**.

   d. Saisissez l'URL du point de terminaison du service SAML pour le nœud d'administration :

      `https://Admin_Node_FQDN/api/saml-response`

      Pour *`Admin_Node_FQDN`* , entrez le nom de domaine complet du nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Cependant, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette approbation de partie de confiance si cette adresse IP change un jour.)

   e. Sur la page Configurer les identifiants, spécifiez l'identifiant de la partie de confiance pour le même nœud d'administration :

      `Admin_Node_Identifier`

      Pour *`Admin_Node_Identifier`* , saisissez l'identifiant de la partie de confiance pour le nœud d'administration, exactement tel qu'il apparaît sur la page d'authentification unique. Par exemple : `SG-DC1-ADM1` .

   f. Vérifiez les paramètres, enregistrez l'approbation de la partie de confiance et fermez l'assistant.

      La boîte de dialogue Modifier la politique d'émission de réclamation s'affiche.

      > ⓘ Si la boîte de dialogue n'apparaît pas, cliquez avec le bouton droit sur la fiducie et sélectionnez **Modifier la politique d'émission de réclamation**.

6. Pour démarrer l'assistant de règle de revendication, sélectionnez **Ajouter une règle** :

   a. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer les attributs LDAP en tant que revendications** dans la liste, puis sélectionnez **Suivant**.

   b. Sur la page Configurer la règle, entrez un nom d'affichage pour cette règle.

      Par exemple, **ObjectGUID vers Name ID** ou **UPN vers Name ID**.

   c. Pour le magasin d'attributs, sélectionnez **Active Directory**.

   d. Dans la colonne Attribut LDAP de la table de mappage, saisissez **objectGUID** ou sélectionnez **User-Principal-Name**.

   e. Dans la colonne Type de réclamation sortante de la table de mappage, sélectionnez **ID de nom** dans la liste déroulante.

   f. Sélectionnez **Terminer**, puis **OK**.

7. Cliquez avec le bouton droit sur l'approbation de la partie de confiance pour ouvrir ses propriétés.

8. Dans l'onglet **Points de terminaison**, configurez le point de terminaison pour la déconnexion unique (SLO) :

   a. Sélectionnez **Ajouter SAML**.

   b. Sélectionnez **Type de point de terminaison** > **Déconnexion SAML**.

   c. Sélectionnez **Liaison** > **Redirection**.

   d. Dans le champ **URL de confiance**, saisissez l'URL utilisée pour la déconnexion unique (SLO) de ce nœud d'administration :

   `https://Admin_Node_FQDN/api/saml-logout`

   Pour *`Admin_Node_FQDN`* , entrez le nom de domaine complet du nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Cependant, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette approbation de partie de confiance si cette adresse IP change un jour.)

   a. Sélectionnez **OK**.

9. Dans l'onglet **Signature**, spécifiez le certificat de signature pour cette approbation de partie de confiance :

   a. Ajoutez le certificat personnalisé :

      - Si vous disposez du certificat de gestion personnalisé que vous avez téléchargé sur StorageGRID, sélectionnez ce certificat.
      - Si vous n'avez pas le certificat personnalisé, connectez-vous au nœud d'administration, accédez à la `/var/local/mgmt-api` répertoire du nœud Admin et ajoutez le `custom-server.crt` fichier de certificat.

      > Utilisation du certificat par défaut du nœud d'administration(`server.crt`) n'est pas recommandé. Si le nœud d'administration échoue, le certificat par défaut sera régénéré lorsque vous récupérerez le nœud et vous devrez mettre à jour l'approbation de la partie de confiance.

   b. Sélectionnez **Appliquer**, puis **OK**.

      Les propriétés de la partie de confiance sont enregistrées et fermées.

10. Répétez ces étapes pour configurer une approbation de partie de confiance pour tous les nœuds d'administration de votre système StorageGRID .
11. Une fois que vous avez terminé, revenez à StorageGRID et testez toutes les approbations des parties de confiance pour confirmer qu'elles sont correctement configurées. Voir"Utiliser le mode sandbox" pour les instructions.

Créer des applications d'entreprise dans Azure AD

Vous utilisez Azure AD pour créer une application d'entreprise pour chaque nœud d'administration de votre système.

Avant de commencer

- Vous avez commencé à configurer l'authentification unique pour StorageGRID et vous avez sélectionné **Azure** comme type d'authentification unique.
- Le **mode Sandbox** est sélectionné sur la page d'authentification unique dans Grid Manager. Voir "Utiliser

le mode sandbox" .

- Vous disposez du **nom de l'application d'entreprise** pour chaque nœud d'administration de votre système. Vous pouvez copier ces valeurs à partir du tableau des détails du nœud d'administration sur la page d'authentification unique StorageGRID .

> Vous devez créer une application d'entreprise pour chaque nœud d'administration de votre système StorageGRID . Disposer d'une application d'entreprise pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration.

- Vous avez de l'expérience dans la création d'applications d'entreprise dans Azure Active Directory.
- Vous disposez d'un compte Azure avec un abonnement actif.
- Vous disposez de l'un des rôles suivants dans le compte Azure : administrateur général, administrateur d'applications cloud, administrateur d'applications ou propriétaire du principal du service.

Accéder à Azure AD

Étapes

1. Connectez-vous à la "Portail Azure" .
2. Accéder à "Azure Active Directory" .
3. Sélectionner "Applications d'entreprise" .

Créez des applications d'entreprise et enregistrez la configuration SSO de StorageGRID

Pour enregistrer la configuration SSO pour Azure dans StorageGRID, vous devez utiliser Azure pour créer une application d'entreprise pour chaque nœud d'administration. Vous copierez les URL de métadonnées de fédération depuis Azure et les collerez dans les champs **URL de métadonnées de fédération** correspondants sur la page d'authentification unique StorageGRID .

Étapes

1. Répétez les étapes suivantes pour chaque nœud d'administration.
   a. Dans le volet Applications Azure Enterprise, sélectionnez **Nouvelle application**.
   b. Sélectionnez **Créer votre propre application**.
   c. Pour le nom, saisissez le **Nom de l'application d'entreprise** que vous avez copié à partir du tableau des détails du nœud d'administration sur la page d'authentification unique StorageGRID .
   d. Laissez le bouton radio **Intégrer toute autre application que vous ne trouvez pas dans la galerie (Hors galerie)** sélectionné.
   e. Sélectionnez **Créer**.
   f. Sélectionnez le lien **Commencer** dans le **2. Configurer l'authentification unique** ou sélectionner le lien **Authentification unique** dans la marge de gauche.
   g. Sélectionnez la case **SAML**.
   h. Copiez l'**URL des métadonnées de la fédération d'applications**, que vous pouvez trouver sous **Étape 3 Certificat de signature SAML**.
   i. Accédez à la page d'authentification unique StorageGRID et collez l'URL dans le champ **URL des métadonnées de la fédération** qui correspond au **nom de l'application d'entreprise** que vous avez utilisé.
2. Après avoir collé une URL de métadonnées de fédération pour chaque nœud d'administration et apporté

toutes les autres modifications nécessaires à la configuration SSO, sélectionnez **Enregistrer** sur la page d'authentification unique StorageGRID .

Téléchargez les métadonnées SAML pour chaque nœud d'administration

Une fois la configuration SSO enregistrée, vous pouvez télécharger un fichier de métadonnées SAML pour chaque nœud d'administration de votre système StorageGRID .

Étapes

1. Répétez ces étapes pour chaque nœud d'administration.
   a. Sign in à StorageGRID à partir du nœud d'administration.
   b. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**.
   c. Sélectionnez le bouton pour télécharger les métadonnées SAML pour ce nœud d'administration.
   d. Enregistrez le fichier que vous téléchargerez dans Azure AD.

Télécharger les métadonnées SAML vers chaque application d'entreprise

Après avoir téléchargé un fichier de métadonnées SAML pour chaque nœud d'administration StorageGRID , effectuez les étapes suivantes dans Azure AD :

Étapes

1. Revenez au portail Azure.
2. Répétez ces étapes pour chaque application d'entreprise :

   > Vous devrez peut-être actualiser la page Applications d'entreprise pour voir les applications que vous avez précédemment ajoutées dans la liste.

   a. Accédez à la page Propriétés de l'application d'entreprise.
   b. Définissez **Affectation requise** sur **Non** (sauf si vous souhaitez configurer les affectations séparément).
   c. Accédez à la page d'authentification unique.
   d. Terminez la configuration SAML.
   e. Sélectionnez le bouton **Télécharger le fichier de métadonnées** et sélectionnez le fichier de métadonnées SAML que vous avez téléchargé pour le nœud d'administration correspondant.
   f. Une fois le fichier chargé, sélectionnez **Enregistrer** puis sélectionnez **X** pour fermer le volet. Vous êtes redirigé vers la page Configurer l'authentification unique avec SAML.
3. Suivez les étapes dans"Utiliser le mode sandbox" pour tester chaque application.

Créer des connexions de fournisseur de services (SP) dans PingFederate

Vous utilisez PingFederate pour créer une connexion de fournisseur de services (SP) pour chaque nœud d'administration de votre système. Pour accélérer le processus, vous importerez les métadonnées SAML depuis StorageGRID.

Avant de commencer

- Vous avez configuré l'authentification unique pour StorageGRID et vous avez sélectionné **Ping Federate** comme type d'authentification unique.

- Le **mode Sandbox** est sélectionné sur la page d'authentification unique dans Grid Manager. Voir "Utiliser le mode sandbox" .
- Vous disposez de l'*ID de connexion SP * pour chaque nœud d'administration de votre système. Vous pouvez trouver ces valeurs dans le tableau détaillé des nœuds d'administration sur la page d'authentification unique StorageGRID .
- Vous avez téléchargé les **métadonnées SAML** pour chaque nœud d'administration de votre système.
- Vous avez de l'expérience dans la création de connexions SP dans PingFederate Server.
- Vous avez lehttps://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html["Guide de référence de l'administrateur"^] pour le serveur PingFederate. La documentation de PingFederate fournit des instructions et des explications détaillées étape par étape.
- Vous avez le"Autorisation d'administrateur" pour le serveur PingFederate.

À propos de cette tâche

Ces instructions résument comment configurer PingFederate Server version 10.3 en tant que fournisseur SSO pour StorageGRID. Si vous utilisez une autre version de PingFederate, vous devrez peut-être adapter ces instructions. Reportez-vous à la documentation du serveur PingFederate pour obtenir des instructions détaillées pour votre version.

Prérequis complets dans PingFederate

Avant de pouvoir créer les connexions SP que vous utiliserez pour StorageGRID, vous devez effectuer les tâches préalables dans PingFederate. Vous utiliserez les informations de ces prérequis lorsque vous configurerez les connexions SP .

Créer un magasin de données

Si vous ne l'avez pas déjà fait, créez un magasin de données pour connecter PingFederate au serveur LDAP AD FS. Utilisez les valeurs que vous avez utilisées lorsque"configuration de la fédération d'identité" dans StorageGRID.

- **Type** : Répertoire (LDAP)
- **Type LDAP** : Active Directory
- **Nom de l'attribut binaire** : saisissez **objectGUID** dans l'onglet Attributs binaires LDAP exactement comme indiqué.

Créer un validateur d'informations d'identification de mot de passe

Si vous ne l'avez pas déjà fait, créez un validateur d'informations d'identification de mot de passe.

- **Type** : Validateur d'informations d'identification de mot de passe de nom d'utilisateur LDAP
- **Magasin de données** : sélectionnez le magasin de données que vous avez créé.
- **Base de recherche** : saisissez les informations de LDAP (par exemple, DC=saml,DC=sgws).
- **Filtre de recherche** : sAMAccountName=${username}
- **Portée** : Sous-arbre

Créer une instance d'adaptateur IdP

Si vous ne l'avez pas déjà fait, créez une instance d'adaptateur IdP.

Étapes

1. Accédez à **Authentification** > **Intégration** > **Adaptateurs IdP**.
2. Sélectionnez **Créer une nouvelle instance**.
3. Dans l'onglet Type, sélectionnez **Adaptateur IdP de formulaire HTML**.
4. Dans l'onglet Adaptateur IdP, sélectionnez **Ajouter une nouvelle ligne à « Validateurs d'informations d'identification »**.
5. Sélectionnez levalidateur d'informations d'identification de mot de passe tu as créé.
6. Dans l'onglet Attributs de l'adaptateur, sélectionnez l'attribut **username** pour **Pseudonyme**.
7. Sélectionnez **Enregistrer**.

Créer ou importer un certificat de signature

Si vous ne l'avez pas déjà fait, créez ou importez le certificat de signature.

Étapes

1. Accédez à **Sécurité** > **Clés et certificats de signature et de déchiffrement**.
2. Créez ou importez le certificat de signature.

Créer une connexion SP dans PingFederate

Lorsque vous créez une connexion SP dans PingFederate, vous importez les métadonnées SAML que vous avez téléchargées à partir de StorageGRID pour le nœud d'administration. Le fichier de métadonnées contient de nombreuses valeurs spécifiques dont vous avez besoin.

> Vous devez créer une connexion SP pour chaque nœud d'administration de votre système StorageGRID , afin que les utilisateurs puissent se connecter et se déconnecter en toute sécurité de n'importe quel nœud. Utilisez ces instructions pour créer la première connexion SP . Ensuite, allez àCréer des connexions SP supplémentaires pour créer toutes les connexions supplémentaires dont vous avez besoin.

Choisissez le type de connexion SP

Étapes

1. Accédez à **Applications** > **Intégration** > *Connexions SP *.
2. Sélectionnez **Créer une connexion**.
3. Sélectionnez **Ne pas utiliser de modèle pour cette connexion**.
4. Sélectionnez **Profils SSO du navigateur** et **SAML 2.0** comme protocole.

Importer les métadonnées SP

Étapes

1. Dans l'onglet Importer des métadonnées, sélectionnez **Fichier**.
2. Choisissez le fichier de métadonnées SAML que vous avez téléchargé à partir de la page d'authentification unique StorageGRID pour le nœud d'administration.
3. Consultez le résumé des métadonnées et les informations fournies dans l'onglet Informations générales.

   L'ID d'entité du partenaire et le nom de connexion sont définis sur l'ID de connexion StorageGRID SP .

(par exemple, 10.96.105.200-DC1-ADM1-105-200). L'URL de base est l'IP du nœud d'administration StorageGRID .

4. Sélectionnez **Suivant**.

Configurer l'authentification unique du navigateur IdP

Étapes

1. Dans l'onglet SSO du navigateur, sélectionnez **Configurer SSO du navigateur**.
2. Dans l'onglet Profils SAML, sélectionnez les options * SP-initiated SSO*, * SP-initial SLO*, **IdP-initiated SSO** et **IdP-initiated SLO**.
3. Sélectionnez **Suivant**.
4. Dans l'onglet Durée de vie de l'assertion, n'apportez aucune modification.
5. Dans l'onglet Création d'assertion, sélectionnez **Configurer la création d'assertion**.
   a. Dans l'onglet Mappage d'identité, sélectionnez **Standard**.
   b. Dans l'onglet Contrat d'attribut, utilisez **SAML_SUBJECT** comme contrat d'attribut et le format de nom non spécifié qui a été importé.
6. Pour prolonger le contrat, sélectionnez **Supprimer** pour supprimer le `urn:oid` , qui n'est pas utilisé.

Instance d'adaptateur de carte

Étapes

1. Dans l'onglet Mappage de la source d'authentification, sélectionnez **Mapper une nouvelle instance d'adaptateur**.
2. Dans l'onglet Instance de l'adaptateur, sélectionnez l'instance d'adaptateur tu as créé.
3. Dans l'onglet Méthode de mappage, sélectionnez **Récupérer des attributs supplémentaires à partir d'un magasin de données**.
4. Dans l'onglet Source d'attribut et recherche d'utilisateur, sélectionnez **Ajouter une source d'attribut**.
5. Dans l'onglet Magasin de données, fournissez une description et sélectionnez l'optionmagasin de données tu as ajouté.
6. Dans l'onglet Recherche d'annuaire LDAP :
   - Saisissez le **DN de base**, qui doit correspondre exactement à la valeur que vous avez saisie dans StorageGRID pour le serveur LDAP.
   - Pour la portée de la recherche, sélectionnez **Sous-arbre**.
   - Pour la classe d'objet racine, recherchez et ajoutez l'un de ces attributs : **objectGUID** ou **userPrincipalName**.
7. Dans l'onglet Types de codage d'attribut binaire LDAP, sélectionnez **Base64** pour l'attribut **objectGUID**.
8. Dans l'onglet Filtre LDAP, saisissez **sAMAccountName=${username}**.
9. Dans l'onglet Exécution du contrat d'attribut, sélectionnez **LDAP (attribut)** dans la liste déroulante Source et sélectionnez **objectGUID** ou **userPrincipalName** dans la liste déroulante Valeur.
10. Vérifiez puis enregistrez la source de l'attribut.
11. Dans l'onglet Source d'attribut Failsave, sélectionnez **Annuler la transaction SSO**.
12. Consultez le résumé et sélectionnez **Terminé**.

13. Sélectionnez **Terminé**.

Configurer les paramètres du protocole

Étapes

1. Dans l'onglet * Connexion SP * > * SSO du navigateur* > * Paramètres du protocole*, sélectionnez * Configurer les paramètres du protocole*.
2. Dans l'onglet URL du service consommateur d'assertions, acceptez les valeurs par défaut, qui ont été importées à partir des métadonnées SAML StorageGRID (**POST** pour la liaison et `/api/saml-response` pour l'URL du point de terminaison).
3. Dans l'onglet URL du service SLO, acceptez les valeurs par défaut, qui ont été importées à partir des métadonnées SAML StorageGRID (**REDIRECT** pour la liaison et `/api/saml-logout` pour l'URL du point de terminaison.
4. Dans l'onglet Liaisons SAML autorisées, décochez **ARTIFACT** et **SOAP**. Seuls **POST** et **REDIRECT** sont obligatoires.
5. Dans l'onglet Politique de signature, laissez les cases à cocher **Exiger que les demandes d'authentification soient signées** et **Toujours signer l'assertion** sélectionnées.
6. Dans l'onglet Politique de chiffrement, sélectionnez **Aucun**.
7. Consultez le résumé et sélectionnez **Terminé** pour enregistrer les paramètres du protocole.
8. Consultez le résumé et sélectionnez **Terminé** pour enregistrer les paramètres SSO du navigateur.

Configurer les informations d'identification

Étapes

1. Dans l'onglet Connexion SP , sélectionnez **Informations d'identification**.
2. Dans l'onglet Informations d'identification, sélectionnez **Configurer les informations d'identification**.
3. Sélectionnez lecertificat de signature vous avez créé ou importé.
4. Sélectionnez **Suivant** pour accéder à **Gérer les paramètres de vérification de signature**.
   a. Dans l'onglet Modèle de confiance, sélectionnez **Non ancré**.
   b. Dans l'onglet Certificat de vérification de signature, vérifiez les informations du certificat de signature, qui ont été importées à partir des métadonnées SAML StorageGRID .
5. Consultez les écrans récapitulatifs et sélectionnez **Enregistrer** pour enregistrer la connexion SP .

Créer des connexions SP supplémentaires

Vous pouvez copier la première connexion SP pour créer les connexions SP dont vous avez besoin pour chaque nœud d'administration de votre grille. Vous téléchargez de nouvelles métadonnées pour chaque copie.

> Les connexions SP pour différents nœuds d'administration utilisent des paramètres identiques, à l'exception de l'ID d'entité du partenaire, de l'URL de base, de l'ID de connexion, du nom de connexion, de la vérification de la signature et de l'URL de réponse SLO.

Étapes

1. Sélectionnez **Action** > **Copier** pour créer une copie de la connexion SP initiale pour chaque nœud d'administration supplémentaire.
2. Saisissez l'ID de connexion et le nom de connexion pour la copie, puis sélectionnez **Enregistrer**.

3. Choisissez le fichier de métadonnées correspondant au nœud d'administration :
   a. Sélectionnez **Action** > **Mettre à jour avec les métadonnées**.
   b. Sélectionnez **Choisir un fichier** et téléchargez les métadonnées.
   c. Sélectionnez **Suivant**.
   d. Sélectionnez **Enregistrer**.
4. Résoudre l'erreur due à l'attribut inutilisé :
   a. Sélectionnez la nouvelle connexion.
   b. Sélectionnez **Configurer l'authentification unique du navigateur > Configurer la création d'assertions > Contrat d'attribut**.
   c. Supprimez l'entrée pour **urn:oid**.
   d. Sélectionnez **Enregistrer**.

Désactiver l'authentification unique

Vous pouvez désactiver l'authentification unique (SSO) si vous ne souhaitez plus utiliser cette fonctionnalité. Vous devez désactiver l'authentification unique avant de pouvoir désactiver la fédération d'identité.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .

Étapes

1. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**.

   La page d'authentification unique s'affiche.

2. Sélectionnez l'option **Désactivé**.
3. Sélectionnez **Enregistrer**.

   Un message d'avertissement apparaît indiquant que les utilisateurs locaux pourront désormais se connecter.

4. Sélectionnez **OK**.

   La prochaine fois que vous vous connectez à StorageGRID , la page de Sign in à StorageGRID s'affiche et vous devez saisir le nom d'utilisateur et le mot de passe d'un utilisateur StorageGRID local ou fédéré.

Désactiver et réactiver temporairement l'authentification unique pour un nœud d'administration

Vous ne pourrez peut-être pas vous connecter au Grid Manager si le système d'authentification unique (SSO) tombe en panne. Dans ce cas, vous pouvez désactiver et réactiver temporairement SSO pour un nœud d'administration. Pour désactiver puis réactiver SSO, vous devez accéder à l'interpréteur de commandes du nœud.

Avant de commencer

- Tu as"autorisations d'accès spécifiques" .

- Vous avez le `Passwords.txt` déposer.
- Vous connaissez le mot de passe de l'utilisateur root local.

À propos de cette tâche

Après avoir désactivé SSO pour un nœud d'administration, vous pouvez vous connecter au gestionnaire de grille en tant qu'utilisateur root local. Pour sécuriser votre système StorageGRID , vous devez utiliser l'interpréteur de commandes du nœud pour réactiver SSO sur le nœud d'administration dès que vous vous déconnectez.

La désactivation de SSO pour un nœud d'administration n'affecte pas les paramètres SSO des autres nœuds d'administration de la grille. La case à cocher **Activer SSO** sur la page Authentification unique dans le Gestionnaire de grille reste sélectionnée et tous les paramètres SSO existants sont conservés, sauf si vous les mettez à jour.

Étapes

1. Connectez-vous à un nœud d'administration :
   a. Entrez la commande suivante : `ssh admin@Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
   c. Entrez la commande suivante pour passer en root : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#` .

2. Exécutez la commande suivante :`disable-saml`

   Un message indique que la commande s'applique uniquement à ce nœud d'administration.

3. Confirmez que vous souhaitez désactiver SSO.

   Un message indique que l'authentification unique est désactivée sur le nœud.

4. À partir d'un navigateur Web, accédez au gestionnaire de grille sur le même nœud d'administration.

   La page de connexion de Grid Manager s'affiche désormais car SSO a été désactivé.

5. Sign in avec le nom d'utilisateur root et le mot de passe de l'utilisateur root local.
6. Si vous avez désactivé temporairement SSO parce que vous deviez corriger la configuration SSO :
   a. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**.
   b. Modifiez les paramètres SSO incorrects ou obsolètes.
   c. Sélectionnez **Enregistrer**.

      La sélection de **Enregistrer** sur la page d'authentification unique réactive automatiquement l'authentification unique pour l'ensemble de la grille.

7. Si vous avez désactivé temporairement SSO parce que vous aviez besoin d'accéder au Grid Manager pour une autre raison :

   a. Effectuez la ou les tâches que vous devez effectuer.

b. Sélectionnez **Déconnexion** et fermez le gestionnaire de grille.
c. Réactiver SSO sur le nœud d'administration. Vous pouvez effectuer l'une des étapes suivantes :

- Exécutez la commande suivante : `enable-saml`

  Un message indique que la commande s'applique uniquement à ce nœud d'administration.

  Confirmez que vous souhaitez activer SSO.

  Un message indique que l'authentification unique est activée sur le nœud.

- Redémarrer le nœud de grille : `reboot`

8. À partir d'un navigateur Web, accédez au gestionnaire de grille à partir du même nœud d'administration.
9. Confirmez que la page de Sign in StorageGRID s'affiche et que vous devez saisir vos informations d'identification SSO pour accéder au Grid Manager.

Utiliser la fédération de grille

Qu'est-ce que la fédération de réseau ?

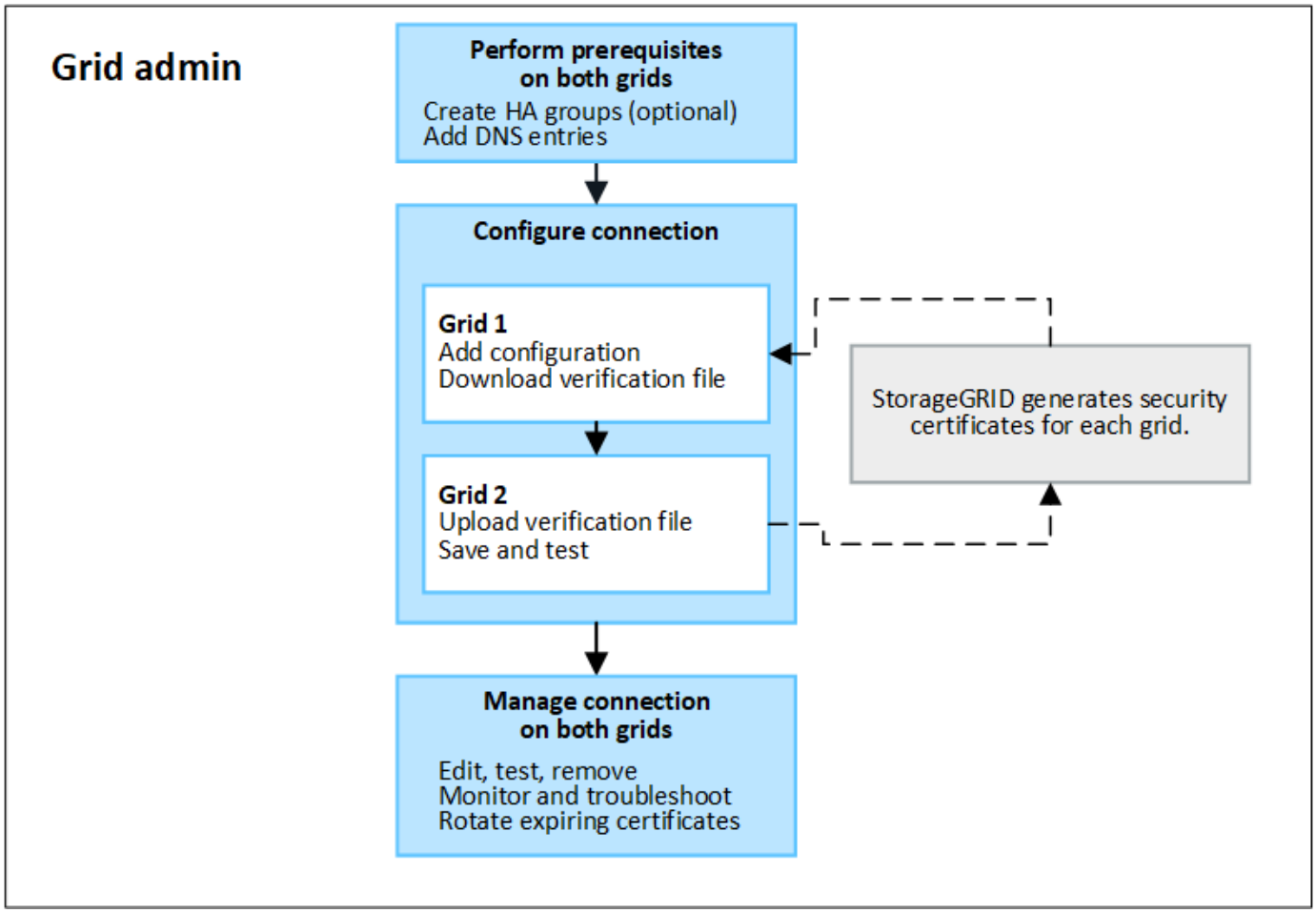
Vous pouvez utiliser la fédération de grille pour cloner des locataires et répliquer leurs objets entre deux systèmes StorageGRID pour la reprise après sinistre.

Qu'est-ce qu'une connexion à une fédération de réseau ?

Une connexion de fédération de grille est une connexion bidirectionnelle, fiable et sécurisée entre les nœuds d'administration et de passerelle dans deux systèmes StorageGRID .

Workflow pour la fédération de grilles

Le diagramme de flux de travail résume les étapes de configuration d'une connexion de fédération de grille entre deux grilles.



Considérations et exigences relatives aux connexions de fédérations de réseaux

- Les grilles utilisées pour la fédération de grilles doivent exécuter des versions de StorageGRID qui sont soit identiques, soit ne présentant pas plus d'une différence de version majeure entre elles.

  Pour plus de détails sur les exigences de version, reportez-vous à la"Notes de version" .

- Une grille peut avoir une ou plusieurs connexions de fédération de grilles à d'autres grilles. Chaque connexion de fédération de grille est indépendante de toutes les autres connexions. Par exemple, si la grille 1 a une connexion avec la grille 2 et une deuxième connexion avec la grille 3, il n'y a pas de connexion implicite entre la grille 2 et la grille 3.
- Les connexions de la fédération de grille sont bidirectionnelles. Une fois la connexion établie, vous pouvez surveiller et gérer la connexion à partir de l'une ou l'autre des grilles.
- Au moins une connexion à une fédération de grille doit exister avant de pouvoir utiliser"clone de compte" ou"réplication inter-réseaux" .

Exigences en matière de réseau et d'adresse IP

- Les connexions de fédération de grille peuvent se produire sur le réseau de grille, le réseau d'administration ou le réseau client.
- Une connexion de fédération de grille connecte une grille à une autre grille. La configuration de chaque grille spécifie un point de terminaison de fédération de grille sur l'autre grille composée de nœuds d'administration, de nœuds de passerelle ou des deux.
- La meilleure pratique consiste à se connecter"groupes de haute disponibilité (HA)" des nœuds de

passerelle et d'administration sur chaque grille. L'utilisation de groupes HA permet de garantir que les connexions de la fédération de grille resteront en ligne si les nœuds deviennent indisponibles. Si l'interface active de l'un des groupes HA échoue, la connexion peut utiliser une interface de sauvegarde.

- Il n'est pas recommandé de créer une connexion de fédération de grille qui utilise l'adresse IP d'un seul nœud d'administration ou nœud de passerelle. Si le nœud devient indisponible, la connexion à la fédération de grille deviendra également indisponible.
- "Réplication inter-réseaux"des objets nécessite que les nœuds de stockage de chaque grille puissent accéder aux nœuds d'administration et de passerelle configurés sur l'autre grille. Pour chaque grille, confirmez que tous les nœuds de stockage disposent d'une route à bande passante élevée vers les nœuds d'administration ou les nœuds de passerelle utilisés pour la connexion.

Utiliser les noms de domaine complets pour équilibrer la charge de la connexion

Pour un environnement de production, utilisez des noms de domaine complets (FQDN) pour identifier chaque grille de la connexion. Ensuite, créez les entrées DNS appropriées, comme suit :

- Le nom de domaine complet (FQDN) de Grid 1 mappé à une ou plusieurs adresses IP virtuelles (VIP) pour les groupes HA de Grid 1 ou à l'adresse IP d'un ou plusieurs nœuds d'administration ou de passerelle de Grid 1.
- Le FQDN de Grid 2 mappé à une ou plusieurs adresses VIP pour Grid 2 ou à l'adresse IP d'un ou plusieurs nœuds d'administration ou de passerelle dans Grid 2.

Lorsque vous utilisez plusieurs entrées DNS, les demandes d'utilisation de la connexion sont équilibrées, comme suit :

- Les entrées DNS qui correspondent aux adresses VIP de plusieurs groupes HA sont équilibrées entre les nœuds actifs des groupes HA.
- Les entrées DNS qui correspondent aux adresses IP de plusieurs nœuds d'administration ou nœuds de passerelle sont équilibrées en charge entre les nœuds mappés.

Exigences portuaires

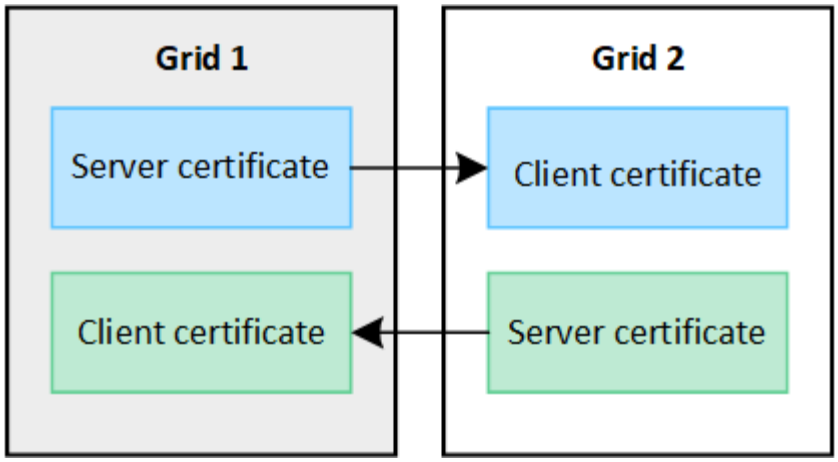
Lors de la création d'une connexion de fédération de grille, vous pouvez spécifier n'importe quel numéro de port inutilisé compris entre 23 000 et 23 999. Les deux réseaux de cette connexion utiliseront le même port.

Vous devez vous assurer qu'aucun nœud de l'une ou l'autre grille n'utilise ce port pour d'autres connexions.

Exigences en matière de certificat

Lorsque vous configurez une connexion de fédération de grille, StorageGRID génère automatiquement quatre certificats SSL :

- Certificats serveur et client pour authentifier et crypter les informations envoyées de la grille 1 à la grille 2
- Certificats serveur et client pour authentifier et crypter les informations envoyées de la grille 2 à la grille 1



Par défaut, les certificats sont valables 730 jours (2 ans). Lorsque ces certificats approchent de leur date d'expiration, l'alerte **Expiration du certificat de fédération de grille** vous rappelle de faire pivoter les certificats, ce que vous pouvez faire à l'aide du gestionnaire de grille.

> Si les certificats à l'une ou l'autre extrémité de la connexion expirent, la connexion cessera de fonctionner. La réplication des données sera en attente jusqu'à ce que les certificats soient mis à jour.

Apprendre encore plus

- "Créer des connexions de fédération de grille"
- "Gérer les connexions de la fédération de réseau"
- "Résoudre les erreurs de fédération de grille"

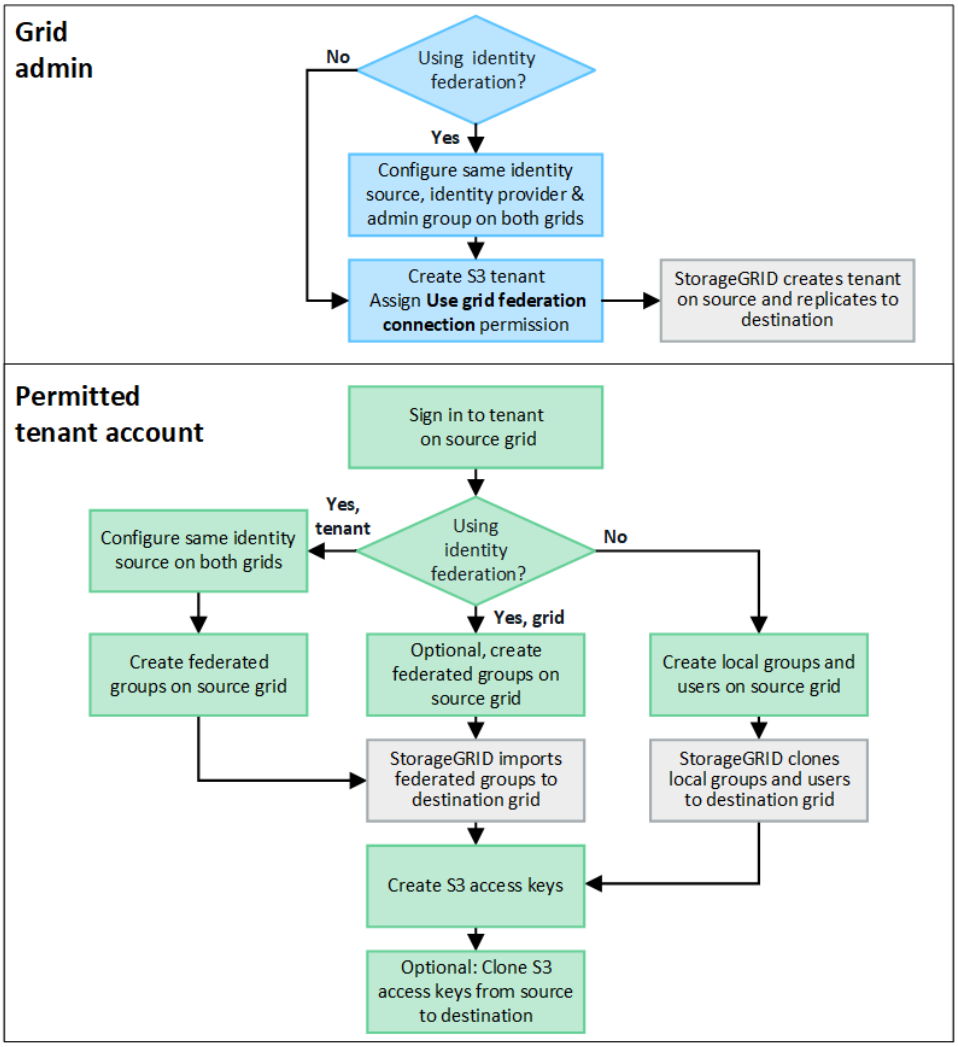
Qu'est-ce que le clonage de compte ?

Le clonage de compte est la réplication automatique d'un compte de locataire, de groupes de locataires, d'utilisateurs de locataires et, éventuellement, de clés d'accès S3 entre les systèmes StorageGRID d'un"connexion à la fédération de réseau" .

Le clonage de compte est requis pour"réplication inter-réseaux" . Le clonage des informations de compte d'un système StorageGRID source vers un système StorageGRID de destination garantit que les utilisateurs et les groupes de locataires peuvent accéder aux compartiments et objets correspondants sur l'une ou l'autre grille.

Flux de travail pour le clonage de compte

Le diagramme de flux de travail montre les étapes que les administrateurs de grille et les locataires autorisés effectueront pour configurer le clonage de compte. Ces étapes sont effectuées après la"la connexion à la fédération de grille est configurée" .



Flux de travail d'administration de la grille

Les étapes effectuées par les administrateurs de grille dépendent du fait que les systèmes StorageGRID du"connexion à la fédération de réseau" utiliser l'authentification unique (SSO) ou la fédération d'identité.

Configurer SSO pour le clonage de compte (facultatif)

Si l'un des systèmes StorageGRID de la connexion de fédération de grille utilise SSO, les deux grilles doivent utiliser SSO. Avant de créer les comptes de locataire pour la fédération de grille, les administrateurs de grille pour les grilles source et de destination du locataire doivent effectuer ces étapes.

Étapes

1. Configurez la même source d'identité pour les deux grilles. Voir "Utiliser la fédération d'identité" .
2. Configurez le même fournisseur d'identité SSO (IdP) pour les deux grilles. Voir "Configurer l'authentification unique" .
3. "Créer le même groupe d'administrateurs"sur les deux grilles en important le même groupe fédéré.

   Lorsque vous créez le locataire, vous sélectionnez ce groupe pour disposer de l'autorisation d'accès racine initiale pour les comptes de locataire source et de destination.

Si ce groupe d'administrateurs n'existe pas sur les deux grilles avant la création du locataire, le locataire n'est pas répliqué vers la destination.

Configurer la fédération d'identité au niveau de la grille pour le clonage de compte (facultatif)

Si l'un des systèmes StorageGRID utilise la fédération d'identité sans SSO, les deux grilles doivent utiliser la fédération d'identité. Avant de créer les comptes de locataire pour la fédération de grille, les administrateurs de grille pour les grilles source et de destination du locataire doivent effectuer ces étapes.

Étapes

1. Configurez la même source d'identité pour les deux grilles. Voir "Utiliser la fédération d'identité" .
2. En option, si un groupe fédéré dispose d'une autorisation d'accès racine initiale pour les comptes locataires source et de destination,"créer le même groupe d'administrateurs" sur les deux grilles en important le même groupe fédéré.

   Si vous attribuez l'autorisation d'accès racine à un groupe fédéré qui n'existe pas sur les deux grilles, le locataire n'est pas répliqué sur la grille de destination.

3. Si vous ne souhaitez pas qu'un groupe fédéré dispose d'une autorisation d'accès root initiale pour les deux comptes, spécifiez un mot de passe pour l'utilisateur root local.

Créer un compte locataire S3 autorisé

Après avoir configuré éventuellement SSO ou la fédération d'identité, un administrateur de grille exécute ces étapes pour déterminer quels locataires peuvent répliquer des objets de bucket vers d'autres systèmes StorageGRID .

Étapes

1. Déterminez la grille que vous souhaitez utiliser comme grille source du locataire pour les opérations de clonage de compte.

   La grille sur laquelle le locataire est créé à l'origine est appelée *grille source* du locataire. La grille sur laquelle le locataire est répliqué est appelée *grille de destination* du locataire.

2. Sur cette grille, créez un nouveau compte locataire S3 ou modifiez un compte existant.
3. Attribuer l'autorisation **Utiliser la connexion à la fédération de grille**.
4. Si le compte locataire doit gérer ses propres utilisateurs fédérés, attribuez l'autorisation **Utiliser sa propre source d'identité**.

   Si cette autorisation est attribuée, les comptes de locataire source et de destination doivent configurer la même source d'identité avant de créer des groupes fédérés. Les groupes fédérés ajoutés au locataire source ne peuvent pas être clonés vers le locataire de destination, sauf si les deux grilles utilisent la même source d'identité.

5. Sélectionnez une connexion de fédération de grille spécifique.
6. Enregistrez le locataire nouveau ou modifié.

   Lorsqu'un nouveau locataire avec l'autorisation **Utiliser la connexion à la fédération de grille** est enregistré, StorageGRID crée automatiquement une réplique de ce locataire sur l'autre grille, comme suit :

   - Les deux comptes locataires ont le même ID de compte, le même nom, le même quota de stockage et

les mêmes autorisations attribuées.

- Si vous avez sélectionné un groupe fédéré pour disposer de l'autorisation d'accès racine pour le locataire, ce groupe est cloné sur le locataire de destination.
- Si vous avez sélectionné un utilisateur local pour disposer de l'autorisation d'accès root pour le locataire, cet utilisateur est cloné sur le locataire de destination. Cependant, le mot de passe de cet utilisateur n'est pas cloné.

Pour plus de détails, consultez la section "Gérer les locataires autorisés pour la fédération de réseau" .

Flux de travail des comptes locataires autorisés

Une fois qu'un locataire avec l'autorisation **Utiliser la connexion à la fédération de grille** est répliqué sur la grille de destination, les comptes de locataire autorisés peuvent effectuer ces étapes pour cloner des groupes de locataires, des utilisateurs et des clés d'accès S3.

Étapes

1. Sign in au compte locataire sur la grille source du locataire.
2. Si cela est autorisé, configurez l'identification de la fédération sur les comptes locataires source et de destination.
3. Créez des groupes et des utilisateurs sur le locataire source.

   Lorsque de nouveaux groupes ou utilisateurs sont créés sur le locataire source, StorageGRID les clone automatiquement vers le locataire de destination, mais aucun clonage n'a lieu de la destination vers la source.

4. Créer des clés d'accès S3.
5. Vous pouvez également cloner les clés d'accès S3 du locataire source vers le locataire de destination.

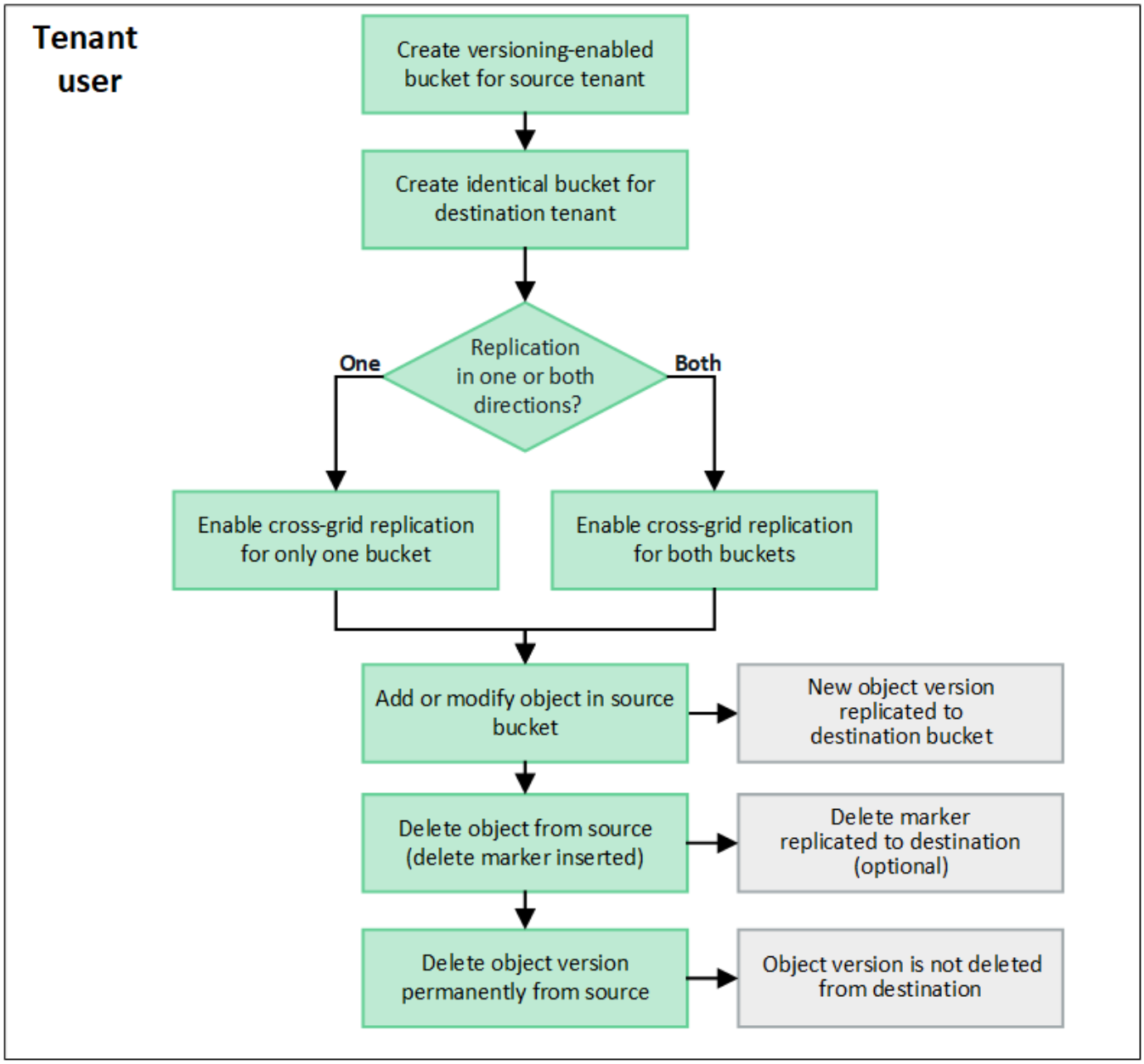
Pour plus de détails sur le flux de travail du compte locataire autorisé et pour savoir comment les groupes, les utilisateurs et les clés d'accès S3 sont clonés, consultez"Cloner des groupes de locataires et des utilisateurs" et"Cloner les clés d'accès S3 à l'aide de l'API" .

Qu'est-ce que la réplication inter-réseau ?

La réplication inter-grille est la réplication automatique d'objets entre des buckets S3 sélectionnés dans deux systèmes StorageGRID connectés dans un"connexion à la fédération de réseau" . "Clonage de compte" est nécessaire pour la réplication inter-grille.

Flux de travail pour la réplication inter-grille

Le diagramme de flux de travail résume les étapes de configuration de la réplication inter-grille entre les buckets sur deux grilles.



Exigences pour la réplication inter-réseaux

Si un compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** pour utiliser une ou plusieurs"connexions de fédération de réseau" , un utilisateur locataire avec l'autorisation d'accès root peut créer des buckets identiques dans les comptes locataires correspondants sur chaque grille. Ces seaux :

- Doit avoir le même nom mais peut avoir des régions différentes
- Doit avoir le contrôle de version activé
- Le verrouillage d'objet S3 doit être désactivé
- Doit être vide

Une fois les deux buckets créés, la réplication inter-grille peut être configurée pour l'un ou les deux buckets.

Apprendre encore plus

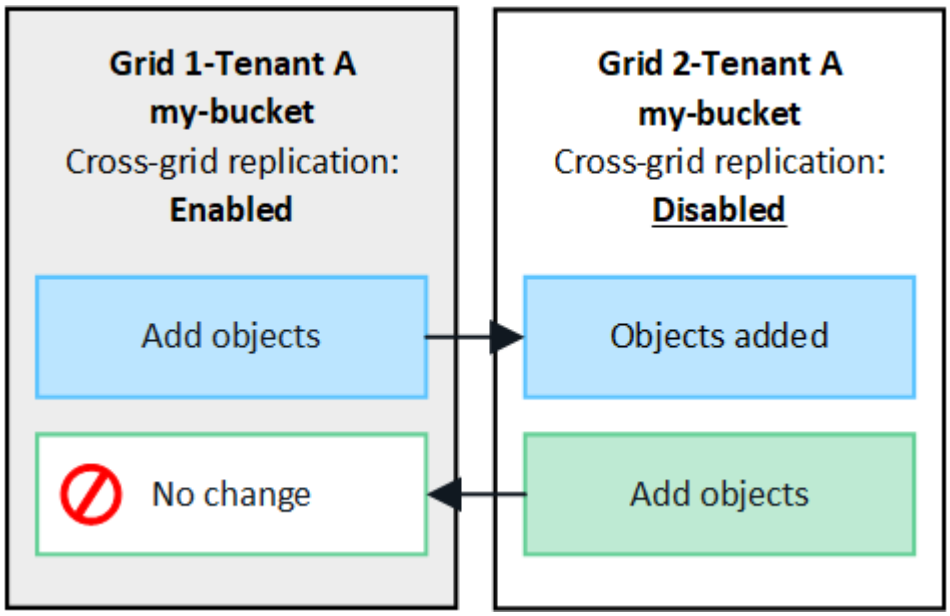
"Gérer la réplication inter-réseaux"

Comment fonctionne la réplication inter-réseaux

La réplication inter-grille peut être configurée pour se produire dans une direction ou dans les deux directions.

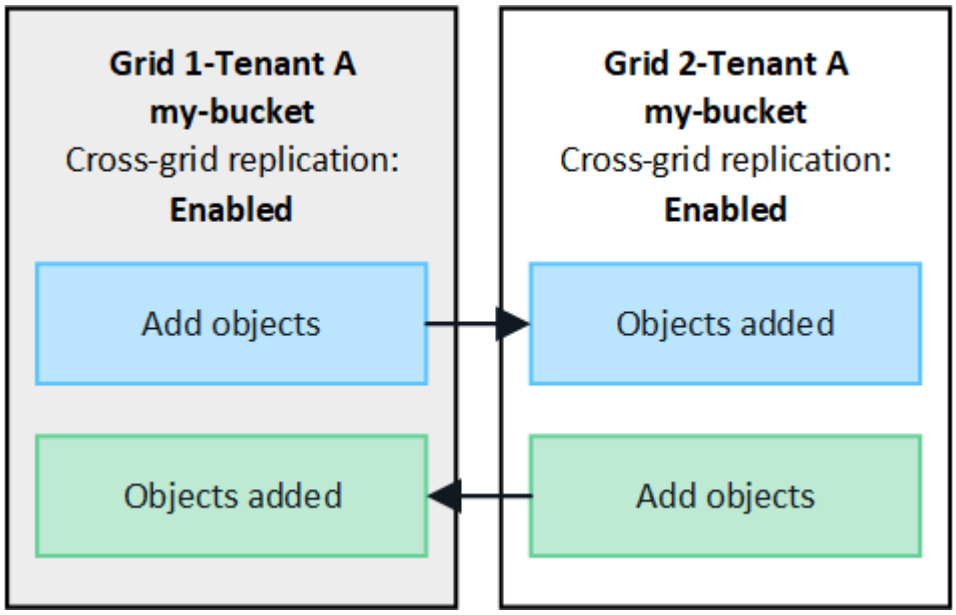
Réplication dans une direction

Si vous activez la réplication inter-grille pour un bucket sur une seule grille, les objets ajoutés à ce bucket (le bucket source) sont répliqués vers le bucket correspondant sur l'autre grille (le bucket de destination). Cependant, les objets ajoutés au bucket de destination ne sont pas répliqués vers la source. Dans la figure, la réplication inter-grille est activée pour `my-bucket` de la grille 1 à la grille 2, mais elle n'est pas activée dans l'autre sens.



Réplication dans les deux sens

Si vous activez la réplication inter-grille pour le même bucket sur les deux grilles, les objets ajoutés à l'un des buckets sont répliqués sur l'autre grille. Dans la figure, la réplication inter-grille est activée pour `my-bucket` dans les deux sens.



Que se passe-t-il lorsque des objets sont ingérés ?

Lorsqu'un client S3 ajoute un objet à un bucket pour lequel la réplication inter-grille est activée, ce qui suit se produit :

1. StorageGRID réplique automatiquement l'objet du bucket source vers le bucket de destination. Le temps nécessaire pour effectuer cette opération de réplication en arrière-plan dépend de plusieurs facteurs, notamment du nombre d'autres opérations de réplication en attente.

   Le client S3 peut vérifier l'état de réplication d'un objet en émettant une requête GetObject ou HeadObject. La réponse inclut un StorageGRID spécifique `x-ntap-sg-cgr-replication-status` en-tête de réponse, qui aura l'une des valeurs suivantes : Le client S3 peut vérifier l'état de réplication d'un objet en émettant une requête GetObject ou HeadObject. La réponse inclut un StorageGRID spécifique `x-ntap-sg-cgr-replication-status` en-tête de réponse, qui aura l'une des valeurs suivantes :

Grille	État de réplication
Source	• **TERMINÉ** : La réplication a réussi pour toutes les connexions au réseau. • **EN ATTENTE** : L'objet n'a pas été répliqué sur au moins une connexion au réseau. • **ÉCHEC** : La réplication n'est en attente pour aucune connexion au réseau et au moins une a échoué avec une panne permanente. Un utilisateur doit résoudre l'erreur.
Destination	**RÉPLIQUE** : L'objet a été répliqué à partir de la grille source.

   > StorageGRID ne prend pas en charge le `x-amz-replication-status` en-tête.

2. StorageGRID utilise les politiques ILM actives de chaque grille pour gérer les objets, comme il le ferait pour tout autre objet. Par exemple, l'objet A sur la grille 1 peut être stocké sous forme de deux copies répliquées et conservées pour toujours, tandis que la copie de l'objet A qui a été répliquée sur la grille 2 peut être stockée à l'aide du codage d'effacement 2+1 et supprimée après trois ans.

Que se passe-t-il lorsque des objets sont supprimés ?

Comme décrit dans"Supprimer le flux de données" StorageGRID peut supprimer un objet pour l'une des raisons suivantes :

- Le client S3 émet une demande de suppression.
- Un utilisateur du gestionnaire de locataires sélectionne le"Supprimer les objets dans le bucket" option permettant de supprimer tous les objets d'un bucket.
- Le bucket a une configuration de cycle de vie qui expire.
- La dernière période de la règle ILM pour l'objet se termine et aucun autre placement n'est spécifié.

Lorsque StorageGRID supprime un objet en raison d'une opération de suppression d'objets dans un bucket, de l'expiration du cycle de vie du bucket ou de l'expiration du placement ILM, l'objet répliqué n'est jamais supprimé de l'autre grille dans une connexion de fédération de grille. Cependant, les marqueurs de suppression ajoutés au bucket source par les suppressions du client S3 peuvent éventuellement être répliqués vers le bucket de destination.

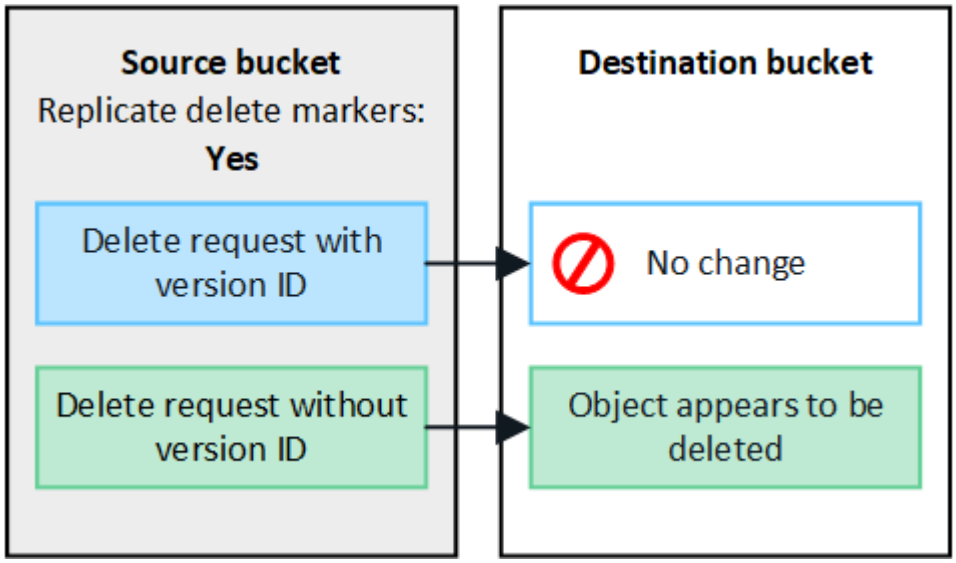
Pour comprendre ce qui se passe lorsqu'un client S3 supprime des objets d'un bucket pour lequel la réplication inter-grille est activée, examinez comment les clients S3 suppriment des objets des buckets pour lesquels le contrôle de version est activé, comme suit :

- Si un client S3 émet une demande de suppression qui inclut un ID de version, cette version de l'objet est définitivement supprimée. Aucun marqueur de suppression n'est ajouté au bucket.
- Si un client S3 émet une demande de suppression qui n'inclut pas d'ID de version, StorageGRID ne supprime aucune version d'objet. Au lieu de cela, il ajoute un marqueur de suppression au bucket. Le marqueur de suppression oblige StorageGRID à agir comme si l'objet avait été supprimé :
  - Une requête GetObject sans ID de version échouera avec `404 No Object Found`
  - Une demande GetObject avec un ID de version valide réussira et renverra la version de l'objet demandée.

Lorsqu'un client S3 supprime un objet d'un bucket pour lequel la réplication inter-grille est activée, StorageGRID détermine s'il faut répliquer la demande de suppression vers la destination, comme suit :

- Si la demande de suppression inclut un ID de version, cette version d'objet est définitivement supprimée de la grille source. Cependant, StorageGRID ne réplique pas les demandes de suppression qui incluent un ID de version, de sorte que la même version d'objet n'est pas supprimée de la destination.
- Si la demande de suppression n'inclut pas d'ID de version, StorageGRID peut éventuellement répliquer le marqueur de suppression, en fonction de la configuration de la réplication inter-grille pour le bucket :
  - Si vous choisissez de répliquer les marqueurs de suppression (par défaut), un marqueur de suppression est ajouté au bucket source et répliqué vers le bucket de destination. En effet, l'objet semble être supprimé sur les deux grilles.
  - Si vous choisissez de ne pas répliquer les marqueurs de suppression, un marqueur de suppression est ajouté au bucket source mais n'est pas répliqué dans le bucket de destination. En effet, les objets supprimés sur la grille source ne sont pas supprimés sur la grille de destination.

Dans la figure, **Répliquer les marqueurs de suppression** était défini sur **Oui** lorsque"la réplication inter-réseau a été activée" . Les demandes de suppression pour le bucket source qui incluent un ID de version ne supprimeront pas les objets du bucket de destination. Les demandes de suppression pour le bucket source qui n'incluent pas d'ID de version sembleront supprimer des objets dans le bucket de destination.



Si vous souhaitez que les suppressions d'objets restent synchronisées entre les grilles, créez des"Configurations du cycle de vie S3" pour les seaux sur les deux grilles.

Comment les objets chiffrés sont répliqués

Lorsque vous utilisez la réplication inter-grille pour répliquer des objets entre des grilles, vous pouvez chiffrer des objets individuels, utiliser le chiffrement de compartiment par défaut ou configurer le chiffrement à l'échelle de la grille. Vous pouvez ajouter, modifier ou supprimer les paramètres de chiffrement par défaut du bucket ou de la grille avant ou après avoir activé la réplication inter-grille pour un bucket.

Pour chiffrer des objets individuels, vous pouvez utiliser SSE (chiffrement côté serveur avec clés gérées par StorageGRID) lors de l'ajout des objets au bucket source. Utilisez le `x-amz-server-side-encryption` en-tête de demande et spécifier `AES256` . Voir "Utiliser le cryptage côté serveur" .

L'utilisation de SSE-C (chiffrement côté serveur avec clés fournies par le client) n'est pas prise en charge pour la réplication inter-grille. L'opération d'ingestion échouera.

Pour utiliser le cryptage par défaut pour un bucket, utilisez une requête PutBucketEncryption et définissez le `SSEAlgorithm` paramètre à `AES256` . Le chiffrement au niveau du bucket s'applique à tous les objets ingérés sans le `x-amz-server-side-encryption` en-tête de requête. Voir "Opérations sur les godets" .

Pour utiliser le chiffrement au niveau de la grille, définissez l'option **Chiffrement des objets stockés** sur **AES-256**. Le chiffrement au niveau de la grille s'applique à tous les objets qui ne sont pas chiffrés au niveau du bucket ou qui sont ingérés sans le `x-amz-server-side-encryption` en-tête de requête. Voir "Configurer les options réseau et objet" .

SSE ne prend pas en charge AES-128. Si l'option **Cryptage d'objet stocké** est activée pour la grille source à l'aide de l'option **AES-128**, l'utilisation de l'algorithme AES-128 ne sera pas propagée à l'objet répliqué. Au lieu de cela, l'objet répliqué utilisera le bucket par défaut de la destination ou le paramètre de chiffrement au niveau de la grille, s'il est disponible.

Lors de la détermination de la manière de chiffrer les objets sources, StorageGRID applique ces règles :

1. Utilisez le `x-amz-server-side-encryption` ingérer l'en-tête, s'il est présent.
2. Si aucun en-tête d'ingestion n'est présent, utilisez le paramètre de chiffrement par défaut du bucket, s'il est configuré.
3. Si aucun paramètre de bucket n'est configuré, utilisez le paramètre de chiffrement à l'échelle de la grille, s'il est configuré.
4. Si un paramètre à l'échelle de la grille n'est pas présent, ne cryptez pas l'objet source.

Lors de la détermination de la manière de chiffrer les objets répliqués, StorageGRID applique ces règles dans cet ordre :

1. Utilisez le même cryptage que l'objet source, sauf si cet objet utilise le cryptage AES-128.
2. Si l'objet source n'est pas chiffré ou s'il utilise AES-128, utilisez le paramètre de chiffrement par défaut du bucket de destination, s'il est configuré.
3. Si le bucket de destination ne dispose pas d'un paramètre de chiffrement, utilisez le paramètre de chiffrement à l'échelle de la grille de destination, s'il est configuré.
4. Si un paramètre à l'échelle de la grille n'est pas présent, ne cryptez pas l'objet de destination.

PutObjectTagging et DeleteObjectTagging ne sont pas pris en charge

Les requêtes PutObjectTagging et DeleteObjectTagging ne sont pas prises en charge pour les objets dans les buckets pour lesquels la réplication inter-grille est activée.

Si un client S3 émet une requête PutObjectTagging ou DeleteObjectTagging, `501 Not Implemented` est retourné. Le message est `Put(Delete) ObjectTagging is not available for buckets that have cross-grid replication configured.`

Comment les objets segmentés sont répliqués

La taille de segment maximale de la grille source s'applique aux objets répliqués sur la grille de destination. Lorsque des objets sont répliqués sur une autre grille, le paramètre **Taille maximale du segment** (**CONFIGURATION** > **Système** > **Options de stockage**) de la grille source sera utilisé sur les deux grilles. Par exemple, supposons que la taille maximale du segment pour la grille source soit de 1 Go, tandis que la taille maximale du segment de la grille de destination soit de 50 Mo. Si vous ingérez un objet de 2 Go sur la grille source, cet objet est enregistré sous forme de deux segments de 1 Go. Il sera également répliqué sur la grille de destination sous forme de deux segments de 1 Go, même si la taille maximale du segment de cette grille est de 50 Mo.

Comparer la réplication inter-grille et la réplication CloudMirror

Lorsque vous commencez à utiliser la fédération de grille, examinez les similitudes et les différences entre"réplication inter-réseaux" et le"Service de réplication StorageGRID CloudMirror" .

	Réplication inter-réseaux	**Service de réplication CloudMirror**
Quel est le but principal ?	Un système StorageGRID agit comme un système de reprise après sinistre. Les objets d'un bucket peuvent être répliqués entre les grilles dans une ou les deux directions.	Permet à un locataire de répliquer automatiquement des objets d'un bucket dans StorageGRID (source) vers un bucket S3 externe (destination). La réplication CloudMirror crée une copie indépendante d'un objet dans une infrastructure S3 indépendante. Cette copie indépendante n'est pas utilisée comme sauvegarde, mais souvent traitée ultérieurement dans le cloud.
Comment est-il configuré ?	1. Configurer une connexion de fédération de grille entre deux grilles. 2. Ajoutez de nouveaux comptes locataires, qui sont automatiquement clonés sur l'autre grille. 3. Ajoutez de nouveaux groupes de locataires et utilisateurs, qui sont également clonés. 4. Créez des buckets correspondants sur chaque grille et activez la réplication inter-grille dans une ou les deux directions.	1. Un utilisateur locataire configure la réplication CloudMirror en définissant un point de terminaison CloudMirror (adresse IP, informations d'identification, etc.) à l'aide du gestionnaire de locataires ou de l'API S3. 2. Tout bucket appartenant à ce compte locataire peut être configuré pour pointer vers le point de terminaison CloudMirror.

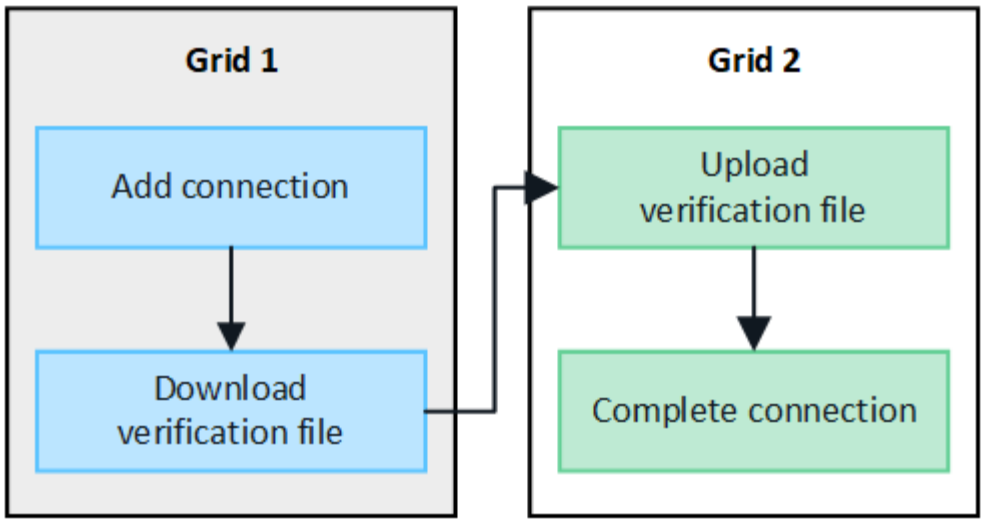
	Réplication inter-réseaux	Service de réplication CloudMirror
Qui est responsable de sa mise en place ?	• Un administrateur de grille configure la connexion et les locataires. • Les utilisateurs locataires configurent les groupes, les utilisateurs, les clés et les buckets.	Généralement, un utilisateur locataire.
Quelle est la destination ?	Un bucket S3 correspondant et identique sur l'autre système StorageGRID dans la connexion de fédération de grille.	• Toute infrastructure S3 compatible (y compris Amazon S3). • Plateforme Google Cloud (GCP)
La gestion des versions d'objets est-elle requise ?	Oui, le contrôle de version des objets doit être activé pour les buckets source et de destination.	Non, la réplication CloudMirror prend en charge toute combinaison de buckets versionnés et non versionnés sur la source et la destination.
Qu'est-ce qui provoque le déplacement des objets vers la destination ?	Les objets sont automatiquement répliqués lorsqu'ils sont ajoutés à un bucket pour lequel la réplication inter-grille est activée.	Les objets sont automatiquement répliqués lorsqu'ils sont ajoutés à un bucket qui a été configuré avec un point de terminaison CloudMirror. Les objets qui existaient dans le bucket source avant que le bucket ne soit configuré avec le point de terminaison CloudMirror ne sont pas répliqués, sauf s'ils sont modifiés.
Comment les objets sont-ils répliqués ?	La réplication inter-grille crée des objets versionnés et réplique l'ID de version du bucket source vers le bucket de destination. Cela permet de maintenir l'ordre des versions sur les deux grilles.	La réplication CloudMirror ne nécessite pas de buckets avec contrôle de version activé. CloudMirror ne peut donc conserver l'ordre d'une clé que dans un site. Il n'y a aucune garantie que la commande soit maintenue pour les demandes concernant un objet sur un site différent.
Que faire si un objet ne peut pas être répliqué ?	L'objet est mis en file d'attente pour la réplication, sous réserve des limites de stockage des métadonnées.	L'objet est mis en file d'attente pour la réplication, sous réserve des limites des services de la plateforme (voir"Recommandations pour l'utilisation des services de la plateforme").
Les métadonnées système de l'objet sont-elles répliquées ?	Oui, lorsqu'un objet est répliqué sur l'autre grille, ses métadonnées système sont également répliquées. Les métadonnées seront identiques sur les deux grilles.	Non, lorsqu'un objet est répliqué dans le bucket externe, ses métadonnées système sont mises à jour. Les métadonnées différeront selon les emplacements, en fonction du moment d'ingestion et du comportement de l'infrastructure S3 indépendante.

	Réplication inter-réseaux	Service de réplication CloudMirror
Comment les objets sont-ils récupérés ?	Les applications peuvent récupérer ou lire des objets en adressant une requête au bucket sur l'une ou l'autre grille.	Les applications peuvent récupérer ou lire des objets en adressant une demande à StorageGRID ou à la destination S3. Par exemple, supposons que vous utilisiez la réplication CloudMirror pour mettre en miroir des objets vers une organisation partenaire. Le partenaire peut utiliser ses propres applications pour lire ou mettre à jour des objets directement depuis la destination S3. L'utilisation de StorageGRID n'est pas requise.
Que se passe-t-il si un objet est supprimé ?	• Les demandes de suppression qui incluent un ID de version ne sont jamais répliquées sur la grille de destination. • Les demandes de suppression qui n'incluent pas d'ID de version ajoutent un marqueur de suppression au bucket source, qui peut éventuellement être répliqué vers la grille de destination. • Si la réplication inter-grille est configurée pour une seule direction, les objets du compartiment de destination peuvent être supprimés sans affecter la source.	Les résultats varient en fonction de l'état de version des buckets source et de destination (qui n'ont pas besoin d'être identiques) : • Si les deux buckets sont versionnés, une demande de suppression ajoutera un marqueur de suppression aux deux emplacements. • Si seul le bucket source est versionné, une demande de suppression ajoutera un marqueur de suppression à la source mais pas à la destination. • Si aucun des deux compartiments n'est versionné, une demande de suppression supprimera l'objet de la source mais pas de la destination. De même, les objets du bucket de destination peuvent être supprimés sans affecter la source.

Créer des connexions de fédération de grille

Vous pouvez créer une connexion de fédération de grille entre deux systèmes StorageGRID si vous souhaitez cloner les détails du locataire et répliquer les données de l'objet.

Comme le montre la figure, la création d'une connexion de fédération de grille comprend des étapes sur les deux grilles. Vous ajoutez la connexion sur une grille et la complétez sur l'autre grille. Vous pouvez commencer à partir de l'une ou l'autre grille.



Avant de commencer

- Vous avez examiné le"considérations et exigences" pour configurer les connexions de fédération de grille.
- Si vous prévoyez d'utiliser des noms de domaine entièrement qualifiés (FQDN) pour chaque grille au lieu d'adresses IP ou VIP, vous savez quels noms utiliser et vous avez confirmé que le serveur DNS de chaque grille dispose des entrées appropriées.
- Vous utilisez un"navigateur Web pris en charge" .
- Vous disposez de l'autorisation d'accès root et de la phrase secrète de provisionnement pour les deux grilles.

Ajouter une connexion

Effectuez ces étapes sur l'un des deux systèmes StorageGRID .

Étapes

1. Sign in au gestionnaire de grille à partir du nœud d'administration principal sur l'une ou l'autre grille.
2. Sélectionnez **CONFIGURATION** > **Système** > **Fédération de grille**.
3. Sélectionnez **Ajouter une connexion**.
4. Entrez les détails de la connexion.

Champ	Description
Nom de la connexion	Un nom unique pour vous aider à reconnaître cette connexion, par exemple « Grille 1-Grille 2 ».
FQDN ou IP pour cette grille	L'un des éléments suivants : • Le FQDN de la grille à laquelle vous êtes actuellement connecté • Une adresse VIP d'un groupe HA sur cette grille • Une adresse IP d'un nœud d'administration ou d'un nœud de passerelle sur cette grille. L'IP peut se trouver sur n'importe quel réseau que la grille de destination peut atteindre.

Champ	Description
Port	Le port que vous souhaitez utiliser pour cette connexion. Vous pouvez saisir n'importe quel numéro de port inutilisé compris entre 23 000 et 23 999. Les deux réseaux de cette connexion utiliseront le même port. Vous devez vous assurer qu'aucun nœud de l'une ou l'autre grille n'utilise ce port pour d'autres connexions.
Jours de validité du certificat pour cette grille	Le nombre de jours pendant lesquels vous souhaitez que les certificats de sécurité pour cette grille dans la connexion soient valides. La valeur par défaut est de 730 jours (2 ans), mais vous pouvez saisir n'importe quelle valeur comprise entre 1 et 762 jours. StorageGRID génère automatiquement des certificats client et serveur pour chaque grille lorsque vous enregistrez la connexion.
Mot de passe d'approvisionnement pour cette grille	La phrase secrète de provisionnement pour la grille à laquelle vous êtes connecté.
FQDN ou IP pour l'autre grille	L'un des éléments suivants : • Le FQDN du réseau auquel vous souhaitez vous connecter • Une adresse VIP d'un groupe HA sur l'autre grille • Une adresse IP d'un nœud d'administration ou d'un nœud de passerelle sur l'autre grille. L'IP peut se trouver sur n'importe quel réseau que la grille source peut atteindre.

5. Sélectionnez **Enregistrer et continuer**.
6. Pour l'étape Télécharger le fichier de vérification, sélectionnez **Télécharger le fichier de vérification**.

   Une fois la connexion établie sur l'autre grille, vous ne pouvez plus télécharger le fichier de vérification à partir de l'une ou l'autre des grilles.

7. Localisez le fichier téléchargé(*`connection-name`*`.grid-federation`), et enregistrez-le dans un endroit sûr.

   Ce fichier contient des secrets (masqués comme *****) et d'autres détails sensibles et doivent être stockés et transmis en toute sécurité.

8. Sélectionnez **Fermer** pour revenir à la page de la fédération Grid.
9. Confirmez que la nouvelle connexion est affichée et que son **Statut de connexion** est **En attente de connexion**.
10. Fournir le *`connection-name`*`.grid-federation` fichier à l'administrateur de la grille pour l'autre grille.

Connexion complète

Effectuez ces étapes sur le système StorageGRID auquel vous vous connectez (l'autre grille).

Étapes

1. Sign in au gestionnaire de grille à partir du nœud d'administration principal.
2. Sélectionnez **CONFIGURATION** > **Système** > **Fédération de grille**.
3. Sélectionnez **Télécharger le fichier de vérification** pour accéder à la page de téléchargement.
4. Sélectionnez **Télécharger le fichier de vérification**. Ensuite, recherchez et sélectionnez le fichier qui a été téléchargé à partir de la première grille(`connection-name.grid-federation`).

   Les détails de la connexion sont affichés.

5. Vous pouvez également saisir un nombre différent de jours de validité pour les certificats de sécurité de cette grille. L'entrée **Jours de validité du certificat** correspond par défaut à la valeur que vous avez saisie dans la première grille, mais chaque grille peut utiliser des dates d'expiration différentes.

   En général, utilisez le même nombre de jours pour les certificats des deux côtés de la connexion.

   > ⚠ Si les certificats à l'une ou l'autre extrémité de la connexion expirent, la connexion cessera de fonctionner et les réplications seront en attente jusqu'à ce que les certificats soient mis à jour.

6. Saisissez la phrase secrète de provisionnement pour la grille à laquelle vous êtes actuellement connecté.
7. Sélectionnez **Enregistrer et tester**.

   Les certificats sont générés et la connexion est testée. Si la connexion est valide, un message de réussite s'affiche et la nouvelle connexion est répertoriée sur la page de la fédération Grid. Le **statut de connexion** sera **Connecté**.

   Si un message d'erreur apparaît, corrigez les problèmes. Voir "Résoudre les erreurs de fédération de grille" .

8. Accédez à la page de la fédération Grid sur la première grille et actualisez le navigateur. Confirmez que le **statut de connexion** est désormais **Connecté**.
9. Une fois la connexion établie, supprimez en toute sécurité toutes les copies du fichier de vérification.

   Si vous modifiez cette connexion, un nouveau fichier de vérification sera créé. Le fichier original ne peut pas être réutilisé.

Après avoir terminé

- Passez en revue les considérations pour"gestion des locataires autorisés" .
- "Créer un ou plusieurs nouveaux comptes locataires", attribuez l'autorisation **Utiliser la connexion à la fédération de grille** et sélectionnez la nouvelle connexion.
- "Gérer la connexion"selon les besoins. Vous pouvez modifier les valeurs de connexion, tester une connexion, faire pivoter les certificats de connexion ou supprimer une connexion.
- "Surveiller la connexion"dans le cadre de vos activités normales de surveillance StorageGRID .
- "Dépanner la connexion", y compris la résolution des alertes et des erreurs liées au clonage de compte et à la réplication inter-grille.

Gérer les connexions de la fédération de réseau

La gestion des connexions de fédération de grille entre les systèmes StorageGRID inclut la modification des détails de connexion, la rotation des certificats, la suppression des autorisations des locataires et la suppression des connexions inutilisées.

Avant de commencer

- Vous êtes connecté au gestionnaire de grille sur l'une ou l'autre grille à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès root" pour la grille à laquelle vous êtes connecté.

Modifier une connexion à une fédération de grille

Vous pouvez modifier une connexion de fédération de grille en vous connectant au nœud d'administration principal sur l'une ou l'autre des grilles de la connexion. Après avoir apporté des modifications à la première grille, vous devez télécharger un nouveau fichier de vérification et le charger sur l'autre grille.

> Pendant que la connexion est en cours de modification, les demandes de clonage de compte ou de réplication inter-grille continueront d'utiliser les paramètres de connexion existants. Toutes les modifications que vous apportez à la première grille sont enregistrées localement mais ne sont pas utilisées tant qu'elles n'ont pas été téléchargées sur la deuxième grille, enregistrées et testées.

Commencer à éditer la connexion

Étapes

1. Sign in au gestionnaire de grille à partir du nœud d'administration principal sur l'une ou l'autre grille.
2. Sélectionnez **NODES** et confirmez que tous les autres nœuds d'administration de votre système sont en ligne.

> Lorsque vous modifiez une connexion de fédération de grille, StorageGRID tente d'enregistrer un fichier de « configuration candidate » sur tous les nœuds d'administration de la première grille. Si ce fichier ne peut pas être enregistré sur tous les nœuds d'administration, un message d'avertissement apparaît lorsque vous sélectionnez **Enregistrer et tester**.

3. Sélectionnez **CONFIGURATION** > **Système** > **Fédération de grille**.
4. Modifiez les détails de la connexion à l'aide du menu **Actions** sur la page de fédération de grille ou sur la page de détails d'une connexion spécifique. Voir"Créer des connexions de fédération de grille" pour quoi entrer.

Menu Actions

a. Sélectionnez le bouton radio pour la connexion.

b. Sélectionnez **Actions** > **Modifier**.

c. Entrez les nouvelles informations.

Page de détails

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

b. Sélectionnez **Modifier**.

c. Entrez les nouvelles informations.

5. Saisissez la phrase secrète de provisionnement pour la grille à laquelle vous êtes connecté.
6. Sélectionnez **Enregistrer et continuer**.

   Les nouvelles valeurs sont enregistrées, mais elles ne seront pas appliquées à la connexion tant que vous n'aurez pas téléchargé le nouveau fichier de vérification sur l'autre grille.

7. Sélectionnez **Télécharger le fichier de vérification**.

   Pour télécharger ce fichier ultérieurement, accédez à la page de détails de la connexion.

8. Localisez le fichier téléchargé(`connection-name.grid-federation`), et enregistrez-le dans un endroit sûr.

   Le fichier de vérification contient des secrets et doit être stocké et transmis en toute sécurité.

9. Sélectionnez **Fermer** pour revenir à la page de la fédération Grid.
10. Confirmez que le **statut de connexion** est **En attente de modification**.

    Si l'état de la connexion était autre que **Connecté** lorsque vous avez commencé à modifier la connexion, il ne passera pas à **En attente de modification**.

11. Fournir le `connection-name.grid-federation` fichier à l'administrateur de la grille pour l'autre grille.

Terminer la modification de la connexion

Terminez la modification de la connexion en téléchargeant le fichier de vérification sur l'autre grille.

Étapes

1. Sign in au gestionnaire de grille à partir du nœud d'administration principal.
2. Sélectionnez **CONFIGURATION** > **Système** > **Fédération de grille**.
3. Sélectionnez **Télécharger le fichier de vérification** pour accéder à la page de téléchargement.
4. Sélectionnez **Télécharger le fichier de vérification**. Ensuite, recherchez et sélectionnez le fichier qui a été téléchargé à partir de la première grille.
5. Saisissez la phrase secrète de provisionnement pour la grille à laquelle vous êtes actuellement connecté.
6. Sélectionnez **Enregistrer et tester**.

Si la connexion peut être établie à l'aide des valeurs modifiées, un message de réussite s'affiche. Sinon, un message d'erreur apparaît. Examinez le message et résolvez les problèmes éventuels.

7. Fermez l'assistant pour revenir à la page de fédération de grille.
8. Confirmez que le **statut de connexion** est **Connecté**.
9. Accédez à la page de la fédération Grid sur la première grille et actualisez le navigateur. Confirmez que le **statut de connexion** est désormais **Connecté**.
10. Une fois la connexion établie, supprimez en toute sécurité toutes les copies du fichier de vérification.

Tester une connexion à une fédération de grille

Étapes

1. Sign in au gestionnaire de grille à partir du nœud d'administration principal.
2. Sélectionnez **CONFIGURATION** > **Système** > **Fédération de grille**.
3. Testez la connexion en utilisant le menu **Actions** sur la page de fédération Grid ou la page de détails d'une connexion spécifique.

Menu Actions

a. Sélectionnez le bouton radio pour la connexion.

b. Sélectionnez **Actions** > **Test**.

Page de détails

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

b. Sélectionnez **Tester la connexion**.

4. Vérifiez l'état de la connexion :

État de la connexion	Description
Connecté	Les deux réseaux sont connectés et communiquent normalement.
Erreur	La connexion est dans un état d'erreur. Par exemple, un certificat a expiré ou une valeur de configuration n'est plus valide.
En attente de modification	Vous avez modifié la connexion sur cette grille, mais la connexion utilise toujours la configuration existante. Pour terminer la modification, téléchargez le nouveau fichier de vérification dans l'autre grille.
En attente de connexion	Vous avez configuré la connexion sur cette grille, mais la connexion n'a pas été établie sur l'autre grille. Téléchargez le fichier de vérification de cette grille et téléchargez-le sur l'autre grille.
Inconnu	La connexion est dans un état inconnu, probablement en raison d'un problème de réseau ou d'un nœud hors ligne.

5. Si l'état de la connexion est **Erreur**, résolvez tous les problèmes. Ensuite, sélectionnez à nouveau **Tester la connexion** pour confirmer que le problème a été résolu.

Faire tourner les certificats de connexion

Chaque connexion à la fédération de grille utilise quatre certificats SSL générés automatiquement pour sécuriser la connexion. Lorsque les deux certificats de chaque grille approchent de leur date d'expiration, l'alerte **Expiration du certificat de fédération de grille** vous rappelle de faire pivoter les certificats.

> Si les certificats à l'une ou l'autre extrémité de la connexion expirent, la connexion cessera de fonctionner et les réplications seront en attente jusqu'à ce que les certificats soient mis à jour.

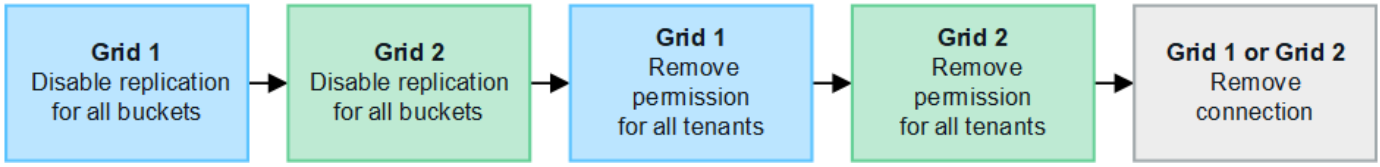
Étapes

1. Sign in au gestionnaire de grille à partir du nœud d'administration principal sur l'une ou l'autre grille.
2. Sélectionnez **CONFIGURATION** > **Système** > **Fédération de grille**.
3. À partir de l'un ou l'autre onglet de la page de fédération Grid, sélectionnez le nom de la connexion pour afficher ses détails.
4. Sélectionnez l'onglet **Certificats**.
5. Sélectionnez **Faire tourner les certificats**.
6. Spécifiez combien de jours les nouveaux certificats doivent être valides.
7. Saisissez la phrase secrète de provisionnement pour la grille à laquelle vous êtes connecté.
8. Sélectionnez **Faire tourner les certificats**.
9. Si nécessaire, répétez ces étapes sur l'autre grille de la connexion.

   En général, utilisez le même nombre de jours pour les certificats des deux côtés de la connexion.

Supprimer une connexion à une fédération de grille

Vous pouvez supprimer une connexion de fédération de grille de l'une ou l'autre des grilles de la connexion. Comme indiqué dans la figure, vous devez effectuer les étapes préalables sur les deux grilles pour confirmer que la connexion n'est utilisée par aucun locataire sur l'une ou l'autre grille.



Avant de supprimer une connexion, notez les points suivants :

- La suppression d'une connexion ne supprime aucun élément qui a déjà été copié entre les grilles. Par exemple, les utilisateurs, groupes et objets locataires qui existent sur les deux grilles ne sont supprimés d'aucune des deux grilles lorsque l'autorisation du locataire est supprimée. Si vous souhaitez supprimer ces éléments, vous devez les supprimer manuellement des deux grilles.
- Lorsque vous supprimez une connexion, la réplication de tous les objets en attente de réplication (ingérés mais pas encore répliqués sur l'autre grille) échouera définitivement.

Désactiver la réplication pour tous les compartiments locataires

Étapes

1. À partir de l'une ou l'autre des grilles, connectez-vous au gestionnaire de grille à partir du nœud d'administration principal.
2. Sélectionnez **CONFIGURATION** > **Système** > **Fédération de grille**.
3. Sélectionnez le nom de la connexion pour afficher ses détails.
4. Dans l'onglet * Locataires autorisés *, déterminez si la connexion est utilisée par des locataires.
5. Si des locataires sont répertoriés, demandez à tous les locataires de"désactiver la réplication inter-grille" pour tous leurs buckets sur les deux grilles de la connexion.

> Vous ne pouvez pas supprimer l'autorisation **Utiliser la connexion à la fédération de grille** si la réplication inter-grille est activée pour l'un des compartiments de locataire. Chaque compte locataire doit désactiver la réplication inter-grille pour ses buckets sur les deux grilles.

Supprimer l'autorisation pour chaque locataire

Une fois la réplication inter-grille désactivée pour tous les compartiments de locataire, supprimez l'autorisation **Utiliser la fédération de grille** de tous les locataires sur les deux grilles.

Étapes

1. Sélectionnez **CONFIGURATION** > **Système** > **Fédération de grille**.
2. Sélectionnez le nom de la connexion pour afficher ses détails.
3. Pour chaque locataire de l'onglet **Locataires autorisés**, supprimez l'autorisation **Utiliser la connexion à la fédération de grille** de chaque locataire. Voir "Gérer les locataires autorisés" .
4. Répétez ces étapes pour les locataires autorisés sur l'autre grille.

Supprimer la connexion

Étapes

1. Lorsqu'aucun locataire sur l'une ou l'autre des grilles n'utilise la connexion, sélectionnez **Supprimer**.
2. Vérifiez le message de confirmation et sélectionnez **Supprimer**.
   - Si la connexion peut être supprimée, un message de réussite s'affiche. La connexion à la fédération de grille est désormais supprimée des deux grilles.
   - Si la connexion ne peut pas être supprimée (par exemple, elle est toujours utilisée ou il y a une erreur de connexion), un message d'erreur s'affiche. Vous pouvez effectuer l'une des opérations suivantes :
     - Résoudre l'erreur (recommandé). Voir "Résoudre les erreurs de fédération de grille" .
     - Retirer la connexion par la force. Voir la section suivante.

Supprimer une connexion à une fédération de grille de force

Si nécessaire, vous pouvez forcer la suppression d'une connexion qui n'a pas le statut **Connecté**.

La suppression forcée supprime uniquement la connexion du réseau local. Pour supprimer complètement la connexion, effectuez les mêmes étapes sur les deux grilles.

Étapes

1. Dans la boîte de dialogue de confirmation, sélectionnez **Forcer la suppression**.

   Un message de réussite apparaît. Cette connexion à la fédération de grille ne peut plus être utilisée. Cependant, les buckets locataires peuvent toujours avoir la réplication inter-grille activée et certaines copies d'objets peuvent avoir déjà été répliquées entre les grilles de la connexion.

2. À partir de l'autre grille de la connexion, connectez-vous au gestionnaire de grille à partir du nœud d'administration principal.
3. Sélectionnez **CONFIGURATION** > **Système** > **Fédération de grille**.
4. Sélectionnez le nom de la connexion pour afficher ses détails.
5. Sélectionnez **Supprimer** et **Oui**.
6. Sélectionnez **Forcer la suppression** pour supprimer la connexion de cette grille.

Gérer les locataires autorisés pour la fédération de réseau

Vous pouvez autoriser les comptes de locataire S3 à utiliser une connexion de fédération de grille entre deux systèmes StorageGRID . Lorsque les locataires sont autorisés à utiliser une connexion, des étapes spéciales sont nécessaires pour modifier les détails du locataire ou pour supprimer définitivement l'autorisation d'un locataire d'utiliser la connexion.

Avant de commencer

- Vous êtes connecté au gestionnaire de grille sur l'une ou l'autre grille à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès root" pour la grille à laquelle vous êtes connecté.
- Tu as"créé une connexion à une fédération de grille" entre deux grilles.
- Vous avez examiné les flux de travail pour"clone de compte" et"réplication inter-réseaux" .
- Si nécessaire, vous avez déjà configuré l'authentification unique (SSO) ou la fédération d'identification pour les deux grilles de la connexion. Voir "Qu'est-ce que le clonage de compte" .

Créer un locataire autorisé

Si vous souhaitez autoriser un compte locataire nouveau ou existant à utiliser une connexion de fédération de grille pour le clonage de compte et la réplication inter-grille, suivez les instructions générales pour"créer un nouveau locataire S3" ou"modifier un compte locataire" et notez ce qui suit :

- Vous pouvez créer le locataire à partir de l'une ou l'autre grille de la connexion. La grille sur laquelle un locataire est créé est la *grille source du locataire*.
- Le statut de la connexion doit être **Connecté**.
- Lorsque le locataire est créé ou modifié pour activer l'autorisation **Utiliser la connexion à la fédération de grille**, puis enregistré sur la première grille, un locataire identique est automatiquement répliqué sur l'autre grille. La grille sur laquelle le locataire est répliqué est la *grille de destination du locataire*.
- Les locataires des deux grilles auront le même identifiant de compte à 20 chiffres, le même nom, la même description, le même quota et les mêmes autorisations. Vous pouvez également utiliser le champ **Description** pour identifier le locataire source et le locataire de destination. Par exemple, cette description pour un locataire créé sur la grille 1 apparaîtra également pour le locataire répliqué sur la grille 2 : « Ce locataire a été créé sur la grille 1. »

- Pour des raisons de sécurité, le mot de passe d'un utilisateur root local n'est pas copié dans la grille de destination.

  Avant qu'un utilisateur root local puisse se connecter au locataire répliqué sur la grille de destination, un administrateur de grille pour cette grille doit"changer le mot de passe de l'utilisateur root local" .

- Une fois que le locataire nouveau ou modifié est disponible sur les deux grilles, les utilisateurs du locataire peuvent effectuer ces opérations :
  - À partir de la grille source du locataire, créez des groupes et des utilisateurs locaux, qui sont automatiquement clonés vers la grille de destination du locataire. Voir "Cloner des groupes de locataires et des utilisateurs" .
  - Créez de nouvelles clés d'accès S3, qui peuvent éventuellement être clonées sur la grille de destination du locataire. Voir "Cloner les clés d'accès S3 à l'aide de l'API" .
  - Créez des buckets identiques sur les deux grilles de la connexion et activez la réplication inter-grille dans une direction ou dans les deux directions. Voir "Gérer la réplication inter-réseaux" .

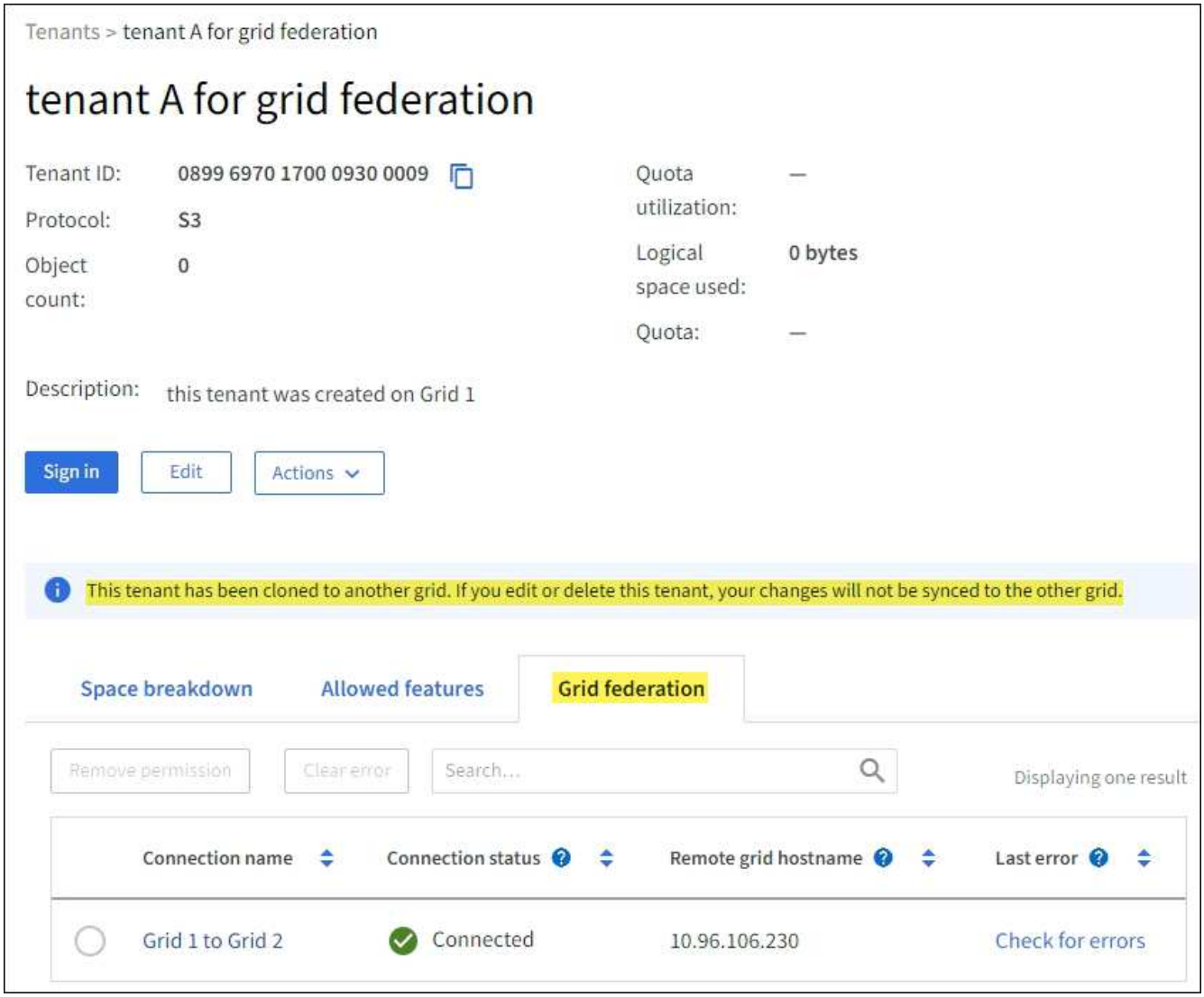
Afficher un locataire autorisé

Vous pouvez voir les détails d'un locataire autorisé à utiliser une connexion de fédération de grille.

Étapes

1. Sélectionnez **LOCATAIRES**.
2. Depuis la page Locataires, sélectionnez le nom du locataire pour afficher la page des détails du locataire.

   S'il s'agit de la grille source du locataire (c'est-à-dire si le locataire a été créé sur cette grille), une bannière apparaît pour vous rappeler que le locataire a été cloné sur une autre grille. Si vous modifiez ou supprimez ce locataire, vos modifications ne seront pas synchronisées avec l'autre grille.



3. Sélectionnez éventuellement l'onglet **Fédération de grille** pour"surveiller la connexion à la fédération du réseau" .

Modifier un locataire autorisé

Si vous devez modifier un locataire disposant de l'autorisation **Utiliser la connexion à la fédération de grille**, suivez les instructions générales pour"modifier un compte locataire" et notez ce qui suit :

- Si un locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, vous pouvez modifier les détails du locataire à partir de l'une ou l'autre des grilles de la connexion. Cependant, les modifications que vous apportez ne seront pas copiées sur l'autre grille. Si vous souhaitez conserver les détails du locataire synchronisés entre les grilles, vous devez effectuer les mêmes modifications sur les deux grilles.
- Vous ne pouvez pas effacer l'autorisation **Utiliser la connexion à la fédération de grille** lorsque vous modifiez un locataire.
- Vous ne pouvez pas sélectionner une connexion de fédération de grille différente lorsque vous modifiez un locataire.

Supprimer un locataire autorisé

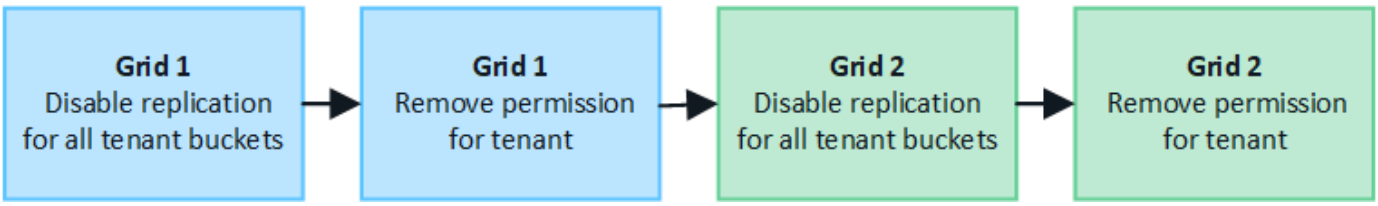
Si vous devez supprimer un locataire disposant de l'autorisation **Utiliser la connexion à la fédération de grille**, suivez les instructions générales pour"suppression d'un compte locataire" et notez ce qui suit :

- Avant de pouvoir supprimer le locataire d'origine sur la grille source, vous devez supprimer tous les buckets du compte sur la grille source.
- Avant de pouvoir supprimer le locataire cloné sur la grille de destination, vous devez supprimer tous les buckets du compte sur la grille de destination.
- Si vous supprimez le locataire d'origine ou cloné, le compte ne peut plus être utilisé pour la réplication inter-grille.
- Si vous supprimez le locataire d'origine sur la grille source, tous les groupes de locataires, utilisateurs ou clés qui ont été clonés sur la grille de destination ne seront pas affectés. Vous pouvez soit supprimer le locataire cloné, soit lui permettre de gérer ses propres groupes, utilisateurs, clés d'accès et buckets.
- Si vous supprimez le locataire cloné sur la grille de destination, des erreurs de clonage se produiront si de nouveaux groupes ou utilisateurs sont ajoutés au locataire d'origine.

  Pour éviter ces erreurs, supprimez l'autorisation du locataire d'utiliser la connexion à la fédération de grille avant de supprimer le locataire de cette grille.

Supprimer l'autorisation Utiliser la connexion à la fédération de grille

Pour empêcher un locataire d'utiliser une connexion de fédération de grille, vous devez supprimer l'autorisation **Utiliser la connexion de fédération de grille**.



Avant de supprimer l'autorisation d'un locataire d'utiliser une connexion à une fédération de réseau, notez les points suivants :

- Vous ne pouvez pas supprimer l'autorisation **Utiliser la connexion à la fédération de grille** si la réplication inter-grille est activée pour l'un des buckets du locataire. Le compte locataire doit d'abord désactiver la réplication inter-grille pour tous ses buckets.
- La suppression de l'autorisation **Utiliser la connexion à la fédération de grille** ne supprime aucun élément qui a déjà été répliqué entre les grilles. Par exemple, les utilisateurs, groupes et objets locataires qui existent sur les deux grilles ne sont supprimés d'aucune des deux grilles lorsque l'autorisation du locataire est supprimée. Si vous souhaitez supprimer ces éléments, vous devez les supprimer manuellement des deux grilles.
- Si vous souhaitez réactiver cette autorisation avec la même connexion de fédération de grille, supprimez d'abord ce locataire sur la grille de destination ; sinon, la réactivation de cette autorisation entraînera une erreur.

> La réactivation de l'autorisation **Utiliser la connexion à la fédération de grille** fait de la grille locale la grille source et déclenche le clonage vers la grille distante spécifiée par la connexion à la fédération de grille sélectionnée. Si le compte locataire existe déjà sur la grille distante, le clonage entraînera une erreur de conflit.

Avant de commencer

- Vous utilisez un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès root" pour les deux grilles.

Désactiver la réplication pour les compartiments locataires

Dans un premier temps, désactivez la réplication inter-grille pour tous les buckets locataires.

Étapes

1. À partir de l'une ou l'autre des grilles, connectez-vous au gestionnaire de grille à partir du nœud d'administration principal.
2. Sélectionnez **CONFIGURATION** > **Système** > **Fédération de grille**.
3. Sélectionnez le nom de la connexion pour afficher ses détails.
4. Dans l'onglet * Locataires autorisés *, déterminez si le locataire utilise la connexion.
5. Si le locataire est répertorié, demandez-lui de"désactiver la réplication inter-grille" pour tous leurs buckets sur les deux grilles de la connexion.

> Vous ne pouvez pas supprimer l'autorisation **Utiliser la connexion à la fédération de grille** si la réplication inter-grille est activée pour l'un des compartiments de locataire. Le locataire doit désactiver la réplication inter-grille pour ses buckets sur les deux grilles.

Supprimer l'autorisation du locataire

Une fois la réplication inter-grille désactivée pour les buckets de locataire, vous pouvez supprimer l'autorisation du locataire d'utiliser la connexion de fédération de grille.

Étapes

1. Sign in au gestionnaire de grille à partir du nœud d'administration principal.
2. Supprimez l'autorisation de la page de la fédération Grid ou de la page Locataires.

Page de la fédération Grid

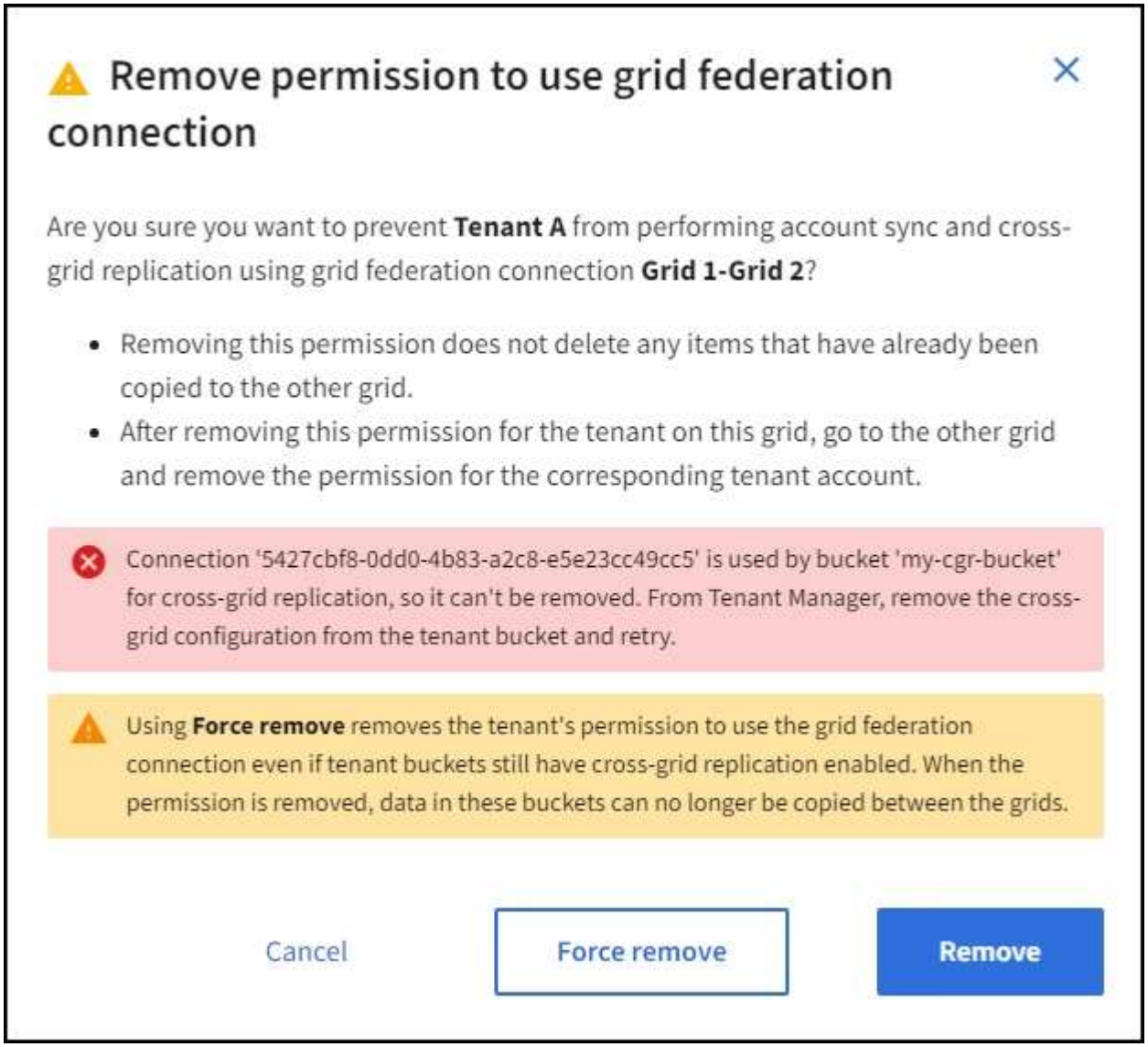
a. Sélectionnez **CONFIGURATION** > **Système** > **Fédération de grille**.
b. Sélectionnez le nom de la connexion pour afficher sa page de détails.
c. Dans l'onglet * Locataires autorisés *, sélectionnez le bouton radio correspondant au locataire.
d. Sélectionnez **Supprimer l'autorisation**.

Page des locataires

a. Sélectionnez **LOCATAIRES**.
b. Sélectionnez le nom du locataire pour afficher la page de détails.
c. Dans l'onglet **Fédération de grille**, sélectionnez le bouton radio pour la connexion.
d. Sélectionnez **Supprimer l'autorisation**.

3. Vérifiez les avertissements dans la boîte de dialogue de confirmation et sélectionnez **Supprimer**.
   - Si l'autorisation peut être supprimée, vous revenez à la page de détails et un message de réussite s'affiche. Ce locataire ne peut plus utiliser la connexion à la fédération de grille.

◦ Si la réplication inter-grille est toujours activée pour un ou plusieurs buckets de locataires, une erreur s'affiche.



Vous pouvez effectuer l'une des opérations suivantes :

- (Recommandé.) Sign in au gestionnaire de locataires et désactivez la réplication pour chacun des compartiments du locataire. Voir "Gérer la réplication inter-réseaux" . Ensuite, répétez les étapes pour supprimer l'autorisation **Utiliser la connexion au réseau**.
- Supprimer l'autorisation par la force. Voir la section suivante.

4. Accédez à l'autre grille et répétez ces étapes pour supprimer l'autorisation du même locataire sur l'autre grille.

Supprimer l'autorisation de force

Si nécessaire, vous pouvez forcer la suppression de l'autorisation d'un locataire à utiliser une connexion de fédération de grille même si la réplication inter-grille est activée pour les buckets de locataire.

Avant de retirer l'autorisation d'un locataire par la force, notez les considérations générales poursupprimer l'autorisation ainsi que ces considérations supplémentaires :

- Si vous supprimez de force l'autorisation **Utiliser la connexion à la fédération de grille**, tous les objets en attente de réplication vers l'autre grille (ingérés mais pas encore répliqués) continueront d'être répliqués. Pour empêcher ces objets en cours d'exécution d'atteindre le bucket de destination, vous devez également supprimer l'autorisation du locataire sur l'autre grille.
- Tous les objets ingérés dans le bucket source après avoir supprimé l'autorisation **Utiliser la connexion à la fédération de grille** ne seront jamais répliqués dans le bucket de destination.

Étapes

1. Sign in au gestionnaire de grille à partir du nœud d'administration principal.
2. Sélectionnez **CONFIGURATION** > **Système** > **Fédération de grille**.
3. Sélectionnez le nom de la connexion pour afficher sa page de détails.
4. Dans l'onglet * Locataires autorisés *, sélectionnez le bouton radio correspondant au locataire.
5. Sélectionnez **Supprimer l'autorisation**.
6. Vérifiez les avertissements dans la boîte de dialogue de confirmation et sélectionnez **Forcer la suppression**.

   Un message de réussite apparaît. Ce locataire ne peut plus utiliser la connexion à la fédération de grille.

7. Si nécessaire, accédez à l'autre grille et répétez ces étapes pour forcer la suppression de l'autorisation pour le même compte locataire sur l'autre grille. Par exemple, vous devez répéter ces étapes sur l'autre grille pour empêcher les objets en cours d'atteindre le bucket de destination.

Résoudre les erreurs de fédération de grille

Vous devrez peut-être résoudre les alertes et les erreurs liées aux connexions de fédération de grille, au clonage de compte et à la réplication inter-grille.

Alertes et erreurs de connexion à la fédération de grille

Vous pourriez recevoir des alertes ou rencontrer des erreurs avec vos connexions à la fédération de réseau.

Après avoir apporté des modifications pour résoudre un problème de connexion, testez la connexion pour vous assurer que l'état de la connexion revient à **Connecté**. Pour les instructions, voir"Gérer les connexions de la fédération de réseau" .

Alerte d'échec de connexion à la fédération de réseau

Problème

L'alerte **Échec de la connexion à la fédération de grille** a été déclenchée.

Détails

Cette alerte indique que la connexion de fédération de grille entre les grilles ne fonctionne pas.

Actions recommandées

1. Vérifiez les paramètres sur la page Grid Federation pour les deux grilles. Confirmez que toutes les valeurs sont correctes. Voir "Gérer les connexions de la fédération de réseau" .
2. Vérifiez les certificats utilisés pour la connexion. Assurez-vous qu'il n'y a pas d'alertes concernant les certificats de fédération de grille expirés et que les détails de chaque certificat sont valides. Consultez les instructions pour la rotation des certificats de connexion dans"Gérer les connexions de la fédération de réseau" .

3. Confirmez que tous les nœuds d'administration et de passerelle des deux grilles sont en ligne et disponibles. Résolvez toutes les alertes susceptibles d'affecter ces nœuds et réessayez.
4. Si vous avez fourni un nom de domaine complet (FQDN) pour la grille locale ou distante, confirmez que le serveur DNS est en ligne et disponible. Voir"Qu'est-ce que la fédération de réseau ?" pour les exigences de mise en réseau, d'adresse IP et de DNS.

Alerte d'expiration du certificat de la fédération de réseau

Problème

L'alerte **Expiration du certificat de la fédération de grille** a été déclenchée.

Détails

Cette alerte indique qu'un ou plusieurs certificats de fédération de grille sont sur le point d'expirer.

Actions recommandées

Consultez les instructions pour la rotation des certificats de connexion dans"Gérer les connexions de la fédération de réseau" .

Erreur lors de la modification d'une connexion à une fédération de grille

Problème

Lors de la modification d'une connexion à une fédération de grille, le message d'avertissement suivant s'affiche lorsque vous sélectionnez **Enregistrer et tester** : « Échec de la création d'un fichier de configuration candidat sur un ou plusieurs nœuds. »

Détails

Lorsque vous modifiez une connexion de fédération de grille, StorageGRID tente d'enregistrer un fichier de « configuration candidate » sur tous les nœuds d'administration de la première grille. Un message d'avertissement s'affiche si ce fichier ne peut pas être enregistré sur tous les nœuds d'administration, par exemple parce qu'un nœud d'administration est hors ligne.

Actions recommandées

1. Dans la grille que vous utilisez pour modifier la connexion, sélectionnez **NODES**.
2. Confirmez que tous les nœuds d'administration de cette grille sont en ligne.
3. Si des nœuds sont hors ligne, remettez-les en ligne et essayez à nouveau de modifier la connexion.

Erreurs de clonage de compte

Impossible de se connecter à un compte locataire cloné

Problème

Vous ne pouvez pas vous connecter à un compte locataire cloné. Le message d'erreur sur la page de connexion du gestionnaire de locataires est « Vos informations d'identification pour ce compte n'étaient pas valides. Veuillez réessayer."

Détails

Pour des raisons de sécurité, lorsqu'un compte de locataire est cloné de la grille source du locataire vers la grille de destination du locataire, le mot de passe que vous avez défini pour l'utilisateur root local du locataire n'est pas cloné. De même, lorsqu'un locataire crée des utilisateurs locaux sur sa grille source, les mots de passe des utilisateurs locaux ne sont pas clonés sur la grille de destination.

Actions recommandées

Avant que l'utilisateur root puisse se connecter à la grille de destination du locataire, un administrateur de grille doit d'abord"changer le mot de passe de l'utilisateur root local" sur la grille de destination.

Avant qu'un utilisateur local cloné puisse se connecter à la grille de destination du locataire, l'utilisateur root du locataire cloné doit ajouter un mot de passe pour l'utilisateur sur la grille de destination. Pour les instructions, voir"Gérer les utilisateurs locaux" dans les instructions d'utilisation du Tenant Manager.

Locataire créé sans clone

Problème

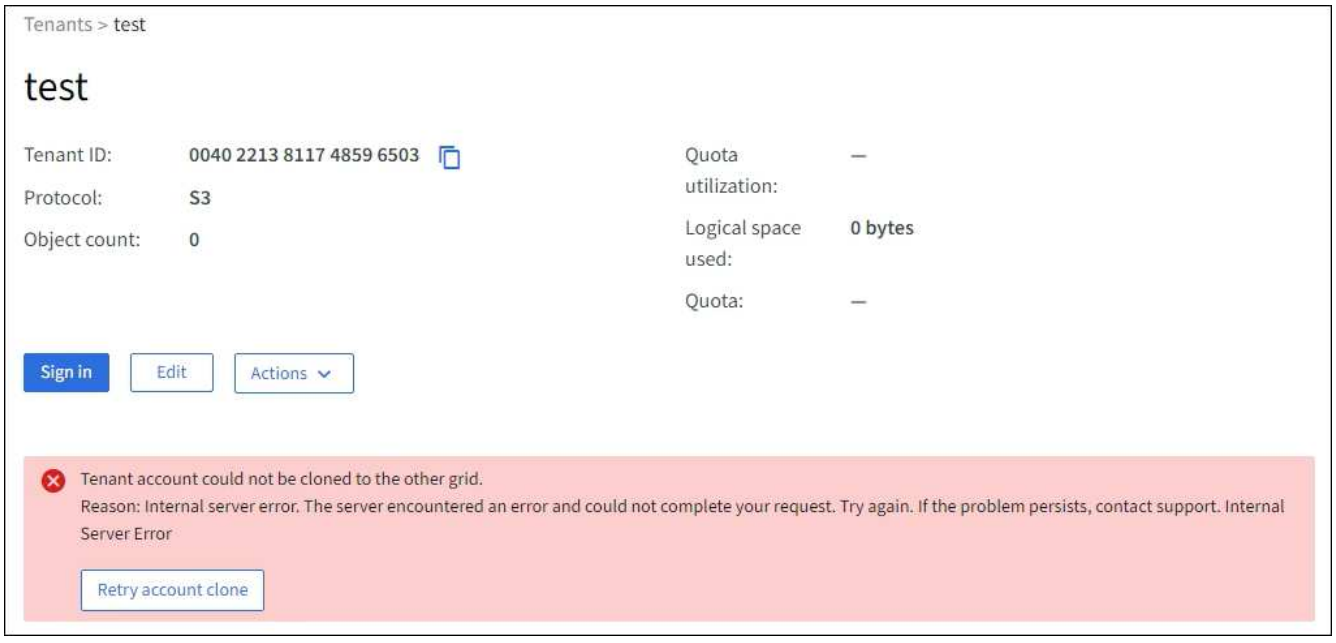
Vous voyez le message « Locataire créé sans clone » après avoir créé un nouveau locataire avec l'autorisation **Utiliser la connexion à la fédération de grille**.

Détails

Ce problème peut se produire si les mises à jour de l'état de la connexion sont retardées, ce qui peut entraîner l'affichage d'une connexion défectueuse comme **Connectée**.

Actions recommandées

1. Vérifiez la raison indiquée dans le message d'erreur et résolvez tout problème de réseau ou autre qui pourrait empêcher la connexion de fonctionner. Voir Alertes et erreurs de connexion à la fédération de grille .
2. Suivez les instructions pour tester une connexion à une fédération de grille dans"Gérer les connexions de la fédération de réseau" pour confirmer que le problème a été résolu.
3. Dans la grille source du locataire, sélectionnez **LOCATAIRES**.
4. Localisez le compte locataire qui n'a pas pu être cloné.
5. Sélectionnez le nom du locataire pour afficher la page de détails.
6. Sélectionnez **Réessayer le clonage du compte**.



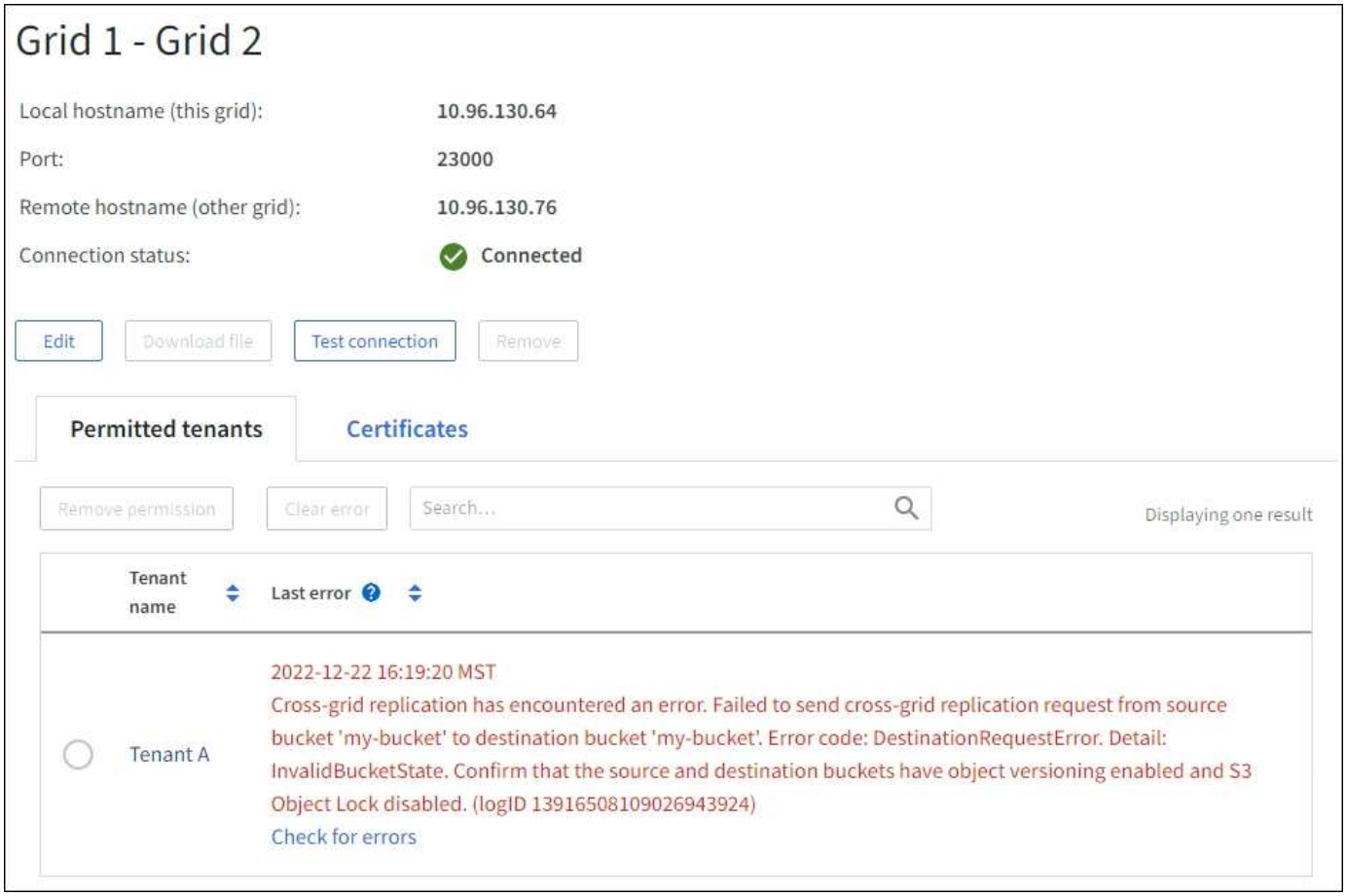
Si l'erreur a été résolue, le compte locataire sera désormais cloné sur l'autre grille.

Alertes et erreurs de réplication inter-réseaux

Dernière erreur affichée pour la connexion ou le locataire

Problème

Quand"visualisation d'une connexion à une fédération de grille" (ou quand"gérer les locataires autorisés" (pour une connexion), vous remarquez une erreur dans la colonne **Dernière erreur** sur la page des détails de la connexion. Par exemple:



Détails

Pour chaque connexion de fédération de grille, la colonne **Dernière erreur** affiche l'erreur la plus récente survenue, le cas échéant, lors de la réplication des données d'un locataire sur l'autre grille. Cette colonne affiche uniquement la dernière erreur de réplication inter-grille survenue ; les erreurs précédentes qui auraient pu se produire ne seront pas affichées. Une erreur dans cette colonne peut se produire pour l'une des raisons suivantes :

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

Actions recommandées

Si un message d'erreur apparaît dans la colonne **Dernière erreur**, procédez comme suit :

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

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

   Une fois l'erreur corrigée, une nouvelle **Dernière erreur** peut apparaître si des objets sont ingérés dans un autre compartiment qui comporte également une erreur.

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

Alerte d'échec permanent de réplication inter-réseau

Problème

L'alerte **Échec permanent de la réplication inter-réseau** a été déclenchée.

Détails

Cette alerte indique que les objets locataires ne peuvent pas être répliqués entre les buckets sur deux grilles pour une raison qui nécessite l'intervention de l'utilisateur pour être résolue. Cette alerte est généralement provoquée par une modification du bucket source ou de destination.

Actions recommandées

1. Sign in à la grille où l'alerte a été déclenchée.
2. Accédez à **CONFIGURATION** > **Système** > **Fédération de grille** et recherchez le nom de connexion répertorié dans l'alerte.
3. Dans l'onglet Locataires autorisés, regardez la colonne **Dernière erreur** pour déterminer quels comptes de locataire présentent des erreurs.
4. Pour en savoir plus sur l'échec, consultez les instructions dans"Surveiller les connexions de la fédération de réseau" pour examiner les mesures de réplication inter-réseaux.
5. Pour chaque compte locataire concerné :
   a. Voir les instructions dans"Surveiller l'activité des locataires" pour confirmer que le locataire n'a pas dépassé son quota sur la grille de destination pour la réplication inter-grille.
   b. Si nécessaire, augmentez le quota du locataire sur la grille de destination pour permettre l'enregistrement de nouveaux objets.
6. Pour chaque locataire concerné, connectez-vous à Tenant Manager sur les deux grilles afin de pouvoir comparer la liste des compartiments.
7. Pour chaque bucket pour lequel la réplication inter-grille est activée, confirmez les éléments suivants :

- Il existe un bucket correspondant pour le même locataire sur l'autre grille (vous devez utiliser le nom exact).
- Les deux buckets ont le contrôle de version des objets activé (le contrôle de version ne peut pas être suspendu sur l'une ou l'autre des grilles).
- Le verrouillage d'objet S3 est désactivé pour les deux buckets.
- Aucun des deux compartiments n'est dans l'état **Suppression d'objets : lecture seule**.

8. Pour confirmer que le problème a été résolu, consultez les instructions dans"Surveiller les connexions de la fédération de réseau" pour examiner les mesures de réplication inter-grille ou effectuez ces étapes :

   a. Retournez à la page de la fédération Grid.
   b. Sélectionnez le locataire concerné et sélectionnez **Effacer l'erreur** dans la colonne **Dernière erreur**.
   c. Sélectionnez **Oui** pour effacer le message et mettre à jour l'état du système.
   d. Attendez 5 à 6 minutes, puis ingérez un nouvel objet dans le seau. Vérifiez que le message d'erreur ne réapparaît pas.

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

   > Il faudra peut-être jusqu'à un jour pour que l'alerte disparaisse une fois résolue.

   a. Aller à"Identifier et réessayer les opérations de réplication ayant échoué" pour identifier les objets ou supprimer les marqueurs qui n'ont pas pu être répliqués sur l'autre grille et pour réessayer la réplication si nécessaire.

Alerte d'indisponibilité des ressources de réplication inter-réseau

Problème

L'alerte **Ressource de réplication inter-grille indisponible** a été déclenchée.

Détails

Cette alerte indique que des demandes de réplication inter-grille sont en attente car une ressource n'est pas disponible. Par exemple, il peut y avoir une erreur réseau.

Actions recommandées

1. Surveillez l'alerte pour voir si le problème se résout de lui-même.
2. Si le problème persiste, déterminez si l'une des grilles présente une alerte **Échec de connexion à la fédération de grille** pour la même connexion ou une alerte **Impossible de communiquer avec le nœud** pour un nœud. Cette alerte pourrait être résolue lorsque vous résolvez ces alertes.
3. Pour en savoir plus sur l'échec, consultez les instructions dans"Surveiller les connexions de la fédération de réseau" pour examiner les mesures de réplication inter-réseaux.
4. Si vous ne parvenez pas à résoudre l'alerte, contactez le support technique.

La réplication inter-grille se poursuivra normalement une fois le problème résolu.

Identifier et réessayer les opérations de réplication ayant échoué

Après avoir résolu l'alerte **Échec permanent de la réplication inter-grille**, vous devez déterminer si des objets ou des marqueurs de suppression n'ont pas pu être répliqués

sur l'autre grille. Vous pouvez ensuite réingérer ces objets ou utiliser l'API de gestion de grille pour réessayer la réplication.

L'alerte **Échec permanent de la réplication inter-grille** indique que les objets locataires ne peuvent pas être répliqués entre les buckets sur deux grilles pour une raison qui nécessite l'intervention de l'utilisateur pour être résolue. Cette alerte est généralement provoquée par une modification du bucket source ou de destination. Pour plus de détails, consultez la section "Résoudre les erreurs de fédération de grille" .

Déterminer si des objets n'ont pas pu être répliqués

Pour déterminer si des objets ou des marqueurs de suppression n'ont pas été répliqués sur l'autre grille, vous pouvez rechercher dans le journal d'audit"CGRR (demande de réplication inter-réseau)" messages. Ce message est ajouté au journal lorsque StorageGRID ne parvient pas à répliquer un objet, un objet en plusieurs parties ou à supprimer un marqueur dans le bucket de destination.

Vous pouvez utiliser le"outil d'audit-explication" pour traduire les résultats dans un format plus facile à lire.

Avant de commencer

- Vous disposez de l'autorisation d'accès root.
- Vous avez le `Passwords.txt` déposer.
- Vous connaissez l'adresse IP du nœud d'administration principal.

Étapes

1. Connectez-vous au nœud d'administration principal :
   a. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
   c. Entrez la commande suivante pour passer en root : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#` .

2. Recherchez les messages CGRR dans le journal d'audit et utilisez l'outil audit-explain pour formater les résultats.

   Par exemple, cette commande recherche tous les messages CGRR au cours des 30 dernières minutes et utilise l'outil audit-explain.

   ```
   # awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date { print }' audit.log | grep CGRR | audit-explain
   ```

   Les résultats de la commande ressembleront à cet exemple, qui comporte des entrées pour six messages CGRR. Dans l'exemple, toutes les demandes de réplication inter-grille ont renvoyé une erreur générale car l'objet n'a pas pu être répliqué. Les trois premières erreurs concernent les opérations de « réplication d'objet » et les trois dernières erreurs concernent les opérations de « réplication de marqueur de suppression ».

```
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-0"
version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-3"
version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-1"
version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-5"
version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
error
```

Chaque entrée contient les informations suivantes :

Champ	Description
Demande de réplication inter-réseau CGRR	Le nom de la demande
locataire	L'identifiant du compte du locataire
connexion	L'ID de la connexion à la fédération de grille
opération	Le type d'opération de réplication qui était tentée : • répliquer l'objet • répliquer supprimer le marqueur • répliquer un objet en plusieurs parties
seau	Le nom du bucket
objet	Le nom de l'objet
version	L'ID de version de l'objet

Champ	Description
erreur	Le type d'erreur. Si la réplication inter-grille échoue, l'erreur est « Erreur générale ».

Réessayer les réplications ayant échoué

Après avoir généré une liste d'objets et supprimé les marqueurs qui n'ont pas été répliqués dans le compartiment de destination et résolu les problèmes sous-jacents, vous pouvez réessayer la réplication de deux manières :

- Réingérez chaque objet dans le bucket source.
- Utilisez l'API privée Grid Management, comme décrit.

Étapes

1. En haut du gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **Documentation API**.
2. Sélectionnez **Accéder à la documentation de l'API privée**.

> Les points de terminaison de l'API StorageGRID marqués « Privé » sont susceptibles d'être modifiés sans préavis. Les points de terminaison privés StorageGRID ignorent également la version API de la demande.

3. Dans la section **cross-grid-replication-advanced**, sélectionnez le point de terminaison suivant :

   ```
   POST /private/cross-grid-replication-retry-failed
   ```

4. Sélectionnez **Essayer**.
5. Dans la zone de texte **body**, remplacez l'exemple d'entrée pour **versionID** par un ID de version du fichier audit.log qui correspond à une demande de réplication inter-grille ayant échoué.

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

6. Sélectionnez **Exécuter**.
7. Confirmez que le code de réponse du serveur est **204**, indiquant que l'objet ou le marqueur de suppression a été marqué comme en attente de réplication inter-grille vers l'autre grille.

> En attente signifie que la demande de réplication inter-grille a été ajoutée à la file d'attente interne pour traitement.

Surveiller les tentatives de réplication

Vous devez surveiller les opérations de nouvelle tentative de réplication pour vous assurer qu'elles se terminent.

> La réplication d'un objet ou d'un marqueur de suppression sur l'autre grille peut prendre plusieurs heures, voire plus.

Vous pouvez surveiller les opérations de nouvelle tentative de deux manières :

- Utiliser un S3"HeadObject" ou"Obtenir l'objet" demande. La réponse inclut le StorageGRID spécifique `x-ntap-sg-cgr-replication-status` en-tête de réponse, qui aura l'une des valeurs suivantes :

Grille	État de réplication
Source	• **TERMINÉ** : La réplication a réussi. • **EN ATTENTE** : L'objet n'a pas encore été répliqué. • **ÉCHEC** : La réplication a échoué avec un échec permanent. Un utilisateur doit résoudre l'erreur.
Destination	**RÉPLIQUE** : L'objet a été répliqué à partir de la grille source.

- Utilisez l'API privée Grid Management, comme décrit.

Étapes

1. Dans la section **cross-grid-replication-advanced** de la documentation de l'API privée, sélectionnez le point de terminaison suivant :

   `GET /private/cross-grid-replication-object-status/{id}`

2. Sélectionnez **Essayer**.
3. Dans la section Paramètres, entrez l'ID de version que vous avez utilisé dans le `cross-grid-replication-retry-failed` demande.
4. Sélectionnez **Exécuter**.
5. Confirmez que le code de réponse du serveur est **200**.
6. Vérifiez l'état de réplication, qui sera l'un des suivants :
   - **EN ATTENTE** : L'objet n'a pas encore été répliqué.
   - **TERMINÉ** : La réplication a réussi.
   - **ÉCHEC** : La réplication a échoué avec un échec permanent. Un utilisateur doit résoudre l'erreur.

Gérer la sécurité

Gérer la sécurité

Vous pouvez configurer divers paramètres de sécurité à partir du Grid Manager pour contribuer à sécuriser votre système StorageGRID .

Gérer le cryptage

StorageGRID fournit plusieurs options pour crypter les données. Tu devrais"examiner les méthodes de cryptage disponibles" pour déterminer ceux qui répondent à vos exigences en matière de protection des données.

Gérer les certificats

Tu peux"configurer et gérer les certificats du serveur" utilisé pour les connexions HTTP ou les certificats clients utilisés pour authentifier l'identité d'un client ou d'un utilisateur auprès du serveur.

Configurer les serveurs de gestion de clés

En utilisant un"serveur de gestion de clés" vous permet de protéger les données StorageGRID même si un appareil est retiré du centre de données. Une fois les volumes de l'appliance chiffrés, vous ne pouvez accéder à aucune donnée sur l'appliance, sauf si le nœud peut communiquer avec le KMS.

> Pour utiliser la gestion des clés de chiffrement, vous devez activer le paramètre **Chiffrement de nœud** pour chaque appliance lors de l'installation, avant que l'appliance ne soit ajoutée à la grille.

Gérer les paramètres de proxy

Si vous utilisez des services de plateforme S3 ou des pools de stockage cloud, vous pouvez configurer un"serveur proxy de stockage" entre les nœuds de stockage et les points de terminaison S3 externes. Si vous envoyez des packages AutoSupport via HTTPS ou HTTP, vous pouvez configurer un"serveur proxy d'administration" entre les nœuds d'administration et le support technique.

Contrôler les pare-feu

Pour améliorer la sécurité de votre système, vous pouvez contrôler l'accès aux nœuds d'administration StorageGRID en ouvrant ou en fermant des ports spécifiques au niveau du"pare-feu externe" . Vous pouvez également contrôler l'accès réseau à chaque nœud en configurant son"pare-feu interne" . Vous pouvez empêcher l'accès sur tous les ports, sauf ceux nécessaires à votre déploiement.

Examiner les méthodes de chiffrement StorageGRID

StorageGRID fournit plusieurs options pour crypter les données. Vous devez examiner les méthodes disponibles pour déterminer celles qui répondent à vos exigences en matière de protection des données.

Le tableau fournit un résumé de haut niveau des méthodes de chiffrement disponibles dans StorageGRID.

Option de cryptage	Comment ça marche	S'applique à
Serveur de gestion de clés (KMS) dans Grid Manager	Toi"configurer un serveur de gestion de clés" pour le site StorageGRID et "activer le chiffrement des nœuds pour l'appliance" . Ensuite, un nœud d'appareil se connecte au KMS pour demander une clé de chiffrement de clé (KEK). Cette clé crypte et décrypte la clé de cryptage des données (DEK) sur chaque volume.	Nœuds d'appareils pour lesquels le **chiffrement de nœud** est activé lors de l'installation. Toutes les données de l'appareil sont protégées contre toute perte physique ou suppression du centre de données. **Remarque** : la gestion des clés de chiffrement avec un KMS est uniquement prise en charge pour les nœuds de stockage et les appliances de services.

Option de cryptage	Comment ça marche	S'applique à
Page de chiffrement de lecteur dans le programme d'installation de l'appliance StorageGRID	Si l'appareil contient des lecteurs prenant en charge le chiffrement matériel, vous pouvez définir une phrase secrète de lecteur lors de l'installation. Lorsque vous définissez une phrase secrète de lecteur, il est impossible pour quiconque de récupérer des données valides à partir de lecteurs qui ont été supprimés du système, à moins de connaître la phrase secrète. Avant de commencer l'installation, accédez à **Configurer le matériel** > **Chiffrement de lecteur** pour définir une phrase secrète de lecteur qui s'applique à tous les lecteurs à chiffrement automatique gérés par StorageGRID dans un nœud.	Appareils contenant des lecteurs à chiffrement automatique. Toutes les données sur les disques sécurisés sont protégées contre toute perte physique ou suppression du centre de données. Le chiffrement des lecteurs ne s'applique pas aux lecteurs gérés par SANtricity. Si vous disposez d'un dispositif de stockage avec des lecteurs à chiffrement automatique et des contrôleurs SANtricity , vous pouvez activer la sécurité des lecteurs dans SANtricity.
Pilotez la sécurité dans SANtricity System Manager	Si la fonctionnalité Drive Security est activée pour votre appliance StorageGRID , vous pouvez utiliser "Gestionnaire de système SANtricity" pour créer et gérer la clé de sécurité. La clé est nécessaire pour accéder aux données sur les lecteurs sécurisés.	Appareils de stockage dotés de lecteurs à chiffrement complet du disque (FDE) ou de lecteurs à chiffrement automatique. Toutes les données sur les disques sécurisés sont protégées contre toute perte physique ou suppression du centre de données. Ne peut pas être utilisé avec certains appareils de stockage ou avec des appareils de service.
Chiffrement des objets stockés	Vous activez le"Chiffrement des objets stockés" option dans le gestionnaire de grille. Lorsque cette option est activée, tous les nouveaux objets qui ne sont pas chiffrés au niveau du bucket ou au niveau de l'objet sont chiffrés lors de l'ingestion.	Données d'objet S3 nouvellement ingérées. Les objets stockés existants ne sont pas chiffrés. Les métadonnées des objets et autres données sensibles ne sont pas chiffrées.

Option de cryptage	Comment ça marche	S'applique à
Chiffrement du compartiment S3	Vous émettez une demande PutBucketEncryption pour activer le chiffrement du bucket. Tous les nouveaux objets qui ne sont pas chiffrés au niveau de l'objet sont chiffrés lors de l'ingestion.	Données d'objet S3 nouvellement ingérées uniquement. Le chiffrement doit être spécifié pour le bucket. Les objets de bucket existants ne sont pas chiffrés. Les métadonnées des objets et autres données sensibles ne sont pas chiffrées. "Opérations sur les godets"
Chiffrement côté serveur d'objets S3 (SSE)	Vous émettez une requête S3 pour stocker un objet et incluez le `x-amz-server-side-encryption` en-tête de requête.	Données d'objet S3 nouvellement ingérées uniquement. Le cryptage doit être spécifié pour l'objet. Les métadonnées des objets et autres données sensibles ne sont pas chiffrées. StorageGRID gère les clés. "Utiliser le cryptage côté serveur"
Chiffrement côté serveur d'objets S3 avec clés fournies par le client (SSE-C)	Vous émettez une requête S3 pour stocker un objet et incluez trois en-têtes de requête. • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	Données d'objet S3 nouvellement ingérées uniquement. Le cryptage doit être spécifié pour l'objet. Les métadonnées des objets et autres données sensibles ne sont pas chiffrées. Les clés sont gérées en dehors de StorageGRID. "Utiliser le cryptage côté serveur"
Chiffrement de volume externe ou de banque de données	Vous utilisez une méthode de chiffrement en dehors de StorageGRID pour chiffrer un volume ou une banque de données entière, si votre plate-forme de déploiement la prend en charge.	Toutes les données d'objet, métadonnées et données de configuration système, en supposant que chaque volume ou banque de données soit chiffré. Une méthode de cryptage externe permet un contrôle plus strict des algorithmes et des clés de cryptage. Peut être combiné avec les autres méthodes répertoriées.

Option de cryptage	Comment ça marche	S'applique à
Chiffrement d'objets en dehors de StorageGRID	Vous utilisez une méthode de chiffrement en dehors de StorageGRID pour chiffrer les données et les métadonnées des objets avant qu'elles ne soient ingérées dans StorageGRID.	Données d'objet et métadonnées uniquement (les données de configuration du système ne sont pas chiffrées). Une méthode de cryptage externe permet un contrôle plus strict des algorithmes et des clés de cryptage. Peut être combiné avec les autres méthodes répertoriées. "Amazon Simple Storage Service - Guide de l'utilisateur : Protection des données à l'aide du chiffrement côté client"

Utiliser plusieurs méthodes de cryptage

Selon vos besoins, vous pouvez utiliser plusieurs méthodes de cryptage à la fois. Par exemple:

- Vous pouvez utiliser un KMS pour protéger les nœuds de l'appliance et également utiliser la fonction de sécurité du lecteur dans SANtricity System Manager pour « doublement crypter » les données sur les lecteurs à chiffrement automatique dans les mêmes appliances.
- Vous pouvez utiliser un KMS pour sécuriser les données sur les nœuds de l'appliance et également utiliser l'option de chiffrement des objets stockés pour chiffrer tous les objets lorsqu'ils sont ingérés.

Si seule une petite partie de vos objets nécessite un chiffrement, envisagez plutôt de contrôler le chiffrement au niveau du bucket ou de l'objet individuel. L'activation de plusieurs niveaux de cryptage entraîne un coût supplémentaire en termes de performances.

Gérer les certificats

Gérer les certificats de sécurité

Les certificats de sécurité sont de petits fichiers de données utilisés pour créer des connexions sécurisées et fiables entre les composants StorageGRID et entre les composants StorageGRID et les systèmes externes.

StorageGRID utilise deux types de certificats de sécurité :

- **Les certificats de serveur** sont requis lorsque vous utilisez des connexions HTTPS. Les certificats de serveur sont utilisés pour établir des connexions sécurisées entre les clients et les serveurs, authentifiant l'identité d'un serveur auprès de ses clients et fournissant un chemin de communication sécurisé pour les données. Le serveur et le client disposent chacun d'une copie du certificat.
- Les **certificats clients** authentifient l'identité d'un client ou d'un utilisateur auprès du serveur, offrant une authentification plus sécurisée que les mots de passe seuls. Les certificats clients ne cryptent pas les données.

Lorsqu'un client se connecte au serveur via HTTPS, le serveur répond avec le certificat du serveur, qui contient une clé publique. Le client vérifie ce certificat en comparant la signature du serveur à la signature sur

sa copie du certificat. Si les signatures correspondent, le client démarre une session avec le serveur en utilisant la même clé publique.

StorageGRID fonctionne comme serveur pour certaines connexions (comme le point de terminaison de l'équilibreur de charge) ou comme client pour d'autres connexions (comme le service de réplication CloudMirror).

Certificat Grid CA par défaut

StorageGRID inclut une autorité de certification (CA) intégrée qui génère un certificat CA Grid interne lors de l'installation du système. Le certificat Grid CA est utilisé, par défaut, pour sécuriser le trafic StorageGRID interne. Une autorité de certification (CA) externe peut émettre des certificats personnalisés entièrement conformes aux politiques de sécurité des informations de votre organisation. Bien que vous puissiez utiliser le certificat Grid CA pour un environnement hors production, la meilleure pratique pour un environnement de production consiste à utiliser des certificats personnalisés signés par une autorité de certification externe. Les connexions non sécurisées sans certificat sont également prises en charge mais ne sont pas recommandées.

- Les certificats CA personnalisés ne suppriment pas les certificats internes ; cependant, les certificats personnalisés doivent être ceux spécifiés pour vérifier les connexions au serveur.
- Tous les certificats personnalisés doivent répondre aux"directives de renforcement du système pour les certificats de serveur" .
- StorageGRID prend en charge le regroupement de certificats d'une autorité de certification dans un seul fichier (appelé regroupement de certificats d'autorité de certification).

> ⓘ StorageGRID inclut également des certificats d'autorité de certification du système d'exploitation qui sont les mêmes sur toutes les grilles. Dans les environnements de production, assurez-vous de spécifier un certificat personnalisé signé par une autorité de certification externe à la place du certificat CA du système d'exploitation.

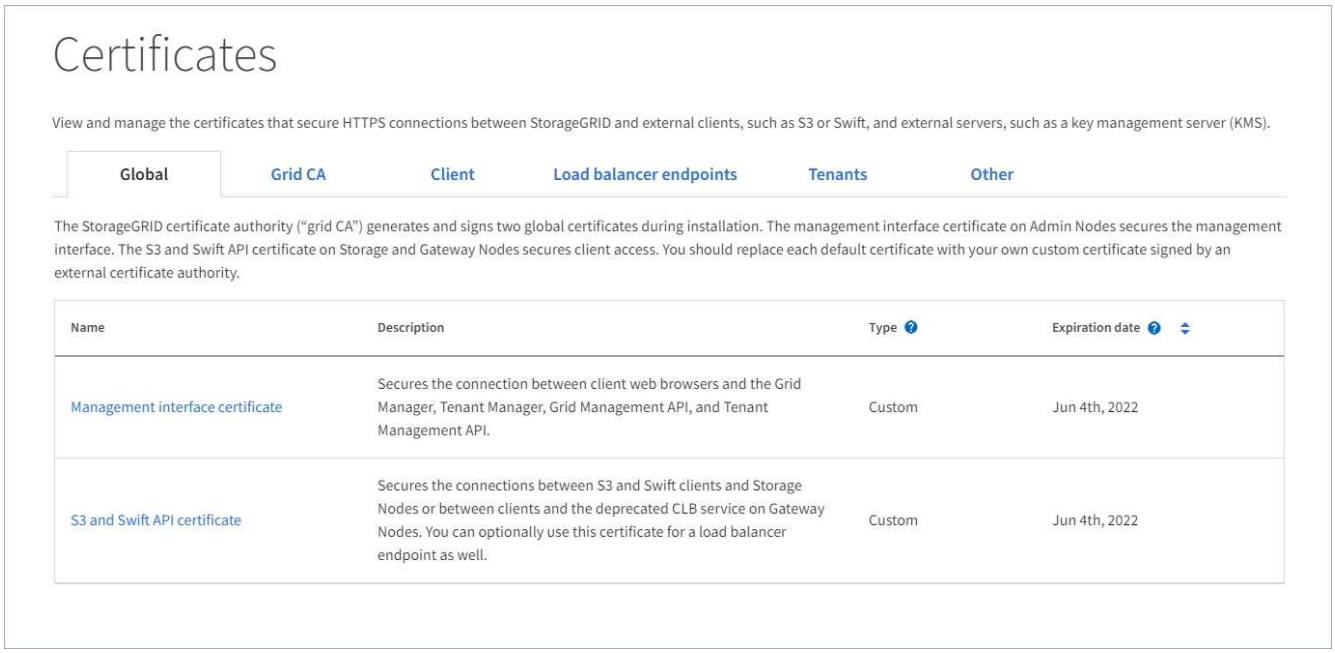
Les variantes des types de certificats serveur et client sont implémentées de plusieurs manières. Vous devez disposer de tous les certificats nécessaires à votre configuration StorageGRID spécifique avant de configurer le système.

Accéder aux certificats de sécurité

Vous pouvez accéder aux informations sur tous les certificats StorageGRID dans un seul emplacement, ainsi qu'aux liens vers le flux de travail de configuration pour chaque certificat.

Étapes

1. Depuis le Gestionnaire de grille, sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats**.



2. Sélectionnez un onglet sur la page Certificats pour obtenir des informations sur chaque catégorie de certificat et pour accéder aux paramètres du certificat. Vous pouvez accéder à un onglet si vous avez le"autorisation appropriée" .

   - **Global** : Sécurise l'accès à StorageGRID à partir des navigateurs Web et des clients API externes.
   - **Grid CA** : sécurise le trafic StorageGRID interne.
   - **Client** : sécurise les connexions entre les clients externes et la base de données StorageGRID Prometheus.
   - **Points de terminaison de l'équilibreur de charge** : sécurise les connexions entre les clients S3 et l'équilibreur de charge StorageGRID .
   - * Locataires * : sécurise les connexions aux serveurs de fédération d'identité ou des points de terminaison de service de la plateforme aux ressources de stockage S3.
   - **Autre** : Sécurise les connexions StorageGRID nécessitant des certificats spécifiques.

     Chaque onglet est décrit ci-dessous avec des liens vers des détails de certificat supplémentaires.

Mondial

Les certificats globaux sécurisent l'accès à StorageGRID à partir des navigateurs Web et des clients API S3 externes. Deux certificats globaux sont initialement générés par l'autorité de certification StorageGRID lors de l'installation. La meilleure pratique pour un environnement de production consiste à utiliser des certificats personnalisés signés par une autorité de certification externe.

- Certificat d'interface de gestion: Sécurise les connexions du navigateur Web client aux interfaces de gestion StorageGRID .
- Certificat API S3:Sécurise les connexions API client aux nœuds de stockage, aux nœuds d'administration et aux nœuds de passerelle, que les applications client S3 utilisent pour télécharger et charger des données d'objet.

Les informations sur les certificats globaux installés incluent :

- **Nom** : Nom du certificat avec lien pour gérer le certificat.
- **Description**
- **Type** : Personnalisé ou par défaut. + Vous devez toujours utiliser un certificat personnalisé pour améliorer la sécurité du réseau.
- **Date d'expiration** : Si vous utilisez le certificat par défaut, aucune date d'expiration n'est affichée.

Tu peux:

- Remplacez les certificats par défaut par des certificats personnalisés signés par une autorité de certification externe pour améliorer la sécurité de la grille :
  - "Remplacer le certificat d'interface de gestion généré par StorageGRID par défaut"utilisé pour les connexions Grid Manager et Tenant Manager.
  - "Remplacer le certificat API S3"utilisé pour les connexions au nœud de stockage et au point de terminaison de l'équilibreur de charge (facultatif).
- "Restaurer le certificat d'interface de gestion par défaut" .
- "Restaurer le certificat API S3 par défaut" .
- "Utiliser un script pour générer un nouveau certificat d'interface de gestion auto-signé" .
- Copiez ou téléchargez le"certificat d'interface de gestion" ou"Certificat API S3" .

Grille CA

LeCertificat Grid CA , généré par l'autorité de certification StorageGRID lors de l'installation de StorageGRID , sécurise tout le trafic interne de StorageGRID .

Les informations du certificat incluent la date d'expiration du certificat et le contenu du certificat.

Tu peux"copier ou télécharger le certificat Grid CA" , mais tu ne peux pas le changer.

Client

Certificats clients, généré par une autorité de certification externe, sécurise les connexions entre les outils de surveillance externes et la base de données StorageGRID Prometheus.

La table des certificats comporte une ligne pour chaque certificat client configuré et indique si le certificat peut être utilisé pour l'accès à la base de données Prometheus, ainsi que la date d'expiration du certificat.

Tu peux:

- "Téléchargez ou générez un nouveau certificat client."
- Sélectionnez un nom de certificat pour afficher les détails du certificat où vous pouvez :
  - "Modifier le nom du certificat client."
  - "Définissez l'autorisation d'accès Prometheus."
  - "Téléchargez et remplacez le certificat client."
  - "Copiez ou téléchargez le certificat client."
  - "Supprimer le certificat client."
- Sélectionnez **Actions** pour rapidement"modifier" ,"attacher" , ou"retirer" un certificat client. Vous pouvez sélectionner jusqu'à 10 certificats clients et les supprimer simultanément en utilisant **Actions** > **Supprimer**.

Points de terminaison de l'équilibreur de charge

Certificats de point de terminaison d'équilibrage de chargesécurisez les connexions entre les clients S3 et le service StorageGRID Load Balancer sur les nœuds de passerelle et les nœuds d'administration.

La table des points de terminaison de l'équilibreur de charge comporte une ligne pour chaque point de terminaison de l'équilibreur de charge configuré et indique si le certificat API S3 global ou un certificat de point de terminaison de l'équilibreur de charge personnalisé est utilisé pour le point de terminaison. La date d'expiration de chaque certificat est également affichée.

> Les modifications apportées à un certificat de point de terminaison peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

Tu peux:

- "Afficher un point de terminaison d'équilibrage de charge", y compris les détails de son certificat.
- "Spécifiez un certificat de point de terminaison d'équilibrage de charge pour FabricPool."
- "Utiliser le certificat API S3 global"au lieu de générer un nouveau certificat de point de terminaison d'équilibrage de charge.

Locataires

Les locataires peuvent utilisercertificats de serveur de fédération d'identité oucertificats de point de terminaison de service de plateforme pour sécuriser leurs connexions avec StorageGRID.

La table des locataires comporte une ligne pour chaque locataire et indique si chaque locataire est autorisé à utiliser sa propre source d'identité ou ses propres services de plateforme.

Tu peux:

- "Sélectionnez un nom de locataire pour vous connecter au gestionnaire de locataires"
- "Sélectionnez un nom de locataire pour afficher les détails de la fédération d'identité du locataire"
- "Sélectionnez un nom de locataire pour afficher les détails des services de la plateforme locataire"
- "Spécifier un certificat de point de terminaison de service de plateforme lors de la création du point de terminaison"

Autre

StorageGRID utilise d'autres certificats de sécurité à des fins spécifiques. Ces certificats sont répertoriés par leur nom fonctionnel. D'autres certificats de sécurité incluent :

- Certificats Cloud Storage Pool
- Certificats de notification d'alerte par courrier électronique
- Certificats de serveur syslog externes
- Certificats de connexion à la fédération de réseau
- Certificats de fédération d'identité
- Certificats du serveur de gestion de clés (KMS)
- Certificats d'authentification unique

Les informations indiquent le type de certificat utilisé par une fonction ainsi que les dates d'expiration de ses certificats serveur et client, le cas échéant. La sélection d'un nom de fonction ouvre un onglet de navigateur dans lequel vous pouvez afficher et modifier les détails du certificat.

> Vous ne pouvez afficher et accéder aux informations des autres certificats que si vous disposez des droits d'accès."autorisation appropriée" .

Tu peux:

- "Spécifier un certificat de pool de stockage cloud pour S3, C2S S3 ou Azure"
- "Spécifier un certificat pour les notifications d'alerte par e-mail"
- "Utiliser un certificat pour un serveur syslog externe"
- "Faire pivoter les certificats de connexion à la fédération de réseau"
- "Afficher et modifier un certificat de fédération d'identité"
- "Télécharger les certificats du serveur de gestion des clés (KMS) et du client"
- "Spécifier manuellement un certificat SSO pour une approbation de partie de confiance"

Détails du certificat de sécurité

Chaque type de certificat de sécurité est décrit ci-dessous, avec des liens vers les instructions de mise en œuvre.

Certificat d'interface de gestion

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les navigateurs Web clients et l'interface de gestion StorageGRID , permettant aux utilisateurs d'accéder à Grid Manager et Tenant Manager sans avertissements de sécurité. Ce certificat authentifie également les connexions à l'API Grid Management et à l'API Tenant Management. Vous pouvez utiliser le certificat par défaut créé lors de l'installation ou télécharger un certificat personnalisé.	**CONFIGURATION** > **Sécurité** > **Certificats**, sélectionnez l'onglet **Global**, puis sélectionnez **Certificat d'interface de gestion**	"Configurer les certificats de l'interface de gestion"

Certificat API S3

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie les connexions client S3 sécurisées à un nœud de stockage et aux points de terminaison de l'équilibreur de charge (facultatif).	**CONFIGURATION** > **Sécurité** > **Certificats**, sélectionnez l'onglet **Global**, puis sélectionnez **Certificat API S3**	"Configurer les certificats API S3"

Certificat Grid CA

Voir leDescription du certificat Grid CA par défaut .

Certificat client administrateur

Type de certificat	Description	Emplacement de navigation	Détails
Client	Installé sur chaque client, permettant à StorageGRID d'authentifier l'accès client externe. • Permet aux clients externes autorisés d'accéder à la base de données StorageGRID Prometheus. • Permet une surveillance sécurisée de StorageGRID à l'aide d'outils externes.	**CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Client**	"Configurer les certificats clients"

Certificat de point de terminaison de l'équilibreur de charge

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les clients S3 et le service d'équilibrage de charge StorageGRID sur les nœuds de passerelle et les nœuds d'administration. Vous pouvez télécharger ou générer un certificat d'équilibreur de charge lorsque vous configurez un point de terminaison d'équilibreur de charge. Les applications clientes utilisent le certificat d'équilibrage de charge lors de la connexion à StorageGRID pour enregistrer et récupérer les données d'objet. Vous pouvez également utiliser une version personnalisée du globalCertificat API S3 certificat pour authentifier les connexions au service Load Balancer. Si le certificat global est utilisé pour authentifier les connexions de l'équilibreur de charge, vous n'avez pas besoin de télécharger ou de générer un certificat distinct pour chaque point de terminaison de l'équilibreur de charge. **Remarque :** le certificat utilisé pour l'authentification de l'équilibreur de charge est le certificat le plus utilisé pendant le fonctionnement normal de StorageGRID .	**CONFIGURATION** > **Réseau** > **Points de terminaison de l'équilibreur de charge**	• "Configurer les points de terminaison de l'équilibreur de charge" • "Créer un point de terminaison d'équilibrage de charge pour FabricPool"

Certificat de point de terminaison du pool de stockage cloud

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion d'un pool de stockage cloud StorageGRID vers un emplacement de stockage externe, tel que S3 Glacier ou le stockage Microsoft Azure Blob. Un certificat différent est requis pour chaque type de fournisseur de cloud.	**ILM** > **Pools de stockage**	"Créer un pool de stockage cloud"

Certificat de notification d'alerte par courrier électronique

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifie la connexion entre un serveur de messagerie SMTP et StorageGRID utilisé pour les notifications d'alerte. • Si les communications avec le serveur SMTP nécessitent Transport Layer Security (TLS), vous devez spécifier le certificat d'autorité de certification du serveur de messagerie. • Spécifiez un certificat client uniquement si le serveur de messagerie SMTP requiert des certificats clients pour l'authentification.	**ALERTES** > **Configuration de la messagerie électronique**	"Configurer des notifications par e-mail pour les alertes"

Certificat de serveur syslog externe

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion TLS ou RELP/TLS entre un serveur syslog externe qui enregistre les événements dans StorageGRID. **Remarque :** un certificat de serveur Syslog externe n'est pas requis pour les connexions TCP, RELP/TCP et UDP à un serveur Syslog externe.	**CONFIGURATION** > **Surveillance** > **Serveur d'audit et syslog**	"Utiliser un serveur syslog externe"

Certificat de connexion à la fédération de réseau

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifiez et cryptez les informations envoyées entre le système StorageGRID actuel et une autre grille dans une connexion de fédération de grille.	**CONFIGURATION** > **Système** > **Fédération de grille**	• "Créer des connexions de fédération de grille" • "Faire tourner les certificats de connexion"

Certificat de fédération d'identité

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre StorageGRID et un fournisseur d'identité externe, tel qu'Active Directory, OpenLDAP ou Oracle Directory Server. Utilisé pour la fédération d'identité, qui permet aux groupes d'administrateurs et aux utilisateurs d'être gérés par un système externe.	**CONFIGURATION** > **Contrôle d'accès** > **Fédération d'identité**	"Utiliser la fédération d'identité"

Certificat du serveur de gestion de clés (KMS)

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifie la connexion entre StorageGRID et un serveur de gestion de clés externe (KMS), qui fournit des clés de chiffrement aux nœuds de l'appliance StorageGRID .	**CONFIGURATION** > **Sécurité** > **Serveur de gestion des clés**	"Ajouter un serveur de gestion de clés (KMS)"

Certificat de point de terminaison des services de plateforme

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion du service de plateforme StorageGRID à une ressource de stockage S3.	**Gestionnaire de locataires** > **STOCKAGE (S3)** > **Points de terminaison des services de plateforme**	"Créer un point de terminaison des services de plateforme" "Modifier le point de terminaison des services de la plateforme"

Certificat d'authentification unique (SSO)

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les services de fédération d'identité, tels que les services de fédération Active Directory (AD FS) et StorageGRID qui sont utilisés pour les demandes d'authentification unique (SSO).	**CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**	"Configurer l'authentification unique"

Exemples de certificats

Exemple 1 : service d'équilibrage de charge

Dans cet exemple, StorageGRID agit comme serveur.

1. Vous configurez un point de terminaison d'équilibrage de charge et téléchargez ou générez un certificat de serveur dans StorageGRID.
2. Vous configurez une connexion client S3 au point de terminaison de l'équilibreur de charge et téléchargez le même certificat sur le client.

3. Lorsque le client souhaite enregistrer ou récupérer des données, il se connecte au point de terminaison de l'équilibreur de charge à l'aide de HTTPS.
4. StorageGRID répond avec le certificat du serveur, qui contient une clé publique, et avec une signature basée sur la clé privée.
5. Le client vérifie ce certificat en comparant la signature du serveur à la signature sur sa copie du certificat. Si les signatures correspondent, le client démarre une session en utilisant la même clé publique.
6. Le client envoie des données d'objet à StorageGRID.

Exemple 2 : Serveur de gestion de clés externe (KMS)

Dans cet exemple, StorageGRID agit en tant que client.

1. À l'aide d'un logiciel de gestion de clés externe, vous configurez StorageGRID en tant que client KMS et obtenez un certificat de serveur signé par une autorité de certification, un certificat client public et la clé privée du certificat client.
2. À l'aide du gestionnaire de grille, vous configurez un serveur KMS et téléchargez les certificats du serveur et du client ainsi que la clé privée du client.
3. Lorsqu'un nœud StorageGRID a besoin d'une clé de chiffrement, il envoie une demande au serveur KMS qui inclut les données du certificat et une signature basée sur la clé privée.
4. Le serveur KMS valide la signature du certificat et décide qu'il peut faire confiance à StorageGRID.
5. Le serveur KMS répond en utilisant la connexion validée.

Types de certificats de serveur pris en charge

Le système StorageGRID prend en charge les certificats personnalisés chiffrés avec RSA ou ECDSA (Elliptic Curve Digital Signature Algorithm).

> Le type de chiffrement de la politique de sécurité doit correspondre au type de certificat du serveur. Par exemple, les chiffrements RSA nécessitent des certificats RSA et les chiffrements ECDSA nécessitent des certificats ECDSA. Voir "Gérer les certificats de sécurité" . Si vous configurez une politique de sécurité personnalisée qui n'est pas compatible avec le certificat du serveur, vous pouvez"revenir temporairement à la politique de sécurité par défaut" .

Pour plus d'informations sur la manière dont StorageGRID sécurise les connexions client, consultez"Sécurité pour les clients S3" .

Configurer les certificats de l'interface de gestion

Vous pouvez remplacer le certificat d'interface de gestion par défaut par un seul certificat personnalisé qui permet aux utilisateurs d'accéder au gestionnaire de grille et au gestionnaire de locataires sans rencontrer d'avertissements de sécurité. Vous pouvez également revenir au certificat d'interface de gestion par défaut ou en générer un nouveau.

À propos de cette tâche

Par défaut, chaque nœud d'administration reçoit un certificat signé par l'autorité de certification de la grille. Ces certificats signés par une autorité de certification peuvent être remplacés par un seul certificat d'interface de gestion personnalisée commune et la clé privée correspondante.

Étant donné qu'un seul certificat d'interface de gestion personnalisé est utilisé pour tous les nœuds d'administration, vous devez spécifier le certificat comme certificat générique ou multi-domaine si les clients doivent vérifier le nom d'hôte lors de la connexion au gestionnaire de grille et au gestionnaire de locataires. Définissez le certificat personnalisé de sorte qu'il corresponde à tous les nœuds d'administration de la grille.

Vous devez terminer la configuration sur le serveur et, en fonction de l'autorité de certification racine (CA) que vous utilisez, les utilisateurs peuvent également avoir besoin d'installer le certificat Grid CA dans le navigateur Web qu'ils utiliseront pour accéder au Grid Manager et au Tenant Manager.

Pour garantir que les opérations ne sont pas perturbées par un certificat de serveur défaillant, l'alerte **Expiration du certificat de serveur pour l'interface de gestion** est déclenchée lorsque ce certificat de serveur est sur le point d'expirer. Si nécessaire, vous pouvez voir quand le certificat actuel expire en sélectionnant **CONFIGURATION** > **Sécurité** > **Certificats** et en regardant la date d'expiration du certificat de l'interface de gestion dans l'onglet Global.

Si vous accédez au Grid Manager ou au Tenant Manager à l'aide d'un nom de domaine au lieu d'une adresse IP, le navigateur affiche une erreur de certificat sans option de contournement si l'une des situations suivantes se produit :

- Votre certificat d'interface de gestion personnalisée expire.
- Toirevenir d'un certificat d'interface de gestion personnalisé au certificat de serveur par défaut .

Ajouter un certificat d'interface de gestion personnalisé

Pour ajouter un certificat d'interface de gestion personnalisé, vous pouvez fournir votre propre certificat ou en générer un à l'aide du gestionnaire de grille.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat d'interface de gestion**.
3. Sélectionnez **Utiliser un certificat personnalisé**.
4. Téléchargez ou générez le certificat.

Télécharger le certificat

Téléchargez les fichiers de certificat de serveur requis.

a. Sélectionnez **Télécharger le certificat**.

b. Téléchargez les fichiers de certificat de serveur requis :

- **Certificat de serveur** : Le fichier de certificat de serveur personnalisé (codé PEM).
- **Clé privée du certificat** : Le fichier de clé privée du certificat du serveur personnalisé(`.key`).

> Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2 048 bits ou plus.

- **CA bundle** : un fichier facultatif unique contenant les certificats de chaque autorité de certification émettrice intermédiaire (CA). Le fichier doit contenir chacun des fichiers de certificat CA codés en PEM, concaténés dans l'ordre de la chaîne de certificats.

c. Développez **Détails du certificat** pour voir les métadonnées de chaque certificat que vous avez téléchargé. Si vous avez téléchargé un bundle CA facultatif, chaque certificat s'affiche sur son propre onglet.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat ou sélectionnez **Télécharger le bundle CA** pour enregistrer le bundle de certificats.

  Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

  Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier le certificat PEM** ou **Copier le bundle CA PEM** pour copier le contenu du certificat afin de le coller ailleurs.

d. Sélectionnez **Enregistrer**. + Le certificat d'interface de gestion personnalisé est utilisé pour toutes les nouvelles connexions ultérieures au Grid Manager, au Tenant Manager, à l'API Grid Manager ou à l'API Tenant Manager.

Générer un certificat

Générer les fichiers de certificat du serveur.

> La meilleure pratique pour un environnement de production consiste à utiliser un certificat d'interface de gestion personnalisé signé par une autorité de certification externe.

a. Sélectionnez **Générer un certificat**.

b. Spécifiez les informations du certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine entièrement qualifiés à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.

Champ	Description
propriété intellectuelle	Une ou plusieurs adresses IP à inclure dans le certificat.
Sujet (facultatif)	Sujet X.509 ou nom distinctif (DN) du propriétaire du certificat. Si aucune valeur n'est saisie dans ce champ, le certificat généré utilise le premier nom de domaine ou adresse IP comme nom commun du sujet (CN).
Jours de validité	Nombre de jours après la création pendant lesquels le certificat expire.
Ajouter des extensions d'utilisation de clés	Si cette option est sélectionnée (par défaut et recommandé), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré. Ces extensions définissent l'objectif de la clé contenue dans le certificat. **Remarque** : laissez cette case à cocher sélectionnée, sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **Générer**.

d. Sélectionnez **Détails du certificat** pour voir les métadonnées du certificat généré.

   - Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

     Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

     Par exemple : `storagegrid_certificate.pem`

   - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.

e. Sélectionnez **Enregistrer**. + Le certificat d'interface de gestion personnalisé est utilisé pour toutes les nouvelles connexions ultérieures au Grid Manager, au Tenant Manager, à l'API Grid Manager ou à l'API Tenant Manager.

5. Actualisez la page pour vous assurer que le navigateur Web est à jour.

   Après avoir téléchargé ou généré un nouveau certificat, prévoyez jusqu'à un jour pour que les alertes d'expiration de certificat associées disparaissent.

6. Une fois que vous avez ajouté un certificat d'interface de gestion personnalisé, la page Certificat d'interface de gestion affiche des informations détaillées sur les certificats en cours d'utilisation. + Vous pouvez télécharger ou copier le certificat PEM selon vos besoins.

Restaurer le certificat d'interface de gestion par défaut

Vous pouvez revenir à l'utilisation du certificat d'interface de gestion par défaut pour les connexions Grid

Manager et Tenant Manager.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat d'interface de gestion**.
3. Sélectionnez **Utiliser le certificat par défaut**.

   Lorsque vous restaurez le certificat d'interface de gestion par défaut, les fichiers de certificat de serveur personnalisé que vous avez configurés sont supprimés et ne peuvent pas être récupérés à partir du système. Le certificat d'interface de gestion par défaut est utilisé pour toutes les nouvelles connexions client ultérieures.

4. Actualisez la page pour vous assurer que le navigateur Web est à jour.

Utiliser un script pour générer un nouveau certificat d'interface de gestion auto-signé

Si une validation stricte du nom d'hôte est requise, vous pouvez utiliser un script pour générer le certificat de l'interface de gestion.

Avant de commencer

- Tu as"autorisations d'accès spécifiques" .
- Vous avez le `Passwords.txt` déposer.

À propos de cette tâche

La meilleure pratique pour un environnement de production consiste à utiliser un certificat signé par une autorité de certification externe.

Étapes

1. Obtenez le nom de domaine complet (FQDN) de chaque nœud d'administration.
2. Connectez-vous au nœud d'administration principal :
   a. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
   c. Entrez la commande suivante pour passer en root : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#` .

3. Configurez StorageGRID avec un nouveau certificat auto-signé.

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - Pour `--domains` , utilisez des caractères génériques pour représenter les noms de domaine complets de tous les nœuds d'administration. Par exemple, `*.ui.storagegrid.example.com` utilise le caractère générique * pour représenter `admin1.ui.storagegrid.example.com` et `admin2.ui.storagegrid.example.com` .
   - Ensemble `--type` à `management` pour configurer le certificat d'interface de gestion, qui est utilisé par Grid Manager et Tenant Manager.
   - Par défaut, les certificats générés sont valables un an (365 jours) et doivent être recréés avant leur

expiration. Vous pouvez utiliser le `--days` argument pour remplacer la période de validité par défaut.

> La période de validité d'un certificat commence lorsque `make-certificate` est exécuté. Vous devez vous assurer que le client de gestion est synchronisé avec la même source horaire que StorageGRID; sinon, le client risque de rejeter le certificat.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 720
```

La sortie résultante contient le certificat public nécessaire à votre client API de gestion.

4. Sélectionnez et copiez le certificat.

   Incluez les balises BEGIN et END dans votre sélection.

5. Déconnectez-vous de l'interpréteur de commandes. `$ exit`
6. Confirmer que le certificat a été configuré :
   a. Accéder au gestionnaire de grille.
   b. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats**
   c. Dans l'onglet **Global**, sélectionnez **Certificat d'interface de gestion**.
7. Configurez votre client de gestion pour utiliser le certificat public que vous avez copié. Inclure les balises BEGIN et END.

Téléchargez ou copiez le certificat de l'interface de gestion

Vous pouvez enregistrer ou copier le contenu du certificat de l'interface de gestion pour l'utiliser ailleurs.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat d'interface de gestion**.
3. Sélectionnez l'onglet **Serveur** ou **Pack CA**, puis téléchargez ou copiez le certificat.

Télécharger le fichier de certificat ou le bundle CA

Téléchargez le certificat ou le bundle CA `.pem` déposer. Si vous utilisez un ensemble d'autorités de certification facultatif, chaque certificat de l'ensemble s'affiche dans son propre sous-onglet.

a. Sélectionnez **Télécharger le certificat** ou **Télécharger le bundle CA**.

   Si vous téléchargez un bundle CA, tous les certificats des onglets secondaires du bundle CA sont téléchargés sous forme de fichier unique.

b. Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

   Par exemple : `storagegrid_certificate.pem`

Copier le certificat ou le bundle CA PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un ensemble d'autorités de certification facultatif, chaque certificat de l'ensemble s'affiche dans son propre sous-onglet.

a. Sélectionnez **Copier le certificat PEM** ou **Copier le bundle CA PEM**.

   Si vous copiez un bundle d'autorités de certification, tous les certificats des onglets secondaires du bundle d'autorités de certification sont copiés ensemble.

b. Collez le certificat copié dans un éditeur de texte.

c. Enregistrez le fichier texte avec l'extension `.pem` .

   Par exemple : `storagegrid_certificate.pem`

Configurer les certificats API S3

Vous pouvez remplacer ou restaurer le certificat de serveur utilisé pour les connexions client S3 aux nœuds de stockage ou aux points de terminaison de l'équilibreur de charge. Le certificat de serveur personnalisé de remplacement est spécifique à votre organisation.

Les détails Swift ont été supprimés de cette version du site de documentation. Voir "StorageGRID 11.8 : Configurer les certificats API S3 et Swift" .

À propos de cette tâche

Par défaut, chaque nœud de stockage reçoit un certificat de serveur X.509 signé par l'autorité de certification de la grille. Ces certificats signés par une autorité de certification peuvent être remplacés par un seul certificat de serveur personnalisé commun et une clé privée correspondante.

Un seul certificat de serveur personnalisé est utilisé pour tous les nœuds de stockage. Vous devez donc spécifier le certificat comme certificat générique ou multi-domaine si les clients doivent vérifier le nom d'hôte lors de la connexion au point de terminaison de stockage. Définissez le certificat personnalisé de sorte qu'il corresponde à tous les nœuds de stockage de la grille.

Une fois la configuration sur le serveur terminée, vous devrez peut-être également installer le certificat Grid CA

dans le client API S3 que vous utiliserez pour accéder au système, en fonction de l'autorité de certification racine (CA) que vous utilisez.

> Pour garantir que les opérations ne sont pas perturbées par un certificat de serveur défaillant, l'alerte **Expiration du certificat de serveur global pour l'API S3** est déclenchée lorsque le certificat du serveur racine est sur le point d'expirer. Si nécessaire, vous pouvez voir quand le certificat actuel expire en sélectionnant **CONFIGURATION** > **Sécurité** > **Certificats** et en regardant la date d'expiration du certificat API S3 dans l'onglet Global.

Vous pouvez télécharger ou générer un certificat API S3 personnalisé.

Ajouter un certificat API S3 personnalisé

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat API S3**.
3. Sélectionnez **Utiliser un certificat personnalisé**.
4. Téléchargez ou générez le certificat.

Télécharger le certificat

Téléchargez les fichiers de certificat de serveur requis.

a. Sélectionnez **Télécharger le certificat**.

b. Téléchargez les fichiers de certificat de serveur requis :

- **Certificat de serveur** : Le fichier de certificat de serveur personnalisé (codé PEM).
- **Clé privée du certificat** : Le fichier de clé privée du certificat du serveur personnalisé(`.key`).

> Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2 048 bits ou plus.

- **CA bundle** : un fichier facultatif unique contenant les certificats de chaque autorité de certification émettrice intermédiaire. Le fichier doit contenir chacun des fichiers de certificat CA codés PEM, concaténés dans l'ordre de la chaîne de certificats.

c. Sélectionnez les détails du certificat pour afficher les métadonnées et le PEM pour chaque certificat API S3 personnalisé qui a été téléchargé. Si vous avez téléchargé un bundle CA facultatif, chaque certificat s'affiche sur son propre onglet.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat ou sélectionnez **Télécharger le bundle CA** pour enregistrer le bundle de certificats.

  Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

  Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier le certificat PEM** ou **Copier le bundle CA PEM** pour copier le contenu du certificat afin de le coller ailleurs.

d. Sélectionnez **Enregistrer**.

Le certificat de serveur personnalisé est utilisé pour les nouvelles connexions client S3 ultérieures.

Générer un certificat

Générer les fichiers de certificat du serveur.

a. Sélectionnez **Générer un certificat**.

b. Spécifiez les informations du certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine entièrement qualifiés à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.
propriété intellectuelle	Une ou plusieurs adresses IP à inclure dans le certificat.

Champ	Description
Sujet (facultatif)	Sujet X.509 ou nom distinctif (DN) du propriétaire du certificat. Si aucune valeur n'est saisie dans ce champ, le certificat généré utilise le premier nom de domaine ou adresse IP comme nom commun du sujet (CN).
Jours de validité	Nombre de jours après la création pendant lesquels le certificat expire.
Ajouter des extensions d'utilisation de clés	Si cette option est sélectionnée (par défaut et recommandé), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré. Ces extensions définissent l'objectif de la clé contenue dans le certificat. **Remarque** : laissez cette case à cocher sélectionnée, sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **Générer**.

d. Sélectionnez **Détails du certificat** pour afficher les métadonnées et le PEM du certificat API S3 personnalisé qui a été généré.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

  Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

  Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.

e. Sélectionnez **Enregistrer**.

Le certificat de serveur personnalisé est utilisé pour les nouvelles connexions client S3 ultérieures.

5. Sélectionnez un onglet pour afficher les métadonnées du certificat de serveur StorageGRID par défaut, d'un certificat signé par une autorité de certification qui a été téléchargé ou d'un certificat personnalisé qui a été généré.

> Après avoir téléchargé ou généré un nouveau certificat, prévoyez jusqu'à un jour pour que les alertes d'expiration de certificat associées disparaissent.

6. Actualisez la page pour vous assurer que le navigateur Web est à jour.
7. Après avoir ajouté un certificat API S3 personnalisé, la page de certificat API S3 affiche des informations détaillées sur le certificat API S3 personnalisé en cours d'utilisation. + Vous pouvez télécharger ou copier le certificat PEM selon vos besoins.

Restaurer le certificat API S3 par défaut

Vous pouvez revenir à l'utilisation du certificat API S3 par défaut pour les connexions client S3 aux nœuds de stockage. Cependant, vous ne pouvez pas utiliser le certificat API S3 par défaut pour un point de terminaison d'équilibreur de charge.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat API S3**.
3. Sélectionnez **Utiliser le certificat par défaut**.

   Lorsque vous restaurez la version par défaut du certificat API S3 global, les fichiers de certificat de serveur personnalisés que vous avez configurés sont supprimés et ne peuvent pas être récupérés à partir du système. Le certificat API S3 par défaut sera utilisé pour les nouvelles connexions client S3 ultérieures aux nœuds de stockage.

4. Sélectionnez **OK** pour confirmer l'avertissement et restaurer le certificat API S3 par défaut.

   Si vous disposez de l'autorisation d'accès racine et que le certificat API S3 personnalisé a été utilisé pour les connexions aux points de terminaison de l'équilibreur de charge, une liste des points de terminaison de l'équilibreur de charge qui ne seront plus accessibles à l'aide du certificat API S3 par défaut s'affiche. Aller à"Configurer les points de terminaison de l'équilibreur de charge" pour modifier ou supprimer les points de terminaison affectés.

5. Actualisez la page pour vous assurer que le navigateur Web est à jour.

Téléchargez ou copiez le certificat API S3

Vous pouvez enregistrer ou copier le contenu du certificat API S3 pour l'utiliser ailleurs.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat API S3**.
3. Sélectionnez l'onglet **Serveur** ou **Pack CA**, puis téléchargez ou copiez le certificat.

Télécharger le fichier de certificat ou le bundle CA

Téléchargez le certificat ou le bundle CA `.pem` déposer. Si vous utilisez un ensemble d'autorités de certification facultatif, chaque certificat de l'ensemble s'affiche dans son propre sous-onglet.

a. Sélectionnez **Télécharger le certificat** ou **Télécharger le bundle CA**.

   Si vous téléchargez un bundle CA, tous les certificats des onglets secondaires du bundle CA sont téléchargés sous forme de fichier unique.

b. Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

   Par exemple : `storagegrid_certificate.pem`

Copier le certificat ou le bundle CA PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un ensemble d'autorités de certification facultatif, chaque certificat de l'ensemble s'affiche dans son propre sous-onglet.

a. Sélectionnez **Copier le certificat PEM** ou **Copier le bundle CA PEM**.

   Si vous copiez un bundle d'autorités de certification, tous les certificats des onglets secondaires du bundle d'autorités de certification sont copiés ensemble.

b. Collez le certificat copié dans un éditeur de texte.

c. Enregistrez le fichier texte avec l'extension `.pem` .

   Par exemple : `storagegrid_certificate.pem`

Informations connexes

- "Utiliser l'API REST S3"
- "Configurer les noms de domaine des points de terminaison S3"

Copier le certificat Grid CA

StorageGRID utilise une autorité de certification interne (CA) pour sécuriser le trafic interne. Ce certificat ne change pas si vous téléchargez vos propres certificats.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .

À propos de cette tâche

Si un certificat de serveur personnalisé a été configuré, les applications clientes doivent vérifier le serveur à l'aide du certificat de serveur personnalisé. Ils ne doivent pas copier le certificat CA du système StorageGRID .

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Grid CA**.

2. Dans la section **Certificat PEM**, téléchargez ou copiez le certificat.

Télécharger le fichier de certificat

Télécharger le certificat `.pem` déposer.

a. Sélectionnez **Télécharger le certificat**.

b. Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

Par exemple : `storagegrid_certificate.pem`

Copie du certificat PEM

Copiez le texte du certificat pour le coller ailleurs.

a. Sélectionnez **Copier le certificat PEM**.

b. Collez le certificat copié dans un éditeur de texte.

c. Enregistrez le fichier texte avec l'extension `.pem` .

Par exemple : `storagegrid_certificate.pem`

Configurer les certificats StorageGRID pour FabricPool

Pour les clients S3 qui effectuent une validation stricte du nom d'hôte et ne prennent pas en charge la désactivation de la validation stricte du nom d'hôte, tels que les clients ONTAP utilisant FabricPool, vous pouvez générer ou télécharger un certificat de serveur lorsque vous configurez le point de terminaison de l'équilibreur de charge.

Avant de commencer

- Tu as"autorisations d'accès spécifiques" .
- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .

À propos de cette tâche

Lorsque vous créez un point de terminaison d'équilibrage de charge, vous pouvez générer un certificat de serveur auto-signé ou télécharger un certificat signé par une autorité de certification (CA) connue. Dans les environnements de production, vous devez utiliser un certificat signé par une autorité de certification connue. Les certificats signés par une autorité de certification peuvent être renouvelés sans interruption. Ils sont également plus sécurisés car ils offrent une meilleure protection contre les attaques de type « man-in-the-middle ».

Les étapes suivantes fournissent des directives générales pour les clients S3 qui utilisent FabricPool. Pour des informations et des procédures plus détaillées, voir"Configurer StorageGRID pour FabricPool" .

Étapes

1. Vous pouvez également configurer un groupe de haute disponibilité (HA) à utiliser par FabricPool .
2. Créez un point de terminaison d'équilibrage de charge S3 à utiliser par FabricPool .

   Lorsque vous créez un point de terminaison d'équilibrage de charge HTTPS, vous êtes invité à télécharger

votre certificat de serveur, votre clé privée de certificat et votre ensemble d'autorités de certification facultatif.

3. Attachez StorageGRID en tant que niveau cloud dans ONTAP.

   Spécifiez le port du point de terminaison de l'équilibreur de charge et le nom de domaine complet utilisé dans le certificat CA que vous avez téléchargé. Ensuite, fournissez le certificat CA.

> Si une autorité de certification intermédiaire a émis le certificat StorageGRID , vous devez fournir le certificat de l'autorité de certification intermédiaire. Si le certificat StorageGRID a été émis directement par l'autorité de certification racine, vous devez fournir le certificat de l'autorité de certification racine.

Configurer les certificats clients

Les certificats clients permettent aux clients externes autorisés d'accéder à la base de données StorageGRID Prometheus, offrant ainsi un moyen sécurisé aux outils externes de surveiller StorageGRID.

Si vous devez accéder à StorageGRID à l'aide d'un outil de surveillance externe, vous devez télécharger ou générer un certificat client à l'aide du Grid Manager et copier les informations du certificat sur l'outil externe.

Voir"Gérer les certificats de sécurité" et"Configurer des certificats de serveur personnalisés" .

> Pour garantir que les opérations ne sont pas perturbées par un certificat de serveur défaillant, l'alerte **Expiration des certificats clients configurés sur la page Certificats** est déclenchée lorsque ce certificat de serveur est sur le point d'expirer. Si nécessaire, vous pouvez voir quand le certificat actuel expire en sélectionnant **CONFIGURATION** > **Sécurité** > **Certificats** et en regardant la date d'expiration du certificat client dans l'onglet Client.

> Si vous utilisez un serveur de gestion de clés (KMS) pour protéger les données sur des nœuds d'appliance spécialement configurés, consultez les informations spécifiques sur"téléchargement d'un certificat client KMS" .

Avant de commencer

- Vous disposez de l'autorisation d'accès root.
- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Pour configurer un certificat client :
  - Vous disposez de l'adresse IP ou du nom de domaine du nœud d'administration.
  - Si vous avez configuré le certificat d'interface de gestion StorageGRID , vous disposez de l'autorité de certification, du certificat client et de la clé privée utilisés pour configurer le certificat d'interface de gestion.
  - Pour télécharger votre propre certificat, la clé privée du certificat est disponible sur votre ordinateur local.
  - La clé privée doit avoir été sauvegardée ou enregistrée au moment de sa création. Si vous ne disposez pas de la clé privée d'origine, vous devez en créer une nouvelle.
- Pour modifier un certificat client :
  - Vous disposez de l'adresse IP ou du nom de domaine du nœud d'administration.

- Pour télécharger votre propre certificat ou un nouveau certificat, la clé privée, le certificat client et l'autorité de certification (si utilisée) sont disponibles sur votre ordinateur local.

Ajouter des certificats clients

Pour ajouter le certificat client, utilisez l'une de ces procédures :

- Certificat d'interface de gestion déjà configuré
- Certificat client émis par l'AC
- Certificat généré à partir de Grid Manager

Certificat d'interface de gestion déjà configuré

Utilisez cette procédure pour ajouter un certificat client si un certificat d'interface de gestion est déjà configuré à l'aide d'une autorité de certification, d'un certificat client et d'une clé privée fournis par le client.

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Client**.
2. Sélectionnez **Ajouter**.
3. Entrez un nom de certificat.
4. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser Prometheus**.
5. Sélectionnez **Continuer**.
6. Pour l'étape **Joindre les certificats**, téléchargez le certificat de l'interface de gestion.
   a. Sélectionnez **Télécharger le certificat**.
   b. Sélectionnez **Parcourir** et sélectionnez le fichier de certificat de l'interface de gestion(`.pem`).
      - Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.
      - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.
   c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

      Le nouveau certificat apparaît dans l'onglet Client.
7. Configurer un outil de surveillance externe, comme Grafana.

Certificat client émis par l'AC

Utilisez cette procédure pour ajouter un certificat client administrateur si aucun certificat d'interface de gestion n'a été configuré et que vous prévoyez d'ajouter un certificat client pour Prometheus qui utilise un certificat client émis par une autorité de certification et une clé privée.

Étapes

1. Effectuez les étapes pour"configurer un certificat d'interface de gestion" .
2. Dans le Gestionnaire de grille, sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Client**.
3. Sélectionnez **Ajouter**.

4. Entrez un nom de certificat.
5. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser Prometheus**.
6. Sélectionnez **Continuer**.
7. Pour l'étape **Joindre les certificats**, téléchargez le certificat client, la clé privée et les fichiers du bundle CA :
   a. Sélectionnez **Télécharger le certificat**.
   b. Sélectionnez **Parcourir** et sélectionnez le certificat client, la clé privée et les fichiers groupés de l'autorité de certification(`.pem`).
      - Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.
      - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.
   c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

      Les nouveaux certificats apparaissent dans l'onglet Client.
8. Configurer un outil de surveillance externe, comme Grafana.

Certificat généré à partir de Grid Manager

Utilisez cette procédure pour ajouter un certificat client administrateur si aucun certificat d'interface de gestion n'a été configuré et que vous prévoyez d'ajouter un certificat client pour Prometheus qui utilise la fonction de génération de certificat dans Grid Manager.

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Client**.
2. Sélectionnez **Ajouter**.
3. Entrez un nom de certificat.
4. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser Prometheus**.
5. Sélectionnez **Continuer**.
6. Pour l'étape **Joindre des certificats**, sélectionnez **Générer un certificat**.
7. Spécifiez les informations du certificat :
   - **Sujet** (facultatif) : sujet X.509 ou nom distinctif (DN) du propriétaire du certificat.
   - **Jours de validité** : Le nombre de jours pendant lesquels le certificat généré est valide, à compter du moment où il est généré.
   - **Ajouter des extensions d'utilisation de clé** : si cette option est sélectionnée (par défaut et recommandé), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré.

     Ces extensions définissent l'objectif de la clé contenue dans le certificat.

     Laissez cette case à cocher sélectionnée, sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

8. Sélectionnez **Générer**.
9. Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.

   > Vous ne pourrez pas afficher la clé privée du certificat après avoir fermé la boîte de dialogue. Copiez ou téléchargez la clé dans un emplacement sûr.

   - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.
   - Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

     Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

   Par exemple : `storagegrid_certificate.pem`

   - Sélectionnez **Copier la clé privée** pour copier la clé privée du certificat afin de la coller ailleurs.
   - Sélectionnez **Télécharger la clé privée** pour enregistrer la clé privée sous forme de fichier.

     Spécifiez le nom du fichier de clé privée et l'emplacement de téléchargement.

10. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

    Le nouveau certificat apparaît dans l'onglet Client.

11. Dans le Gestionnaire de grille, sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Global**.
12. Sélectionnez **Certificat d'interface de gestion**.
13. Sélectionnez **Utiliser un certificat personnalisé**.
14. Téléchargez les fichiers certificate.pem et private_key.pem depuis ledétails du certificat client étape. Il n'est pas nécessaire de télécharger le bundle CA.
    a. Sélectionnez **Télécharger le certificat** puis sélectionnez **Continuer**.
    b. Téléchargez chaque fichier de certificat(`.pem`).
    c. Sélectionnez **Enregistrer** pour enregistrer le certificat dans le gestionnaire de grille.

       Le nouveau certificat apparaît sur la page des certificats de l'interface de gestion.

15. Configurer un outil de surveillance externe, comme Grafana.

Configurer un outil de surveillance externe

Étapes

1. Configurez les paramètres suivants sur votre outil de surveillance externe, tel que Grafana.
   a. **Nom**: Saisissez un nom pour la connexion.

      StorageGRID ne nécessite pas ces informations, mais vous devez fournir un nom pour tester la connexion.

   b. **URL**: Saisissez le nom de domaine ou l'adresse IP du nœud d'administration. Spécifiez HTTPS et le port 9091.

Par exemple : `https://admin-node.example.com:9091`

c. Activez **TLS Client Auth** et **Avec certificat CA**.

d. Sous Détails d'authentification TLS/SSL, copiez et collez :

- L'interface de gestion du certificat CA vers **CA Cert**
- Le certificat client de **Client Cert**
- La clé privée de **Clé client**

e. **ServerName**: saisissez le nom de domaine du nœud d'administration.

ServerName doit correspondre au nom de domaine tel qu'il apparaît dans le certificat de l'interface de gestion.

2. Enregistrez et testez le certificat et la clé privée que vous avez copiés à partir de StorageGRID ou d'un fichier local.

Vous pouvez désormais accéder aux métriques Prometheus depuis StorageGRID avec votre outil de surveillance externe.

Pour plus d'informations sur les mesures, consultez le"instructions pour la surveillance de StorageGRID" .

Modifier les certificats clients

Vous pouvez modifier un certificat client administrateur pour changer son nom, activer ou désactiver l'accès à Prometheus ou télécharger un nouveau certificat lorsque le certificat actuel a expiré.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Client**.

Les dates d'expiration des certificats et les autorisations d'accès Prometheus sont répertoriées dans le tableau. Si un certificat expire bientôt ou est déjà expiré, un message apparaît dans le tableau et une alerte est déclenchée.

2. Sélectionnez le certificat que vous souhaitez modifier.
3. Sélectionnez **Modifier** puis sélectionnez **Modifier le nom et l'autorisation**
4. Entrez un nom de certificat.
5. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser Prometheus**.
6. Sélectionnez **Continuer** pour enregistrer le certificat dans le gestionnaire de grille.

Le certificat mis à jour s'affiche dans l'onglet Client.

Joindre un nouveau certificat client

Vous pouvez télécharger un nouveau certificat lorsque le certificat actuel a expiré.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Client**.

Les dates d'expiration des certificats et les autorisations d'accès Prometheus sont répertoriées dans le

tableau. Si un certificat expire bientôt ou est déjà expiré, un message apparaît dans le tableau et une alerte est déclenchée.

2. Sélectionnez le certificat que vous souhaitez modifier.
3. Sélectionnez **Modifier** puis sélectionnez une option de modification.

Télécharger le certificat

Copiez le texte du certificat pour le coller ailleurs.

a. Sélectionnez **Télécharger le certificat** puis sélectionnez **Continuer**.

b. Télécharger le nom du certificat client(`.pem`).

   Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.

   - Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

     Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

   Par exemple : `storagegrid_certificate.pem`

   - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.

c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

   Le certificat mis à jour s'affiche dans l'onglet Client.

Générer un certificat

Générez le texte du certificat à coller ailleurs.

a. Sélectionnez **Générer un certificat**.

b. Spécifiez les informations du certificat :

   - **Sujet** (facultatif) : sujet X.509 ou nom distinctif (DN) du propriétaire du certificat.
   - **Jours de validité** : Le nombre de jours pendant lesquels le certificat généré est valide, à compter du moment où il est généré.
   - **Ajouter des extensions d'utilisation de clé** : si cette option est sélectionnée (par défaut et recommandé), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré.

     Ces extensions définissent l'objectif de la clé contenue dans le certificat.

     Laissez cette case à cocher sélectionnée, sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **Générer**.

d. Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.

   Vous ne pourrez pas afficher la clé privée du certificat après avoir fermé la boîte de dialogue. Copiez ou téléchargez la clé dans un emplacement sûr.

   - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller

ailleurs.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

  Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

  Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier la clé privée** pour copier la clé privée du certificat afin de la coller ailleurs.
- Sélectionnez **Télécharger la clé privée** pour enregistrer la clé privée sous forme de fichier.

  Spécifiez le nom du fichier de clé privée et l'emplacement de téléchargement.

e. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

Le nouveau certificat apparaît dans l'onglet Client.

Télécharger ou copier les certificats clients

Vous pouvez télécharger ou copier un certificat client pour l'utiliser ailleurs.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Client**.
2. Sélectionnez le certificat que vous souhaitez copier ou télécharger.
3. Téléchargez ou copiez le certificat.

Télécharger le fichier de certificat

Télécharger le certificat `.pem` déposer.

a. Sélectionnez **Télécharger le certificat**.

b. Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

Par exemple : `storagegrid_certificate.pem`

Copie du certificat

Copiez le texte du certificat pour le coller ailleurs.

a. Sélectionnez **Copier le certificat PEM**.

b. Collez le certificat copié dans un éditeur de texte.

c. Enregistrez le fichier texte avec l'extension `.pem` .

Par exemple : `storagegrid_certificate.pem`

Supprimer les certificats clients

Si vous n'avez plus besoin d'un certificat client administrateur, vous pouvez le supprimer.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Client**.
2. Sélectionnez le certificat que vous souhaitez supprimer.
3. Sélectionnez **Supprimer** puis confirmez.

> Pour supprimer jusqu'à 10 certificats, sélectionnez chaque certificat à supprimer dans l'onglet Client, puis sélectionnez **Actions** > **Supprimer**.

Une fois un certificat supprimé, les clients qui ont utilisé le certificat doivent spécifier un nouveau certificat client pour accéder à la base de données StorageGRID Prometheus.

Configurer les paramètres de sécurité

Gérer la politique TLS et SSH

La politique TLS et SSH détermine les protocoles et chiffrements utilisés pour établir des connexions TLS sécurisées avec les applications clientes et des connexions SSH sécurisées aux services StorageGRID internes.

La politique de sécurité contrôle la manière dont TLS et SSH chiffrent les données en mouvement. En général, utilisez la politique de compatibilité moderne (par défaut), sauf si votre système doit être conforme aux critères communs ou si vous devez utiliser d'autres chiffrements.

> Certains services StorageGRID n'ont pas été mis à jour pour utiliser les chiffrements dans ces politiques.

Avant de commencer

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

Sélectionnez une politique de sécurité

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Paramètres de sécurité**.

   L'onglet **Politiques TLS et SSH** affiche les politiques disponibles. La politique actuellement active est indiquée par une coche verte sur la vignette de la politique.

2. Consultez les tuiles pour en savoir plus sur les politiques disponibles.

Politique	Description
Compatibilité moderne (par défaut)	Utilisez la politique par défaut si vous avez besoin d'un cryptage fort et à moins que vous n'ayez des exigences particulières. Cette politique est compatible avec la plupart des clients TLS et SSH.
Compatibilité héritée	Utilisez cette politique si vous avez besoin d'options de compatibilité supplémentaires pour les clients plus anciens. Les options supplémentaires de cette politique peuvent la rendre moins sécurisée que la politique de compatibilité moderne.
Critères communs	Utilisez cette politique si vous avez besoin d'une certification Critères communs.
FIPS strict	Utilisez cette politique si vous avez besoin d'une certification Common Criteria et devez utiliser le module de sécurité cryptographique NetApp 3.0.8 pour les connexions client externes aux points de terminaison de l'équilibreur de charge, au gestionnaire de locataires et au gestionnaire de grille. L'utilisation de cette politique peut réduire les performances. **Remarque** : après avoir sélectionné cette politique, tous les nœuds doivent être"redémarré de manière continue" pour activer le module de sécurité cryptographique NetApp . Utilisez **Maintenance** > **Redémarrage progressif** pour lancer et surveiller les redémarrages.
Coutume	Créez une politique personnalisée si vous devez appliquer vos propres chiffrements.

3. Pour voir les détails sur les chiffrements, les protocoles et les algorithmes de chaque politique, sélectionnez **Afficher les détails**.
4. Pour modifier la politique actuelle, sélectionnez **Utiliser la politique**.

   Une coche verte apparaît à côté de **Politique actuelle** sur la vignette de la politique.

Créer une politique de sécurité personnalisée

Vous pouvez créer une politique personnalisée si vous devez appliquer vos propres chiffrements.

Étapes

1. À partir de la vignette de la politique la plus similaire à la politique personnalisée que vous souhaitez créer, sélectionnez **Afficher les détails**.
2. Sélectionnez **Copier dans le presse-papiers**, puis sélectionnez **Annuler**.

3. Dans la mosaïque **Politique personnalisée**, sélectionnez **Configurer et utiliser**.
4. Collez le JSON que vous avez copié et apportez les modifications nécessaires.
5. Sélectionnez **Utiliser la politique**.

   Une coche verte apparaît à côté de **Politique actuelle** sur la mosaïque Politique personnalisée.

6. Vous pouvez également sélectionner **Modifier la configuration** pour apporter d'autres modifications à la nouvelle politique personnalisée.

Revenir temporairement à la politique de sécurité par défaut

Si vous avez configuré une politique de sécurité personnalisée, vous ne pourrez peut-être pas vous connecter au Grid Manager si la politique TLS configurée est incompatible avec la"certificat de serveur configuré" .

Vous pouvez revenir temporairement à la politique de sécurité par défaut.

Étapes

1. Connectez-vous à un nœud d'administration :
   a. Entrez la commande suivante : `ssh admin@Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
   c. Entrez la commande suivante pour passer en root : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#` .

2. Exécutez la commande suivante :

   ```
   restore-default-cipher-configurations
   ```

3. À partir d'un navigateur Web, accédez au gestionnaire de grille sur le même nœud d'administration.
4. Suivez les étapes dansSélectionnez une politique de sécurité pour configurer à nouveau la politique.

Configurer la sécurité du réseau et des objets

Vous pouvez configurer la sécurité du réseau et des objets pour chiffrer les objets stockés, pour empêcher certaines requêtes S3 ou pour autoriser les connexions client aux nœuds de stockage à utiliser HTTP au lieu de HTTPS.

Chiffrement des objets stockés

Le chiffrement des objets stockés permet le chiffrement de toutes les données d'objets lorsqu'elles sont ingérées via S3. Par défaut, les objets stockés ne sont pas chiffrés, mais vous pouvez choisir de crypter les objets à l'aide de l'algorithme de chiffrement AES-128 ou AES-256. Lorsque vous activez le paramètre, tous les objets nouvellement ingérés sont chiffrés, mais aucune modification n'est apportée aux objets stockés existants. Si vous désactivez le chiffrement, les objets actuellement chiffrés restent chiffrés, mais les objets nouvellement ingérés ne sont pas chiffrés.

Le paramètre de chiffrement d'objet stocké s'applique uniquement aux objets S3 qui n'ont pas été chiffrés par un chiffrement au niveau du bucket ou au niveau de l'objet.

Pour plus de détails sur les méthodes de chiffrement StorageGRID , voir"Examiner les méthodes de chiffrement StorageGRID" .

Empêcher la modification du client

Empêcher la modification du client est un paramètre à l'échelle du système. Lorsque l'option **Empêcher la modification du client** est sélectionnée, les demandes suivantes sont refusées.

API REST S3

- Requêtes DeleteBucket
- Toute demande de modification des données d'un objet existant, des métadonnées définies par l'utilisateur ou du balisage d'un objet S3

Activer HTTP pour les connexions aux nœuds de stockage

Par défaut, les applications clientes utilisent le protocole réseau HTTPS pour toutes les connexions directes aux nœuds de stockage. Vous pouvez éventuellement activer HTTP pour ces connexions, par exemple lors du test d'une grille non productive.

Utilisez HTTP pour les connexions aux nœuds de stockage uniquement si les clients S3 doivent établir des connexions HTTP directement aux nœuds de stockage. Vous n'avez pas besoin d'utiliser cette option pour les clients qui utilisent uniquement des connexions HTTPS ou pour les clients qui se connectent au service Load Balancer (car vous pouvez"configurer chaque point de terminaison de l'équilibreur de charge" (utiliser soit HTTP soit HTTPS).

Voir"Résumé : Adresses IP et ports pour les connexions client" pour savoir quels ports les clients S3 utilisent lors de la connexion aux nœuds de stockage via HTTP ou HTTPS.

Sélectionnez les options

Avant de commencer

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

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Paramètres de sécurité**.
2. Sélectionnez l'onglet **Réseau et objets**.
3. Pour le chiffrement des objets stockés, utilisez le paramètre **Aucun** (par défaut) si vous ne souhaitez pas que les objets stockés soient chiffrés, ou sélectionnez **AES-128** ou **AES-256** pour chiffrer les objets stockés.
4. Sélectionnez éventuellement **Empêcher la modification du client** si vous souhaitez empêcher les clients S3 d'effectuer des demandes spécifiques.

   Si vous modifiez ce paramètre, l'application du nouveau paramètre prendra environ une minute. La valeur configurée est mise en cache pour les performances et la mise à l'échelle.

5. Sélectionnez éventuellement **Activer HTTP pour les connexions aux nœuds de stockage** si les clients se connectent directement aux nœuds de stockage et que vous souhaitez utiliser des connexions HTTP.

   Soyez prudent lorsque vous activez HTTP pour une grille de production car les requêtes seront envoyées non chiffrées.

6. Sélectionnez **Enregistrer**.

Modifier les paramètres de sécurité de l'interface

Les paramètres de sécurité de l'interface vous permettent de contrôler si les utilisateurs sont déconnectés s'ils sont inactifs pendant plus de la durée spécifiée et si une trace de pile est incluse dans les réponses d'erreur d'API.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"Autorisation d'accès root" .

À propos de cette tâche

La page **Paramètres de sécurité** inclut les paramètres **Délai d'inactivité du navigateur** et **Trace de la pile de l'API de gestion**.

Délai d'inactivité du navigateur

Indique combien de temps le navigateur d'un utilisateur peut être inactif avant que l'utilisateur ne soit déconnecté. La valeur par défaut est de 15 minutes.

Le délai d'inactivité du navigateur est également contrôlé par les éléments suivants :

- Un minuteur StorageGRID distinct et non configurable, inclus pour la sécurité du système. Le jeton d'authentification de chaque utilisateur expire 16 heures après la connexion de l'utilisateur. Lorsque l'authentification d'un utilisateur expire, cet utilisateur est automatiquement déconnecté, même si le délai d'inactivité du navigateur est désactivé ou si la valeur du délai d'expiration du navigateur n'a pas été atteinte. Pour renouveler le jeton, l'utilisateur doit se reconnecter.
- Paramètres de délai d'expiration pour le fournisseur d'identité, en supposant que l'authentification unique (SSO) est activée pour StorageGRID.

  Si SSO est activé et que le navigateur d'un utilisateur expire, l'utilisateur doit ressaisir ses informations d'identification SSO pour accéder à nouveau à StorageGRID . Voir "Configurer l'authentification unique" .

Trace de pile de l'API de gestion

Contrôle si une trace de pile est renvoyée dans les réponses d'erreur de l'API Grid Manager et Tenant Manager.

Cette option est désactivée par défaut, mais vous souhaiterez peut-être activer cette fonctionnalité pour un environnement de test. En général, vous devez laisser la trace de pile désactivée dans les environnements de production pour éviter de révéler les détails internes du logiciel lorsque des erreurs d'API se produisent.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Paramètres de sécurité**.
2. Sélectionnez l'onglet **Interface**.
3. Pour modifier le paramètre de délai d'inactivité du navigateur :
   a. Développez l'accordéon.
   b. Pour modifier le délai d'expiration, spécifiez une valeur comprise entre 60 secondes et 7 jours. Le délai d'expiration par défaut est de 15 minutes.
   c. Pour désactiver cette fonctionnalité, décochez la case.
   d. Sélectionnez **Enregistrer**.

      Le nouveau paramètre n'affecte pas les utilisateurs actuellement connectés. Les utilisateurs doivent se reconnecter ou actualiser leur navigateur pour que le nouveau paramètre de délai d'expiration prenne effet.
4. Pour modifier le paramètre de la trace de la pile de l'API de gestion :
   a. Développez l'accordéon.
   b. Cochez la case pour renvoyer une trace de pile dans les réponses d'erreur de l'API Grid Manager et Tenant Manager.

      Laissez la trace de pile désactivée dans les environnements de production pour éviter de révéler les détails internes du logiciel lorsque des erreurs d'API se produisent.

   c. Sélectionnez **Enregistrer**.

Configurer les serveurs de gestion de clés

Qu'est-ce qu'un serveur de gestion de clés (KMS) ?

Un serveur de gestion de clés (KMS) est un système externe tiers qui fournit des clés de chiffrement aux nœuds d'appliance StorageGRID sur le site StorageGRID associé à l'aide du protocole d'interopérabilité de gestion de clés (KMIP).

StorageGRID prend en charge uniquement certains serveurs de gestion de clés. Pour obtenir la liste des produits et versions pris en charge, utilisez le "Outil de matrice d'interopérabilité NetApp (IMT)" .

Vous pouvez utiliser un ou plusieurs serveurs de gestion de clés pour gérer les clés de chiffrement de nœud pour tous les nœuds d'appliance StorageGRID dont le paramètre **Chiffrement de nœud** est activé lors de l'installation. L'utilisation de serveurs de gestion de clés avec ces nœuds d'appliance vous permet de protéger vos données même si une appliance est supprimée du centre de données. Une fois les volumes de l'appliance chiffrés, vous ne pouvez accéder à aucune donnée sur l'appliance, sauf si le nœud peut communiquer avec le KMS.

StorageGRID ne crée ni ne gère les clés externes utilisées pour chiffrer et déchiffrer les nœuds de l'appliance. Si vous prévoyez d'utiliser un serveur de gestion de clés externe pour protéger les données StorageGRID , vous devez comprendre comment configurer ce serveur et comment gérer les clés de chiffrement. L'exécution des tâches de gestion des clés dépasse le cadre de ces instructions. Si vous avez besoin d'aide, consultez la documentation de votre serveur de gestion de clés ou contactez le support technique.

Configuration KMS et appliance

Avant de pouvoir utiliser un serveur de gestion de clés (KMS) pour sécuriser les données StorageGRID sur les nœuds de l'appliance, vous devez effectuer deux tâches de configuration : configurer un ou plusieurs serveurs KMS et activer le chiffrement des nœuds pour les nœuds de l'appliance. Une fois ces deux tâches de configuration terminées, le processus de gestion des clés se déroule automatiquement.

L'organigramme montre les étapes de haut niveau pour utiliser un KMS pour sécuriser les données StorageGRID sur les nœuds de l'appliance.

L'organigramme montre la configuration de KMS et la configuration de l'appliance se déroulant en parallèle ; cependant, vous pouvez configurer les serveurs de gestion de clés avant ou après avoir activé le chiffrement des nœuds pour les nouveaux nœuds de l'appliance, en fonction de vos besoins.

Configurer le serveur de gestion des clés (KMS)

La configuration d'un serveur de gestion de clés comprend les étapes de haut niveau suivantes.

Étape	Se référer à
Accédez au logiciel KMS et ajoutez un client pour StorageGRID à chaque KMS ou cluster KMS.	"Configurer StorageGRID en tant que client dans le KMS"
Obtenez les informations requises pour le client StorageGRID sur le KMS.	"Configurer StorageGRID en tant que client dans le KMS"
Ajoutez le KMS au Grid Manager, attribuez-le à un site unique ou à un groupe de sites par défaut, téléchargez les certificats requis et enregistrez la configuration KMS.	"Ajouter un serveur de gestion de clés (KMS)"

Installer l'appareil

La configuration d'un nœud d'appareil pour l'utilisation de KMS comprend les étapes de haut niveau suivantes.

1. Au cours de l'étape de configuration matérielle de l'installation de l'appliance, utilisez le programme d'installation de l'appliance StorageGRID pour activer le paramètre **Chiffrement de nœud** pour l'appliance.

Vous ne pouvez pas activer le paramètre **Chiffrement de nœud** après l'ajout d'un appareil à la grille, et vous ne pouvez pas utiliser la gestion des clés externes pour les appareils sur lesquels le chiffrement de nœud n'est pas activé.

2. Exécutez le programme d'installation de l'appliance StorageGRID . Lors de l'installation, une clé de chiffrement de données aléatoire (DEK) est attribuée à chaque volume d'appareil, comme suit :
   - Les DEK sont utilisés pour crypter les données sur chaque volume. Ces clés sont générées à l'aide du chiffrement de disque Linux Unified Key Setup (LUKS) dans le système d'exploitation de l'appliance et ne peuvent pas être modifiées.
   - Chaque DEK individuel est chiffré par une clé de chiffrement à clé principale (KEK). La KEK initiale est une clé temporaire qui crypte les DEK jusqu'à ce que l'appareil puisse se connecter au KMS.
3. Ajoutez le nœud de l'appliance à StorageGRID.

Voir "Activer le cryptage des nœuds" pour plus de détails.

Processus de cryptage de gestion des clés (se produit automatiquement)

Le chiffrement de gestion des clés comprend les étapes de haut niveau suivantes qui sont exécutées automatiquement.

1. Lorsque vous installez un dispositif sur lequel le chiffrement de nœud est activé dans la grille, StorageGRID détermine si une configuration KMS existe pour le site qui contient le nouveau nœud.
   - Si un KMS a déjà été configuré pour le site, l'appliance reçoit la configuration KMS.
   - Si un KMS n'a pas encore été configuré pour le site, les données sur l'appliance continuent d'être chiffrées par le KEK temporaire jusqu'à ce que vous configuriez un KMS pour le site et que l'appliance reçoive la configuration KMS.
2. L'appareil utilise la configuration KMS pour se connecter au KMS et demander une clé de chiffrement.
3. Le KMS envoie une clé de chiffrement à l'appareil. La nouvelle clé du KMS remplace la KEK temporaire et est désormais utilisée pour chiffrer et déchiffrer les DEK pour les volumes de l'appliance.

> ⚠ Toutes les données qui existent avant que le nœud de l'appareil chiffré ne se connecte au KMS configuré sont chiffrées avec une clé temporaire. Toutefois, les volumes de l'appareil ne doivent pas être considérés comme protégés contre le retrait du centre de données tant que la clé temporaire n'est pas remplacée par la clé de chiffrement KMS.

4. Si l'appareil est sous tension ou redémarré, il se reconnecte au KMS pour demander la clé. La clé, qui est enregistrée dans la mémoire volatile, ne peut pas survivre à une panne de courant ou à un redémarrage.

Considérations et exigences relatives à l'utilisation d'un serveur de gestion de clés

Avant de configurer un serveur de gestion de clés externe (KMS), vous devez comprendre les considérations et les exigences.

Quelle version de KMIP est prise en charge ?

StorageGRID prend en charge la version 1.4 de KMIP.

"Spécification du protocole d'interopérabilité de gestion des clés version 1.4"

Quelles sont les considérations relatives au réseau ?

Les paramètres du pare-feu réseau doivent permettre à chaque nœud d'appareil de communiquer via le port utilisé pour les communications du protocole KMIP (Key Management Interoperability Protocol). Le port KMIP par défaut est 5696.

Vous devez vous assurer que chaque nœud d'appliance qui utilise le chiffrement de nœud dispose d'un accès réseau au KMS ou au cluster KMS que vous avez configuré pour le site.

Quelles versions de TLS sont prises en charge ?

Les communications entre les nœuds de l'appliance et le KMS configuré utilisent des connexions TLS sécurisées. StorageGRID peut prendre en charge le protocole TLS 1.2 ou TLS 1.3 lorsqu'il établit des connexions KMIP à un cluster KMS ou KMS, en fonction de ce que le KMS prend en charge et de ce qu'il prend en charge."Politique TLS et SSH" vous utilisez.

StorageGRID négocie le protocole et le chiffrement (TLS 1.2) ou la suite de chiffrement (TLS 1.3) avec le KMS lorsqu'il établit la connexion. Pour voir quelles versions de protocole et quels chiffrements/suites de chiffrement sont disponibles, consultez le `tlsOutbound` section de la politique TLS et SSH active de la grille (**CONFIGURATION** > **Sécurité Paramètres de sécurité**).

Quels appareils sont pris en charge ?

Vous pouvez utiliser un serveur de gestion de clés (KMS) pour gérer les clés de chiffrement de tout dispositif StorageGRID de votre grille sur lequel le paramètre **Chiffrement de nœud** est activé. Ce paramètre ne peut être activé que pendant l'étape de configuration matérielle de l'installation de l'appliance à l'aide du programme d'installation de l'appliance StorageGRID .

> Vous ne pouvez pas activer le chiffrement des nœuds après l'ajout d'un appareil à la grille, et vous ne pouvez pas utiliser la gestion des clés externes pour les appareils sur lesquels le chiffrement des nœuds n'est pas activé.

Vous pouvez utiliser le KMS configuré pour les appliances StorageGRID et les nœuds d'appliance.

Vous ne pouvez pas utiliser le KMS configuré pour les nœuds basés sur des logiciels (non-appliances), y compris les suivants :

- Nœuds déployés en tant que machines virtuelles (VM)
- Nœuds déployés dans des moteurs de conteneurs sur des hôtes Linux

Les nœuds déployés sur ces autres plates-formes peuvent utiliser le chiffrement en dehors de StorageGRID au niveau de la banque de données ou du disque.

Quand dois-je configurer les serveurs de gestion de clés ?

Pour une nouvelle installation, vous devez généralement configurer un ou plusieurs serveurs de gestion de clés dans Grid Manager avant de créer des locataires. Cet ordre garantit que les nœuds sont protégés avant que des données d'objet ne soient stockées sur eux.

Vous pouvez configurer les serveurs de gestion de clés dans Grid Manager avant ou après l'installation des nœuds de l'appliance.

De combien de serveurs de gestion de clés ai-je besoin ?

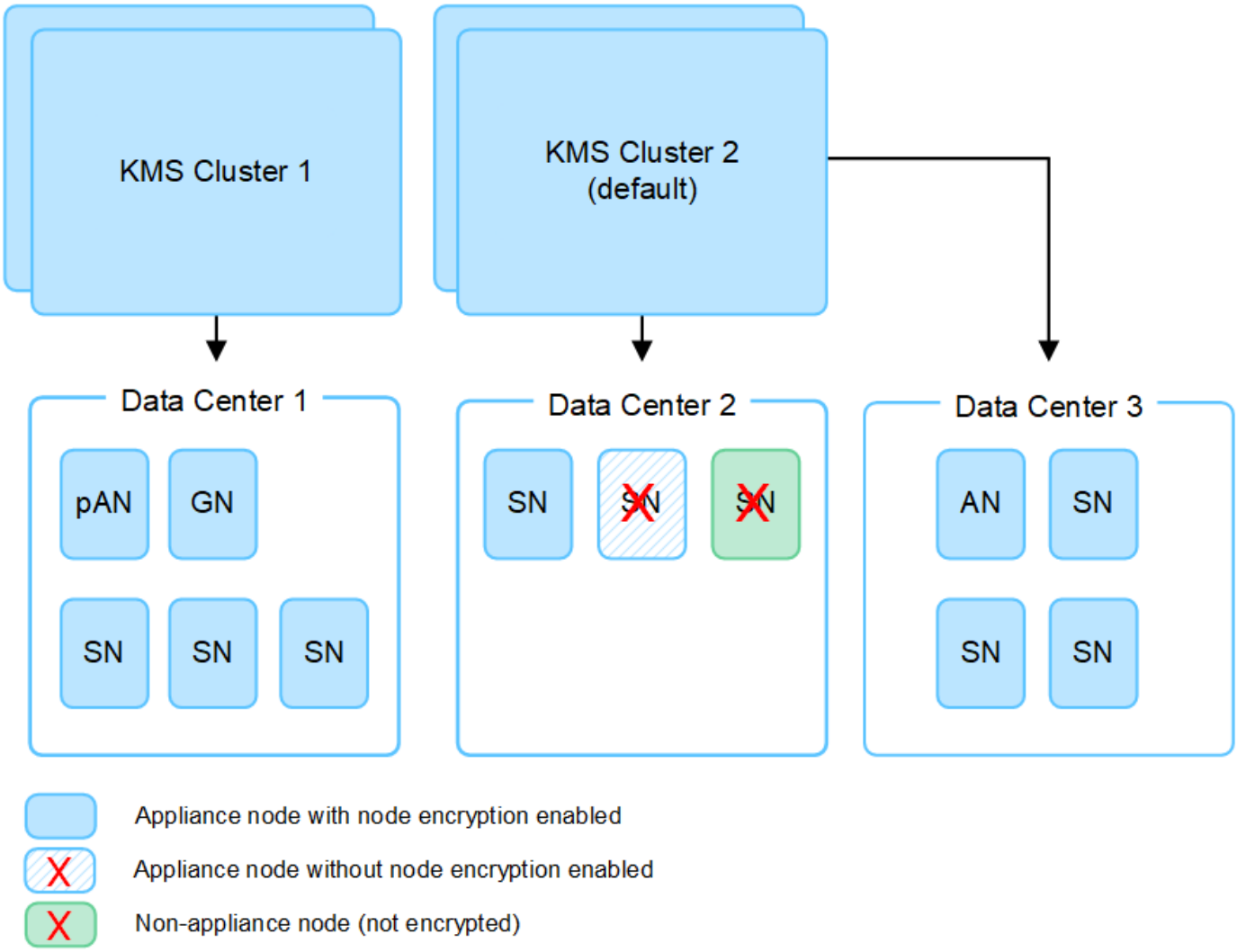
Vous pouvez configurer un ou plusieurs serveurs de gestion de clés externes pour fournir des clés de chiffrement aux nœuds d'appliance de votre système StorageGRID . Chaque KMS fournit une clé de chiffrement unique aux nœuds de l'appliance StorageGRID sur un site unique ou sur un groupe de sites.

StorageGRID prend en charge l'utilisation de clusters KMS. Chaque cluster KMS contient plusieurs serveurs de gestion de clés répliqués qui partagent les paramètres de configuration et les clés de chiffrement.

L'utilisation de clusters KMS pour la gestion des clés est recommandée car elle améliore les capacités de basculement d'une configuration haute disponibilité.

Par exemple, supposons que votre système StorageGRID dispose de trois sites de centre de données. Vous pouvez configurer un cluster KMS pour fournir une clé à tous les nœuds d'appliance du centre de données 1 et un deuxième cluster KMS pour fournir une clé à tous les nœuds d'appliance de tous les autres sites. Lorsque vous ajoutez le deuxième cluster KMS, vous pouvez configurer un KMS par défaut pour Data Center 2 et Data Center 3.

Notez que vous ne pouvez pas utiliser un KMS pour les nœuds non-appliance ou pour les nœuds d'appliance dont le paramètre **Chiffrement de nœud** n'a pas été activé lors de l'installation.



Que se passe-t-il lorsqu'une clé est tournée ?

En tant que bonne pratique de sécurité, vous devez périodiquement"faire pivoter la clé de cryptage" utilisé par chaque KMS configuré.

Lorsque la nouvelle version de clé sera disponible :

- Il est automatiquement distribué aux nœuds d'appareils chiffrés sur le ou les sites associés au KMS. La distribution devrait avoir lieu dans l'heure qui suit la rotation de la clé.
- Si le nœud de l'appareil chiffré est hors ligne lorsque la nouvelle version de clé est distribuée, le nœud

recevra la nouvelle clé dès son redémarrage.

- Si la nouvelle version de clé ne peut pas être utilisée pour chiffrer les volumes de l'appliance pour une raison quelconque, l'alerte **Échec de la rotation de la clé de chiffrement KMS** est déclenchée pour le nœud de l'appliance. Vous devrez peut-être contacter le support technique pour obtenir de l'aide pour résoudre cette alerte.

Puis-je réutiliser un nœud d'appareil après l'avoir chiffré ?

Si vous devez installer un dispositif chiffré dans un autre système StorageGRID , vous devez d'abord mettre hors service le nœud de grille pour déplacer les données d'objet vers un autre nœud. Ensuite, vous pouvez utiliser le programme d'installation de l'appliance StorageGRID pour "effacer la configuration KMS" . La suppression de la configuration KMS désactive le paramètre **Chiffrement de nœud** et supprime l'association entre le nœud de l'appliance et la configuration KMS pour le site StorageGRID .

> Sans accès à la clé de cryptage KMS, toutes les données restantes sur l'appareil ne sont plus accessibles et sont verrouillées de manière permanente.

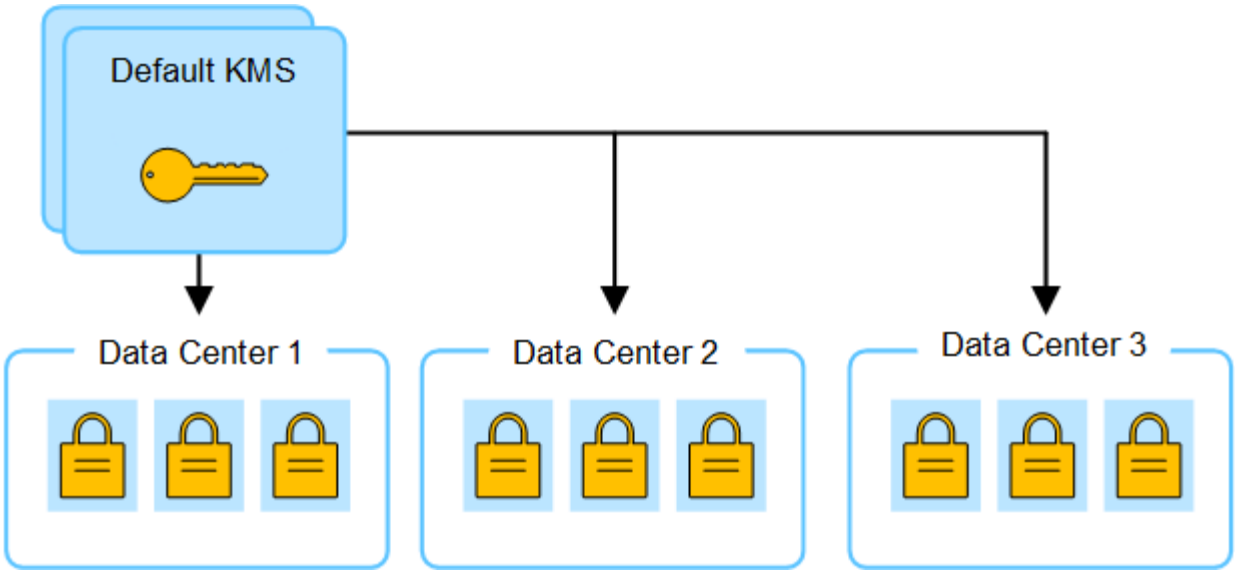
Considérations relatives à la modification du KMS d'un site

Chaque serveur de gestion de clés (KMS) ou cluster KMS fournit une clé de chiffrement à tous les nœuds d'appliance sur un site unique ou sur un groupe de sites. Si vous devez modifier le KMS utilisé pour un site, vous devrez peut-être copier la clé de chiffrement d'un KMS à un autre.

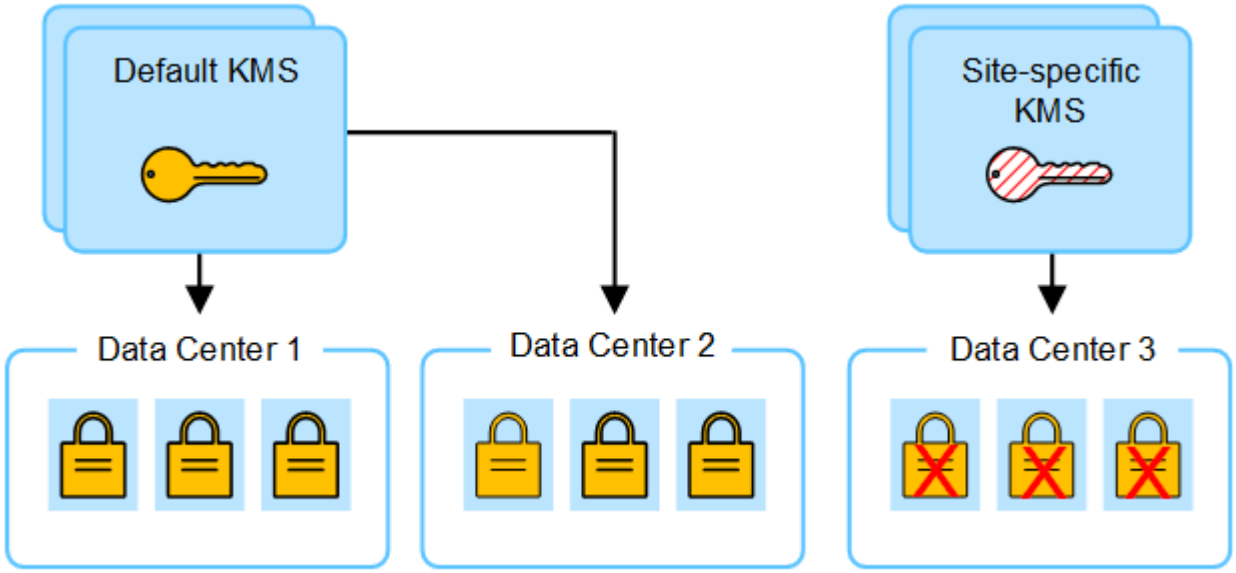
Si vous modifiez le KMS utilisé pour un site, vous devez vous assurer que les nœuds d'appliance précédemment chiffrés sur ce site peuvent être déchiffrés à l'aide de la clé stockée sur le nouveau KMS. Dans certains cas, vous devrez peut-être copier la version actuelle de la clé de chiffrement du KMS d'origine vers le nouveau KMS. Vous devez vous assurer que le KMS dispose de la clé correcte pour déchiffrer les nœuds d'appliance chiffrés sur le site.

Par exemple:

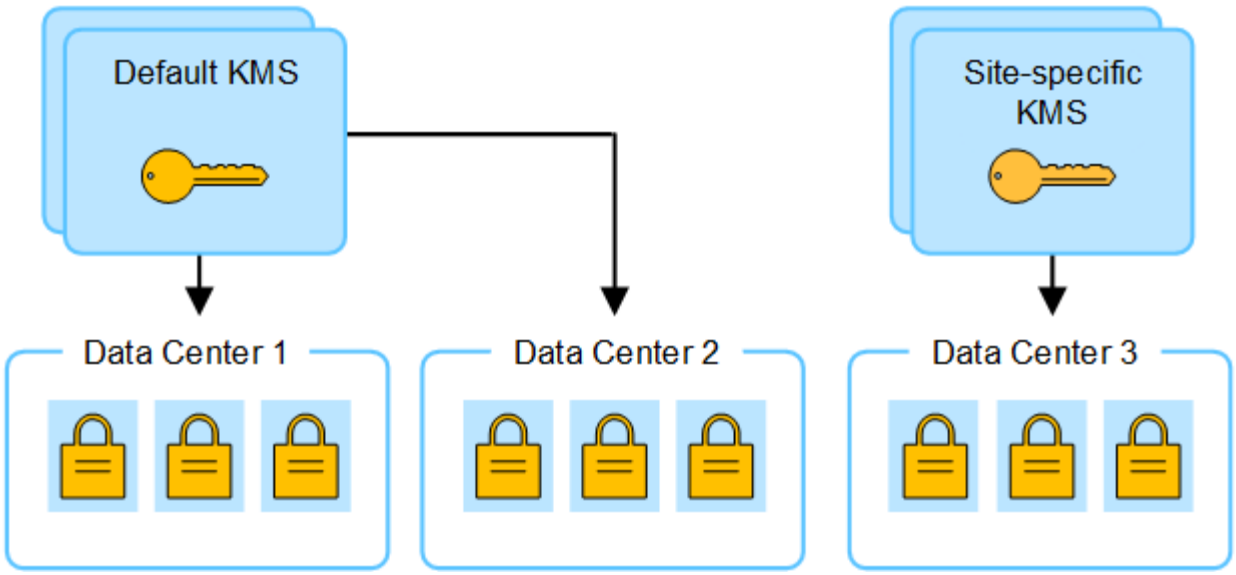
1. Vous configurez initialement un KMS par défaut qui s'applique à tous les sites qui ne disposent pas d'un KMS dédié.
2. Une fois le KMS enregistré, tous les nœuds d'appliance dont le paramètre **Chiffrement de nœud** est activé se connectent au KMS et demandent la clé de chiffrement. Cette clé est utilisée pour crypter les nœuds de l'appliance sur tous les sites. Cette même clé doit également être utilisée pour décrypter ces appareils.



3. Vous décidez d'ajouter un KMS spécifique au site pour un site (Data Center 3 sur la figure). Cependant, étant donné que les nœuds de l'appliance sont déjà chiffrés, une erreur de validation se produit lorsque vous tentez d'enregistrer la configuration du KMS spécifique au site. L'erreur se produit car le KMS spécifique au site ne dispose pas de la clé correcte pour déchiffrer les nœuds de ce site.



4. Pour résoudre le problème, copiez la version actuelle de la clé de chiffrement du KMS par défaut vers le nouveau KMS. (Techniquement, vous copiez la clé d'origine sur une nouvelle clé avec le même alias. La clé d'origine devient une version antérieure de la nouvelle clé.) Le KMS spécifique au site dispose désormais de la clé correcte pour déchiffrer les nœuds de l'appliance dans le centre de données 3, afin qu'il puisse être enregistré dans StorageGRID.



Cas d'utilisation pour modifier le KMS utilisé pour un site

Le tableau résume les étapes requises pour les cas les plus courants de modification du KMS d'un site.

Cas d'utilisation pour modifier le KMS d'un site	Étapes requises
Vous disposez d'une ou plusieurs entrées KMS spécifiques au site et vous souhaitez utiliser l'une d'entre elles comme KMS par défaut.	Modifier le KMS spécifique au site. Dans le champ **Gère les clés pour**, sélectionnez **Sites non gérés par un autre KMS (KMS par défaut)**. Le KMS spécifique au site sera désormais utilisé comme KMS par défaut. Cela s'appliquera à tous les sites qui ne disposent pas d'un KMS dédié. "Modifier un serveur de gestion de clés (KMS)"
Vous disposez d'un KMS par défaut et vous ajoutez un nouveau site dans une extension. Vous ne souhaitez pas utiliser le KMS par défaut pour le nouveau site.	1. Si les nœuds de l'appliance sur le nouveau site ont déjà été chiffrés par le KMS par défaut, utilisez le logiciel KMS pour copier la version actuelle de la clé de chiffrement du KMS par défaut vers un nouveau KMS. 2. À l'aide du gestionnaire de grille, ajoutez le nouveau KMS et sélectionnez le site. "Ajouter un serveur de gestion de clés (KMS)"
Vous souhaitez que le KMS d'un site utilise un serveur différent.	1. Si les nœuds d'appareils du site ont déjà été chiffrés par le KMS existant, utilisez le logiciel KMS pour copier la version actuelle de la clé de chiffrement du KMS existant vers le nouveau KMS. 2. À l'aide du gestionnaire de grille, modifiez la configuration KMS existante et entrez le nouveau nom d'hôte ou la nouvelle adresse IP. "Ajouter un serveur de gestion de clés (KMS)"

Configurer StorageGRID en tant que client dans le KMS

Vous devez configurer StorageGRID en tant que client pour chaque serveur de gestion

de clés externe ou cluster KMS avant de pouvoir ajouter le KMS à StorageGRID.

> Ces instructions s'appliquent à Thales CipherTrust Manager et Hashicorp Vault. Pour obtenir la liste des produits et versions pris en charge, utilisez le "Outil de matrice d'interopérabilité NetApp (IMT)" .

Étapes

1. À partir du logiciel KMS, créez un client StorageGRID pour chaque KMS ou cluster KMS que vous prévoyez d'utiliser.

   Chaque KMS gère une clé de chiffrement unique pour les nœuds d'appliances StorageGRID sur un seul site ou sur un groupe de sites.

2. Créez une clé en utilisant l'une des deux méthodes suivantes :
   - Utilisez la page de gestion des clés de votre produit KMS. Créez une clé de chiffrement AES pour chaque KMS ou cluster KMS.

     La clé de chiffrement doit être de 2 048 bits ou plus et doit être exportable.

   - Demandez à StorageGRID de créer la clé. Vous serez invité à tester et à enregistrer après"téléchargement de certificats clients" .
3. Enregistrez les informations suivantes pour chaque KMS ou cluster KMS.

   Vous avez besoin de ces informations lorsque vous ajoutez le KMS à StorageGRID:

   - Nom d'hôte ou adresse IP pour chaque serveur.
   - Port KMIP utilisé par le KMS.
   - Alias de clé pour la clé de chiffrement dans le KMS.
4. Pour chaque KMS ou cluster KMS, obtenez un certificat de serveur signé par une autorité de certification (CA) ou un ensemble de certificats contenant chacun des fichiers de certificat CA codés PEM, concaténés dans l'ordre de la chaîne de certificats.

   Le certificat du serveur permet au KMS externe de s'authentifier auprès de StorageGRID.

   - Le certificat doit utiliser le format X.509 codé en base 64 (Privacy Enhanced Mail) PEM.
   - Le champ Nom alternatif du sujet (SAN) de chaque certificat de serveur doit inclure le nom de domaine complet (FQDN) ou l'adresse IP auquel StorageGRID se connectera.

     > Lorsque vous configurez le KMS dans StorageGRID, vous devez saisir les mêmes noms de domaine complets ou adresses IP dans le champ **Nom d'hôte**.

   - Le certificat du serveur doit correspondre au certificat utilisé par l'interface KMIP du KMS, qui utilise généralement le port 5696.
5. Obtenez le certificat client public émis à StorageGRID par le KMS externe et la clé privée du certificat client.

   Le certificat client permet à StorageGRID de s'authentifier auprès du KMS.

Ajouter un serveur de gestion de clés (KMS)

Vous utilisez l'assistant du serveur de gestion de clés StorageGRID pour ajouter chaque KMS ou cluster KMS.

Avant de commencer

- Vous avez examiné le"considérations et exigences relatives à l'utilisation d'un serveur de gestion de clés" .
- Tu as"configuré StorageGRID en tant que client dans le KMS" , et vous disposez des informations requises pour chaque KMS ou cluster KMS.
- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès root" .

À propos de cette tâche

Si possible, configurez tous les serveurs de gestion de clés spécifiques au site avant de configurer un KMS par défaut qui s'applique à tous les sites non gérés par un autre KMS. Si vous créez d'abord le KMS par défaut, tous les appareils chiffrés par nœud dans la grille seront chiffrés par le KMS par défaut. Si vous souhaitez créer ultérieurement un KMS spécifique au site, vous devez d'abord copier la version actuelle de la clé de chiffrement du KMS par défaut vers le nouveau KMS. Voir"Considérations relatives à la modification du KMS d'un site" pour plus de détails.

Étape 1 : Détails KMS

À l'étape 1 (Détails KMS) de l'assistant Ajouter un serveur de gestion de clés, vous fournissez des détails sur le KMS ou le cluster KMS.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Serveur de gestion des clés**.

   La page du serveur de gestion des clés s'affiche avec l'onglet Détails de configuration sélectionné.

2. Sélectionnez **Créer**.

   L'étape 1 (détails KMS) de l'assistant Ajouter un serveur de gestion de clés s'affiche.

3. Saisissez les informations suivantes pour le KMS et le client StorageGRID que vous avez configuré dans ce KMS.

Champ	Description
Nom du KMS	Un nom descriptif pour vous aider à identifier ce KMS. Doit comporter entre 1 et 64 caractères.
Nom de la clé	L'alias de clé exact pour le client StorageGRID dans le KMS. Doit comporter entre 1 et 255 caractères. **Remarque** : si vous n'avez pas créé de clé à l'aide de votre produit KMS, vous serez invité à demander à StorageGRID de créer la clé.

Champ	Description
Gère les clés pour	Le site StorageGRID qui sera associé à ce KMS. Si possible, vous devez configurer tous les serveurs de gestion de clés spécifiques au site avant de configurer un KMS par défaut qui s'applique à tous les sites non gérés par un autre KMS. • Sélectionnez un site si ce KMS doit gérer les clés de chiffrement pour les nœuds d'appliance sur un site spécifique. • Sélectionnez **Sites non gérés par un autre KMS (KMS par défaut)** pour configurer un KMS par défaut qui s'appliquera à tous les sites qui ne disposent pas d'un KMS dédié et à tous les sites que vous ajouterez dans les extensions ultérieures. **Remarque :** une erreur de validation se produit lorsque vous enregistrez la configuration KMS si vous sélectionnez un site qui était précédemment chiffré par le KMS par défaut mais que vous n'avez pas fourni la version actuelle de la clé de chiffrement d'origine au nouveau KMS.
Port	Le port utilisé par le serveur KMS pour les communications du protocole d'interopérabilité de gestion de clés (KMIP). La valeur par défaut est 5696, qui est le port standard KMIP.
Nom d'hôte	Le nom de domaine complet ou l'adresse IP du KMS. **Remarque :** le champ Nom alternatif du sujet (SAN) du certificat du serveur doit inclure le nom de domaine complet ou l'adresse IP que vous saisissez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ou à tous les serveurs d'un cluster KMS.

4. Si vous configurez un cluster KMS, sélectionnez **Ajouter un autre nom d'hôte** pour ajouter un nom d'hôte pour chaque serveur du cluster.
5. Sélectionnez **Continuer**.

Étape 2 : Télécharger le certificat du serveur

À l'étape 2 (Télécharger le certificat du serveur) de l'assistant Ajouter un serveur de gestion de clés, vous téléchargez le certificat du serveur (ou le groupe de certificats) pour le KMS. Le certificat du serveur permet au KMS externe de s'authentifier auprès de StorageGRID.

Étapes

1. À partir de l'**Étape 2 (Télécharger le certificat du serveur)**, accédez à l'emplacement du certificat de serveur ou du groupe de certificats enregistré.
2. Téléchargez le fichier de certificat.

   Les métadonnées du certificat du serveur apparaissent.

   Si vous avez téléchargé un ensemble de certificats, les métadonnées de chaque certificat apparaissent sur son propre onglet.

3. Sélectionnez **Continuer**.

Étape 3 : Télécharger les certificats clients

À l'étape 3 (Télécharger les certificats clients) de l'assistant Ajouter un serveur de gestion de clés, vous téléchargez le certificat client et la clé privée du certificat client. Le certificat client permet à StorageGRID de s'authentifier auprès du KMS.

Étapes

1. À partir de l'**Étape 3 (Télécharger les certificats clients)**, accédez à l'emplacement du certificat client.
2. Téléchargez le fichier de certificat client.

   Les métadonnées du certificat client apparaissent.
3. Accédez à l'emplacement de la clé privée du certificat client.
4. Téléchargez le fichier de clé privée.
5. Sélectionnez **Tester et enregistrer**.

   Si une clé n'existe pas, vous êtes invité à demander à StorageGRID d'en créer une.

   Les connexions entre le serveur de gestion des clés et les nœuds de l'appliance sont testées. Si toutes les connexions sont valides et que la clé correcte est trouvée sur le KMS, le nouveau serveur de gestion de clés est ajouté au tableau sur la page Serveur de gestion de clés.

   > Immédiatement après avoir ajouté un KMS, l'état du certificat sur la page Serveur de gestion des clés apparaît comme Inconnu. Il faudra peut-être jusqu'à 30 minutes à StorageGRID pour obtenir le statut réel de chaque certificat. Vous devez actualiser votre navigateur Web pour voir l'état actuel.
6. Si un message d'erreur s'affiche lorsque vous sélectionnez **Tester et enregistrer**, vérifiez les détails du message, puis sélectionnez **OK**.

   Par exemple, vous pouvez recevoir une erreur 422 : Entité non traitable si un test de connexion a échoué.
7. Si vous devez enregistrer la configuration actuelle sans tester la connexion externe, sélectionnez **Forcer l'enregistrement**.

   > La sélection de **Forcer l'enregistrement** enregistre la configuration KMS, mais ne teste pas la connexion externe de chaque appareil à ce KMS. En cas de problème avec la configuration, vous ne pourrez peut-être pas redémarrer les nœuds de l'appliance dont le chiffrement de nœud est activé sur le site concerné. Vous risquez de perdre l'accès à vos données jusqu'à ce que les problèmes soient résolus.
8. Vérifiez l'avertissement de confirmation et sélectionnez **OK** si vous êtes sûr de vouloir forcer l'enregistrement de la configuration.

   La configuration KMS est enregistrée mais la connexion au KMS n'est pas testée.

Gérer un KMS

La gestion d'un serveur de gestion de clés (KMS) implique l'affichage ou la modification

des détails, la gestion des certificats, l'affichage des nœuds chiffrés et la suppression d'un KMS lorsqu'il n'est plus nécessaire.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"autorisation d'accès requise" .

Afficher les détails du KMS

Vous pouvez afficher des informations sur chaque serveur de gestion de clés (KMS) dans votre système StorageGRID , y compris les détails des clés et l'état actuel des certificats serveur et client.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Serveur de gestion des clés**.

   La page du serveur de gestion des clés apparaît et affiche les informations suivantes :

   - L'onglet Détails de configuration répertorie tous les serveurs de gestion de clés configurés.
   - L'onglet Nœuds chiffrés répertorie tous les nœuds pour lesquels le chiffrement de nœud est activé.

2. Pour afficher les détails d'un KMS spécifique et effectuer des opérations sur ce KMS, sélectionnez le nom du KMS. La page de détails du KMS répertorie les informations suivantes :

Champ	Description
Gère les clés pour	Le site StorageGRID associé au KMS. Ce champ affiche le nom d'un site StorageGRID spécifique ou **Sites non gérés par un autre KMS (KMS par défaut).**
Nom d'hôte	Le nom de domaine complet ou l'adresse IP du KMS. S'il existe un cluster de deux serveurs de gestion de clés, le nom de domaine complet ou l'adresse IP des deux serveurs sont répertoriés. S'il existe plus de deux serveurs de gestion de clés dans un cluster, le nom de domaine complet ou l'adresse IP du premier KMS est répertorié avec le nombre de serveurs de gestion de clés supplémentaires dans le cluster. Par exemple: `10.10.10.10 and 10.10.10.11` ou `10.10.10.10 and 2 others` . Pour afficher tous les noms d'hôtes d'un cluster, sélectionnez un KMS et sélectionnez **Modifier** ou **Actions** > **Modifier**.

3. Sélectionnez un onglet sur la page des détails du KMS pour afficher les informations suivantes :

Languette	Champ	Description
Détails clés	Nom de la clé	L'alias de clé pour le client StorageGRID dans le KMS.

Languette	Champ	Description
Clé UID	L'identifiant unique de la dernière version de la clé.	Dernière modification
La date et l'heure de la dernière version de la clé.	Certificat de serveur	Métadonnées
Les métadonnées du certificat, telles que le numéro de série, la date et l'heure d'expiration et le PEM du certificat.	Certificat PEM	Le contenu du fichier PEM (privacy enhanced mail) pour le certificat.
Certificat client	Métadonnées	Les métadonnées du certificat, telles que le numéro de série, la date et l'heure d'expiration et le PEM du certificat.

4. Aussi souvent que l'exigent les pratiques de sécurité de votre organisation, sélectionnez **Rotate key** ou utilisez le logiciel KMS pour créer une nouvelle version de la clé.

   Lorsque la rotation des clés est réussie, les champs UID de la clé et Dernière modification sont mis à jour.

> Si vous faites pivoter la clé de chiffrement à l'aide du logiciel KMS, faites-la pivoter de la dernière version utilisée de la clé vers une nouvelle version de la même clé. Ne tournez pas vers une clé entièrement différente.
>
> N'essayez jamais de faire pivoter une clé en modifiant le nom de la clé (alias) pour le KMS. StorageGRID exige que toutes les versions de clés précédemment utilisées (ainsi que toutes les futures) soient accessibles depuis le KMS avec le même alias de clé. Si vous modifiez l'alias de clé d'un KMS configuré, StorageGRID risque de ne pas être en mesure de déchiffrer vos données.

Gérer les certificats

Résolvez rapidement tout problème de certificat de serveur ou de client. Si possible, remplacez les certificats avant leur expiration.

> Vous devez résoudre tout problème de certificat dès que possible pour maintenir l'accès aux données.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Serveur de gestion des clés**.
2. Dans le tableau, regardez la valeur d'expiration du certificat pour chaque KMS.
3. Si l'expiration du certificat pour un KMS est inconnue, attendez jusqu'à 30 minutes, puis actualisez votre navigateur Web.

4. Si la colonne Expiration du certificat indique qu'un certificat a expiré ou est sur le point d'expirer, sélectionnez le KMS pour accéder à la page des détails du KMS.
   a. Sélectionnez **Certificat de serveur** et vérifiez la valeur du champ « Expire le ».
   b. Pour remplacer le certificat, sélectionnez **Modifier le certificat** pour télécharger un nouveau certificat.
   c. Répétez ces sous-étapes et sélectionnez **Certificat client** au lieu de Certificat serveur.
5. Lorsque les alertes **Expiration du certificat KMS CA**, **Expiration du certificat client KMS** et **Expiration du certificat serveur KMS** sont déclenchées, notez la description de chaque alerte et effectuez les actions recommandées.

   Il faudra peut-être jusqu'à 30 minutes à StorageGRID pour obtenir les mises à jour concernant l'expiration du certificat. Actualisez votre navigateur Web pour voir les valeurs actuelles.

> Si vous obtenez le statut **L'état du certificat du serveur est inconnu**, assurez-vous que votre KMS permet d'obtenir un certificat de serveur sans nécessiter de certificat client.

Afficher les nœuds chiffrés

Vous pouvez afficher des informations sur les nœuds d'appliance de votre système StorageGRID sur lesquels le paramètre **Chiffrement de nœud** est activé.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Serveur de gestion des clés**.

   La page Serveur de gestion des clés s'affiche. L'onglet Détails de configuration affiche tous les serveurs de gestion de clés qui ont été configurés.

2. En haut de la page, sélectionnez l'onglet **Nœuds chiffrés**.

   L'onglet Nœuds chiffrés répertorie les nœuds d'appliance de votre système StorageGRID pour lesquels le paramètre **Chiffrement de nœud** est activé.

3. Consultez les informations du tableau pour chaque nœud d'appareil.

Colonne	Description
Nom du nœud	Le nom du nœud de l'appareil.
Type de nœud	Le type de nœud : Stockage, Admin ou Passerelle.
Site	Le nom du site StorageGRID sur lequel le nœud est installé.
Nom du KMS	Le nom descriptif du KMS utilisé pour le nœud. Si aucun KMS n'est répertorié, sélectionnez l'onglet Détails de configuration pour ajouter un KMS. "Ajouter un serveur de gestion de clés (KMS)"

Colonne	Description
Clé UID	L'ID unique de la clé de chiffrement utilisée pour chiffrer et déchiffrer les données sur le nœud de l'appliance. Pour afficher l'UID d'une clé entière, sélectionnez le texte. Un tiret (--) indique que l'UID de la clé est inconnu, probablement en raison d'un problème de connexion entre le nœud de l'appliance et le KMS.
Statut	L'état de la connexion entre le KMS et le nœud de l'appliance. Si le nœud est connecté, l'horodatage est mis à jour toutes les 30 minutes. La mise à jour de l'état de la connexion après les modifications de la configuration KMS peut prendre plusieurs minutes. **Remarque :** actualisez votre navigateur Web pour voir les nouvelles valeurs.

4. Si la colonne Statut indique un problème KMS, résolvez le problème immédiatement.

   Pendant les opérations KMS normales, le statut sera **Connecté à KMS**. Si un nœud est déconnecté du réseau, l'état de connexion du nœud est affiché (Administrativement hors service ou Inconnu).

   D'autres messages d'état correspondent aux alertes StorageGRID portant les mêmes noms :

   - Échec du chargement de la configuration KMS
   - Erreur de connectivité KMS
   - Nom de la clé de chiffrement KMS introuvable
   - Échec de la rotation de la clé de chiffrement KMS
   - La clé KMS n'a pas réussi à déchiffrer un volume d'appareil
   - KMS n'est pas configuré

   Effectuez les actions recommandées pour ces alertes.

> Vous devez résoudre tout problème immédiatement pour garantir que vos données sont entièrement protégées.

Modifier un KMS

Vous devrez peut-être modifier la configuration d'un serveur de gestion de clés, par exemple, si un certificat est sur le point d'expirer.

Avant de commencer

- Si vous envisagez de mettre à jour le site sélectionné pour un KMS, vous avez examiné les"considérations pour modifier le KMS d'un site" .
- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès root" .

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Serveur de gestion des clés**.

La page Serveur de gestion des clés apparaît et affiche tous les serveurs de gestion des clés qui ont été configurés.

2. Sélectionnez le KMS que vous souhaitez modifier, puis sélectionnez **Actions** > **Modifier**.

   Vous pouvez également modifier un KMS en sélectionnant le nom du KMS dans le tableau et en sélectionnant **Modifier** sur la page des détails du KMS.

3. Vous pouvez également mettre à jour les détails de l'**Étape 1 (Détails KMS)** de l'assistant Modifier un serveur de gestion de clés.

Champ	Description
Nom du KMS	Un nom descriptif pour vous aider à identifier ce KMS. Doit comporter entre 1 et 64 caractères.
Nom de la clé	L'alias de clé exact pour le client StorageGRID dans le KMS. Doit comporter entre 1 et 255 caractères. Vous n'avez besoin de modifier le nom de la clé que dans de rares cas. Par exemple, vous devez modifier le nom de la clé si l'alias est renommé dans le KMS ou si toutes les versions de la clé précédente ont été copiées dans l'historique des versions du nouvel alias.
Gère les clés pour	Si vous modifiez un KMS spécifique à un site et que vous ne disposez pas déjà d'un KMS par défaut, sélectionnez éventuellement **Sites non gérés par un autre KMS (KMS par défaut)**. Cette sélection convertit un KMS spécifique au site en KMS par défaut, qui s'appliquera à tous les sites qui n'ont pas de KMS dédié et à tous les sites ajoutés dans une extension. **Remarque :** si vous modifiez un KMS spécifique à un site, vous ne pouvez pas sélectionner un autre site. Si vous modifiez le KMS par défaut, vous ne pouvez pas sélectionner un site spécifique.
Port	Le port utilisé par le serveur KMS pour les communications du protocole d'interopérabilité de gestion de clés (KMIP). La valeur par défaut est 5696, qui est le port standard KMIP.
Nom d'hôte	Le nom de domaine complet ou l'adresse IP du KMS. **Remarque :** le champ Nom alternatif du sujet (SAN) du certificat du serveur doit inclure le nom de domaine complet ou l'adresse IP que vous saisissez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ou à tous les serveurs d'un cluster KMS.

4. Si vous configurez un cluster KMS, sélectionnez **Ajouter un autre nom d'hôte** pour ajouter un nom d'hôte pour chaque serveur du cluster.
5. Sélectionnez **Continuer**.

   L'étape 2 (Télécharger le certificat du serveur) de l'assistant Modifier un serveur de gestion de clés s'affiche.

6. Si vous devez remplacer le certificat du serveur, sélectionnez **Parcourir** et téléchargez le nouveau fichier.
7. Sélectionnez **Continuer**.

   L'étape 3 (Télécharger les certificats clients) de l'assistant Modifier un serveur de gestion de clés s'affiche.

8. Si vous devez remplacer le certificat client et la clé privée du certificat client, sélectionnez **Parcourir** et téléchargez les nouveaux fichiers.
9. Sélectionnez **Tester et enregistrer**.

   Les connexions entre le serveur de gestion des clés et tous les nœuds d'appareil chiffrés sur les sites concernés sont testées. Si toutes les connexions de nœuds sont valides et que la clé correcte est trouvée sur le KMS, le serveur de gestion de clés est ajouté au tableau sur la page Serveur de gestion de clés.

10. Si un message d'erreur s'affiche, vérifiez les détails du message et sélectionnez **OK**.

    Par exemple, vous pouvez recevoir une erreur 422 : Entité non traitable si le site que vous avez sélectionné pour ce KMS est déjà géré par un autre KMS ou si un test de connexion a échoué.

11. Si vous devez enregistrer la configuration actuelle avant de résoudre les erreurs de connexion, sélectionnez **Forcer l'enregistrement**.

    > La sélection de **Forcer l'enregistrement** enregistre la configuration KMS, mais ne teste pas la connexion externe de chaque appareil à ce KMS. En cas de problème avec la configuration, vous ne pourrez peut-être pas redémarrer les nœuds de l'appliance dont le chiffrement de nœud est activé sur le site concerné. Vous risquez de perdre l'accès à vos données jusqu'à ce que les problèmes soient résolus.

    La configuration KMS est enregistrée.

12. Vérifiez l'avertissement de confirmation et sélectionnez **OK** si vous êtes sûr de vouloir forcer l'enregistrement de la configuration.

    La configuration KMS est enregistrée, mais la connexion au KMS n'est pas testée.

Supprimer un serveur de gestion de clés (KMS)

Vous souhaiterez peut-être supprimer un serveur de gestion de clés dans certains cas. Par exemple, vous souhaiterez peut-être supprimer un KMS spécifique à un site si vous avez mis le site hors service.

Avant de commencer

- Vous avez examiné le"considérations et exigences relatives à l'utilisation d'un serveur de gestion de clés" .
- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès root" .

À propos de cette tâche

Vous pouvez supprimer un KMS dans ces cas :

- Vous pouvez supprimer un KMS spécifique à un site si le site a été mis hors service ou si le site n'inclut aucun nœud d'appliance avec le chiffrement de nœud activé.
- Vous pouvez supprimer le KMS par défaut si un KMS spécifique au site existe déjà pour chaque site disposant de nœuds d'appliance avec chiffrement de nœud activé.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Serveur de gestion des clés**.

   La page Serveur de gestion des clés apparaît et affiche tous les serveurs de gestion des clés qui ont été configurés.

2. Sélectionnez le KMS que vous souhaitez supprimer, puis sélectionnez **Actions** > **Supprimer**.

   Vous pouvez également supprimer un KMS en sélectionnant le nom du KMS dans le tableau et en sélectionnant **Supprimer** sur la page des détails du KMS.

3. Confirmez que ce qui suit est vrai :
   - Vous supprimez un KMS spécifique au site pour un site qui ne possède aucun nœud d'appliance avec le chiffrement de nœud activé.
   - Vous supprimez le KMS par défaut, mais un KMS spécifique au site existe déjà pour chaque site avec chiffrement de nœud.
4. Sélectionnez **Oui**.

   La configuration KMS est supprimée.

Gérer les paramètres de proxy

Configurer le proxy de stockage

Si vous utilisez des services de plateforme ou des pools de stockage cloud, vous pouvez configurer un proxy non transparent entre les nœuds de stockage et les points de terminaison S3 externes. Par exemple, vous pourriez avoir besoin d'un proxy non transparent pour permettre l'envoi de messages de services de plateforme à des points de terminaison externes, tels qu'un point de terminaison sur Internet.

> Les paramètres de proxy de stockage configurés ne s'appliquent pas aux points de terminaison des services de la plateforme Kafka.

Avant de commencer

- Tu as"autorisations d'accès spécifiques" .
- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .

À propos de cette tâche

Vous pouvez configurer les paramètres d'un seul proxy de stockage.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Paramètres proxy**.
2. Dans l'onglet **Stockage**, cochez la case **Activer le proxy de stockage**.
3. Sélectionnez le protocole pour le proxy de stockage.
4. Entrez le nom d'hôte ou l'adresse IP du serveur proxy.
5. Si vous le souhaitez, saisissez le port utilisé pour vous connecter au serveur proxy.

   Laissez ce champ vide pour utiliser le port par défaut pour le protocole : 80 pour HTTP ou 1080 pour

SOCKS5.

6. Sélectionnez **Enregistrer**.

   Une fois le proxy de stockage enregistré, de nouveaux points de terminaison pour les services de plateforme ou les pools de stockage cloud peuvent être configurés et testés.

   > Les modifications de proxy peuvent prendre jusqu'à 10 minutes pour prendre effet.

7. Vérifiez les paramètres de votre serveur proxy pour vous assurer que les messages liés au service de la plateforme provenant de StorageGRID ne seront pas bloqués.
8. Si vous devez désactiver un proxy de stockage, décochez la case et sélectionnez **Enregistrer**.

Configurer les paramètres du proxy d'administration

Si vous envoyez des packages AutoSupport via HTTP ou HTTPS, vous pouvez configurer un serveur proxy non transparent entre les nœuds d'administration et le support technique (AutoSupport).

Pour plus d'informations sur AutoSupport, voir"Configurer AutoSupport" .

Avant de commencer

- Tu as"autorisations d'accès spécifiques" .
- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .

À propos de cette tâche

Vous pouvez configurer les paramètres pour un seul proxy administrateur.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Paramètres proxy**.

   La page Paramètres du proxy s'affiche. Par défaut, Stockage est sélectionné dans le menu des onglets.

2. Sélectionnez l'onglet **Admin**.
3. Cochez la case **Activer le proxy administrateur**.
4. Entrez le nom d'hôte ou l'adresse IP du serveur proxy.
5. Entrez le port utilisé pour se connecter au serveur proxy.
6. Vous pouvez également saisir un nom d'utilisateur et un mot de passe pour le serveur proxy.

   Laissez ces champs vides si votre serveur proxy ne nécessite pas de nom d'utilisateur ou de mot de passe.

7. Sélectionnez l'une des options suivantes :

   - Si vous souhaitez sécuriser la connexion au proxy administrateur, sélectionnez **Vérifier le certificat proxy**. Téléchargez un bundle CA pour vérifier l'authenticité des certificats SSL présentés par le serveur proxy d'administration.

AutoSupport à la demande, AutoSupport de la série E via StorageGRID et la détermination du chemin de mise à jour sur la page de mise à niveau de StorageGRID ne fonctionneront pas si un certificat proxy est vérifié.

Une fois le bundle CA téléchargé, ses métadonnées s'affichent.

- Si vous ne souhaitez pas valider les certificats lors de la communication avec le serveur proxy d'administration, sélectionnez **Ne pas vérifier le certificat proxy**.

8. Sélectionnez **Enregistrer**.

   Une fois le proxy d'administration enregistré, le serveur proxy entre les nœuds d'administration et le support technique est configuré.

   Les modifications de proxy peuvent prendre jusqu'à 10 minutes pour prendre effet.

9. Si vous devez désactiver le proxy d'administration, décochez la case **Activer le proxy d'administration**, puis sélectionnez **Enregistrer**.

Contrôler les pare-feu

Contrôler l'accès au pare-feu externe

Vous pouvez ouvrir ou fermer des ports spécifiques au niveau du pare-feu externe.

Vous pouvez contrôler l'accès aux interfaces utilisateur et aux API sur les nœuds d'administration StorageGRID en ouvrant ou en fermant des ports spécifiques au niveau du pare-feu externe. Par exemple, vous souhaiterez peut-être empêcher les locataires de se connecter au Grid Manager au niveau du pare-feu, en plus d'utiliser d'autres méthodes pour contrôler l'accès au système.

Si vous souhaitez configurer le pare-feu interne StorageGRID , consultez"Configurer le pare-feu interne" .

Port	Description	Si le port est ouvert…
443	Port HTTPS par défaut pour les nœuds d'administration	Les navigateurs Web et les clients de l'API de gestion peuvent accéder au gestionnaire de grille, à l'API de gestion de grille, au gestionnaire de locataires et à l'API de gestion de locataires. **Remarque :** le port 443 est également utilisé pour certains trafics internes.
8443	Port Grid Manager restreint sur les nœuds d'administration	• Les navigateurs Web et les clients de l'API de gestion peuvent accéder au Grid Manager et à l'API de gestion de grille à l'aide de HTTPS. • Les navigateurs Web et les clients de l'API de gestion ne peuvent pas accéder au gestionnaire de locataires ni à l'API de gestion des locataires. • Les demandes de contenu interne seront rejetées.

Port	Description	Si le port est ouvert…
9443	Port du gestionnaire de locataires restreint sur les nœuds d'administration	• Les navigateurs Web et les clients de l'API de gestion peuvent accéder au gestionnaire de locataires et à l'API de gestion des locataires à l'aide de HTTPS. • Les navigateurs Web et les clients de l'API de gestion ne peuvent pas accéder au gestionnaire de grille ou à l'API de gestion de grille. • Les demandes de contenu interne seront rejetées.

L'authentification unique (SSO) n'est pas disponible sur les ports restreints Grid Manager ou Tenant Manager. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec l'authentification unique.

Informations connexes

- "Sign in au gestionnaire de grille"
- "Créer un compte locataire"
- "Communications externes"

Gérer les contrôles du pare-feu interne

StorageGRID inclut un pare-feu interne sur chaque nœud qui améliore la sécurité de votre grille en vous permettant de contrôler l'accès réseau au nœud. Utilisez le pare-feu pour empêcher l'accès au réseau sur tous les ports, à l'exception de ceux nécessaires à votre déploiement de grille spécifique. Les modifications de configuration que vous effectuez sur la page de contrôle du pare-feu sont déployées sur chaque nœud.

Utilisez les trois onglets de la page de contrôle du pare-feu pour personnaliser l'accès dont vous avez besoin pour votre grille.

- **Liste d'adresses privilégiées** : utilisez cet onglet pour autoriser l'accès sélectionné aux ports fermés. Vous pouvez ajouter des adresses IP ou des sous-réseaux en notation CIDR qui peuvent accéder aux ports fermés à l'aide de l'onglet Gérer l'accès externe.
- **Gérer l'accès externe** : utilisez cet onglet pour fermer les ports ouverts par défaut ou rouvrir les ports précédemment fermés.
- **Réseau client non approuvé** : utilisez cet onglet pour spécifier si un nœud approuve le trafic entrant provenant du réseau client.

  Les paramètres de cet onglet remplacent les paramètres de l'onglet Gérer l'accès externe.

  - Un nœud avec un réseau client non approuvé acceptera uniquement les connexions sur les ports de point de terminaison de l'équilibreur de charge configurés sur ce nœud (points de terminaison globaux, d'interface de nœud et de type de nœud).
  - Les ports de point de terminaison de l'équilibreur de charge *sont les seuls ports ouverts* sur les réseaux clients non approuvés, quels que soient les paramètres de l'onglet Gérer les réseaux externes.

- Lorsqu'ils sont approuvés, tous les ports ouverts sous l'onglet Gérer l'accès externe sont accessibles, ainsi que tous les points de terminaison d'équilibrage de charge ouverts sur le réseau client.

> Les paramètres que vous définissez sur un onglet peuvent affecter les modifications d'accès que vous effectuez sur un autre onglet. Assurez-vous de vérifier les paramètres de tous les onglets pour vous assurer que votre réseau se comporte comme vous l'attendez.

Pour configurer les contrôles du pare-feu interne, voir"Configurer les contrôles du pare-feu" .

Pour plus d'informations sur les pare-feu externes et la sécurité du réseau, consultez"Contrôler l'accès au pare-feu externe" .

Liste d'adresses privilégiées et onglets Gérer les accès externes

L'onglet Liste d'adresses privilégiées vous permet d'enregistrer une ou plusieurs adresses IP auxquelles l'accès aux ports de grille fermés est accordé. L'onglet Gérer l'accès externe vous permet de fermer l'accès externe aux ports externes sélectionnés ou à tous les ports externes ouverts (les ports externes sont des ports accessibles par défaut par les nœuds non-grille). Ces deux onglets peuvent souvent être utilisés ensemble pour personnaliser l'accès réseau exact dont vous avez besoin pour autoriser votre grille.

> Les adresses IP privilégiées n'ont pas d'accès au port de grille interne par défaut.

Exemple 1 : Utiliser un hôte de saut pour les tâches de maintenance

Supposons que vous souhaitiez utiliser un hôte de saut (un hôte renforcé en termes de sécurité) pour l'administration du réseau. Vous pouvez utiliser ces étapes générales :

1. Utilisez l'onglet Liste d'adresses privilégiées pour ajouter l'adresse IP de l'hôte de saut.
2. Utilisez l'onglet Gérer l'accès externe pour bloquer tous les ports.

> Ajoutez l'adresse IP privilégiée avant de bloquer les ports 443 et 8443. Tous les utilisateurs actuellement connectés sur un port bloqué, y compris vous, perdront l'accès à Grid Manager, sauf si leur adresse IP a été ajoutée à la liste d'adresses privilégiées.

Après avoir enregistré votre configuration, tous les ports externes du nœud d'administration de votre grille seront bloqués pour tous les hôtes, à l'exception de l'hôte de saut. Vous pouvez ensuite utiliser l'hôte de saut pour effectuer des tâches de maintenance sur votre réseau de manière plus sécurisée.

Exemple 2 : Verrouiller les ports sensibles

Supposons que vous souhaitiez verrouiller les ports sensibles et le service sur ce port (par exemple, SSH sur le port 22). Vous pouvez utiliser les étapes générales suivantes :

1. Utilisez l'onglet Liste d'adresses privilégiées pour accorder l'accès uniquement aux hôtes qui ont besoin d'accéder au service.
2. Utilisez l'onglet Gérer l'accès externe pour bloquer tous les ports.

> Ajoutez l'adresse IP privilégiée avant de bloquer l'accès à tous les ports attribués pour accéder à Grid Manager et Tenant Manager (les ports prédéfinis sont 443 et 8443). Tous les utilisateurs actuellement connectés sur un port bloqué, y compris vous, perdront l'accès à Grid Manager, sauf si leur adresse IP a été ajoutée à la liste d'adresses privilégiées.

Après avoir enregistré votre configuration, le port 22 et le service SSH seront disponibles pour les hôtes de la liste d'adresses privilégiées. Tous les autres hôtes se verront refuser l'accès au service, quelle que soit l'interface d'où provient la demande.

Exemple 3 : Désactiver l'accès aux services inutilisés

Au niveau du réseau, vous pouvez désactiver certains services que vous n'avez pas l'intention d'utiliser. Par exemple, pour bloquer le trafic client HTTP S3, vous utiliseriez le bouton bascule de l'onglet Gérer l'accès externe pour bloquer le port 18084.

Onglet Réseaux de clients non approuvés

Si vous utilisez un réseau client, vous pouvez contribuer à sécuriser StorageGRID contre les attaques hostiles en acceptant le trafic client entrant uniquement sur les points de terminaison explicitement configurés.

Par défaut, le réseau client sur chaque nœud de grille est *fiable*. Autrement dit, par défaut, StorageGRID approuve les connexions entrantes vers chaque nœud de grille sur tous les"ports externes disponibles" .

Vous pouvez réduire la menace d'attaques hostiles sur votre système StorageGRID en spécifiant que le réseau client sur chaque nœud doit être *non fiable*. Si le réseau client d'un nœud n'est pas approuvé, le nœud accepte uniquement les connexions entrantes sur les ports explicitement configurés comme points de terminaison d'équilibrage de charge. Voir"Configurer les points de terminaison de l'équilibreur de charge" et"Configurer les contrôles du pare-feu" .

Exemple 1 : le nœud de passerelle accepte uniquement les requêtes HTTPS S3

Supposons que vous souhaitiez qu'un nœud de passerelle refuse tout le trafic entrant sur le réseau client, à l'exception des requêtes HTTPS S3. Vous effectueriez ces étapes générales :

1. De la"Points de terminaison de l'équilibreur de charge" page, configurez un point de terminaison d'équilibrage de charge pour S3 via HTTPS sur le port 443.
2. Dans la page de contrôle du pare-feu, sélectionnez Non approuvé pour spécifier que le réseau client sur le nœud de passerelle n'est pas approuvé.

Une fois votre configuration enregistrée, tout le trafic entrant sur le réseau client du nœud de passerelle est supprimé, à l'exception des requêtes HTTPS S3 sur le port 443 et des requêtes d'écho ICMP (ping).

Exemple 2 : Le nœud de stockage envoie des demandes de services de la plateforme S3

Supposons que vous souhaitiez activer le trafic sortant des services de la plateforme S3 à partir d'un nœud de stockage, mais que vous souhaitiez empêcher toute connexion entrante vers ce nœud de stockage sur le réseau client. Vous effectueriez cette étape générale :

- Dans l'onglet Réseaux clients non approuvés de la page de contrôle du pare-feu, indiquez que le réseau client sur le nœud de stockage n'est pas approuvé.

Une fois votre configuration enregistrée, le nœud de stockage n'accepte plus aucun trafic entrant sur le réseau client, mais il continue d'autoriser les demandes sortantes vers les destinations des services de plate-forme configurées.

Exemple 3 : Limitation de l'accès à Grid Manager à un sous-réseau

Supposons que vous souhaitiez autoriser l'accès de Grid Manager uniquement sur un sous-réseau spécifique. Vous effectuerez les étapes suivantes :

1. Connectez le réseau client de vos nœuds d'administration au sous-réseau.
2. Utilisez l'onglet Réseau client non approuvé pour configurer le réseau client comme non approuvé.
3. Lorsque vous créez un point de terminaison d'équilibrage de charge d'interface de gestion, entrez le port et sélectionnez l'interface de gestion à laquelle le port accédera.
4. Sélectionnez **Oui** pour le réseau client non approuvé.
5. Utilisez l'onglet Gérer l'accès externe pour bloquer tous les ports externes (avec ou sans adresses IP privilégiées définies pour les hôtes en dehors de ce sous-réseau).

Une fois votre configuration enregistrée, seuls les hôtes du sous-réseau que vous avez spécifié peuvent accéder au gestionnaire de grille. Tous les autres hôtes sont bloqués.

Configurer le pare-feu interne

Vous pouvez configurer le pare-feu StorageGRID pour contrôler l'accès réseau à des ports spécifiques sur vos nœuds StorageGRID .

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .
- Vous avez examiné les informations contenues dans"Gérer les contrôles du pare-feu" et"Directives de mise en réseau" .
- Si vous souhaitez qu'un nœud d'administration ou un nœud de passerelle accepte le trafic entrant uniquement sur des points de terminaison explicitement configurés, vous avez défini les points de terminaison de l'équilibreur de charge.

> ⓘ Lors de la modification de la configuration du réseau client, les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.

À propos de cette tâche

StorageGRID inclut un pare-feu interne sur chaque nœud qui vous permet d'ouvrir ou de fermer certains des ports sur les nœuds de votre grille. Vous pouvez utiliser les onglets de contrôle du pare-feu pour ouvrir ou fermer les ports ouverts par défaut sur le réseau de grille, le réseau d'administration et le réseau client. Vous pouvez également créer une liste d'adresses IP privilégiées pouvant accéder aux ports de grille fermés. Si vous utilisez un réseau client, vous pouvez spécifier si un nœud approuve le trafic entrant provenant du réseau client et vous pouvez configurer l'accès de ports spécifiques sur le réseau client.

Limiter le nombre de ports ouverts aux adresses IP en dehors de votre réseau à ceux qui sont absolument nécessaires améliore la sécurité de votre réseau. Vous utilisez les paramètres de chacun des trois onglets de contrôle du pare-feu pour vous assurer que seuls les ports nécessaires sont ouverts.

Pour plus d'informations sur l'utilisation des contrôles de pare-feu, y compris des exemples, consultez"Gérer les contrôles du pare-feu" .

Pour plus d'informations sur les pare-feu externes et la sécurité du réseau, consultez"Contrôler l'accès au pare-feu externe" .

Contrôles du pare-feu d'accès

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Contrôle du pare-feu**.

   Les trois onglets de cette page sont décrits dans"Gérer les contrôles du pare-feu" .

2. Sélectionnez n'importe quel onglet pour configurer les contrôles du pare-feu.

   Vous pouvez utiliser ces onglets dans n'importe quel ordre. Les configurations que vous définissez sur un onglet ne limitent pas ce que vous pouvez faire sur les autres onglets ; cependant, les modifications de configuration que vous apportez sur un onglet peuvent modifier le comportement des ports configurés sur d'autres onglets.

Liste d'adresses privilégiées

Vous utilisez l'onglet Liste d'adresses privilégiées pour accorder aux hôtes l'accès aux ports fermés par défaut ou fermés par les paramètres de l'onglet Gérer l'accès externe.

Les adresses IP privilégiées et les sous-réseaux n'ont pas d'accès au réseau interne par défaut. De plus, les points de terminaison de l'équilibreur de charge et les ports supplémentaires ouverts dans l'onglet Liste d'adresses privilégiées sont accessibles même s'ils sont bloqués dans l'onglet Gérer l'accès externe.

Les paramètres de l'onglet Liste d'adresses privilégiées ne peuvent pas remplacer les paramètres de l'onglet Réseau client non approuvé.

Étapes

1. Dans l'onglet Liste d'adresses privilégiées, entrez l'adresse ou le sous-réseau IP auquel vous souhaitez accorder l'accès aux ports fermés.
2. Vous pouvez également sélectionner **Ajouter une autre adresse IP ou un autre sous-réseau en notation CIDR** pour ajouter des clients privilégiés supplémentaires.

   Ajoutez le moins d'adresses possible à la liste privilégiée.

3. Si vous le souhaitez, sélectionnez *Autoriser les adresses IP privilégiées à accéder aux ports internes de StorageGRID *. Voir "Ports internes StorageGRID" .

   Cette option supprime certaines protections pour les services internes. Laissez-le désactivé si possible.

4. Sélectionnez **Enregistrer**.

Gérer les accès externes

Lorsqu'un port est fermé dans l'onglet Gérer l'accès externe, le port n'est pas accessible par une adresse IP non-grille, sauf si vous ajoutez l'adresse IP à la liste d'adresses privilégiées. Vous ne pouvez fermer que les ports ouverts par défaut et vous ne pouvez ouvrir que les ports que vous avez fermés.

Les paramètres de l'onglet Gérer l'accès externe ne peuvent pas remplacer les paramètres de l'onglet Réseau client non approuvé. Par exemple, si un nœud n'est pas approuvé, le port SSH/22 est bloqué sur le réseau client même s'il est ouvert dans l'onglet Gérer l'accès externe. Les paramètres de l'onglet Réseau client non approuvé remplacent les ports fermés (tels que 443, 8443, 9443) sur le réseau client.

Étapes

1. Sélectionnez **Gérer l'accès externe**. L'onglet affiche un tableau avec tous les ports externes (ports accessibles par défaut par les nœuds non-grille) pour les nœuds de votre grille.
2. Configurez les ports que vous souhaitez ouvrir et fermer à l'aide des options suivantes :
   - Utilisez le bouton bascule à côté de chaque port pour ouvrir ou fermer le port sélectionné.
   - Sélectionnez **Ouvrir tous les ports affichés** pour ouvrir tous les ports répertoriés dans le tableau.
   - Sélectionnez **Fermer tous les ports affichés** pour fermer tous les ports répertoriés dans le tableau.

   Si vous fermez les ports 443 ou 8443 de Grid Manager, tous les utilisateurs actuellement connectés sur un port bloqué, y compris vous, perdront l'accès à Grid Manager, sauf si leur adresse IP a été ajoutée à la liste d'adresses privilégiées.

   Utilisez la barre de défilement sur le côté droit du tableau pour vous assurer d'avoir visualisé tous les ports disponibles. Utilisez le champ de recherche pour trouver les paramètres de n'importe quel port externe en saisissant un numéro de port. Vous pouvez saisir un numéro de port partiel. Par exemple, si vous entrez un **2**, tous les ports dont le nom contient la chaîne « 2 » sont affichés.
3. Sélectionnez **Enregistrer**

Réseau de clients non fiables

Si le réseau client d'un nœud n'est pas approuvé, le nœud accepte uniquement le trafic entrant sur les ports configurés comme points de terminaison d'équilibrage de charge et, éventuellement, les ports supplémentaires que vous sélectionnez dans cet onglet. Vous pouvez également utiliser cet onglet pour spécifier le paramètre par défaut des nouveaux nœuds ajoutés dans une extension.

Les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.

Les modifications de configuration que vous effectuez dans l'onglet **Réseau client non approuvé** remplacent les paramètres de l'onglet **Gérer l'accès externe**.

Étapes

1. Sélectionnez **Réseau client non approuvé**.
2. Dans la section Définir la valeur par défaut du nouveau nœud, spécifiez le paramètre par défaut à utiliser lorsque de nouveaux nœuds sont ajoutés à la grille dans le cadre d'une procédure d'extension.
   - **Fiable** (par défaut) : lorsqu'un nœud est ajouté dans une extension, son réseau client est approuvé.
   - **Non fiable** : lorsqu'un nœud est ajouté dans une extension, son réseau client n'est pas fiable.

     Si nécessaire, vous pouvez revenir à cet onglet pour modifier le paramètre d'un nouveau nœud spécifique.

Ce paramètre n'affecte pas les nœuds existants dans votre système StorageGRID .

3. Utilisez les options suivantes pour sélectionner les nœuds qui doivent autoriser les connexions client uniquement sur les points de terminaison d'équilibrage de charge explicitement configurés ou sur des ports sélectionnés supplémentaires :

   - Sélectionnez **Ne pas faire confiance aux nœuds affichés** pour ajouter tous les nœuds affichés dans le tableau à la liste des réseaux clients non approuvés.
   - Sélectionnez **Faire confiance aux nœuds affichés** pour supprimer tous les nœuds affichés dans le tableau de la liste Réseau client non approuvé.
   - Utilisez le bouton bascule à côté de chaque nœud pour définir le réseau client comme approuvé ou non approuvé pour le nœud sélectionné.

   Par exemple, vous pouvez sélectionner **Ne pas faire confiance aux nœuds affichés** pour ajouter tous les nœuds à la liste des réseaux clients non approuvés, puis utiliser le bouton bascule à côté d'un nœud individuel pour ajouter ce nœud unique à la liste des réseaux clients approuvés.

   Utilisez la barre de défilement sur le côté droit du tableau pour vous assurer d'avoir visualisé tous les nœuds disponibles. Utilisez le champ de recherche pour trouver les paramètres de n'importe quel nœud en saisissant le nom du nœud. Vous pouvez saisir un nom partiel. Par exemple, si vous entrez un **GW**, tous les nœuds dont le nom contient la chaîne « GW » sont affichés.

4. Sélectionnez **Enregistrer**.

   Les nouveaux paramètres du pare-feu sont immédiatement appliqués et mis en œuvre. Les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.

Gérer les locataires

Que sont les comptes locataires ?

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

Les détails Swift ont été supprimés de cette version du site de documentation. Voir "StorageGRID 11.8 : Gérer les locataires" .

En tant qu'administrateur de grille, vous créez et gérez les comptes locataires que les clients S3 utilisent pour stocker et récupérer des objets.

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

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

- **Cas d'utilisation d'entreprise :** si vous administrez un système StorageGRID dans une application d'entreprise, vous souhaiterez peut-être séparer le stockage d'objets de la grille par les différents services

de votre organisation. Dans ce cas, vous pouvez créer des comptes locataires pour le service marketing, le service d'assistance client, le service des ressources humaines, etc.

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

- **Cas d'utilisation du fournisseur de services :** si vous administrez un système StorageGRID en tant que fournisseur de services, vous pouvez séparer le stockage d'objets de la grille par les différentes entités qui loueront le stockage sur votre grille. Dans ce cas, vous créeriez des comptes locataires pour la société A, la société B, la société C, etc.

Pour plus d'informations, consultez la section "Utiliser un compte locataire" .

Comment créer un compte locataire ?

Utilisez le gestionnaire de grille pour créer un compte locataire. Lorsque vous créez un compte locataire, vous spécifiez les informations suivantes :

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

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

À quoi sert Tenant Manager ?

Après avoir créé le compte locataire, les utilisateurs locataires peuvent se connecter au gestionnaire de locataires pour effectuer des tâches telles que les suivantes :

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

> Bien que les utilisateurs de locataires S3 puissent créer et gérer des clés d'accès et des compartiments S3 avec Tenant Manager, ils doivent utiliser une application cliente S3 pour ingérer et gérer des objets. Voir"Utiliser l'API REST S3" pour plus de détails.

Créer un compte locataire

Vous devez créer au moins un compte locataire pour contrôler l'accès au stockage dans votre système StorageGRID .

Les étapes de création d'un compte locataire varient selon que"fédération d'identité" et"authentification unique" sont configurés et si le compte Grid Manager que vous utilisez pour créer le compte locataire appartient à un groupe d'administrateurs avec l'autorisation d'accès root.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Accès root ou autorisation des comptes locataires" .
- Si le compte locataire doit utiliser la source d'identité configurée pour le gestionnaire de grille et que vous souhaitez accorder l'autorisation d'accès racine pour le compte locataire à un groupe fédéré, vous devez importer ce groupe fédéré dans le gestionnaire de grille. Vous n'avez pas besoin d'attribuer des autorisations Grid Manager à ce groupe d'administrateurs. Voir "Gérer les groupes d'administrateurs" .
- Si vous souhaitez autoriser un locataire S3 à cloner des données de compte et à répliquer des objets de compartiment sur une autre grille à l'aide d'une connexion de fédération de grille :
  - Tu as"configuré la connexion à la fédération de grille" .
  - Le statut de la connexion est **Connecté**.
  - Vous disposez de l'autorisation d'accès root.
  - Vous avez examiné les considérations relatives à"gérer les locataires autorisés pour la fédération du réseau" .
  - Si le compte locataire doit utiliser la source d'identité configurée pour Grid Manager, vous avez importé le même groupe fédéré dans Grid Manager sur les deux grilles.

    Lorsque vous créez le locataire, vous sélectionnez ce groupe pour disposer de l'autorisation d'accès racine initiale pour les comptes de locataire source et de destination.

> Si ce groupe d'administrateurs n'existe pas sur les deux grilles avant la création du locataire, le locataire n'est pas répliqué vers la destination.

Accéder à l'assistant

Étapes

1. Sélectionnez **LOCATAIRES**.
2. Sélectionnez **Créer**.

Entrez les détails

Étapes

1. Saisissez les détails du locataire.

Champ	Description
Nom	Un nom pour le compte locataire. Les noms des locataires n'ont pas besoin d'être uniques. Lorsque le compte locataire est créé, il reçoit un identifiant de compte unique à 20 chiffres.
Description (facultatif)	Une description pour aider à identifier le locataire. Si vous créez un locataire qui utilisera une connexion de fédération de grille, utilisez éventuellement ce champ pour vous aider à identifier quel est le locataire source et quel est le locataire de destination. Par exemple, cette description pour un locataire créé sur la grille 1 apparaîtra également pour le locataire répliqué sur la grille 2 : « Ce locataire a été créé sur la grille 1. »
Type de client	Le type de protocole client que ce locataire utilisera, soit **S3** ou **Swift**. **Remarque** : la prise en charge des applications clientes Swift est obsolète et sera supprimée dans une prochaine version.
Quota de stockage (facultatif)	Si vous souhaitez que ce locataire dispose d'un quota de stockage, une valeur numérique pour le quota et les unités.

2. Sélectionnez **Continuer**.

Sélectionner les autorisations

Étapes

1. Vous pouvez également sélectionner les autorisations de base que vous souhaitez attribuer à ce locataire.

> Certaines de ces autorisations ont des exigences supplémentaires. Pour plus de détails, sélectionnez l'icône d'aide pour chaque autorisation.

Autorisation	Si sélectionné…
Autoriser les services de la plateforme	Le locataire peut utiliser les services de la plateforme S3 tels que CloudMirror. Voir "Gérer les services de plateforme pour les comptes locataires S3" .
Utiliser sa propre source d'identité	Le locataire peut configurer et gérer sa propre source d'identité pour les groupes et utilisateurs fédérés. Cette option est désactivée si vous avez"SSO configuré" pour votre système StorageGRID .
Autoriser la sélection S3	Le locataire peut émettre des requêtes API S3 SelectObjectContent pour filtrer et récupérer les données d'objet. Voir "Gérer S3 Select pour les comptes locataires" . **Important** : les demandes SelectObjectContent peuvent réduire les performances de l'équilibreur de charge pour tous les clients S3 et tous les locataires. Activez cette fonctionnalité uniquement lorsque cela est nécessaire et uniquement pour les locataires de confiance.

2. Vous pouvez également sélectionner les autorisations avancées que vous souhaitez accorder à ce locataire.

Autorisation	Si sélectionné…
Connexion à la fédération de réseau	Le locataire peut utiliser une connexion de fédération de grille, qui : • Fait en sorte que ce locataire et tous les groupes de locataires et utilisateurs ajoutés au compte soient clonés de cette grille (la *grille source*) vers l'autre grille de la connexion sélectionnée (la *grille de destination*). • Permet à ce locataire de configurer la réplication inter-grille entre les buckets correspondants sur chaque grille. Voir "Gérer les locataires autorisés pour la fédération de réseau" .
Verrouillage d'objet S3	Autoriser le locataire à utiliser des fonctionnalités spécifiques de S3 Object Lock : • **Définir la période de conservation maximale** définit la durée pendant laquelle les nouveaux objets ajoutés à ce bucket doivent être conservés, à compter du moment où ils sont ingérés. • **Le mode de conformité autorisé** empêche les utilisateurs d'écraser ou de supprimer les versions d'objets protégées pendant la période de conservation.

3. Sélectionnez **Continuer**.

Définir l'accès root et créer un locataire

Étapes

1. Définissez l'accès root pour le compte locataire, selon que votre système StorageGRID utilise la fédération d'identité, l'authentification unique (SSO) ou les deux.

Option	Fais ceci
Si la fédération d'identité n'est pas activée	Spécifiez le mot de passe à utiliser lors de la connexion au locataire en tant qu'utilisateur root local.
Si la fédération d'identité est activée	a. Sélectionnez un groupe fédéré existant pour disposer de l'autorisation d'accès root pour le locataire. b. Vous pouvez également spécifier le mot de passe à utiliser lors de la connexion au locataire en tant qu'utilisateur root local.
Si la fédération d'identité et l'authentification unique (SSO) sont activées	Sélectionnez un groupe fédéré existant pour disposer de l'autorisation d'accès root pour le locataire. Aucun utilisateur local ne peut se connecter.

2. Sélectionnez **Créer un locataire**.

   Un message de réussite s'affiche et le nouveau locataire est répertorié sur la page Locataires. Pour savoir

comment afficher les détails des locataires et surveiller leur activité, consultez"Surveiller l'activité des locataires" .

> L'application des paramètres du locataire sur la grille peut prendre 15 minutes ou plus en fonction de la connectivité réseau, de l'état du nœud et des opérations Cassandra.

3. Si vous avez sélectionné l'autorisation **Utiliser la connexion à la fédération de grille** pour le locataire :
   a. Confirmez qu'un locataire identique a été répliqué sur l'autre grille dans la connexion. Les locataires des deux grilles auront le même identifiant de compte à 20 chiffres, le même nom, la même description, le même quota et les mêmes autorisations.

      > Si vous voyez le message d'erreur « Locataire créé sans clone », reportez-vous aux instructions de"Résoudre les erreurs de fédération de grille" .

   b. Si vous avez fourni un mot de passe d'utilisateur root local lors de la définition de l'accès root,"changer le mot de passe de l'utilisateur root local" pour le locataire répliqué.

      > Un utilisateur root local ne peut pas se connecter à Tenant Manager sur la grille de destination tant que le mot de passe n'est pas modifié.

Sign in au locataire (facultatif)

Si nécessaire, vous pouvez vous connecter au nouveau locataire maintenant pour terminer la configuration, ou vous pouvez vous connecter au locataire ultérieurement. Les étapes de connexion dépendent du fait que vous soyez connecté au Grid Manager à l'aide du port par défaut (443) ou d'un port restreint. Voir "Contrôler l'accès au pare-feu externe" .

Sign in maintenant

Si vous utilisez…	Fais ceci…
Port 443 et vous définissez un mot de passe pour l'utilisateur root local	1. Sélectionnez * Sign in en tant que root*. Lorsque vous vous connectez, des liens s'affichent pour configurer les buckets, la fédération d'identité, les groupes et les utilisateurs. 2. Sélectionnez les liens pour configurer le compte locataire. Chaque lien ouvre la page correspondante dans le gestionnaire de locataires. Pour compléter la page, voir le"instructions d'utilisation des comptes locataires" .
Port 443 et vous n'avez pas défini de mot de passe pour l'utilisateur root local	Sélectionnez * Sign in* et saisissez les informations d'identification d'un utilisateur dans le groupe fédéré d'accès racine.

Si vous utilisez…	Fais ceci…
Un port restreint	1. Sélectionnez **Terminer** 2. Sélectionnez **Restreint** dans le tableau Locataire pour en savoir plus sur l'accès à ce compte locataire. L'URL du Tenant Manager a ce format : `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ `*FQDN_or_Admin_Node_IP*` est un nom de domaine complet ou l'adresse IP d'un nœud d'administration ◦ `*port*` est le port réservé aux locataires ◦ `*20-digit-account-id*` est l'identifiant de compte unique du locataire

Sign in plus tard

Si vous utilisez…	Faites l'une de ces choses…
Port 443	• Depuis le Gestionnaire de grille, sélectionnez **LOCATAIRES**, puis sélectionnez * Sign in* à droite du nom du locataire. • Saisissez l'URL du locataire dans un navigateur Web : `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ `*FQDN_or_Admin_Node_IP*` est un nom de domaine complet ou l'adresse IP d'un nœud d'administration ◦ `*20-digit-account-id*` est l'identifiant de compte unique du locataire
Un port restreint	• Depuis le gestionnaire de grille, sélectionnez **LOCATAIRES**, puis **Restreint**. • Saisissez l'URL du locataire dans un navigateur Web : `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ `*FQDN_or_Admin_Node_IP*` est un nom de domaine complet ou l'adresse IP d'un nœud d'administration ◦ `*port*` est le port restreint réservé aux locataires ◦ `*20-digit-account-id*` est l'identifiant de compte unique du locataire

Configurer le locataire

Suivez les instructions dans"Utiliser un compte locataire" pour gérer les groupes de locataires et les utilisateurs, les clés d'accès S3, les buckets, les services de plateforme, le clonage de compte et la réplication inter-grille.

Modifier le compte locataire

Vous pouvez modifier un compte locataire pour modifier le nom d'affichage, le quota de stockage ou les autorisations du locataire.

Si un locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, vous pouvez modifier les détails du locataire à partir de l'une ou l'autre des grilles de la connexion. Cependant, toutes les modifications que vous apportez sur une grille de la connexion ne seront pas copiées sur l'autre grille. Si vous souhaitez que les détails du locataire soient exactement synchronisés entre les grilles, effectuez les mêmes modifications sur les deux grilles. Voir "Gérer les locataires autorisés pour la connexion à la fédération de réseau" .

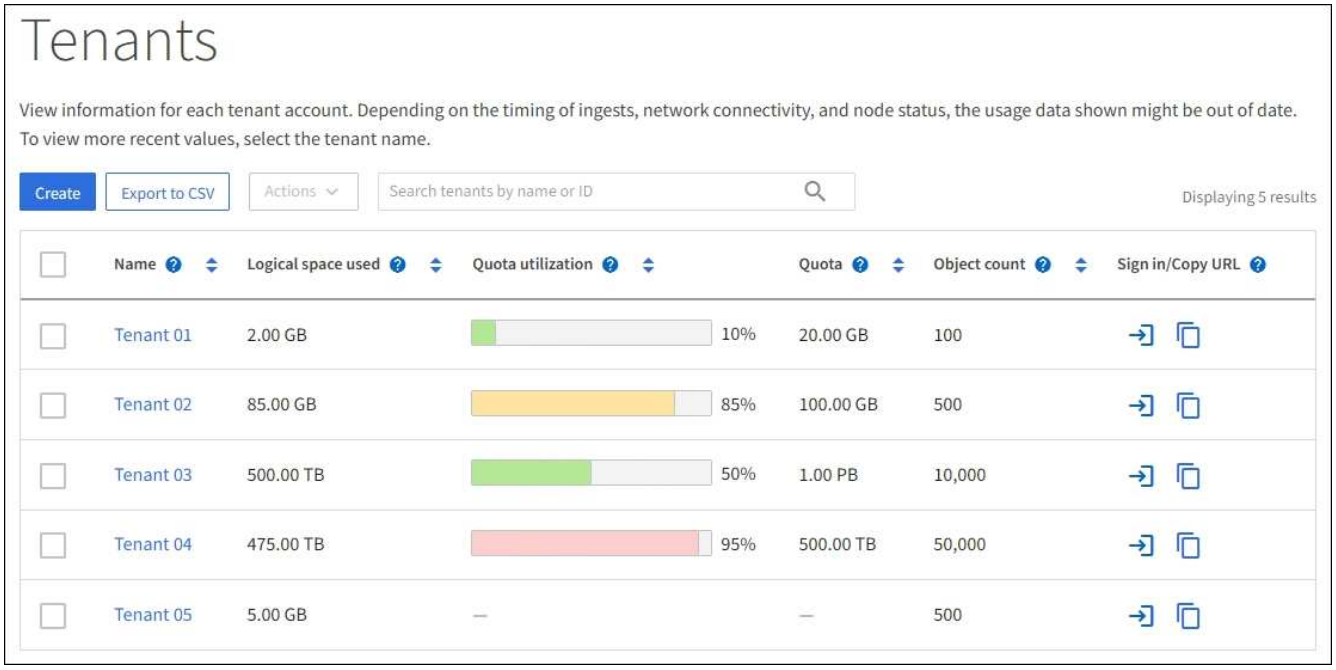
Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Accès root ou autorisation des comptes locataires" .

L'application des paramètres du locataire sur la grille peut prendre 15 minutes ou plus en fonction de la connectivité réseau, de l'état du nœud et des opérations Cassandra.

Étapes

1. Sélectionnez **LOCATAIRES**.



2. Localisez le compte locataire que vous souhaitez modifier.

   Utilisez le champ de recherche pour rechercher un locataire par nom ou par ID de locataire.

3. Sélectionnez le locataire. Vous pouvez effectuer l'une des opérations suivantes :
   - Cochez la case correspondant au locataire, puis sélectionnez **Actions** > **Modifier**.
   - Sélectionnez le nom du locataire pour afficher la page de détails et sélectionnez **Modifier**.
4. Vous pouvez également modifier les valeurs de ces champs :

- **Nom**
- **Description**
- **Quota de stockage**

5. Sélectionnez **Continuer**.
6. Sélectionnez ou effacez les autorisations pour le compte locataire.
   - Si vous désactivez les **services de plateforme** pour un locataire qui les utilise déjà, les services qu'il a configurés pour ses compartiments S3 cesseront de fonctionner. Aucun message d'erreur n'est envoyé au locataire. Par exemple, si le locataire a configuré la réplication CloudMirror pour un bucket S3, il peut toujours stocker des objets dans le bucket, mais les copies de ces objets ne seront plus effectuées dans le bucket S3 externe qu'il a configuré comme point de terminaison. Voir "Gérer les services de plateforme pour les comptes locataires S3" .
   - Modifiez le paramètre **Utiliser sa propre source d'identité** pour déterminer si le compte de locataire utilisera sa propre source d'identité ou la source d'identité configurée pour le gestionnaire de grille.

     Si **Utiliser sa propre source d'identité** est :

     - Désactivé et sélectionné, le locataire a déjà activé sa propre source d'identité. Un locataire doit désactiver sa source d'identité avant de pouvoir utiliser la source d'identité configurée pour Grid Manager.
     - Désactivé et non sélectionné, SSO est activé pour le système StorageGRID . Le locataire doit utiliser la source d'identité qui a été configurée pour le gestionnaire de grille.
   - Sélectionnez ou désactivez l'autorisation **Autoriser la sélection S3** selon vos besoins. Voir "Gérer S3 Select pour les comptes locataires" .
   - Pour supprimer l'autorisation **Utiliser la connexion à la fédération de grille** :
     i. Sélectionnez l'onglet **Fédération de grille**.
     ii. Sélectionnez **Supprimer l'autorisation**.
   - Pour ajouter l'autorisation **Utiliser la connexion à la fédération de grille** :
     i. Sélectionnez l'onglet **Fédération de grille**.
     ii. Cochez la case **Utiliser la connexion à la fédération de grille**.
     iii. Vous pouvez également sélectionner **Cloner les utilisateurs et groupes locaux existants** pour les cloner sur la grille distante. Si vous le souhaitez, vous pouvez arrêter le clonage en cours ou réessayer le clonage si certains utilisateurs ou groupes locaux n'ont pas pu être clonés après la fin de la dernière opération de clonage.
   - Pour définir une période de conservation maximale ou autoriser le mode de conformité :

     > ⓘ Le verrouillage d'objet S3 doit être activé sur la grille avant de pouvoir utiliser ces paramètres.

     i. Sélectionnez l'onglet **Verrouillage d'objet S3**.
     ii. Pour **Définir la période de conservation maximale**, saisissez une valeur et sélectionnez la période dans le menu déroulant.
     iii. Pour **Autoriser le mode de conformité**, cochez la case.

Modifier le mot de passe de l'utilisateur root local du locataire

Vous devrez peut-être modifier le mot de passe de l'utilisateur root local d'un locataire si l'utilisateur root est exclu du compte.

Avant de commencer

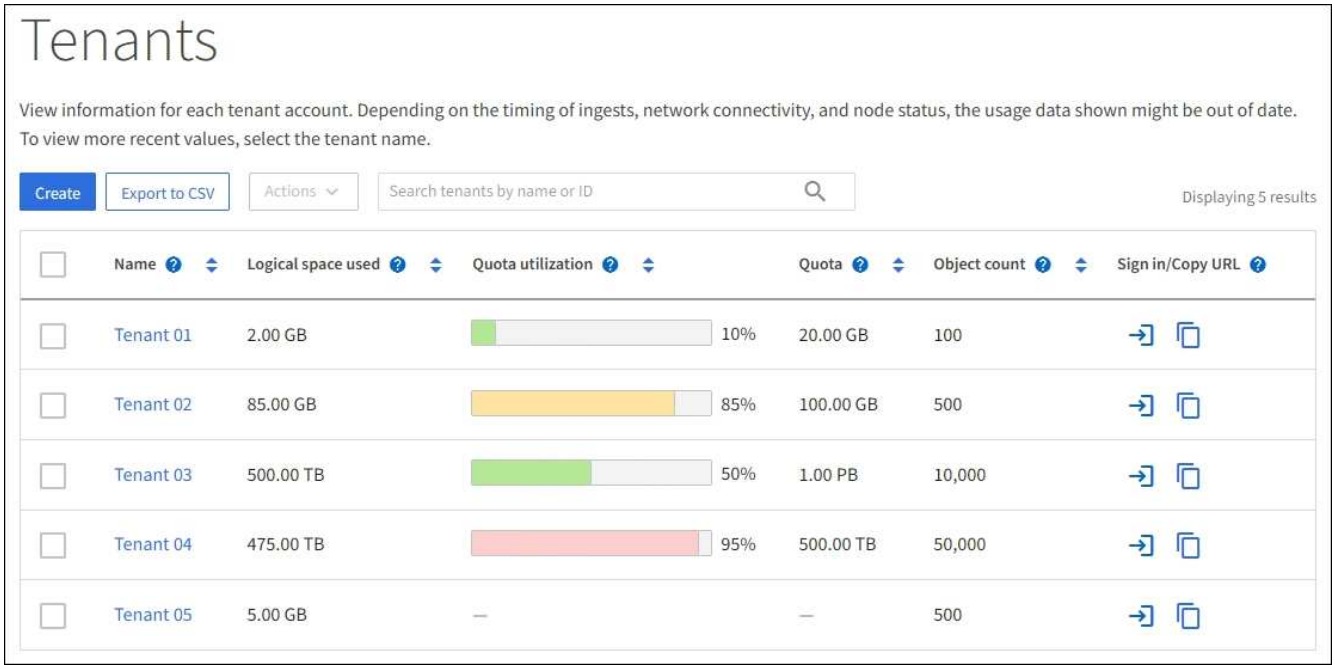
- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .

À propos de cette tâche

Si l'authentification unique (SSO) est activée pour votre système StorageGRID , l'utilisateur root local ne peut pas se connecter au compte locataire. Pour effectuer des tâches d'utilisateur root, les utilisateurs doivent appartenir à un groupe fédéré disposant de l'autorisation d'accès root pour le locataire.

Étapes

1. Sélectionnez **LOCATAIRES**.



2. Sélectionnez le compte locataire. Vous pouvez effectuer l'une des opérations suivantes :
   - Cochez la case correspondant au locataire, puis sélectionnez **Actions** > **Modifier le mot de passe root**.
   - Sélectionnez le nom du locataire pour afficher la page de détails, puis sélectionnez **Actions** > **Modifier le mot de passe root**.
3. Saisissez le nouveau mot de passe du compte locataire.
4. Sélectionnez **Enregistrer**.

Supprimer le compte locataire

Vous pouvez supprimer un compte locataire si vous souhaitez supprimer définitivement l'accès du locataire au système.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .
- Vous avez supprimé tous les compartiments et objets S3 associés au compte locataire.
- Si le locataire est autorisé à utiliser une connexion à une fédération de réseau, vous avez examiné les considérations relatives à"suppression d'un locataire avec l'autorisation Utiliser la connexion à la fédération de grille" .

Étapes

1. Sélectionnez **LOCATAIRES**.
2. Localisez le ou les comptes locataires que vous souhaitez supprimer.

   Utilisez le champ de recherche pour rechercher un locataire par nom ou par ID de locataire.

3. Pour supprimer plusieurs locataires, cochez les cases et sélectionnez **Actions** > **Supprimer**.
4. Pour supprimer un seul locataire, effectuez l'une des opérations suivantes :
   - Cochez la case, puis sélectionnez **Actions** > **Supprimer**.
   - Sélectionnez le nom du locataire pour afficher la page de détails, puis sélectionnez **Actions** > **Supprimer**.
5. Sélectionnez **Oui**.

Gérer les services de la plateforme

Que sont les services de plateforme ?

Les services de la plateforme incluent la réplication CloudMirror, les notifications d'événements et le service d'intégration de recherche.

Si vous activez les services de plateforme pour les comptes de locataire S3, vous devez configurer votre grille afin que les locataires puissent accéder aux ressources externes nécessaires pour utiliser ces services.

Réplication CloudMirror

Le service de réplication StorageGRID CloudMirror est utilisé pour mettre en miroir des objets spécifiques d'un bucket StorageGRID vers une destination externe spécifiée.

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

> La réplication CloudMirror présente certaines similitudes et différences importantes avec la fonctionnalité de réplication inter-grille. Pour en savoir plus, voir"Comparer la réplication inter-grille et la réplication CloudMirror" .

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

Notifications

Les notifications d'événements par compartiment sont utilisées pour envoyer des notifications sur des actions

spécifiques effectuées sur des objets à un cluster Kafka externe spécifié ou à Amazon Simple Notification Service.

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

> Bien que la notification d'événement puisse être configurée sur un bucket avec le verrouillage d'objet S3 activé, les métadonnées du verrouillage d'objet S3 (y compris la date de conservation et le statut de conservation légale) des objets ne seront pas incluses dans les messages de notification.

Service d'intégration de recherche

Le service d'intégration de recherche est utilisé pour envoyer des métadonnées d'objet S3 à un index Elasticsearch spécifié où les métadonnées peuvent être recherchées ou analysées à l'aide du service externe.

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

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

Les services de plateforme offrent aux locataires la possibilité d'utiliser des ressources de stockage externes, des services de notification et des services de recherche ou d'analyse avec leurs données. Étant donné que l'emplacement cible des services de plateforme est généralement externe à votre déploiement StorageGRID , vous devez décider si vous souhaitez autoriser les locataires à utiliser ces services. Si vous le faites, vous devez activer l'utilisation des services de plateforme lorsque vous créez ou modifiez des comptes locataires. Vous devez également configurer votre réseau de manière à ce que les messages des services de plateforme générés par les locataires puissent atteindre leurs destinations.

Recommandations pour l'utilisation des services de la plateforme

Avant d'utiliser les services de la plateforme, tenez compte des recommandations suivantes :

- Si le contrôle de version et la réplication CloudMirror sont activés pour un compartiment S3 du système StorageGRID , vous devez également activer le contrôle de version du compartiment S3 pour le point de terminaison de destination. Cela permet à la réplication CloudMirror de générer des versions d'objet similaires sur le point de terminaison.
- Vous ne devez pas utiliser plus de 100 locataires actifs avec des requêtes S3 nécessitant une réplication CloudMirror, des notifications et une intégration de recherche. Avoir plus de 100 locataires actifs peut entraîner des performances client S3 plus lentes.
- Les demandes adressées à un point de terminaison qui ne peuvent pas être traitées seront mises en file d'attente jusqu'à un maximum de 500 000 demandes. Cette limite est partagée équitablement entre les locataires actifs. Les nouveaux locataires sont autorisés à dépasser temporairement cette limite de 500 000 afin que les locataires nouvellement créés ne soient pas injustement pénalisés.

Informations connexes

- "Gérer les services de la plateforme"
- "Configurer les paramètres du proxy de stockage"

- "Surveiller StorageGRID"

Réseau et ports pour les services de la plateforme

Si vous autorisez un locataire S3 à utiliser les services de plateforme, vous devez configurer la mise en réseau de la grille pour garantir que les messages des services de plateforme peuvent être livrés à leurs destinations.

Vous pouvez activer les services de plateforme pour un compte locataire S3 lorsque vous créez ou mettez à jour le compte locataire. Si les services de plateforme sont activés, le locataire peut créer des points de terminaison qui servent de destination pour la réplication CloudMirror, les notifications d'événements ou les messages d'intégration de recherche à partir de ses compartiments S3. Ces messages de services de plateforme sont envoyés depuis les nœuds de stockage qui exécutent le service ADC vers les points de terminaison de destination.

Par exemple, les locataires peuvent configurer les types de points de terminaison de destination suivants :

- Un cluster Elasticsearch hébergé localement
- Une application locale qui prend en charge la réception de messages Amazon Simple Notification Service
- Un cluster Kafka hébergé localement
- Un bucket S3 hébergé localement sur la même instance ou sur une autre instance de StorageGRID
- Un point de terminaison externe, tel qu'un point de terminaison sur Amazon Web Services.

Pour garantir que les messages des services de plateforme peuvent être délivrés, vous devez configurer le ou les réseaux contenant les nœuds de stockage ADC. Vous devez vous assurer que les ports suivants peuvent être utilisés pour envoyer des messages de services de plateforme aux points de terminaison de destination.

Par défaut, les messages des services de la plateforme sont envoyés sur les ports suivants :

- **80** : pour les URI de point de terminaison commençant par http (la plupart des points de terminaison)
- **443** : pour les URI de point de terminaison commençant par https (la plupart des points de terminaison)
- **9092** : pour les URI de point de terminaison commençant par http ou https (points de terminaison Kafka uniquement)

Les locataires peuvent spécifier un port différent lorsqu'ils créent ou modifient un point de terminaison.

> Si un déploiement StorageGRID est utilisé comme destination pour la réplication CloudMirror, les messages de réplication peuvent être reçus sur un port autre que 80 ou 443. Assurez-vous que le port utilisé pour S3 par le déploiement StorageGRID de destination est spécifié dans le point de terminaison.

Si vous utilisez un serveur proxy non transparent, vous devez également"configurer les paramètres du proxy de stockage" pour permettre l'envoi de messages à des points de terminaison externes, tels qu'un point de terminaison sur Internet.

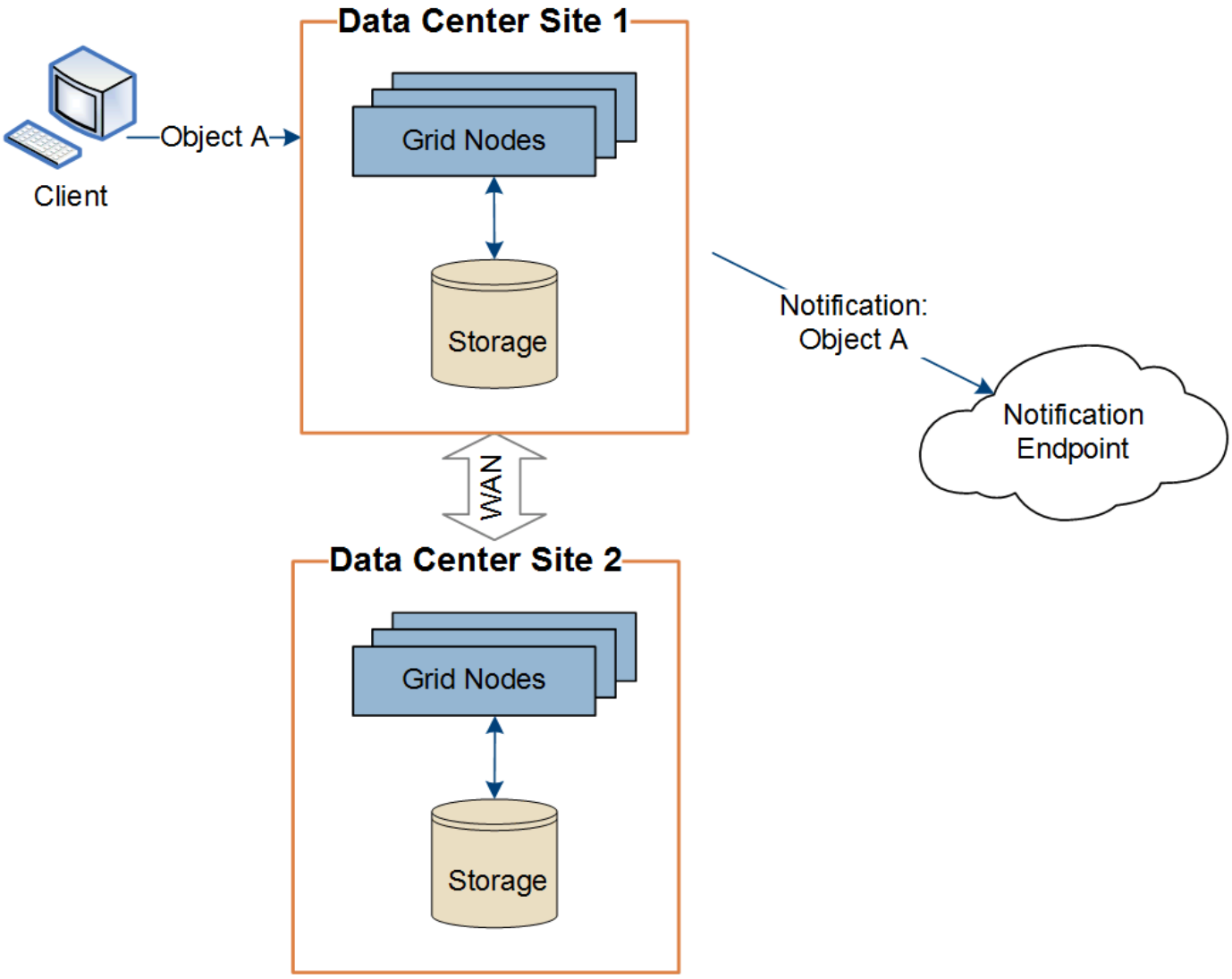
Informations connexes

"Utiliser un compte locataire"

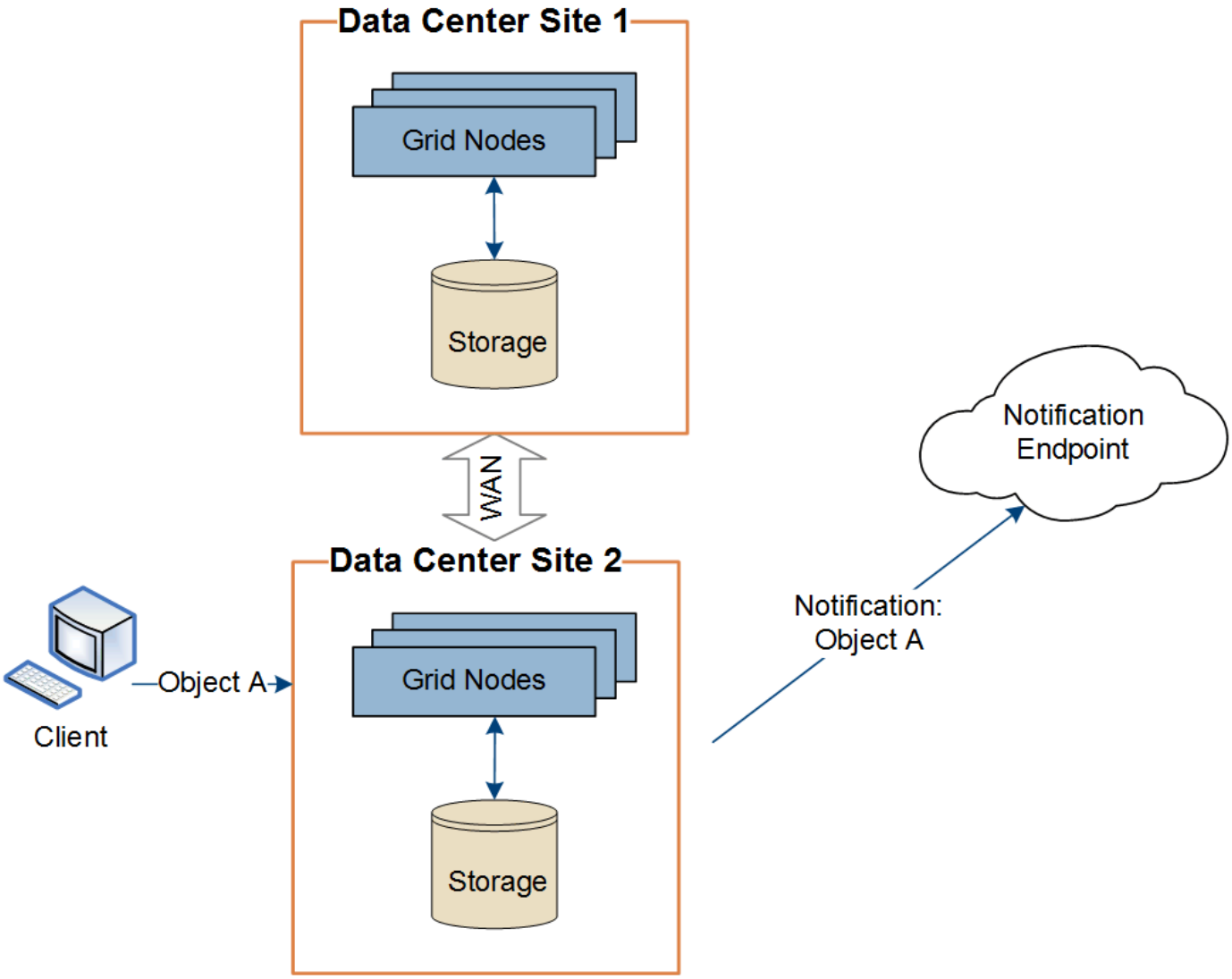
Livraison par site des messages des services de la plateforme

Toutes les opérations de services de la plateforme sont effectuées site par site.

Autrement dit, si un locataire utilise un client pour effectuer une opération de création d'API S3 sur un objet en se connectant à un nœud de passerelle sur le site 1 du centre de données, la notification concernant cette action est déclenchée et envoyée depuis le site 1 du centre de données.



Si le client effectue ensuite une opération de suppression d'API S3 sur ce même objet à partir du site de centre de données 2, la notification concernant l'action de suppression est déclenchée et envoyée à partir du site de centre de données 2.



Assurez-vous que le réseau de chaque site est configuré de manière à ce que les messages des services de la plateforme puissent être délivrés à leurs destinations.

Dépanner les services de la plateforme

Les points de terminaison utilisés dans les services de plateforme sont créés et gérés par les utilisateurs locataires dans le gestionnaire de locataires. Toutefois, si un locataire rencontre des problèmes lors de la configuration ou de l'utilisation des services de plateforme, vous pourrez peut-être utiliser le gestionnaire de grille pour vous aider à résoudre le problème.

Problèmes avec les nouveaux points de terminaison

Avant qu'un locataire puisse utiliser les services de la plateforme, il doit créer un ou plusieurs points de terminaison à l'aide du gestionnaire de locataires. Chaque point de terminaison représente une destination externe pour un service de plateforme, tel qu'un bucket StorageGRID S3, un bucket Amazon Web Services, une rubrique Amazon Simple Notification Service, une rubrique Kafka ou un cluster Elasticsearch hébergé localement ou sur AWS. Chaque point de terminaison inclut à la fois l'emplacement de la ressource externe et les informations d'identification nécessaires pour accéder à cette ressource.

Lorsqu'un locataire crée un point de terminaison, le système StorageGRID valide que le point de terminaison existe et qu'il peut être atteint à l'aide des informations d'identification spécifiées. La connexion au point de terminaison est validée à partir d'un nœud sur chaque site.

Si la validation du point de terminaison échoue, un message d'erreur explique pourquoi la validation du point de terminaison a échoué. L'utilisateur locataire doit résoudre le problème, puis essayer à nouveau de créer le point de terminaison.

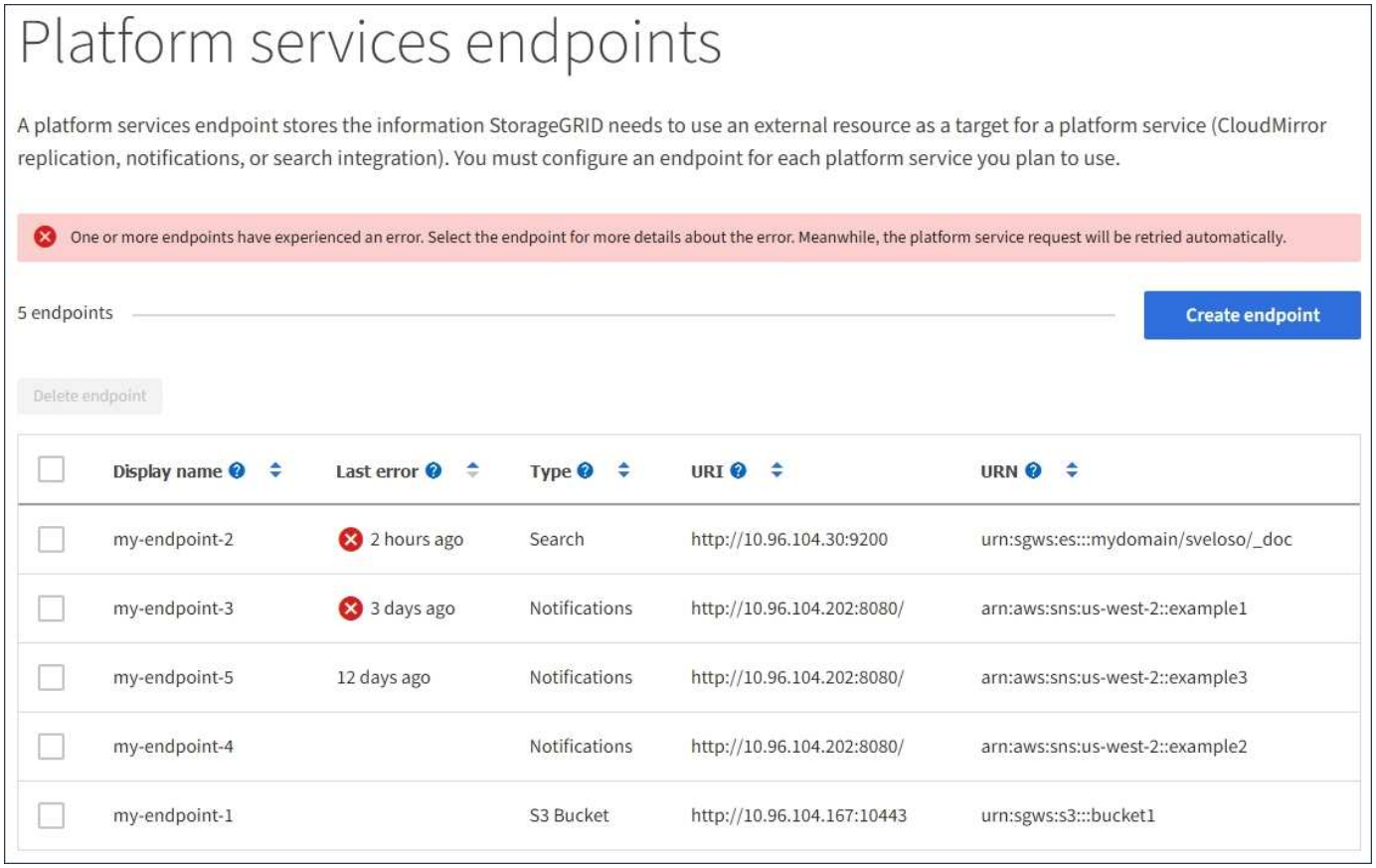
> La création du point de terminaison échouera si les services de plateforme ne sont pas activés pour le compte locataire.

Problèmes avec les points de terminaison existants

Si une erreur se produit lorsque StorageGRID tente d'atteindre un point de terminaison existant, un message s'affiche sur le tableau de bord dans le gestionnaire de locataires.

> One or more endpoints have experienced an error and might not be functioning properly. Go to the Endpoints page to view the error details. The last error occurred 2 hours ago.

Les utilisateurs locataires peuvent accéder à la page Points de terminaison pour consulter le message d'erreur le plus récent pour chaque point de terminaison et déterminer depuis combien de temps l'erreur s'est produite. La colonne **Dernière erreur** affiche le message d'erreur le plus récent pour chaque point de terminaison et indique depuis combien de temps l'erreur s'est produite. Les erreurs qui incluent le l'icône s'est produite au cours des 7 derniers jours.



Certains messages d'erreur dans la colonne **Dernière erreur** peuvent inclure un logID entre parenthèses. Un administrateur de grille ou un support technique peut utiliser cet ID pour localiser des informations plus détaillées sur l'erreur dans le fichier bycast.log.

Problèmes liés aux serveurs proxy

Si vous avez configuré un"proxy de stockage" entre les nœuds de stockage et les points de terminaison du service de la plateforme, des erreurs peuvent se produire si votre service proxy n'autorise pas les messages provenant de StorageGRID. Pour résoudre ces problèmes, vérifiez les paramètres de votre serveur proxy pour vous assurer que les messages liés au service de la plateforme ne sont pas bloqués.

Déterminer si une erreur s'est produite

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

Les opérations client échouent

Certains problèmes de services de plateforme peuvent entraîner l'échec des opérations client sur le bucket S3. Par exemple, les opérations du client S3 échoueront si le service interne de machine à états répliquée (RSM) s'arrête ou s'il y a trop de messages de services de plateforme en file d'attente pour livraison.

Pour vérifier l'état des services :

1. Sélectionnez **SUPPORT** > **Outils** > **Topologie de grille**.
2. Sélectionnez ***site*** > ***Nœud de stockage*** > **SSM** > **Services**.

Erreurs de point de terminaison récupérables et irrécupérables

Une fois les points de terminaison créés, des erreurs de demande de service de plateforme peuvent se produire pour diverses raisons. Certaines erreurs sont récupérables avec l'intervention de l'utilisateur. Par exemple, des erreurs récupérables peuvent se produire pour les raisons suivantes :

- Les informations d'identification de l'utilisateur ont été supprimées ou ont expiré.
- Le bucket de destination n'existe pas.
- La notification ne peut pas être délivrée.

Si StorageGRID rencontre une erreur récupérable, la demande de service de plateforme sera relancée jusqu'à ce qu'elle réussisse.

D'autres erreurs sont irrécupérables. Par exemple, une erreur irrécupérable se produit si le point de terminaison est supprimé.

Si StorageGRID rencontre une erreur de point de terminaison irrécupérable :

- Dans le gestionnaire de grille, accédez à **Support** > **Outils** > **Métriques** > **Grafana** > **Présentation des services de la plateforme** pour afficher les détails de l'erreur.
- Dans le gestionnaire de locataires, accédez à **STOCKAGE (S3)** > **Points de terminaison des services de plateforme** pour afficher les détails de l'erreur.
- Vérifiez le `/var/local/log/bycast-err.log` pour les erreurs liées. Les nœuds de stockage dotés du service ADC contiennent ce fichier journal.

Les messages des services de la plateforme ne peuvent pas être livrés

Si la destination rencontre un problème qui l'empêche d'accepter les messages des services de plateforme, l'opération client sur le bucket réussit, mais le message des services de plateforme n'est pas remis. Par exemple, cette erreur peut se produire si les informations d'identification sont mises à jour sur la destination de telle sorte que StorageGRID ne peut plus s'authentifier auprès du service de destination.

Vérifiez les alertes associées.

Des performances plus lentes pour les demandes de service de la plateforme

Le logiciel StorageGRID peut limiter les requêtes S3 entrantes pour un bucket si la vitesse à laquelle les requêtes sont envoyées dépasse la vitesse à laquelle le point de terminaison de destination peut recevoir les requêtes. La limitation se produit uniquement lorsqu'il existe un arriéré de requêtes en attente d'être envoyées au point de terminaison de destination.

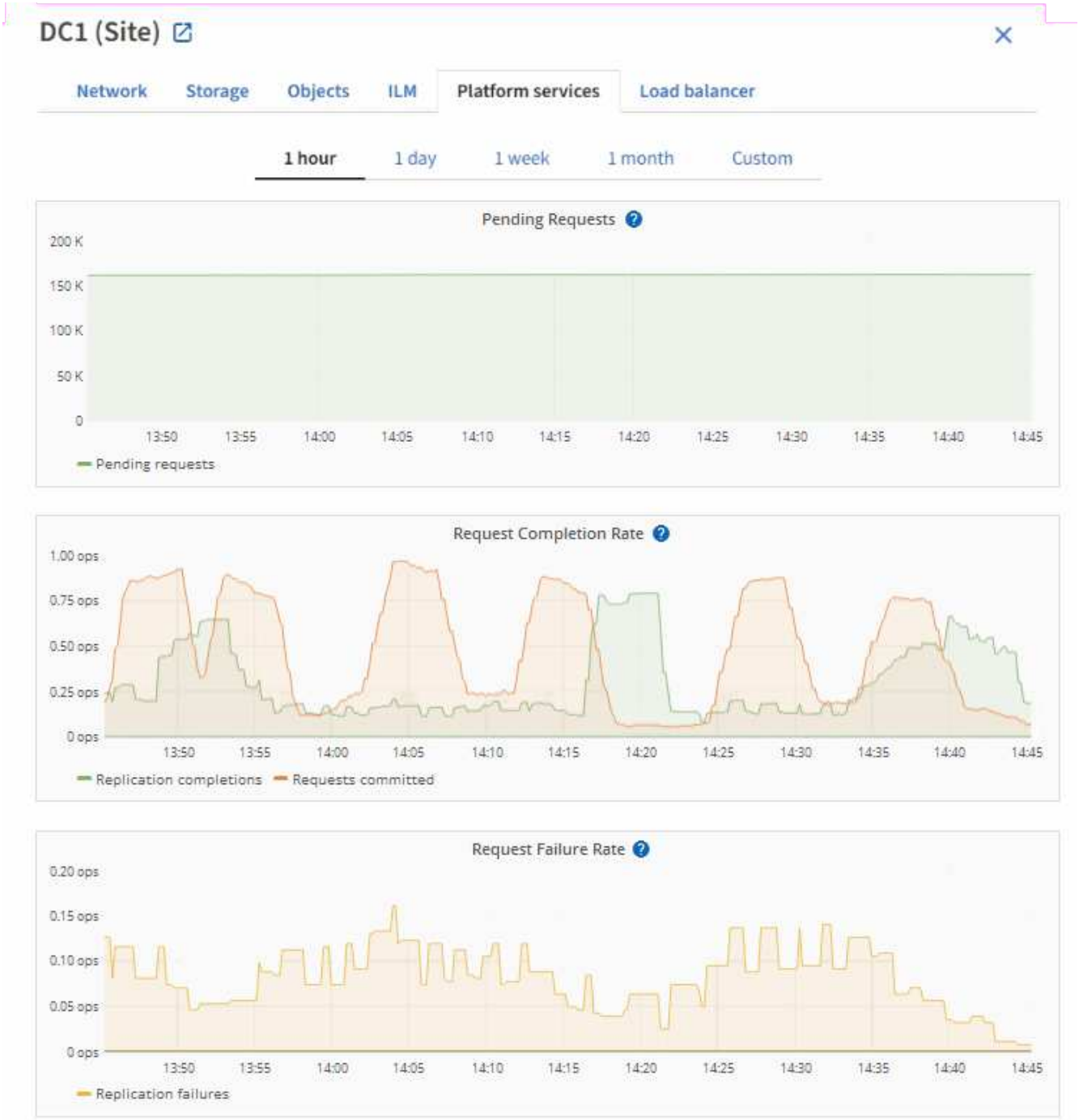
Le seul effet visible est que les requêtes S3 entrantes prendront plus de temps à s'exécuter. Si vous commencez à détecter des performances nettement plus lentes, vous devez réduire le taux d'ingestion ou utiliser un point de terminaison avec une capacité supérieure. Si l'arriéré des demandes continue de croître, les opérations S3 du client (telles que les demandes PUT) finiront par échouer.

Les requêtes CloudMirror sont plus susceptibles d'être affectées par les performances du point de terminaison de destination, car ces requêtes impliquent généralement plus de transfert de données que les requêtes d'intégration de recherche ou de notification d'événements.

Les demandes de service de la plateforme échouent

Pour afficher le taux d'échec des demandes pour les services de la plateforme :

1. Sélectionnez **NODES**.
2. Sélectionnez ***site*** > **Services de plateforme**.
3. Consultez le graphique des taux d'erreur des demandes.



Alerte d'indisponibilité des services de la plateforme

L'alerte **Services de plateforme indisponibles** indique qu'aucune opération de service de plateforme ne peut être effectuée sur un site car trop peu de nœuds de stockage avec le service RSM sont en cours d'exécution ou disponibles.

Le service RSM garantit que les demandes de service de la plateforme sont envoyées à leurs points de terminaison respectifs.

Pour résoudre cette alerte, déterminez quels nœuds de stockage du site incluent le service RSM. (Le service RSM est présent sur les nœuds de stockage qui incluent également le service ADC.) Ensuite, assurez-vous qu'une simple majorité de ces nœuds de stockage sont en cours d'exécution et disponibles.

Si plusieurs nœuds de stockage contenant le service RSM échouent sur un site, vous perdez toutes les demandes de service de plateforme en attente pour ce site.

Conseils de dépannage supplémentaires pour les points de terminaison des services de plateforme

Pour plus d'informations, voir**Utiliser un compte locataire › Résoudre les problèmes des points de terminaison des services de la plateforme** .

Informations connexes

"Dépannage du système StorageGRID"

Gérer S3 Select pour les comptes locataires

Vous pouvez autoriser certains locataires S3 à utiliser S3 Select pour émettre des demandes SelectObjectContent sur des objets individuels.

S3 Select offre un moyen efficace de rechercher dans de grandes quantités de données sans avoir à déployer une base de données et les ressources associées pour permettre les recherches. Cela réduit également le coût et la latence de récupération des données.

Qu'est-ce que S3 Select ?

S3 Select permet aux clients S3 d'utiliser les requêtes SelectObjectContent pour filtrer et récupérer uniquement les données nécessaires à un objet. L'implémentation StorageGRID de S3 Select inclut un sous-ensemble de commandes et de fonctionnalités S3 Select.

Considérations et exigences relatives à l'utilisation de S3 Select

Exigences en matière d'administration du réseau

L'administrateur du réseau doit accorder aux locataires la capacité S3 Select. Sélectionnez **Autoriser la sélection S3** lorsque"créer un locataire" ou"modifier un locataire" .

Exigences relatives au format des objets

L'objet que vous souhaitez interroger doit être dans l'un des formats suivants :

- **CSV**. Peut être utilisé tel quel ou compressé dans des archives GZIP ou BZIP2.
- **Parquet**. Exigences supplémentaires pour les objets Parquet :
  - S3 Select prend uniquement en charge la compression en colonnes à l'aide de GZIP ou Snappy. S3 Select ne prend pas en charge la compression d'objets entiers pour les objets Parquet.
  - S3 Select ne prend pas en charge la sortie Parquet. Vous devez spécifier le format de sortie au format CSV ou JSON.
  - La taille maximale du groupe de lignes non compressé est de 512 Mo.
  - Vous devez utiliser les types de données spécifiés dans le schéma de l'objet.
  - Vous ne pouvez pas utiliser les types logiques INTERVAL, JSON, LIST, TIME ou UUID.

Exigences relatives aux points de terminaison

La requête SelectObjectContent doit être envoyée à un"Point de terminaison de l'équilibreur de charge

StorageGRID" .

Les nœuds d'administration et de passerelle utilisés par le point de terminaison doivent être l'un des suivants :

- Un nœud d'appareil de services
- Un nœud logiciel basé sur VMware
- Un nœud bare metal exécutant un noyau avec cgroup v2 activé

Considérations générales

Les requêtes ne peuvent pas être envoyées directement aux nœuds de stockage.

> Les demandes SelectObjectContent peuvent réduire les performances de l'équilibreur de charge pour tous les clients S3 et tous les locataires. Activez cette fonctionnalité uniquement lorsque cela est nécessaire et uniquement pour les locataires de confiance.

Voir le"instructions d'utilisation de S3 Select" .

Pour voir"Cartes Grafana" pour les opérations S3 Sélectionnez au fil du temps, sélectionnez **SUPPORT** > **Outils** > **Métriques** dans le Gestionnaire de grille.

Configurer les connexions client

Configurer les connexions client S3

En tant qu'administrateur de grille, vous gérez les options de configuration qui contrôlent la manière dont les applications clientes S3 se connectent à votre système StorageGRID pour stocker et récupérer des données.

> Les détails Swift ont été supprimés de cette version du site de documentation. Voir "StorageGRID 11.8 : Configurer les connexions client S3 et Swift" .

Tâches de configuration

1. Exécutez les tâches prérequises dans StorageGRID, en fonction de la manière dont l'application cliente se connectera à StorageGRID.

Tâches requises

Vous devez obtenir :

- adresses IP
- noms de domaine
- Certificat SSL

Tâches facultatives

En option, configurez :

- Fédération d'identité
- SSO

1. Utilisez StorageGRID pour obtenir les valeurs dont l'application a besoin pour se connecter à la grille. Vous pouvez utiliser l'assistant de configuration S3 ou configurer chaque entité StorageGRID manuellement.

Utiliser l'assistant de configuration S3

Suivez les étapes de l'assistant de configuration S3.

Configurer manuellement

1. Créer un groupe de haute disponibilité
2. Créer un point de terminaison d'équilibrage de charge
3. Créer un compte locataire
4. Créer un bucket et accéder aux clés
5. Configurer la règle et la politique ILM

1. Utilisez l'application S3 pour terminer la connexion à StorageGRID. Créez des entrées DNS pour associer des adresses IP à tous les noms de domaine que vous prévoyez d'utiliser.

   Si nécessaire, effectuez une configuration d'application supplémentaire.

2. Exécutez des tâches continues dans l'application et dans StorageGRID pour gérer et surveiller le stockage d'objets au fil du temps.

Informations nécessaires pour attacher StorageGRID à une application cliente

Avant de pouvoir attacher StorageGRID à une application client S3, vous devez effectuer des étapes de configuration dans StorageGRID et obtenir une certaine valeur.

De quelles valeurs ai-je besoin ?

Le tableau suivant indique les valeurs que vous devez configurer dans StorageGRID et où ces valeurs sont utilisées par l'application S3 et le serveur DNS.

Valeur	Où la valeur est configurée	Où la valeur est utilisée
Adresses IP virtuelles (VIP)	StorageGRID > Groupe HA	Entrée DNS
Port	StorageGRID > Point de terminaison de l'équilibreur de charge	Application client
Certificat SSL	StorageGRID > Point de terminaison de l'équilibreur de charge	Application client
Nom du serveur (FQDN)	StorageGRID > Point de terminaison de l'équilibreur de charge	• Application client • Entrée DNS
ID de clé d'accès S3 et clé d'accès secrète	StorageGRID > Locataire et bucket	Application client
Nom du seau/conteneur	StorageGRID > Locataire et bucket	Application client

Comment puis-je obtenir ces valeurs ?

Selon vos besoins, vous pouvez procéder de l'une des manières suivantes pour obtenir les informations dont vous avez besoin :

- *Utilisez le"Assistant de configuration S3" *. L'assistant de configuration S3 vous aide à configurer rapidement les valeurs requises dans StorageGRID et génère un ou deux fichiers que vous pouvez utiliser lorsque vous configurez l'application S3. L'assistant vous guide à travers les étapes requises et vous aide à garantir que vos paramètres sont conformes aux meilleures pratiques de StorageGRID .

  Si vous configurez une application S3, il est recommandé d'utiliser l'assistant de configuration S3, sauf si vous savez que vous avez des exigences particulières ou que votre implémentation nécessitera une personnalisation importante.

- *Utilisez le"Assistant de configuration de FabricPool" *. Semblable à l'assistant de configuration S3, l'assistant de configuration FabricPool vous aide à configurer rapidement les valeurs requises et génère un fichier que vous pouvez utiliser lorsque vous configurez un niveau de cloud FabricPool dans ONTAP.

  Si vous prévoyez d'utiliser StorageGRID comme système de stockage d'objets pour un niveau cloud FabricPool , il est recommandé d'utiliser l'assistant de configuration FabricPool , sauf si vous savez que vous avez des exigences particulières ou que votre implémentation nécessitera une personnalisation importante.

- **Configurer les éléments manuellement**. Si vous vous connectez à une application S3 et préférez ne pas utiliser l'assistant de configuration S3, vous pouvez obtenir les valeurs requises en effectuant la configuration manuellement. Suivez ces étapes :

  a. Configurez le groupe de haute disponibilité (HA) que vous souhaitez utiliser pour l'application S3. Voir "Configurer des groupes de haute disponibilité" .

b. Créez le point de terminaison de l'équilibreur de charge que l'application S3 utilisera. Voir "Configurer les points de terminaison de l'équilibreur de charge" .

c. Créez le compte locataire que l'application S3 utilisera. Voir "Créer un compte locataire" .

d. Pour un locataire S3, connectez-vous au compte locataire et générez un ID de clé d'accès et une clé d'accès secrète pour chaque utilisateur qui accédera à l'application. Voir "Créez vos propres clés d'accès" .

e. Créez un ou plusieurs compartiments S3 dans le compte locataire. Pour S3, voir"Créer un bucket S3" .

f. Pour ajouter des instructions de placement spécifiques pour les objets appartenant au nouveau locataire ou bucket/conteneur, créez une nouvelle règle ILM et activez une nouvelle stratégie ILM pour utiliser cette règle. Voir"Créer une règle ILM" et"Créer une politique ILM" .

Sécurité pour les clients S3

Les comptes locataires StorageGRID utilisent des applications clientes S3 pour enregistrer les données d'objet dans StorageGRID. Vous devez examiner les mesures de sécurité mises en œuvre pour les applications clientes.

Résumé

La liste suivante résume la manière dont la sécurité est implémentée pour l'API REST S3 :

Sécurité de connexion
: TLS

Authentification du serveur
: Certificat de serveur X.509 signé par l'autorité de certification système ou certificat de serveur personnalisé fourni par l'administrateur

Authentification du client
: ID de clé d'accès au compte S3 et clé d'accès secrète

Autorisation du client
: Propriété du bucket et toutes les politiques de contrôle d'accès applicables

Comment StorageGRID assure la sécurité des applications clientes

Les applications clientes S3 peuvent se connecter au service Load Balancer sur les nœuds de passerelle ou les nœuds d'administration ou directement aux nœuds de stockage.

- Les clients qui se connectent au service Load Balancer peuvent utiliser HTTPS ou HTTP, selon la façon dont vous"configurer le point de terminaison de l'équilibreur de charge" .

  HTTPS fournit une communication sécurisée et cryptée TLS et est recommandé. Vous devez joindre un certificat de sécurité au point de terminaison.

  HTTP fournit une communication moins sécurisée et non chiffrée et ne doit être utilisé que pour les grilles de non-production ou de test.

- Les clients qui se connectent aux nœuds de stockage peuvent également utiliser HTTPS ou HTTP.

  HTTPS est la valeur par défaut et est recommandé.

HTTP fournit une communication moins sécurisée et non chiffrée, mais peut être facultative"activé" pour les grilles hors production ou de test.

- Les communications entre StorageGRID et le client sont chiffrées à l'aide de TLS.
- Les communications entre le service d'équilibrage de charge et les nœuds de stockage au sein de la grille sont chiffrées, que le point de terminaison de l'équilibrage de charge soit configuré pour accepter les connexions HTTP ou HTTPS.
- Les clients doivent fournir"En-têtes d'authentification HTTP" à StorageGRID pour effectuer des opérations d'API REST.

Certificats de sécurité et applications clientes

Dans tous les cas, les applications clientes peuvent établir des connexions TLS à l'aide d'un certificat de serveur personnalisé téléchargé par l'administrateur de la grille ou d'un certificat généré par le système StorageGRID :

- Lorsque les applications clientes se connectent au service Load Balancer, elles utilisent le certificat qui a été configuré pour le point de terminaison de l'équilibreur de charge. Chaque point de terminaison d'équilibrage de charge possède son propre certificat : soit un certificat de serveur personnalisé téléchargé par l'administrateur de la grille, soit un certificat que l'administrateur de la grille a généré dans StorageGRID lors de la configuration du point de terminaison.

  Voir "Considérations relatives à l'équilibrage de charge" .

- Lorsque les applications clientes se connectent directement à un nœud de stockage, elles utilisent soit les certificats de serveur générés par le système pour les nœuds de stockage lors de l'installation du système StorageGRID (qui sont signés par l'autorité de certification du système), soit un seul certificat de serveur personnalisé fourni pour la grille par un administrateur de grille. Voir "ajouter un certificat API S3 personnalisé" .

Les clients doivent être configurés pour faire confiance à l'autorité de certification qui a signé le certificat qu'ils utilisent pour établir des connexions TLS.

Algorithmes de hachage et de chiffrement pris en charge pour les bibliothèques TLS

Le système StorageGRID prend en charge un ensemble de suites de chiffrement que les applications clientes peuvent utiliser lors de l'établissement d'une session TLS. Pour configurer les chiffrements, accédez à **CONFIGURATION** > **Sécurité** > **Paramètres de sécurité** et sélectionnez **Politiques TLS et SSH**.

Versions prises en charge de TLS

StorageGRID prend en charge TLS 1.2 et TLS 1.3.

SSLv3 et TLS 1.1 (ou versions antérieures) ne sont plus pris en charge.

Utiliser l'assistant de configuration S3

Utiliser l'assistant de configuration S3 : considérations et exigences

Vous pouvez utiliser l'assistant de configuration S3 pour configurer StorageGRID comme système de stockage d'objets pour une application S3.

Quand utiliser l'assistant de configuration S3

L'assistant de configuration S3 vous guide à travers chaque étape de la configuration de StorageGRID pour une utilisation avec une application S3. Dans le cadre de l'exécution de l'assistant, vous téléchargez des fichiers que vous pouvez utiliser pour saisir des valeurs dans l'application S3. Utilisez l'assistant pour configurer votre système plus rapidement et vous assurer que vos paramètres sont conformes aux meilleures pratiques de StorageGRID .

Si vous avez le"Autorisation d'accès root" , vous pouvez terminer l'assistant de configuration S3 lorsque vous commencez à utiliser StorageGRID Grid Manager, ou vous pouvez accéder à l'assistant et le terminer à tout moment ultérieurement. Selon vos besoins, vous pouvez également configurer manuellement certains ou tous les éléments requis, puis utiliser l'assistant pour assembler les valeurs dont une application S3 a besoin.

Avant d'utiliser l'assistant

Avant d'utiliser l'assistant, vérifiez que vous avez rempli ces conditions préalables.

Obtenir des adresses IP et configurer des interfaces VLAN

Si vous configurez un groupe haute disponibilité (HA), vous savez à quels nœuds l'application S3 se connectera et quel réseau StorageGRID sera utilisé. Vous savez également quelles valeurs saisir pour le sous-réseau CIDR, l'adresse IP de la passerelle et les adresses IP virtuelles (VIP).

Si vous prévoyez d'utiliser un réseau local virtuel pour séparer le trafic de l'application S3, vous avez déjà configuré l'interface VLAN. Voir "Configurer les interfaces VLAN" .

Configurer la fédération d'identité et l'authentification unique

Si vous prévoyez d'utiliser la fédération d'identité ou l'authentification unique (SSO) pour votre système StorageGRID , vous avez activé ces fonctionnalités. Vous savez également quel groupe fédéré doit avoir un accès root pour le compte locataire que l'application S3 utilisera. Voir"Utiliser la fédération d'identité" et"Configurer l'authentification unique" .

Obtenir et configurer des noms de domaine

Vous savez quel nom de domaine complet (FQDN) utiliser pour StorageGRID. Les entrées du serveur de noms de domaine (DNS) mapperont ce nom de domaine complet aux adresses IP virtuelles (VIP) du groupe HA que vous créez à l'aide de l'assistant.

Si vous prévoyez d'utiliser des requêtes hébergées virtuellement de type S3, vous devez disposer"noms de domaine de point de terminaison S3 configurés" . Il est recommandé d'utiliser des requêtes de type hébergé virtuellement.

Examiner les exigences relatives à l'équilibreur de charge et aux certificats de sécurité

Si vous prévoyez d'utiliser l'équilibreur de charge StorageGRID , vous avez examiné les considérations générales relatives à l'équilibrage de charge. Vous disposez des certificats que vous allez télécharger ou des valeurs dont vous avez besoin pour générer un certificat.

Si vous prévoyez d'utiliser un point de terminaison d'équilibrage de charge externe (tiers), vous disposez du nom de domaine complet (FQDN), du port et du certificat pour cet équilibreur de charge.

Configurer toutes les connexions de fédération de grille

Si vous souhaitez autoriser le locataire S3 à cloner les données de compte et à répliquer les objets de compartiment sur une autre grille à l'aide d'une connexion de fédération de grille, confirmez les éléments suivants avant de démarrer l'assistant :

- Tu as"configuré la connexion à la fédération de grille" .

- Le statut de la connexion est **Connecté**.
- Vous disposez de l'autorisation d'accès root.

Accéder et terminer l'assistant de configuration S3

Vous pouvez utiliser l'assistant de configuration S3 pour configurer StorageGRID pour une utilisation avec une application S3. L'assistant de configuration fournit les valeurs dont l'application a besoin pour accéder à un bucket StorageGRID et enregistrer des objets.

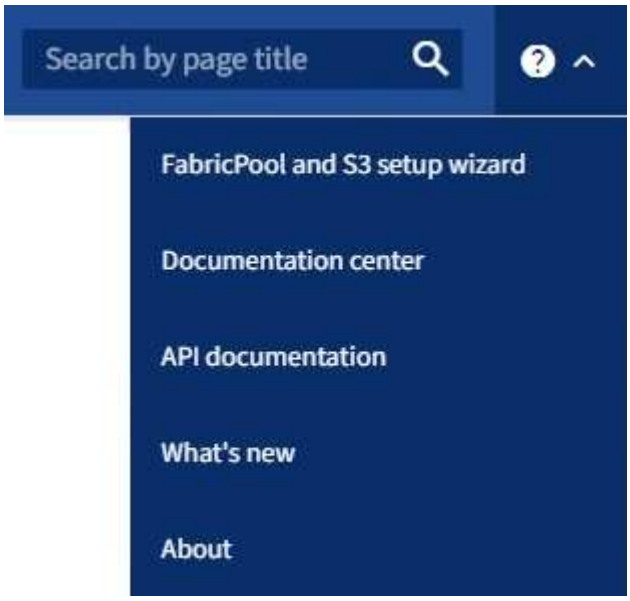
Avant de commencer

- Vous avez le"Autorisation d'accès root" .
- Vous avez examiné le"considérations et exigences" pour utiliser l'assistant.

Accéder à l'assistant

Étapes

1. Sign in au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
2. Si la bannière * Assistant de configuration FabricPool et S3* apparaît sur le tableau de bord, sélectionnez le lien dans la bannière. Si la bannière n'apparaît plus, sélectionnez l'icône d'aide dans la barre d'en-tête du gestionnaire de grille et sélectionnez * Assistant de configuration FabricPool et S3*.



3. Dans la section Application S3 de la page de l'assistant de configuration de FabricPool et S3, sélectionnez **Configurer maintenant**.

Étape 1 sur 6 : Configurer le groupe HA

Un groupe HA est un ensemble de nœuds contenant chacun le service StorageGRID Load Balancer. Un groupe HA peut contenir des nœuds de passerelle, des nœuds d'administration ou les deux.

Vous pouvez utiliser un groupe HA pour aider à maintenir les connexions de données S3 disponibles. Si l'interface active du groupe HA échoue, une interface de sauvegarde peut gérer la charge de travail avec peu d'impact sur les opérations S3.

Pour plus de détails sur cette tâche, voir"Gérer les groupes de haute disponibilité" .

Étapes

1. Si vous prévoyez d'utiliser un équilibreur de charge externe, vous n'avez pas besoin de créer un groupe HA. Sélectionnez **Ignorer cette étape** et accédez àÉtape 2 sur 6 : Configurer le point de terminaison de l'équilibreur de charge .
2. Pour utiliser l'équilibreur de charge StorageGRID , vous pouvez créer un nouveau groupe HA ou utiliser un groupe HA existant.

Créer un groupe HA

a. Pour créer un nouveau groupe HA, sélectionnez **Créer un groupe HA**.

b. Pour l'étape **Entrer les détails**, remplissez les champs suivants.

Champ	Description
Nom du groupe HA	Un nom d'affichage unique pour ce groupe HA.
Description (facultatif)	La description de ce groupe HA.

c. Pour l'étape **Ajouter des interfaces**, sélectionnez les interfaces de nœud que vous souhaitez utiliser dans ce groupe HA.

Utilisez les en-têtes de colonnes pour trier les lignes ou saisissez un terme de recherche pour localiser les interfaces plus rapidement.

Vous pouvez sélectionner un ou plusieurs nœuds, mais vous ne pouvez sélectionner qu'une seule interface pour chaque nœud.

d. Pour l'étape **Prioriser les interfaces**, déterminez l'interface principale et toutes les interfaces de sauvegarde pour ce groupe HA.

Faites glisser les lignes pour modifier les valeurs dans la colonne **Ordre de priorité**.

La première interface de la liste est l'interface principale. L'interface principale est l'interface active sauf en cas de panne.

Si le groupe HA comprend plusieurs interfaces et que l'interface active échoue, les adresses IP virtuelles (VIP) se déplacent vers la première interface de secours dans l'ordre de priorité. Si cette interface échoue, les adresses VIP se déplacent vers l'interface de sauvegarde suivante, et ainsi de suite. Une fois les échecs résolus, les adresses VIP reviennent à l'interface la plus prioritaire disponible.

e. Pour l'étape **Saisir les adresses IP**, remplissez les champs suivants.

Champ	Description
Sous-réseau CIDR	L'adresse du sous-réseau VIP en notation CIDR : une adresse IPv4 suivie d'une barre oblique et de la longueur du sous-réseau (0-32). L'adresse réseau ne doit avoir aucun bit d'hôte défini. Par exemple : `192.16.0.0/22` .
Adresse IP de la passerelle (facultatif)	Si les adresses IP S3 utilisées pour accéder à StorageGRID ne se trouvent pas sur le même sous-réseau que les adresses VIP StorageGRID , saisissez l'adresse IP de la passerelle locale VIP StorageGRID . L'adresse IP de la passerelle locale doit se trouver dans le sous-réseau VIP.

Champ	Description
Adresse IP virtuelle	Saisissez au moins une et pas plus de dix adresses VIP pour l'interface active dans le groupe HA. Toutes les adresses VIP doivent se trouver dans le sous-réseau VIP. Au moins une adresse doit être IPv4. En option, vous pouvez spécifier des adresses IPv4 et IPv6 supplémentaires.

f. Sélectionnez **Créer un groupe HA**, puis sélectionnez **Terminer** pour revenir à l'assistant de configuration S3.

g. Sélectionnez **Continuer** pour accéder à l'étape de l'équilibrage de charge.

Utiliser le groupe HA existant

a. Pour utiliser un groupe HA existant, sélectionnez le nom du groupe HA dans **Sélectionner un groupe HA**.

b. Sélectionnez **Continuer** pour accéder à l'étape de l'équilibrage de charge.

Étape 2 sur 6 : Configurer le point de terminaison de l'équilibreur de charge

StorageGRID utilise un équilibreur de charge pour gérer la charge de travail des applications clientes. L'équilibrage de charge maximise la vitesse et la capacité de connexion sur plusieurs nœuds de stockage.

Vous pouvez utiliser le service d'équilibrage de charge StorageGRID , qui existe sur tous les nœuds de passerelle et d'administration, ou vous connecter à un équilibreur de charge externe (tiers). L'utilisation de l'équilibreur de charge StorageGRID est recommandée.

Pour plus de détails sur cette tâche, voir"Considérations relatives à l'équilibrage de charge" .

Pour utiliser le service StorageGRID Load Balancer, sélectionnez l'onglet * StorageGRID load balancer*, puis créez ou sélectionnez le point de terminaison de l'équilibreur de charge que vous souhaitez utiliser. Pour utiliser un équilibreur de charge externe, sélectionnez l'onglet **Équilibreur de charge externe** et fournissez des détails sur le système que vous avez déjà configuré.

Créer un point de terminaison

Étapes

1. Pour créer un point de terminaison d'équilibrage de charge, sélectionnez **Créer un point de terminaison**.
2. Pour l'étape **Saisir les détails du point de terminaison**, remplissez les champs suivants.

Champ	Description
Nom	Un nom descriptif pour le point de terminaison.
Port	Le port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est défini par défaut sur 10433 pour le premier point de terminaison que vous créez, mais vous pouvez saisir n'importe quel port externe inutilisé. Si vous entrez 80 ou 443, le point de terminaison est configuré uniquement sur les nœuds de passerelle, car ces ports sont réservés sur les nœuds d'administration. **Remarque :** les ports utilisés par d'autres services de grille ne sont pas autorisés. Voir le"Référence du port réseau" .
Type de client	Doit être **S3**.
Protocole réseau	Sélectionnez **HTTPS**. **Remarque** : la communication avec StorageGRID sans chiffrement TLS est prise en charge mais non recommandée.

3. Pour l'étape **Sélectionner le mode de liaison**, spécifiez le mode de liaison. Le mode de liaison contrôle la manière dont le point de terminaison est accessible à l'aide de n'importe quelle adresse IP ou à l'aide d'adresses IP et d'interfaces réseau spécifiques.

Mode	Description
Global (par défaut)	Les clients peuvent accéder au point de terminaison à l'aide de l'adresse IP de n'importe quel nœud de passerelle ou nœud d'administration, de l'adresse IP virtuelle (VIP) de n'importe quel groupe HA sur n'importe quel réseau ou d'un nom de domaine complet correspondant. Utilisez le paramètre **Global** (par défaut) sauf si vous devez restreindre l'accessibilité de ce point de terminaison.
IP virtuelles des groupes HA	Les clients doivent utiliser une adresse IP virtuelle (ou un nom de domaine complet correspondant) d'un groupe HA pour accéder à ce point de terminaison. Les points de terminaison avec ce mode de liaison peuvent tous utiliser le même numéro de port, à condition que les groupes HA que vous sélectionnez pour les points de terminaison ne se chevauchent pas.

Mode	Description
Interfaces de nœuds	Les clients doivent utiliser les adresses IP (ou les noms de domaine complets correspondants) des interfaces de nœuds sélectionnées pour accéder à ce point de terminaison.
Type de nœud	En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel nœud d'administration, soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel nœud de passerelle pour accéder à ce point de terminaison.

4. Pour l'étape Accès locataire, sélectionnez l'une des options suivantes :

Champ	Description
Autoriser tous les locataires (par défaut)	Tous les comptes locataires peuvent utiliser ce point de terminaison pour accéder à leurs buckets.
Autoriser les locataires sélectionnés	Seuls les comptes locataires sélectionnés peuvent utiliser ce point de terminaison pour accéder à leurs compartiments.
Bloquer les locataires sélectionnés	Les comptes locataires sélectionnés ne peuvent pas utiliser ce point de terminaison pour accéder à leurs compartiments. Tous les autres locataires peuvent utiliser ce point de terminaison.

5. Pour l'étape **Joindre le certificat**, sélectionnez l'une des options suivantes :

Champ	Description
Télécharger le certificat (recommandé)	Utilisez cette option pour télécharger un certificat de serveur signé par une autorité de certification, une clé privée de certificat et un ensemble d'autorité de certification facultatif.
Générer un certificat	Utilisez cette option pour générer un certificat auto-signé. Voir"Configurer les points de terminaison de l'équilibreur de charge" pour plus de détails sur ce qu'il faut saisir.
Utiliser le certificat StorageGRID S3	Utilisez cette option uniquement si vous avez déjà téléchargé ou généré une version personnalisée du certificat global StorageGRID . Voir"Configurer les certificats API S3" pour plus de détails.

6. Sélectionnez **Terminer** pour revenir à l'assistant de configuration S3.
7. Sélectionnez **Continuer** pour accéder à l'étape du locataire et du bucket.

> Les modifications apportées à un certificat de point de terminaison peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

Utiliser le point de terminaison de l'équilibreur de charge existant

Étapes

1. Pour utiliser un point de terminaison existant, sélectionnez son nom dans **Sélectionner un point de terminaison d'équilibrage de charge**.
2. Sélectionnez **Continuer** pour accéder à l'étape du locataire et du bucket.

Utiliser un équilibreur de charge externe

Étapes

1. Pour utiliser un équilibreur de charge externe, remplissez les champs suivants.

Champ	Description
Nom de domaine complet	Le nom de domaine complet (FQDN) de l'équilibreur de charge externe.
Port	Le numéro de port que l'application S3 utilisera pour se connecter à l'équilibreur de charge externe.
Certificat	Copiez le certificat du serveur pour l'équilibreur de charge externe et collez-le dans ce champ.

2. Sélectionnez **Continuer** pour accéder à l'étape du locataire et du bucket.

Étape 3 sur 6 : Créer un locataire et un bucket

Un locataire est une entité qui peut utiliser des applications S3 pour stocker et récupérer des objets dans StorageGRID. Chaque locataire possède ses propres utilisateurs, clés d'accès, buckets, objets et un ensemble spécifique de fonctionnalités.

Un bucket est un conteneur utilisé pour stocker les objets et les métadonnées d'objet d'un locataire. Bien que les locataires puissent avoir de nombreux compartiments, l'assistant vous aide à créer un locataire et un compartiment de la manière la plus rapide et la plus simple. Si vous devez ajouter des buckets ou définir des options ultérieurement, vous pouvez utiliser le gestionnaire de locataires.

Pour plus de détails sur cette tâche, voir"Créer un compte locataire" et"Créer un bucket S3" .

Étapes

1. Saisissez un nom pour le compte locataire.

   Les noms des locataires n'ont pas besoin d'être uniques. Lorsque le compte locataire est créé, il reçoit un ID de compte numérique unique.

2. Définissez l'accès root pour le compte locataire, selon que votre système StorageGRID utilise"fédération d'identité" ,"authentification unique (SSO)" , ou les deux.

Option	Fais ceci
Si la fédération d'identité n'est pas activée	Spécifiez le mot de passe à utiliser lors de la connexion au locataire en tant qu'utilisateur root local.

Option	Fais ceci
Si la fédération d'identité est activée	a. Sélectionnez un groupe fédéré existant pour avoir"Autorisation d'accès root" pour le locataire. b. Vous pouvez également spécifier le mot de passe à utiliser lors de la connexion au locataire en tant qu'utilisateur root local.
Si la fédération d'identité et l'authentification unique (SSO) sont activées	Sélectionnez un groupe fédéré existant pour avoir"Autorisation d'accès root" pour le locataire. Aucun utilisateur local ne peut se connecter.

3. Si vous souhaitez que l'assistant crée l'ID de clé d'accès et la clé d'accès secrète pour l'utilisateur root, sélectionnez **Créer automatiquement la clé d'accès S3 de l'utilisateur root**.

   Sélectionnez cette option si le seul utilisateur du locataire sera l'utilisateur root. Si d'autres utilisateurs utilisent ce locataire,"utiliser Tenant Manager" pour configurer les clés et les autorisations.

4. Si vous souhaitez créer un bucket pour ce locataire maintenant, sélectionnez **Créer un bucket pour ce locataire**.

   Si le verrouillage d'objet S3 est activé pour la grille, le compartiment créé à cette étape n'a pas le verrouillage d'objet S3 activé. Si vous devez utiliser un bucket S3 Object Lock pour cette application S3, ne choisissez pas de créer un bucket maintenant. Utilisez plutôt Tenant Manager pour"créer le bucket" plus tard.

   a. Saisissez le nom du bucket que l'application S3 utilisera. Par exemple : `s3-bucket` .

      Vous ne pouvez pas modifier le nom du bucket après l'avoir créé.

   b. Sélectionnez la **Région** pour ce bucket.

      Utiliser la région par défaut(`us-east-1`) sauf si vous prévoyez d'utiliser ILM à l'avenir pour filtrer les objets en fonction de la région du bucket.

5. Sélectionnez **Créer et continuer**.

Étape 4 sur 6 : Télécharger les données

À l'étape de téléchargement des données, vous pouvez télécharger un ou deux fichiers pour enregistrer les détails de ce que vous venez de configurer.

Étapes

1. Si vous avez sélectionné **Créer automatiquement la clé d'accès S3 de l'utilisateur root**, effectuez l'une des opérations suivantes ou les deux :
   - Sélectionnez **Télécharger les clés d'accès** pour télécharger un `.csv` fichier contenant le nom du compte du locataire, l'ID de la clé d'accès et la clé d'accès secrète.
   - Sélectionnez l'icône de copie ( ) pour copier l'ID de la clé d'accès et la clé d'accès secrète dans le presse-papiers.
2. Sélectionnez **Télécharger les valeurs de configuration** pour télécharger un `.txt` fichier contenant les paramètres du point de terminaison de l'équilibreur de charge, du locataire, du bucket et de l'utilisateur root.

3. Enregistrez ces informations dans un endroit sûr.

> Ne fermez pas cette page tant que vous n'avez pas copié les deux clés d'accès. Les clés ne seront plus disponibles après avoir fermé cette page. Assurez-vous de sauvegarder ces informations dans un endroit sûr, car elles peuvent être utilisées pour obtenir des données de votre système StorageGRID .

4. Si vous y êtes invité, cochez la case pour confirmer que vous avez téléchargé ou copié les clés.
5. Sélectionnez **Continuer** pour accéder à l'étape de la règle et de la politique ILM.

Étape 5 sur 6 : Examiner la règle ILM et la politique ILM pour S3

Les règles de gestion du cycle de vie des informations (ILM) contrôlent le placement, la durée et le comportement d'ingestion de tous les objets de votre système StorageGRID . La politique ILM incluse avec StorageGRID crée deux copies répliquées de tous les objets. Cette politique est en vigueur jusqu'à ce que vous activiez au moins une nouvelle politique.

Étapes

1. Consultez les informations fournies sur la page.
2. Si vous souhaitez ajouter des instructions spécifiques pour les objets appartenant au nouveau locataire ou au nouveau bucket, créez une nouvelle règle et une nouvelle politique. Voir"Créer une règle ILM" et"Utiliser les politiques ILM" .
3. Sélectionnez **J'ai lu ces étapes et je comprends ce que je dois faire**.
4. Cochez la case pour indiquer que vous comprenez ce qu'il faut faire ensuite.
5. Sélectionnez **Continuer** pour accéder au **Résumé**.

Étape 6 sur 6 : Révision du résumé

Étapes

1. Consultez le résumé.
2. Prenez note des détails dans les étapes suivantes, qui décrivent la configuration supplémentaire qui pourrait être nécessaire avant de vous connecter au client S3. Par exemple, la sélection de * Sign in en tant que root* vous amène au gestionnaire de locataires, où vous pouvez ajouter des utilisateurs locataires, créer des buckets supplémentaires et mettre à jour les paramètres des buckets.
3. Sélectionnez **Terminer**.
4. Configurez l'application à l'aide du fichier que vous avez téléchargé depuis StorageGRID ou des valeurs que vous avez obtenues manuellement.

Gérer les groupes HA

Que sont les groupes de haute disponibilité (HA) ?

Les groupes haute disponibilité (HA) fournissent des connexions de données hautement disponibles pour les clients S3 et des connexions hautement disponibles au Grid Manager et au Tenant Manager.

Vous pouvez regrouper les interfaces réseau de plusieurs nœuds d'administration et de passerelle dans un groupe haute disponibilité (HA). Si l'interface active du groupe HA échoue, une interface de sauvegarde peut gérer la charge de travail.

Chaque groupe HA fournit un accès aux services partagés sur les nœuds sélectionnés.

- Les groupes HA qui incluent des nœuds de passerelle, des nœuds d'administration ou les deux fournissent des connexions de données hautement disponibles pour les clients S3.
- Les groupes HA qui incluent uniquement des nœuds d'administration fournissent des connexions hautement disponibles au gestionnaire de grille et au gestionnaire de locataires.
- Un groupe HA qui comprend uniquement des appliances de services et des nœuds logiciels basés sur VMware peut fournir des connexions hautement disponibles pour"Locataires S3 qui utilisent S3 Select" . Les groupes HA sont recommandés lors de l'utilisation de S3 Select, mais pas obligatoires.

Comment créer un groupe HA ?

1. Vous sélectionnez une interface réseau pour un ou plusieurs nœuds d'administration ou nœuds de passerelle. Vous pouvez utiliser une interface Grid Network (eth0), une interface Client Network (eth2), une interface VLAN ou une interface d'accès que vous avez ajoutée au nœud.

   > Vous ne pouvez pas ajouter une interface à un groupe HA si elle dispose d'une adresse IP attribuée par DHCP.

2. Vous spécifiez une interface comme interface principale. L'interface principale est l'interface active sauf en cas de panne.
3. Vous déterminez l'ordre de priorité pour toutes les interfaces de sauvegarde.
4. Vous attribuez une à dix adresses IP virtuelles (VIP) au groupe. Les applications clientes peuvent utiliser n'importe laquelle de ces adresses VIP pour se connecter à StorageGRID.

Pour les instructions, voir"Configurer des groupes de haute disponibilité" .

Quelle est l'interface active ?

En fonctionnement normal, toutes les adresses VIP du groupe HA sont ajoutées à l'interface principale, qui est la première interface dans l'ordre de priorité. Tant que l'interface principale reste disponible, elle est utilisée lorsque les clients se connectent à n'importe quelle adresse VIP du groupe. Autrement dit, pendant le fonctionnement normal, l'interface principale est l'interface « active » du groupe.

De même, pendant le fonctionnement normal, toutes les interfaces de priorité inférieure pour le groupe HA agissent comme des interfaces de « secours ». Ces interfaces de sauvegarde ne sont pas utilisées à moins que l'interface principale (actuellement active) ne devienne indisponible.

Afficher l'état actuel du groupe HA d'un nœud

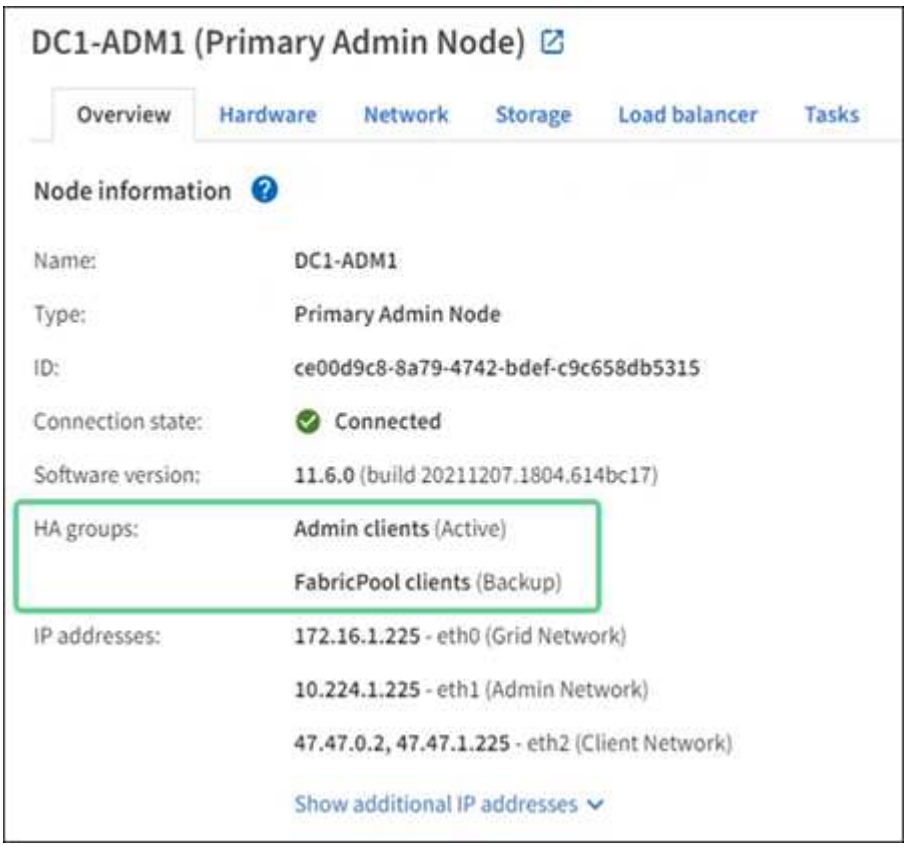
Pour voir si un nœud est affecté à un groupe HA et déterminer son état actuel, sélectionnez **NODES** > ***node***.

Si l'onglet **Vue d'ensemble** inclut une entrée pour les **groupes HA**, le nœud est attribué aux groupes HA répertoriés. La valeur après le nom du groupe est l'état actuel du nœud dans le groupe HA :

- **Actif** : Le groupe HA est actuellement hébergé sur ce nœud.
- **Sauvegarde** : Le groupe HA n'utilise pas actuellement ce nœud ; il s'agit d'une interface de sauvegarde.
- **Arrêté** : le groupe HA ne peut pas être hébergé sur ce nœud car le service Haute disponibilité (maintenu en vie) a été arrêté manuellement.
- **Erreur** : Le groupe HA ne peut pas être hébergé sur ce nœud en raison d'une ou plusieurs des raisons suivantes :

- Le service Load Balancer (nginx-gw) n'est pas en cours d'exécution sur le nœud.
- L'interface eth0 ou VIP du nœud est en panne.
- Le nœud est en panne.

Dans cet exemple, le nœud d'administration principal a été ajouté à deux groupes HA. Ce nœud est actuellement l'interface active pour le groupe de clients Admin et une interface de sauvegarde pour le groupe de clients FabricPool .



Que se passe-t-il lorsque l'interface active échoue ?

L'interface qui héberge actuellement les adresses VIP est l'interface active. Si le groupe HA comprend plusieurs interfaces et que l'interface active échoue, les adresses VIP se déplacent vers la première interface de sauvegarde disponible dans l'ordre de priorité. Si cette interface échoue, les adresses VIP se déplacent vers la prochaine interface de sauvegarde disponible, et ainsi de suite.

Le basculement peut être déclenché pour l'une des raisons suivantes :

- Le nœud sur lequel l'interface est configurée tombe en panne.
- Le nœud sur lequel l'interface est configurée perd la connectivité avec tous les autres nœuds pendant au moins 2 minutes.
- L'interface active tombe en panne.
- Le service Load Balancer s'arrête.
- Le service de haute disponibilité s'arrête.

Le basculement peut ne pas être déclenché par des pannes de réseau externes au nœud qui héberge l'interface active. De même, le basculement n'est pas déclenché par les services du Grid Manager ou du Tenant Manager.

Le processus de basculement ne prend généralement que quelques secondes et est suffisamment rapide pour que les applications clientes subissent peu d'impact et puissent compter sur des comportements de nouvelle tentative normaux pour continuer à fonctionner.

Lorsque l'échec est résolu et qu'une interface de priorité supérieure redevient disponible, les adresses VIP sont automatiquement déplacées vers l'interface de priorité la plus élevée disponible.

Comment les groupes HA sont-ils utilisés ?

Vous pouvez utiliser des groupes haute disponibilité (HA) pour fournir des connexions hautement disponibles à StorageGRID pour les données d'objet et pour une utilisation administrative.

- Un groupe HA peut fournir des connexions administratives hautement disponibles au Grid Manager ou au Tenant Manager.
- Un groupe HA peut fournir des connexions de données hautement disponibles pour les clients S3.
- Un groupe HA qui contient une seule interface vous permet de fournir plusieurs adresses VIP et de définir explicitement des adresses IPv6.

Un groupe HA ne peut fournir une haute disponibilité que si tous les nœuds inclus dans le groupe fournissent les mêmes services. Lorsque vous créez un groupe HA, ajoutez des interfaces à partir des types de nœuds qui fournissent les services dont vous avez besoin.

- **Nœuds d'administration** : inclure le service d'équilibrage de charge et activer l'accès au gestionnaire de grille ou au gestionnaire de locataires.
- **Nœuds de passerelle** : inclure le service d'équilibrage de charge.

Objectif du groupe HA	Ajouter des nœuds de ce type au groupe HA
Accès au Grid Manager	• Nœud d'administration principal (**Primaire**) • Nœuds d'administration non principaux **Remarque :** le nœud d'administration principal doit être l'interface principale. Certaines procédures de maintenance ne peuvent être effectuées qu'à partir du nœud d'administration principal.
Accès au gestionnaire de locataires uniquement	• Nœuds d'administration principaux ou non principaux
Accès client S3 – Service d'équilibrage de charge	• Nœuds d'administration • Nœuds de passerelle

Objectif du groupe HA	Ajouter des nœuds de ce type au groupe HA
Accès client S3 pour"S3 Select"	• Appareils de service • Nœuds logiciels basés sur VMware **Remarque** : les groupes HA sont recommandés lors de l'utilisation de S3 Select, mais pas obligatoires.

Limitations de l'utilisation des groupes HA avec Grid Manager ou Tenant Manager

Si un service Grid Manager ou Tenant Manager échoue, le basculement du groupe HA n'est pas déclenché.

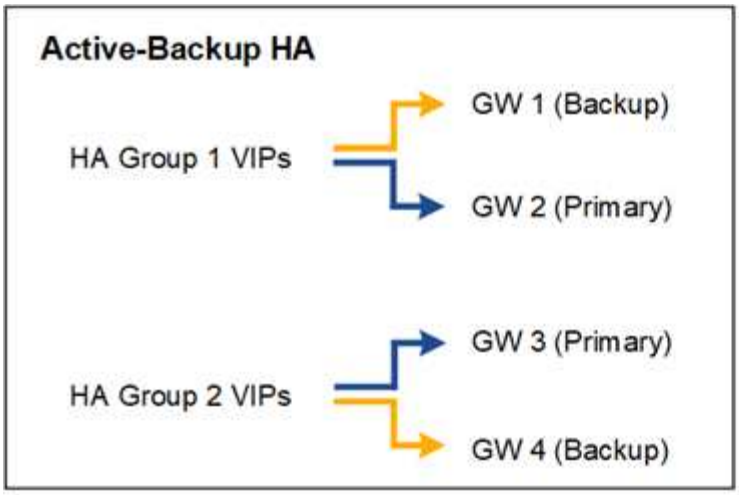
Si vous êtes connecté au Grid Manager ou au Tenant Manager lors du basculement, vous êtes déconnecté et devez vous reconnecter pour reprendre votre tâche.

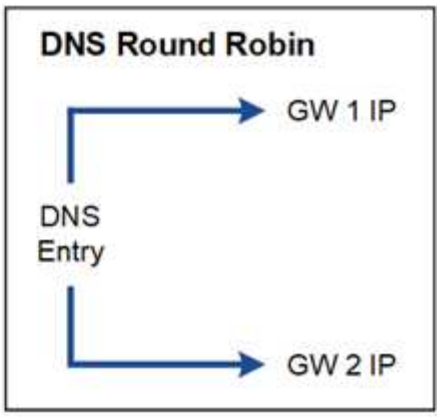
Certaines procédures de maintenance ne peuvent pas être effectuées lorsque le nœud d'administration principal n'est pas disponible. Lors du basculement, vous pouvez utiliser Grid Manager pour surveiller votre système StorageGRID .

Options de configuration pour les groupes HA

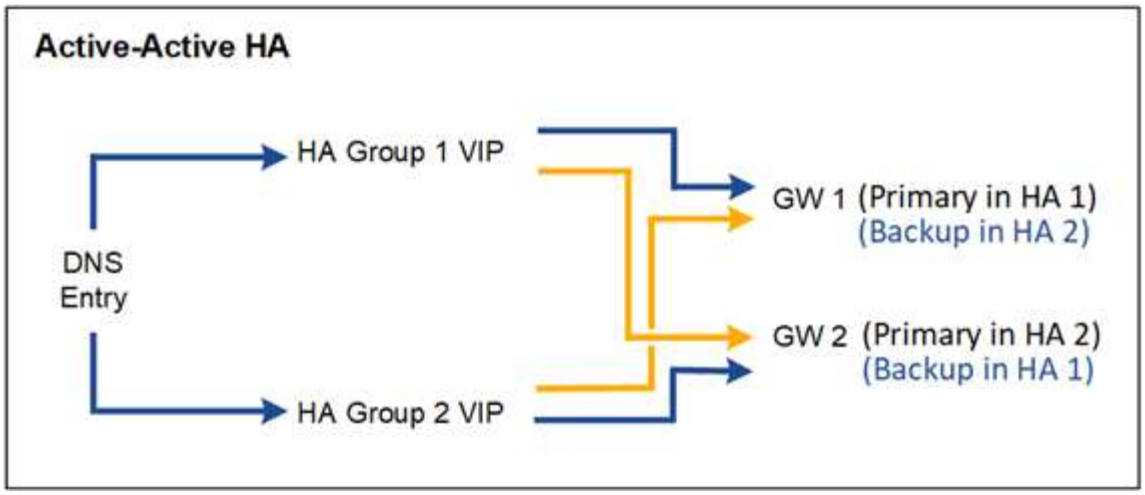
Les diagrammes suivants fournissent des exemples de différentes manières de configurer des groupes HA. Chaque option présente des avantages et des inconvénients.

Dans les diagrammes, le bleu indique l'interface principale du groupe HA et le jaune indique l'interface de sauvegarde du groupe HA.





GW = Gateway Node
VIP = Virtual IP address



Le tableau résume les avantages de chaque configuration HA présentée dans le diagramme.

Configuration	Avantages	Inconvénients
HA de sauvegarde active	• Géré par StorageGRID sans dépendances externes. • Basculement rapide.	• Un seul nœud dans un groupe HA est actif. Au moins un nœud par groupe HA sera inactif.
DNS Round Robin	• Augmentation du débit global. • Aucun hôte inactif.	• Basculement lent, qui peut dépendre du comportement du client. • Nécessite une configuration matérielle en dehors de StorageGRID. • Nécessite un contrôle de santé mis en œuvre par le client.

Configuration	Avantages	Inconvénients
HA actif-actif	• Le trafic est réparti sur plusieurs groupes HA. • Débit global élevé qui évolue avec le nombre de groupes HA. • Basculement rapide.	• Plus complexe à configurer. • Nécessite une configuration matérielle en dehors de StorageGRID. • Nécessite un contrôle de santé mis en œuvre par le client.

Configurer des groupes de haute disponibilité

Vous pouvez configurer des groupes de haute disponibilité (HA) pour fournir un accès hautement disponible aux services sur les nœuds d'administration ou les nœuds de passerelle.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès root" .
- Si vous prévoyez d'utiliser une interface VLAN dans un groupe HA, vous avez créé l'interface VLAN. Voir "Configurer les interfaces VLAN" .
- Si vous prévoyez d'utiliser une interface d'accès pour un nœud dans un groupe HA, vous avez créé l'interface :
  - **Red Hat Enterprise Linux (avant l'installation du nœud)**:"Créer des fichiers de configuration de nœud"
  - **Ubuntu ou Debian (avant d'installer le nœud)** :"Créer des fichiers de configuration de nœud"
  - **Linux (après l'installation du nœud)**:"Linux : ajouter des interfaces trunk ou d'accès à un nœud"
  - **VMware (après l'installation du nœud)**:"VMware : ajouter des interfaces de jonction ou d'accès à un nœud"

Créer un groupe de haute disponibilité

Lorsque vous créez un groupe de haute disponibilité, vous sélectionnez une ou plusieurs interfaces et les organisez par ordre de priorité. Ensuite, vous attribuez une ou plusieurs adresses VIP au groupe.

Une interface doit être disponible pour qu'un nœud de passerelle ou un nœud d'administration soit inclus dans un groupe HA. Un groupe HA ne peut utiliser qu'une seule interface pour un nœud donné ; cependant, d'autres interfaces pour le même nœud peuvent être utilisées dans d'autres groupes HA.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION** > **Réseau** > **Groupes de haute disponibilité**.
2. Sélectionnez **Créer**.

Entrez les détails du groupe HA

Étapes

1. Fournissez un nom unique pour le groupe HA.

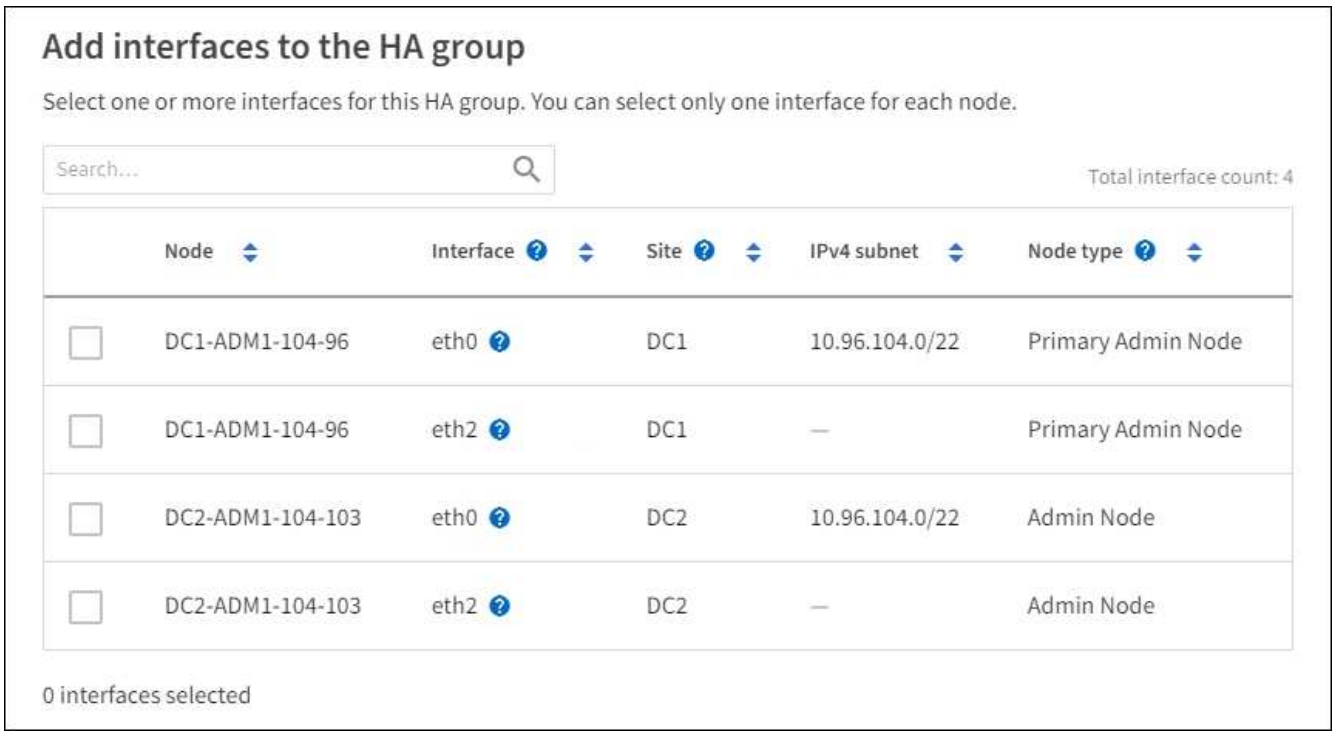
2. Si vous le souhaitez, saisissez une description pour le groupe HA.
3. Sélectionnez **Continuer**.

Ajouter des interfaces au groupe HA

Étapes

1. Sélectionnez une ou plusieurs interfaces à ajouter à ce groupe HA.

   Utilisez les en-têtes de colonnes pour trier les lignes ou saisissez un terme de recherche pour localiser les interfaces plus rapidement.

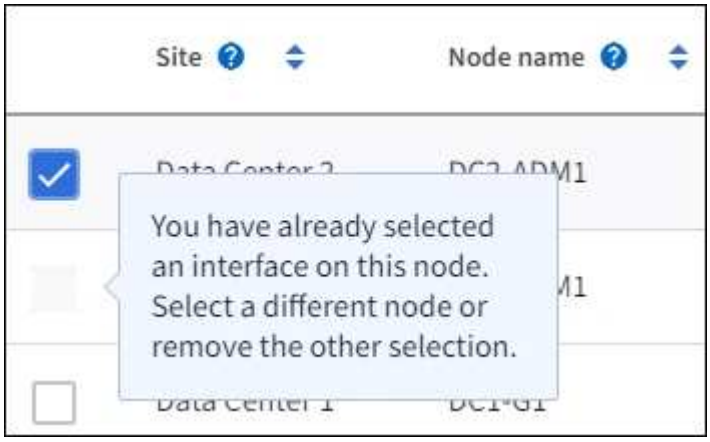


> Après avoir créé une interface VLAN, attendez jusqu'à 5 minutes pour que la nouvelle interface apparaisse dans le tableau.

Lignes directrices pour la sélection des interfaces

- Vous devez sélectionner au moins une interface.
- Vous ne pouvez sélectionner qu'une seule interface pour un nœud.
- Si le groupe HA est destiné à la protection HA des services du nœud d'administration, qui incluent le gestionnaire de grille et le gestionnaire de locataires, sélectionnez les interfaces sur les nœuds d'administration uniquement.
- Si le groupe HA est destiné à la protection HA du trafic client S3, sélectionnez les interfaces sur les nœuds d'administration, les nœuds de passerelle ou les deux.
- Si vous sélectionnez des interfaces sur différents types de nœuds, une note d'information s'affiche. Il est rappelé qu'en cas de basculement, les services fournis par le nœud précédemment actif peuvent ne pas être disponibles sur le nœud nouvellement actif. Par exemple, un nœud de passerelle de sauvegarde ne peut pas fournir une protection HA des services du nœud d'administration. De même, un nœud d'administration de sauvegarde ne peut pas effectuer toutes les procédures de maintenance que le nœud d'administration principal peut fournir.

- Si vous ne pouvez pas sélectionner une interface, sa case à cocher est désactivée. L'info-bulle fournit plus d'informations.



- Vous ne pouvez pas sélectionner une interface si sa valeur de sous-réseau ou sa passerelle est en conflit avec une autre interface sélectionnée.
- Vous ne pouvez pas sélectionner une interface configurée si elle ne possède pas d'adresse IP statique.

2. Sélectionnez **Continuer**.

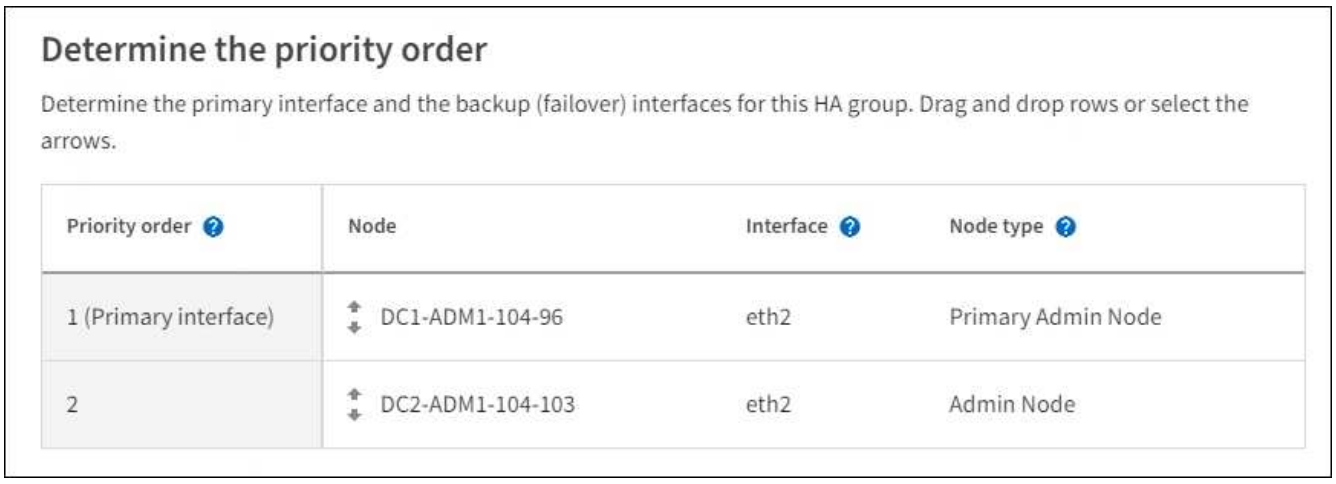
Déterminer l'ordre de priorité

Si le groupe HA comprend plusieurs interfaces, vous pouvez déterminer quelle est l'interface principale et quelles sont les interfaces de sauvegarde (basculement). Si l'interface principale échoue, les adresses VIP se déplacent vers l'interface de priorité la plus élevée disponible. Si cette interface échoue, les adresses VIP se déplacent vers l'interface de priorité la plus élevée disponible, et ainsi de suite.

Étapes

1. Faites glisser les lignes dans la colonne **Ordre de priorité** pour déterminer l'interface principale et toutes les interfaces de sauvegarde.

   La première interface de la liste est l'interface principale. L'interface principale est l'interface active sauf en cas de panne.



Si le groupe HA fournit un accès au gestionnaire de grille, vous devez sélectionner une interface sur le nœud d'administration principal pour être l'interface principale. Certaines procédures de maintenance ne peuvent être effectuées qu'à partir du nœud d'administration principal.

2. Sélectionnez **Continuer**.

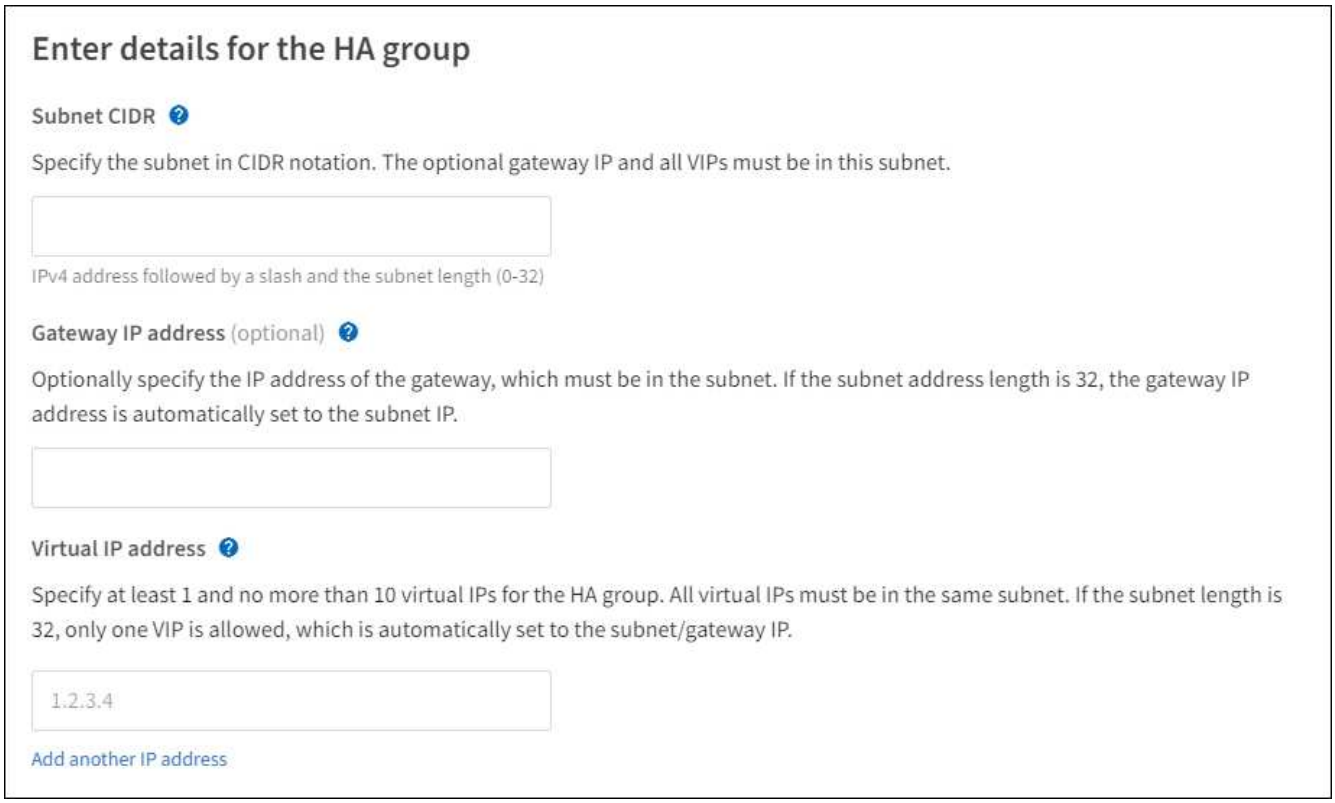
Entrez les adresses IP

Étapes

1. Dans le champ **Sous-réseau CIDR**, spécifiez le sous-réseau VIP en notation CIDR : une adresse IPv4 suivie d'une barre oblique et de la longueur du sous-réseau (0-32).

   L'adresse réseau ne doit avoir aucun bit d'hôte défini. Par exemple : `192.16.0.0/22` .

   Si vous utilisez un préfixe 32 bits, l'adresse réseau VIP sert également d'adresse de passerelle et d'adresse VIP.



2. En option, si des clients administratifs ou locataires S3 accèdent à ces adresses VIP à partir d'un sous-réseau différent, saisissez l'**adresse IP de la passerelle**. L'adresse de la passerelle doit être dans le sous-réseau VIP.

   Les utilisateurs clients et administrateurs utiliseront cette passerelle pour accéder aux adresses IP virtuelles.

3. Saisissez au moins une et pas plus de dix adresses VIP pour l'interface active dans le groupe HA. Toutes les adresses VIP doivent se trouver dans le sous-réseau VIP et toutes seront actives en même temps sur l'interface active.

Vous devez fournir au moins une adresse IPv4. En option, vous pouvez spécifier des adresses IPv4 et IPv6 supplémentaires.

4. Sélectionnez **Créer un groupe HA** et sélectionnez **Terminer**.

   Le groupe HA est créé et vous pouvez désormais utiliser les adresses IP virtuelles configurées.

Prochaines étapes

Si vous utilisez ce groupe HA pour l'équilibrage de charge, créez un point de terminaison d'équilibrage de charge pour déterminer le port et le protocole réseau et pour joindre tous les certificats requis. Voir "Configurer les points de terminaison de l'équilibreur de charge" .

Modifier un groupe de haute disponibilité

Vous pouvez modifier un groupe haute disponibilité (HA) pour changer son nom et sa description, ajouter ou supprimer des interfaces, modifier l'ordre de priorité ou ajouter ou mettre à jour des adresses IP virtuelles.

Par exemple, vous devrez peut-être modifier un groupe HA si vous souhaitez supprimer le nœud associé à une interface sélectionnée dans une procédure de mise hors service d'un site ou d'un nœud.

Étapes

1. Sélectionnez **CONFIGURATION** > **Réseau** > **Groupes de haute disponibilité**.

   La page Groupes de haute disponibilité affiche tous les groupes HA existants.

2. Cochez la case correspondant au groupe HA que vous souhaitez modifier.
3. Effectuez l'une des opérations suivantes, en fonction de ce que vous souhaitez mettre à jour :
   - Sélectionnez **Actions** > **Modifier l'adresse IP virtuelle** pour ajouter ou supprimer des adresses VIP.
   - Sélectionnez **Actions** > **Modifier le groupe HA** pour mettre à jour le nom ou la description du groupe, ajouter ou supprimer des interfaces, modifier l'ordre de priorité ou ajouter ou supprimer des adresses VIP.
4. Si vous avez sélectionné **Modifier l'adresse IP virtuelle** :
   a. Mettre à jour les adresses IP virtuelles pour le groupe HA.
   b. Sélectionnez **Enregistrer**.
   c. Sélectionnez **Terminer**.
5. Si vous avez sélectionné **Modifier le groupe HA** :
   a. Vous pouvez également mettre à jour le nom ou la description du groupe.
   b. Vous pouvez également cocher ou décocher les cases pour ajouter ou supprimer des interfaces.

      > Si le groupe HA fournit un accès au gestionnaire de grille, vous devez sélectionner une interface sur le nœud d'administration principal pour être l'interface principale. Certaines procédures de maintenance ne peuvent être effectuées qu'à partir du nœud d'administration principal

   c. Vous pouvez également faire glisser les lignes pour modifier l'ordre de priorité de l'interface principale et de toutes les interfaces de sauvegarde pour ce groupe HA.
   d. En option, mettez à jour les adresses IP virtuelles.

e. Sélectionnez **Enregistrer** puis **Terminer**.

Supprimer un groupe de haute disponibilité

Vous pouvez supprimer un ou plusieurs groupes de haute disponibilité (HA) à la fois.

> Vous ne pouvez pas supprimer un groupe HA s'il est lié à un point de terminaison d'équilibrage de charge. Pour supprimer un groupe HA, vous devez le supprimer de tous les points de terminaison d'équilibrage de charge qui l'utilisent.

Pour éviter toute interruption du client, mettez à jour toutes les applications clientes S3 concernées avant de supprimer un groupe HA. Mettez à jour chaque client pour se connecter à l'aide d'une autre adresse IP, par exemple, l'adresse IP virtuelle d'un groupe HA différent ou l'adresse IP configurée pour une interface lors de l'installation.

Étapes

1. Sélectionnez **CONFIGURATION** > **Réseau** > **Groupes de haute disponibilité**.
2. Consultez la colonne **Points de terminaison de l'équilibreur de charge** pour chaque groupe HA que vous souhaitez supprimer. Si des points de terminaison d'équilibrage de charge sont répertoriés :
   a. Accédez à **CONFIGURATION** > **Réseau** > **Points de terminaison de l'équilibreur de charge**.
   b. Cochez la case correspondant au point de terminaison.
   c. Sélectionnez **Actions** > **Modifier le mode de liaison du point de terminaison**.
   d. Mettez à jour le mode de liaison pour supprimer le groupe HA.
   e. Sélectionnez **Enregistrer les modifications**.
3. Si aucun point de terminaison d'équilibrage de charge n'est répertorié, cochez la case correspondant à chaque groupe HA que vous souhaitez supprimer.
4. Sélectionnez **Actions** > **Supprimer le groupe HA**.
5. Consultez le message et sélectionnez **Supprimer le groupe HA** pour confirmer votre sélection.

   Tous les groupes HA que vous avez sélectionnés sont supprimés. Une bannière de réussite verte apparaît sur la page Groupes de haute disponibilité.

Gérer l'équilibrage de charge

Considérations relatives à l'équilibrage de charge

Vous pouvez utiliser l'équilibrage de charge pour gérer les charges de travail d'ingestion et de récupération des clients S3.

Qu'est-ce que l'équilibrage de charge ?

Lorsqu'une application cliente enregistre ou récupère des données à partir d'un système StorageGRID , StorageGRID utilise un équilibreur de charge pour gérer la charge de travail d'ingestion et de récupération. L'équilibrage de charge maximise la vitesse et la capacité de connexion en répartissant la charge de travail sur plusieurs nœuds de stockage.

Le service StorageGRID Load Balancer est installé sur tous les nœuds d'administration et tous les nœuds de passerelle et fournit un équilibrage de charge de couche 7. Il effectue la terminaison TLS (Transport Layer Security) des demandes client, inspecte les demandes et établit de nouvelles connexions sécurisées aux

nœuds de stockage.

Le service d'équilibrage de charge sur chaque nœud fonctionne indépendamment lors du transfert du trafic client vers les nœuds de stockage. Grâce à un processus de pondération, le service Load Balancer achemine davantage de requêtes vers les nœuds de stockage avec une disponibilité CPU plus élevée.

> Bien que le service StorageGRID Load Balancer soit le mécanisme d'équilibrage de charge recommandé, vous souhaiterez peut-être intégrer un équilibreur de charge tiers à la place. Pour plus d'informations, contactez votre représentant de compte NetApp ou reportez-vous à "TR-4626 : Équilibreurs de charge tiers et globaux StorageGRID" .

De combien de nœuds d'équilibrage de charge ai-je besoin ?

En règle générale, chaque site de votre système StorageGRID doit inclure deux nœuds ou plus avec le service Load Balancer. Par exemple, un site peut inclure deux nœuds de passerelle ou un nœud d'administration et un nœud de passerelle. Assurez-vous qu'il existe une infrastructure réseau, matérielle ou de virtualisation adéquate pour chaque nœud d'équilibrage de charge, que vous utilisiez des appliances de services, des nœuds bare metal ou des nœuds basés sur des machines virtuelles (VM).

Qu'est-ce qu'un point de terminaison d'équilibrage de charge ?

Un point de terminaison d'équilibrage de charge définit le port et le protocole réseau (HTTPS ou HTTP) que les demandes d'application client entrantes et sortantes utiliseront pour accéder aux nœuds contenant le service d'équilibrage de charge. Le point de terminaison définit également le type de client (S3), le mode de liaison et éventuellement une liste de locataires autorisés ou bloqués.

Pour créer un point de terminaison d'équilibrage de charge, sélectionnez **CONFIGURATION** > **Réseau** > **Points de terminaison d'équilibrage de charge** ou suivez l'assistant de configuration de FabricPool et S3. Pour les instructions :

- "Configurer les points de terminaison de l'équilibreur de charge"
- "Utiliser l'assistant de configuration S3"
- "Utiliser l'assistant de configuration de FabricPool"

Considérations pour le port

Le port d'un point de terminaison d'équilibrage de charge est par défaut 10433 pour le premier point de terminaison que vous créez, mais vous pouvez spécifier n'importe quel port externe inutilisé entre 1 et 65535. Si vous utilisez le port 80 ou 443, le point de terminaison utilisera le service Load Balancer sur les nœuds de passerelle uniquement. Ces ports sont réservés sur les nœuds d'administration. Si vous utilisez le même port pour plusieurs points de terminaison, vous devez spécifier un mode de liaison différent pour chaque point de terminaison.

Les ports utilisés par d'autres services de grille ne sont pas autorisés. Voir le"Référence du port réseau" .

Considérations relatives au protocole réseau

Dans la plupart des cas, les connexions entre les applications clientes et StorageGRID doivent utiliser le cryptage TLS (Transport Layer Security). La connexion à StorageGRID sans cryptage TLS est prise en charge mais non recommandée, en particulier dans les environnements de production. Lorsque vous sélectionnez le protocole réseau pour le point de terminaison de l'équilibreur de charge StorageGRID , vous devez sélectionner **HTTPS**.

Considérations relatives aux certificats de point de terminaison d'équilibrage de charge

Si vous sélectionnez **HTTPS** comme protocole réseau pour le point de terminaison de l'équilibreur de charge, vous devez fournir un certificat de sécurité. Vous pouvez utiliser l'une de ces trois options lorsque vous créez le point de terminaison de l'équilibreur de charge :

- **Télécharger un certificat signé (recommandé)**. Ce certificat peut être signé par une autorité de certification (CA) publique ou privée. L'utilisation d'un certificat de serveur CA publiquement approuvé pour sécuriser la connexion est la meilleure pratique. Contrairement aux certificats générés, les certificats signés par une autorité de certification peuvent être renouvelés sans interruption, ce qui peut aider à éviter les problèmes d'expiration.

  Vous devez obtenir les fichiers suivants avant de créer le point de terminaison de l'équilibreur de charge :

  - Le fichier de certificat du serveur personnalisé.
  - Le fichier de clé privée du certificat de serveur personnalisé.
  - En option, un ensemble de certificats CA provenant de chaque autorité de certification émettrice intermédiaire.
- **Générer un certificat auto-signé**.
- **Utilisez le certificat global StorageGRID S3**. Vous devez télécharger ou générer une version personnalisée de ce certificat avant de pouvoir le sélectionner pour le point de terminaison de l'équilibreur de charge. Voir "Configurer les certificats API S3" .

De quelles valeurs ai-je besoin ?

Pour créer le certificat, vous devez connaître tous les noms de domaine et adresses IP que les applications clientes S3 utiliseront pour accéder au point de terminaison.

L'entrée **Subject DN** (Distinguished Name) du certificat doit inclure le nom de domaine complet que l'application cliente utilisera pour StorageGRID. Par exemple:

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

Si nécessaire, le certificat peut utiliser des caractères génériques pour représenter les noms de domaine complets de tous les nœuds d'administration et nœuds de passerelle exécutant le service d'équilibrage de charge. Par exemple, `*.storagegrid.example.com` utilise le caractère générique * pour représenter `adm1.storagegrid.example.com` et `gn1.storagegrid.example.com` .

Si vous prévoyez d'utiliser des requêtes de type hébergé virtuel S3, le certificat doit également inclure une entrée **Nom alternatif** pour chaque"Nom de domaine du point de terminaison S3" vous avez configuré, y compris tous les noms génériques. Par exemple:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

> Si vous utilisez des caractères génériques pour les noms de domaine, consultez le"Directives de renforcement pour les certificats de serveur" .

Vous devez également définir une entrée DNS pour chaque nom dans le certificat de sécurité.

Comment gérer les certificats expirés ?

> Si le certificat utilisé pour sécuriser la connexion entre l'application S3 et StorageGRID expire, l'application peut perdre temporairement l'accès à StorageGRID.

Pour éviter les problèmes d'expiration des certificats, suivez ces bonnes pratiques :

- Surveillez attentivement toutes les alertes qui avertissent de l'approche de la date d'expiration du certificat, telles que les alertes **Expiration du certificat du point de terminaison de l'équilibreur de charge** et **Expiration du certificat du serveur global pour l'API S3**.
- Gardez toujours les versions du certificat de l'application StorageGRID et S3 synchronisées. Si vous remplacez ou renouvelez le certificat utilisé pour un point de terminaison d'équilibrage de charge, vous devez remplacer ou renouveler le certificat équivalent utilisé par l'application S3.
- Utilisez un certificat CA signé publiquement. Si vous utilisez un certificat signé par une autorité de certification, vous pouvez remplacer les certificats sur le point d'expirer sans interruption.
- Si vous avez généré un certificat StorageGRID auto-signé et que ce certificat est sur le point d'expirer, vous devez remplacer manuellement le certificat dans StorageGRID et dans l'application S3 avant l'expiration du certificat existant.

Considérations sur le mode de liaison

Le mode de liaison vous permet de contrôler les adresses IP qui peuvent être utilisées pour accéder à un point de terminaison d'équilibrage de charge. Si un point de terminaison utilise un mode de liaison, les applications clientes ne peuvent accéder au point de terminaison que si elles utilisent une adresse IP autorisée ou son nom de domaine complet (FQDN) correspondant. Les applications clientes utilisant une autre adresse IP ou un nom de domaine complet ne peuvent pas accéder au point de terminaison.

Vous pouvez spécifier l'un des modes de liaison suivants :

- **Global** (par défaut) : les applications clientes peuvent accéder au point de terminaison à l'aide de l'adresse IP de n'importe quel nœud de passerelle ou nœud d'administration, de l'adresse IP virtuelle (VIP) de n'importe quel groupe HA sur n'importe quel réseau ou d'un nom de domaine complet correspondant. Utilisez ce paramètre sauf si vous devez restreindre l'accessibilité d'un point de terminaison.
- **IP virtuelles des groupes HA**. Les applications clientes doivent utiliser une adresse IP virtuelle (ou un nom de domaine complet correspondant) d'un groupe HA.
- **Interfaces de nœuds**. Les clients doivent utiliser les adresses IP (ou les noms de domaine complets correspondants) des interfaces de nœuds sélectionnées.
- **Type de nœud**. En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel nœud d'administration, soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel nœud de passerelle.

Considérations relatives à l'accès des locataires

L'accès des locataires est une fonctionnalité de sécurité facultative qui vous permet de contrôler les comptes de locataires StorageGRID qui peuvent utiliser un point de terminaison d'équilibrage de charge pour accéder à leurs buckets. Vous pouvez autoriser tous les locataires à accéder à un point de terminaison (par défaut), ou vous pouvez spécifier une liste des locataires autorisés ou bloqués pour chaque point de terminaison.

Vous pouvez utiliser cette fonctionnalité pour fournir une meilleure isolation de sécurité entre les locataires et leurs points de terminaison. Par exemple, vous pouvez utiliser cette fonctionnalité pour garantir que les documents top secret ou hautement classifiés appartenant à un locataire restent totalement inaccessibles aux autres locataires.

Aux fins du contrôle d'accès, le locataire est déterminé à partir des clés d'accès utilisées dans la demande du client. Si aucune clé d'accès n'est fournie dans le cadre de la demande (comme dans le cas d'un accès anonyme), le propriétaire du bucket est utilisé pour déterminer le locataire.

Exemple d'accès des locataires

Pour comprendre comment fonctionne cette fonctionnalité de sécurité, considérez l'exemple suivant :

1. Vous avez créé deux points de terminaison d'équilibrage de charge, comme suit :
   - Point de terminaison **public** : utilise le port 10443 et autorise l'accès à tous les locataires.
   - Point de terminaison **Top secret** : utilise le port 10444 et autorise l'accès au locataire **Top secret** uniquement. Tous les autres locataires ne peuvent pas accéder à ce point de terminaison.
2. Le `top-secret.pdf` se trouve dans un bucket appartenant au locataire **Top secret**.

Pour accéder au `top-secret.pdf` , un utilisateur du locataire **Top secret** peut émettre une requête GET pour `https://w.x.y.z:10444/top-secret.pdf` . Étant donné que ce locataire est autorisé à utiliser le point de terminaison 10444, l'utilisateur peut accéder à l'objet. Cependant, si un utilisateur appartenant à un autre locataire émet la même demande à la même URL, il reçoit immédiatement un message d'accès refusé. L'accès est refusé même si les informations d'identification et la signature sont valides.

Disponibilité du processeur

Le service d'équilibrage de charge sur chaque nœud d'administration et nœud de passerelle fonctionne indépendamment lors du transfert du trafic S3 vers les nœuds de stockage. Grâce à un processus de pondération, le service Load Balancer achemine davantage de requêtes vers les nœuds de stockage avec une disponibilité CPU plus élevée. Les informations sur la charge du processeur du nœud sont mises à jour toutes les quelques minutes, mais la pondération peut être mise à jour plus fréquemment. Une valeur de pondération de base minimale est attribuée à tous les nœuds de stockage, même si un nœud signale une utilisation à 100 % ou ne parvient pas à signaler son utilisation.

Dans certains cas, les informations sur la disponibilité du processeur sont limitées au site sur lequel se trouve le service Load Balancer.

Configurer les points de terminaison de l'équilibreur de charge

Les points de terminaison de l'équilibreur de charge déterminent les ports et les protocoles réseau que les clients S3 peuvent utiliser lors de la connexion à l'équilibreur de charge StorageGRID sur les nœuds de passerelle et d'administration. Vous pouvez également utiliser des points de terminaison pour accéder au gestionnaire de grille, au gestionnaire de locataires ou aux deux.

Les détails Swift ont été supprimés de cette version du site de documentation. Voir "Configurer les connexions client S3 et Swift" .

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès root" .
- Vous avez examiné le"considérations pour l'équilibrage de charge" .

- Si vous avez précédemment remappé un port que vous avez l'intention d'utiliser pour le point de terminaison de l'équilibreur de charge, vous avez"supprimé le remappage du port" .
- Vous avez créé tous les groupes de haute disponibilité (HA) que vous prévoyez d'utiliser. Les groupes HA sont recommandés, mais pas obligatoires. Voir "Gérer les groupes de haute disponibilité" .
- Si le point de terminaison de l'équilibreur de charge doit être utilisé par"Locataires S3 pour S3 Select" , il ne doit pas utiliser les adresses IP ou les noms de domaine complets de nœuds bare-metal. Seuls les dispositifs de services et les nœuds logiciels basés sur VMware sont autorisés pour les points de terminaison d'équilibrage de charge utilisés pour S3 Select.
- Vous avez configuré toutes les interfaces VLAN que vous prévoyez d'utiliser. Voir "Configurer les interfaces VLAN" .
- Si vous créez un point de terminaison HTTPS (recommandé), vous disposez des informations relatives au certificat du serveur.

> Les modifications apportées à un certificat de point de terminaison peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

  - Pour télécharger un certificat, vous avez besoin du certificat du serveur, de la clé privée du certificat et, éventuellement, d'un bundle CA.
  - Pour générer un certificat, vous avez besoin de tous les noms de domaine et adresses IP que les clients S3 utiliseront pour accéder au point de terminaison. Vous devez également connaître le sujet (Nom distinctif).
  - Si vous souhaitez utiliser le certificat API StorageGRID S3 (qui peut également être utilisé pour les connexions directes aux nœuds de stockage), vous avez déjà remplacé le certificat par défaut par un certificat personnalisé signé par une autorité de certification externe. Voir "Configurer les certificats API S3" .

Créer un point de terminaison d'équilibrage de charge

Chaque point de terminaison d'équilibrage de charge client S3 spécifie un port, un type de client (S3) et un protocole réseau (HTTP ou HTTPS). Les points de terminaison de l'équilibreur de charge de l'interface de gestion spécifient un port, un type d'interface et un réseau client non approuvé.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION** > **Réseau** > **Points de terminaison de l'équilibreur de charge**.
2. Pour créer un point de terminaison pour un client S3 ou Swift, sélectionnez l'onglet **Client S3 ou Swift**.
3. Pour créer un point de terminaison pour l'accès au Grid Manager, au Tenant Manager ou aux deux, sélectionnez l'onglet **Interface de gestion**.
4. Sélectionnez **Créer**.

Entrez les détails du point de terminaison

Étapes

1. Sélectionnez les instructions appropriées pour saisir les détails du type de point de terminaison que vous souhaitez créer.

Client S3 ou Swift

Champ	Description
Nom	Un nom descriptif pour le point de terminaison, qui apparaîtra dans le tableau de la page Points de terminaison de l'équilibreur de charge.
Port	Le port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est défini par défaut sur 10433 pour le premier point de terminaison que vous créez, mais vous pouvez saisir n'importe quel port externe inutilisé compris entre 1 et 65535. Si vous entrez **80** ou **8443**, le point de terminaison est configuré uniquement sur les nœuds de passerelle, sauf si vous avez libéré le port 8443. Vous pouvez ensuite utiliser le port 8443 comme point de terminaison S3, et le port sera configuré sur les nœuds de passerelle et d'administration.
Type de client	Le type d'application cliente qui utilisera ce point de terminaison, soit **S3** ou **Swift**.
Protocole réseau	Le protocole réseau que les clients utiliseront lors de la connexion à ce point de terminaison. • Sélectionnez **HTTPS** pour une communication sécurisée et cryptée TLS (recommandé). Vous devez joindre un certificat de sécurité avant de pouvoir enregistrer le point de terminaison. • Sélectionnez **HTTP** pour une communication moins sécurisée et non chiffrée. Utilisez HTTP uniquement pour une grille non destinée à la production.

Interface de gestion

Champ	Description
Nom	Un nom descriptif pour le point de terminaison, qui apparaîtra dans le tableau de la page Points de terminaison de l'équilibreur de charge.
Port	Le port StorageGRID que vous souhaitez utiliser pour accéder au Grid Manager, au Tenant Manager ou aux deux. • Gestionnaire de grille : **8443** • Gestionnaire locataire : **9443** • Gestionnaire de réseau et gestionnaire de locataire : **443** **Remarque** : Vous pouvez utiliser ces ports prédéfinis ou d'autres ports disponibles.
Type d'interface	Sélectionnez le bouton radio correspondant à l'interface StorageGRID à laquelle vous accéderez à l'aide de ce point de terminaison.

Champ	Description
Réseau de clients non fiables	Sélectionnez **Oui** si ce point de terminaison doit être accessible aux réseaux clients non approuvés. Sinon, sélectionnez **Non**. Lorsque vous sélectionnez **Oui**, le port est ouvert sur tous les réseaux clients non approuvés. **Remarque** : vous ne pouvez configurer un port pour qu'il soit ouvert ou fermé sur des réseaux clients non approuvés que lorsque vous créez le point de terminaison de l'équilibreur de charge.

1. Sélectionnez **Continuer**.

Sélectionnez un mode de reliure

Étapes

1. Sélectionnez un mode de liaison pour le point de terminaison afin de contrôler la manière dont le point de terminaison est accessible à l'aide de n'importe quelle adresse IP ou à l'aide d'adresses IP et d'interfaces réseau spécifiques.

   Certains modes de liaison sont disponibles pour les points de terminaison client ou les points de terminaison d'interface de gestion. Tous les modes pour les deux types de points de terminaison sont répertoriés ici.

Mode	Description
Global (par défaut pour les points de terminaison client)	Les clients peuvent accéder au point de terminaison à l'aide de l'adresse IP de n'importe quel nœud de passerelle ou nœud d'administration, de l'adresse IP virtuelle (VIP) de n'importe quel groupe HA sur n'importe quel réseau ou d'un nom de domaine complet correspondant. Utilisez le paramètre **Global** sauf si vous devez restreindre l'accessibilité de ce point de terminaison.
IP virtuelles des groupes HA	Les clients doivent utiliser une adresse IP virtuelle (ou un nom de domaine complet correspondant) d'un groupe HA pour accéder à ce point de terminaison. Les points de terminaison avec ce mode de liaison peuvent tous utiliser le même numéro de port, à condition que les groupes HA que vous sélectionnez pour les points de terminaison ne se chevauchent pas.
Interfaces de nœuds	Les clients doivent utiliser les adresses IP (ou les noms de domaine complets correspondants) des interfaces de nœuds sélectionnées pour accéder à ce point de terminaison.

Mode	Description
Type de nœud (points de terminaison client uniquement)	En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel nœud d'administration, soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel nœud de passerelle pour accéder à ce point de terminaison.
Tous les nœuds d'administration (par défaut pour les points de terminaison de l'interface de gestion)	Les clients doivent utiliser l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel nœud d'administration pour accéder à ce point de terminaison.

Si plusieurs points de terminaison utilisent le même port, StorageGRID utilise cet ordre de priorité pour décider quel point de terminaison utiliser : **IP virtuelles des groupes HA** > **Interfaces de nœud** > **Type de nœud** > **Global**.

Si vous créez des points de terminaison d'interface de gestion, seuls les nœuds d'administration sont autorisés.

2. Si vous avez sélectionné **IP virtuelles de groupes HA**, sélectionnez un ou plusieurs groupes HA.

   Si vous créez des points de terminaison d'interface de gestion, sélectionnez les VIP associés uniquement aux nœuds d'administration.

3. Si vous avez sélectionné **Interfaces de nœud**, sélectionnez une ou plusieurs interfaces de nœud pour chaque nœud d'administration ou nœud de passerelle que vous souhaitez associer à ce point de terminaison.
4. Si vous avez sélectionné **Type de nœud**, sélectionnez soit les nœuds d'administration, qui incluent à la fois le nœud d'administration principal et tous les nœuds d'administration non principaux, soit les nœuds de passerelle.

Contrôler l'accès des locataires

> Un point de terminaison d'interface de gestion peut contrôler l'accès des locataires uniquement lorsque le point de terminaison dispose dutype d'interface de Tenant Manager .

Étapes

1. Pour l'étape **Accès locataire**, sélectionnez l'une des options suivantes :

Champ	Description
Autoriser tous les locataires (par défaut)	Tous les comptes locataires peuvent utiliser ce point de terminaison pour accéder à leurs buckets. Vous devez sélectionner cette option si vous n'avez pas encore créé de compte locataire. Après avoir ajouté des comptes locataires, vous pouvez modifier le point de terminaison de l'équilibreur de charge pour autoriser ou bloquer des comptes spécifiques.

Champ	Description
Autoriser les locataires sélectionnés	Seuls les comptes locataires sélectionnés peuvent utiliser ce point de terminaison pour accéder à leurs compartiments.
Bloquer les locataires sélectionnés	Les comptes locataires sélectionnés ne peuvent pas utiliser ce point de terminaison pour accéder à leurs compartiments. Tous les autres locataires peuvent utiliser ce point de terminaison.

2. Si vous créez un point de terminaison **HTTP**, vous n'avez pas besoin de joindre un certificat. Sélectionnez **Créer** pour ajouter le nouveau point de terminaison de l'équilibreur de charge. Ensuite, allez àAprès avoir terminé . Sinon, sélectionnez **Continuer** pour joindre le certificat.

Joindre un certificat

Étapes

1. Si vous créez un point de terminaison **HTTPS**, sélectionnez le type de certificat de sécurité que vous souhaitez attacher au point de terminaison.

   Le certificat sécurise les connexions entre les clients S3 et le service Load Balancer sur le nœud d'administration ou les nœuds de passerelle.

   - **Télécharger le certificat**. Sélectionnez cette option si vous avez des certificats personnalisés à télécharger.
   - **Générer un certificat**. Sélectionnez cette option si vous disposez des valeurs nécessaires pour générer un certificat personnalisé.
   - **Utilisez le certificat StorageGRID S3**. Sélectionnez cette option si vous souhaitez utiliser le certificat API S3 global, qui peut également être utilisé pour les connexions directes aux nœuds de stockage.

     Vous ne pouvez pas sélectionner cette option à moins d'avoir remplacé le certificat API S3 par défaut, signé par l'autorité de certification de grille, par un certificat personnalisé signé par une autorité de certification externe. Voir "Configurer les certificats API S3" .

   - **Utiliser le certificat d'interface de gestion**. Sélectionnez cette option si vous souhaitez utiliser le certificat d'interface de gestion globale, qui peut également être utilisé pour les connexions directes aux nœuds d'administration.
2. Si vous n'utilisez pas le certificat StorageGRID S3, téléchargez ou générez le certificat.

Télécharger le certificat

a. Sélectionnez **Télécharger le certificat**.

b. Téléchargez les fichiers de certificat de serveur requis :

- **Certificat de serveur** : Le fichier de certificat de serveur personnalisé au format PEM.
- **Clé privée du certificat** : Le fichier de clé privée du certificat du serveur personnalisé(`.key`).

> Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2 048 bits ou plus.

- **CA bundle** : un fichier facultatif unique contenant les certificats de chaque autorité de certification émettrice intermédiaire (CA). Le fichier doit contenir chacun des fichiers de certificat CA codés en PEM, concaténés dans l'ordre de la chaîne de certificats.

c. Développez **Détails du certificat** pour voir les métadonnées de chaque certificat que vous avez téléchargé. Si vous avez téléchargé un bundle CA facultatif, chaque certificat s'affiche sur son propre onglet.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat ou sélectionnez **Télécharger le bundle CA** pour enregistrer le bundle de certificats.

  Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

  Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier le certificat PEM** ou **Copier le bundle CA PEM** pour copier le contenu du certificat afin de le coller ailleurs.

d. Sélectionnez **Créer**. + Le point de terminaison de l'équilibreur de charge est créé. Le certificat personnalisé est utilisé pour toutes les nouvelles connexions ultérieures entre les clients S3 ou l'interface de gestion et le point de terminaison.

Générer un certificat

a. Sélectionnez **Générer un certificat**.

b. Spécifiez les informations du certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine entièrement qualifiés à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.
propriété intellectuelle	Une ou plusieurs adresses IP à inclure dans le certificat.
Sujet (facultatif)	Sujet X.509 ou nom distinctif (DN) du propriétaire du certificat. Si aucune valeur n'est saisie dans ce champ, le certificat généré utilise le premier nom de domaine ou adresse IP comme nom commun du sujet (CN).

Champ	Description
Jours de validité	Nombre de jours après la création pendant lesquels le certificat expire.
Ajouter des extensions d'utilisation de clés	Si cette option est sélectionnée (par défaut et recommandé), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré. Ces extensions définissent l'objectif de la clé contenue dans le certificat. **Remarque** : laissez cette case à cocher sélectionnée, sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **Générer**.

d. Sélectionnez **Détails du certificat** pour voir les métadonnées du certificat généré.

   - Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

     Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

     Par exemple : `storagegrid_certificate.pem`

   - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.

e. Sélectionnez **Créer**.

   Le point de terminaison de l'équilibreur de charge est créé. Le certificat personnalisé est utilisé pour toutes les nouvelles connexions ultérieures entre les clients S3 ou l'interface de gestion et ce point de terminaison.

Après avoir terminé

Étapes

1. Si vous utilisez un DNS, assurez-vous que le DNS inclut un enregistrement pour associer le nom de domaine complet (FQDN) StorageGRID à chaque adresse IP que les clients utiliseront pour établir des connexions.

   L'adresse IP que vous entrez dans l'enregistrement DNS dépend du fait que vous utilisez ou non un groupe HA de nœuds d'équilibrage de charge :

   - Si vous avez configuré un groupe HA, les clients se connecteront aux adresses IP virtuelles de ce groupe HA.
   - Si vous n'utilisez pas de groupe HA, les clients se connecteront au service StorageGRID Load Balancer à l'aide de l'adresse IP d'un nœud de passerelle ou d'un nœud d'administration.

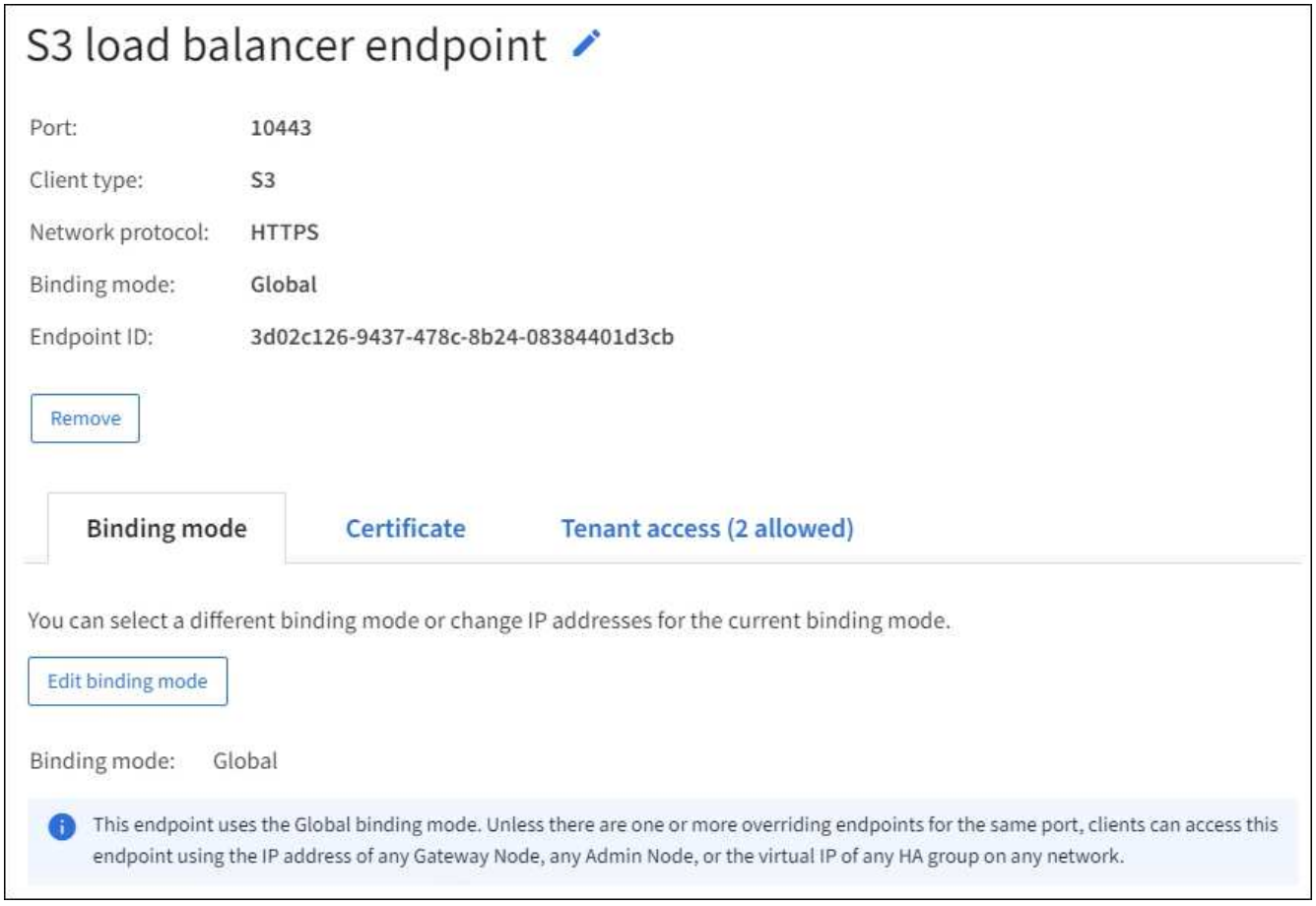
     Vous devez également vous assurer que l'enregistrement DNS référence tous les noms de domaine de point de terminaison requis, y compris tous les noms génériques.

2. Fournissez aux clients S3 les informations nécessaires pour se connecter au point de terminaison :
    - Numéro de port
    - Nom de domaine entièrement qualifié ou adresse IP
    - Tous les détails du certificat requis

Afficher et modifier les points de terminaison de l'équilibreur de charge

Vous pouvez afficher les détails des points de terminaison d'équilibrage de charge existants, y compris les métadonnées du certificat pour un point de terminaison sécurisé. Vous pouvez modifier certains paramètres d'un point de terminaison.

- Pour afficher les informations de base de tous les points de terminaison de l'équilibreur de charge, consultez les tableaux sur la page Points de terminaison de l'équilibreur de charge.
- Pour afficher tous les détails sur un point de terminaison spécifique, y compris les métadonnées du certificat, sélectionnez le nom du point de terminaison dans le tableau. Les informations affichées varient en fonction du type de point de terminaison et de sa configuration.



- Pour modifier un point de terminaison, utilisez le menu **Actions** sur la page Points de terminaison de l'équilibreur de charge.

> Si vous perdez l'accès à Grid Manager lors de la modification du port d'un point de terminaison d'interface de gestion, mettez à jour l'URL et le port pour retrouver l'accès.

Après avoir modifié un point de terminaison, vous devrez peut-être attendre jusqu'à 15 minutes pour que vos modifications soient appliquées à tous les nœuds.

Tâche	Menu Actions	Page de détails
Modifier le nom du point de terminaison	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez **Actions** > **Modifier le nom du point de terminaison**. c. Entrez le nouveau nom. d. Sélectionnez **Enregistrer**.	a. Sélectionnez le nom du point de terminaison pour afficher les détails. b. Sélectionnez l'icône d'édition . c. Entrez le nouveau nom. d. Sélectionnez **Enregistrer**.
Modifier le port du point de terminaison	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez **Actions** > **Modifier le port du point de terminaison** c. Entrez un numéro de port valide. d. Sélectionnez **Enregistrer**.	*n / A*
Modifier le mode de liaison du point de terminaison	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez **Actions** > **Modifier le mode de liaison du point de terminaison**. c. Mettez à jour le mode de liaison si nécessaire. d. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom du point de terminaison pour afficher les détails. b. Sélectionnez **Modifier le mode de liaison**. c. Mettez à jour le mode de liaison si nécessaire. d. Sélectionnez **Enregistrer les modifications**.
Modifier le certificat du point de terminaison	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez **Actions** > **Modifier le certificat du point de terminaison**. c. Téléchargez ou générez un nouveau certificat personnalisé ou commencez à utiliser le certificat S3 global, selon vos besoins. d. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom du point de terminaison pour afficher les détails. b. Sélectionnez l'onglet **Certificat**. c. Sélectionnez **Modifier le certificat**. d. Téléchargez ou générez un nouveau certificat personnalisé ou commencez à utiliser le certificat S3 global, selon vos besoins. e. Sélectionnez **Enregistrer les modifications**.

Tâche	Menu Actions	Page de détails
Modifier l'accès des locataires	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez **Actions** > **Modifier l'accès du locataire**. c. Choisissez une option d'accès différente, sélectionnez ou supprimez des locataires de la liste, ou faites les deux. d. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom du point de terminaison pour afficher les détails. b. Sélectionnez l'onglet **Accès locataire**. c. Sélectionnez **Modifier l'accès du locataire**. d. Choisissez une option d'accès différente, sélectionnez ou supprimez des locataires de la liste, ou faites les deux. e. Sélectionnez **Enregistrer les modifications**.

Supprimer les points de terminaison de l'équilibreur de charge

Vous pouvez supprimer un ou plusieurs points de terminaison à l'aide du menu **Actions**, ou vous pouvez supprimer un seul point de terminaison à partir de la page de détails.

> Pour éviter toute interruption du client, mettez à jour toutes les applications clientes S3 affectées avant de supprimer un point de terminaison d'équilibrage de charge. Mettez à jour chaque client pour qu'il se connecte à l'aide d'un port attribué à un autre point de terminaison d'équilibrage de charge. Assurez-vous également de mettre à jour toutes les informations de certificat requises.

> Si vous perdez l'accès à Grid Manager lors de la suppression d'un point de terminaison d'interface de gestion, mettez à jour l'URL.

- Pour supprimer un ou plusieurs points de terminaison :
  a. Sur la page Équilibreur de charge, cochez la case correspondant à chaque point de terminaison que vous souhaitez supprimer.
  b. Sélectionnez **Actions** > **Supprimer**.
  c. Sélectionnez **OK**.
- Pour supprimer un point de terminaison de la page de détails :
  a. Depuis la page Équilibreur de charge, sélectionnez le nom du point de terminaison.
  b. Sélectionnez **Supprimer** sur la page de détails.
  c. Sélectionnez **OK**.

Configurer les noms de domaine des points de terminaison S3

Pour prendre en charge les demandes de type S3 hébergées virtuellement, vous devez utiliser le gestionnaire de grille pour configurer la liste des noms de domaine de point de terminaison S3 auxquels les clients S3 se connectent.

L'utilisation d'une adresse IP pour un nom de domaine de point de terminaison n'est pas prise en charge. Les versions futures empêcheront cette configuration.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .
- Vous avez confirmé qu'une mise à niveau du réseau n'est pas en cours.

N'apportez aucune modification à la configuration du nom de domaine lorsqu'une mise à niveau de la grille est en cours.

À propos de cette tâche

Pour permettre aux clients d'utiliser les noms de domaine de point de terminaison S3, vous devez effectuer toutes les opérations suivantes :

- Utilisez le gestionnaire de grille pour ajouter les noms de domaine de point de terminaison S3 au système StorageGRID .
- Assurez-vous que le"certificat que le client utilise pour les connexions HTTPS à StorageGRID" est signé pour tous les noms de domaine dont le client a besoin.

  Par exemple, si le point final est `s3.company.com` , vous devez vous assurer que le certificat utilisé pour les connexions HTTPS inclut le `s3.company.com` point de terminaison et le nom alternatif du sujet (SAN) générique du point de terminaison : `*.s3.company.com` .

- Configurer le serveur DNS utilisé par le client. Incluez les enregistrements DNS pour les adresses IP que les clients utilisent pour établir des connexions et assurez-vous que les enregistrements font référence à tous les noms de domaine de point de terminaison S3 requis, y compris tous les noms génériques.

Les clients peuvent se connecter à StorageGRID à l'aide de l'adresse IP d'un nœud de passerelle, d'un nœud d'administration ou d'un nœud de stockage, ou en se connectant à l'adresse IP virtuelle d'un groupe de haute disponibilité. Vous devez comprendre comment les applications clientes se connectent à la grille afin d'inclure les adresses IP correctes dans les enregistrements DNS.

Les clients qui utilisent des connexions HTTPS (recommandées) à la grille peuvent utiliser l'un de ces certificats :

- Les clients qui se connectent à un point de terminaison d'équilibrage de charge peuvent utiliser un certificat personnalisé pour ce point de terminaison. Chaque point de terminaison d'équilibrage de charge peut être configuré pour reconnaître différents noms de domaine de point de terminaison S3.
- Les clients qui se connectent à un point de terminaison d'équilibrage de charge ou directement à un nœud de stockage peuvent personnaliser le certificat API S3 global pour inclure tous les noms de domaine de point de terminaison S3 requis.

Si vous n'ajoutez pas de noms de domaine de point de terminaison S3 et que la liste est vide, la prise en charge des demandes de type S3 hébergées virtuellement est désactivée.

Ajouter un nom de domaine de point de terminaison S3

Étapes

1. Sélectionnez **CONFIGURATION** > **Réseau** > **Noms de domaine de point de terminaison S3**.
2. Saisissez le nom de domaine dans le champ **Nom de domaine 1**. Sélectionnez **Ajouter un autre nom de domaine** pour ajouter d'autres noms de domaine.
3. Sélectionnez **Enregistrer**.
4. Assurez-vous que les certificats de serveur utilisés par les clients correspondent aux noms de domaine de point de terminaison S3 requis.
   - Si les clients se connectent à un point de terminaison d'équilibrage de charge qui utilise son propre certificat,"mettre à jour le certificat associé au point de terminaison" .
   - Si les clients se connectent à un point de terminaison d'équilibrage de charge qui utilise le certificat API S3 global ou directement aux nœuds de stockage,"mettre à jour le certificat API S3 global" .
5. Ajoutez les enregistrements DNS requis pour garantir que les demandes de nom de domaine de point de terminaison peuvent être résolues.

Résultat

Désormais, lorsque les clients utilisent le point de terminaison `bucket.s3.company.com` , le serveur DNS résout le point de terminaison correct et le certificat authentifie le point de terminaison comme prévu.

Renommer un nom de domaine de point de terminaison S3

Si vous modifiez un nom utilisé par les applications S3, les demandes de type hébergé virtuellement échoueront.

Étapes

1. Sélectionnez **CONFIGURATION** > **Réseau** > **Noms de domaine de point de terminaison S3**.
2. Sélectionnez le champ du nom de domaine que vous souhaitez modifier et effectuez les modifications nécessaires.
3. Sélectionnez **Enregistrer**.
4. Sélectionnez **Oui** pour confirmer votre modification.

Supprimer un nom de domaine de point de terminaison S3

Si vous supprimez un nom utilisé par les applications S3, les demandes de type hébergé virtuellement échoueront.

Étapes

1. Sélectionnez **CONFIGURATION** > **Réseau** > **Noms de domaine de point de terminaison S3**.
2. Sélectionnez l'icône de suppression ✕ à côté du nom de domaine.
3. Sélectionnez **Oui** pour confirmer la suppression.

Informations connexes

- "Utiliser l'API REST S3"
- "Afficher les adresses IP"
- "Configurer des groupes de haute disponibilité"

Résumé : Adresses IP et ports pour les connexions client

Pour stocker ou récupérer des objets, les applications clientes S3 se connectent au service Load Balancer, inclus sur tous les nœuds d'administration et les nœuds de passerelle, ou au service Local Distribution Router (LDR), inclus sur tous les nœuds de stockage.

Les applications clientes peuvent se connecter à StorageGRID à l'aide de l'adresse IP d'un nœud de grille et du numéro de port du service sur ce nœud. En option, vous pouvez créer des groupes haute disponibilité (HA) de nœuds d'équilibrage de charge pour fournir des connexions hautement disponibles qui utilisent des adresses IP virtuelles (VIP). Si vous souhaitez vous connecter à StorageGRID à l'aide d'un nom de domaine complet (FQDN) au lieu d'une adresse IP ou VIP, vous pouvez configurer des entrées DNS.

Ce tableau résume les différentes manières dont les clients peuvent se connecter à StorageGRID ainsi que les adresses IP et les ports utilisés pour chaque type de connexion. Si vous avez déjà créé des points de terminaison d'équilibrage de charge et des groupes de haute disponibilité (HA), consultezOù trouver les adresses IP pour localiser ces valeurs dans le gestionnaire de grille.

Où la connexion est établie	Service auquel le client se connecte	adresse IP	Port
groupe HA	Équilibreur de charge	Adresse IP virtuelle d'un groupe HA	Port attribué au point de terminaison de l'équilibreur de charge
Nœud d'administration	Équilibreur de charge	Adresse IP du nœud d'administration	Port attribué au point de terminaison de l'équilibreur de charge
Nœud de passerelle	Équilibreur de charge	Adresse IP du nœud de passerelle	Port attribué au point de terminaison de l'équilibreur de charge
Nœud de stockage	LDR	Adresse IP du nœud de stockage	Ports S3 par défaut : • HTTPS : 18082 • HTTP : 18084

Exemples d'URL

Pour connecter une application cliente au point de terminaison de l'équilibreur de charge d'un groupe HA de nœuds de passerelle, utilisez une URL structurée comme indiqué ci-dessous :

`https://VIP-of-HA-group:LB-endpoint-port`

Par exemple, si l'adresse IP virtuelle du groupe HA est 192.0.2.5 et que le numéro de port du point de terminaison de l'équilibreur de charge est 10443, une application peut utiliser l'URL suivante pour se connecter à StorageGRID:

`https://192.0.2.5:10443`

Où trouver les adresses IP

1. Sign in au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
2. Pour trouver l'adresse IP d'un nœud de grille :
   a. Sélectionnez **NODES**.
   b. Sélectionnez le nœud d'administration, le nœud de passerelle ou le nœud de stockage auquel vous souhaitez vous connecter.
   c. Sélectionnez l'onglet **Aperçu**.
   d. Dans la section Informations sur le nœud, notez les adresses IP du nœud.
   e. Sélectionnez **Afficher plus** pour afficher les adresses IPv6 et les mappages d'interface.

      Vous pouvez établir des connexions à partir d'applications clientes vers n'importe laquelle des adresses IP de la liste :

      - **eth0:** Réseau de grille
      - **eth1:** Réseau administrateur (facultatif)
      - **eth2:** Réseau client (facultatif)

      > Si vous visualisez un nœud d'administration ou un nœud de passerelle et qu'il s'agit du nœud actif dans un groupe haute disponibilité, l'adresse IP virtuelle du groupe HA est affichée sur eth2.

3. Pour trouver l'adresse IP virtuelle d'un groupe de haute disponibilité :
   a. Sélectionnez **CONFIGURATION** > **Réseau** > **Groupes de haute disponibilité**.
   b. Dans le tableau, notez l'adresse IP virtuelle du groupe HA.
4. Pour trouver le numéro de port d'un point de terminaison d'équilibreur de charge :
   a. Sélectionnez **CONFIGURATION** > **Réseau** > **Points de terminaison de l'équilibreur de charge**.
   b. Notez le numéro de port du point de terminaison que vous souhaitez utiliser.

      > Si le numéro de port est 80 ou 443, le point de terminaison est configuré uniquement sur les nœuds de passerelle, car ces ports sont réservés sur les nœuds d'administration. Tous les autres ports sont configurés sur les nœuds de passerelle et les nœuds d'administration.

   c. Sélectionnez le nom du point de terminaison dans le tableau.
   d. Confirmez que le **Type de client** (S3) correspond à l'application cliente qui utilisera le point de terminaison.

Gérer les réseaux et les connexions

Configurer les paramètres réseau

Vous pouvez configurer divers paramètres réseau à partir du Grid Manager pour affiner le fonctionnement de votre système StorageGRID .

Configurer les interfaces VLAN

Tu peux"créer des interfaces LAN virtuelles (VLAN)" pour isoler et partitionner le trafic pour la sécurité, la flexibilité et les performances. Chaque interface VLAN est associée à une ou plusieurs interfaces parentes sur les nœuds d'administration et les nœuds de passerelle. Vous pouvez utiliser des interfaces VLAN dans des groupes HA et dans des points de terminaison d'équilibrage de charge pour séparer le trafic client ou administrateur par application ou locataire.

Politiques de classification du trafic

Vous pouvez utiliser"politiques de classification du trafic" pour identifier et gérer différents types de trafic réseau, y compris le trafic lié à des compartiments spécifiques, des locataires, des sous-réseaux clients ou des points de terminaison d'équilibrage de charge. Ces politiques peuvent aider à limiter et à surveiller le trafic.

Lignes directrices pour les réseaux StorageGRID

Vous pouvez utiliser Grid Manager pour configurer et gérer les réseaux et connexions StorageGRID .

Voir"Configurer les connexions client S3" pour apprendre à connecter des clients S3.

Réseaux StorageGRID par défaut

Par défaut, StorageGRID prend en charge trois interfaces réseau par nœud de grille, ce qui vous permet de configurer la mise en réseau de chaque nœud de grille individuel afin de répondre à vos exigences de sécurité et d'accès.

Pour plus d'informations sur la topologie du réseau, voir"Directives de mise en réseau" .

Réseau de grille

Requis. Le réseau Grid est utilisé pour tout le trafic interne StorageGRID . Il fournit une connectivité entre tous les nœuds du réseau, sur tous les sites et sous-réseaux.

Réseau d'administration

Facultatif. Le réseau d'administration est généralement utilisé pour l'administration et la maintenance du système. Il peut également être utilisé pour l'accès au protocole client. Le réseau d'administration est généralement un réseau privé et n'a pas besoin d'être routable entre les sites.

Réseau de clients

Facultatif. Le réseau client est un réseau ouvert généralement utilisé pour fournir un accès aux applications client S3, de sorte que le réseau Grid peut être isolé et sécurisé. Le réseau client peut communiquer avec n'importe quel sous-réseau accessible via la passerelle locale.

Lignes directrices

- Chaque nœud StorageGRID nécessite une interface réseau dédiée, une adresse IP, un masque de sous-réseau et une passerelle pour chaque réseau auquel il est attribué.
- Un nœud de grille ne peut pas avoir plus d'une interface sur un réseau.
- Une seule passerelle, par réseau, par nœud de grille est prise en charge et elle doit se trouver sur le même sous-réseau que le nœud. Vous pouvez implémenter un routage plus complexe dans la passerelle,

si nécessaire.

- Sur chaque nœud, chaque réseau est mappé à une interface réseau spécifique.

Réseau	Nom de l'interface
Grille	eth0
Administrateur (facultatif)	eth1
Client (facultatif)	eth2

- Si le nœud est connecté à un dispositif StorageGRID , des ports spécifiques sont utilisés pour chaque réseau. Pour plus de détails, consultez les instructions d'installation de votre appareil.
- L'itinéraire par défaut est généré automatiquement, par nœud. Si eth2 est activé, alors 0.0.0.0/0 utilise le réseau client sur eth2. Si eth2 n'est pas activé, alors 0.0.0.0/0 utilise le réseau Grid sur eth0.
- Le réseau client ne devient opérationnel que lorsque le nœud de grille a rejoint le réseau
- Le réseau d'administration peut être configuré pendant le déploiement du nœud de grille pour permettre l'accès à l'interface utilisateur d'installation avant que la grille ne soit entièrement installée.

Interfaces optionnelles

En option, vous pouvez ajouter des interfaces supplémentaires à un nœud. Par exemple, vous souhaiterez peut-être ajouter une interface de jonction à un nœud d'administration ou de passerelle, afin de pouvoir l'utiliser"Interfaces VLAN" pour séparer le trafic appartenant à différentes applications ou locataires. Ou, vous souhaiterez peut-être ajouter une interface d'accès à utiliser dans un"groupe de haute disponibilité (HA)" .

Pour ajouter des interfaces de jonction ou d'accès, consultez les éléments suivants :

- **VMware (après l'installation du nœud)**:"VMware : ajouter des interfaces de jonction ou d'accès à un nœud"
  - **Red Hat Enterprise Linux (avant l'installation du nœud)**:"Créer des fichiers de configuration de nœud"
  - **Ubuntu ou Debian (avant d'installer le nœud)** :"Créer des fichiers de configuration de nœud"
  - **RHEL, Ubuntu ou Debian (après l'installation du nœud)** :"Linux : ajouter des interfaces trunk ou d'accès à un nœud"

Afficher les adresses IP

Vous pouvez afficher l'adresse IP de chaque nœud de grille dans votre système StorageGRID . Vous pouvez ensuite utiliser cette adresse IP pour vous connecter au nœud de grille sur la ligne de commande et effectuer diverses procédures de maintenance.

Avant de commencer

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

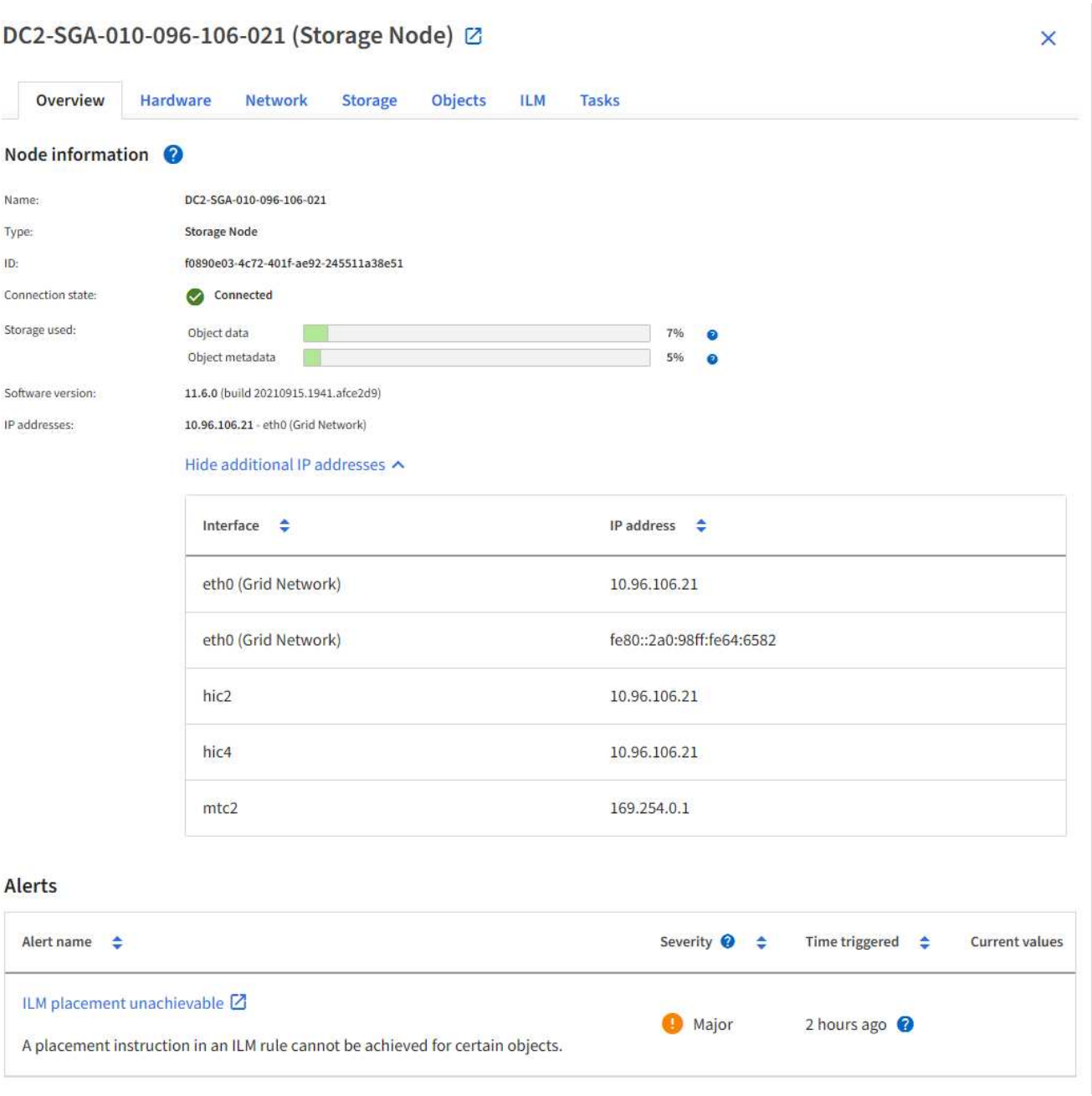
À propos de cette tâche

Pour plus d'informations sur la modification des adresses IP, consultez"Configurer les adresses IP" .

Étapes

1. Sélectionnez **NODES** > ***grid node*** > **Aperçu**.
2. Sélectionnez **Afficher plus** à droite du titre Adresses IP.

   Les adresses IP de ce nœud de grille sont répertoriées dans un tableau.



Configurer les interfaces VLAN

Vous pouvez créer des interfaces LAN virtuelles (VLAN) sur des nœuds d'administration et des nœuds de passerelle et les utiliser dans des groupes HA et des points de terminaison d'équilibrage de charge pour isoler et partitionner le trafic pour la sécurité, la flexibilité et les performances. Les nœuds sélectionnés dans le groupe HA peuvent utiliser les interfaces VLAN pour partager jusqu'à 10 adresses IP virtuelles, de sorte que

si un nœud tombe en panne, un autre nœud prend en charge le trafic vers et depuis les adresses IP virtuelles.

Considérations relatives aux interfaces VLAN

- Vous créez une interface VLAN en saisissant un ID VLAN et en choisissant une interface parent sur un ou plusieurs nœuds.
- Une interface parent doit être configurée comme interface de jonction au niveau du commutateur.
- Une interface parent peut être le réseau Grid (eth0), le réseau client (eth2) ou une interface de jonction supplémentaire pour la machine virtuelle ou l'hôte bare-metal (par exemple, ens256).
- Pour chaque interface VLAN, vous ne pouvez sélectionner qu'une seule interface parent pour un nœud donné. Par exemple, vous ne pouvez pas utiliser à la fois l'interface réseau Grid et l'interface réseau client sur le même nœud de passerelle que l'interface parent pour le même VLAN.
- Si l'interface VLAN est destinée au trafic du nœud d'administration, qui inclut le trafic lié au gestionnaire de grille et au gestionnaire de locataires, sélectionnez les interfaces sur les nœuds d'administration uniquement.
- Si l'interface VLAN est destinée au trafic client S3, sélectionnez les interfaces sur les nœuds d'administration ou sur les nœuds de passerelle.
- Si vous devez ajouter des interfaces de jonction, consultez les éléments suivants pour plus de détails :
  - **VMware (après l'installation du nœud)**:"VMware : ajouter des interfaces de jonction ou d'accès à un nœud"
  - **RHEL (avant l'installation du nœud)**:"Créer des fichiers de configuration de nœud"
  - **Ubuntu ou Debian (avant d'installer le nœud)** :"Créer des fichiers de configuration de nœud"
  - **RHEL, Ubuntu ou Debian (après l'installation du nœud)** :"Linux : ajouter des interfaces trunk ou d'accès à un nœud"

Créer une interface VLAN

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès root" .
- Une interface de jonction a été configurée dans le réseau et attachée au nœud VM ou Linux. Vous connaissez le nom de l'interface trunk.
- Vous connaissez l'ID du VLAN que vous configurez.

À propos de cette tâche

Votre administrateur réseau a peut-être configuré une ou plusieurs interfaces de jonction et un ou plusieurs VLAN pour séparer le trafic client ou administrateur appartenant à différentes applications ou locataires. Chaque VLAN est identifié par un ID numérique ou une balise. Par exemple, votre réseau peut utiliser le VLAN 100 pour le trafic FabricPool et le VLAN 200 pour une application d'archivage.

Vous pouvez utiliser Grid Manager pour créer des interfaces VLAN qui permettent aux clients d'accéder à StorageGRID sur un VLAN spécifique. Lorsque vous créez des interfaces VLAN, vous spécifiez l'ID VLAN et sélectionnez les interfaces parentes (trunk) sur un ou plusieurs nœuds.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION** > **Réseau** > **Interfaces VLAN**.
2. Sélectionnez **Créer**.

Saisissez les détails des interfaces VLAN

Étapes

1. Spécifiez l'ID du VLAN dans votre réseau. Vous pouvez saisir n'importe quelle valeur entre 1 et 4094.

   Les ID VLAN n'ont pas besoin d'être uniques. Par exemple, vous pouvez utiliser l'ID VLAN 200 pour le trafic administrateur sur un site et le même ID VLAN pour le trafic client sur un autre site. Vous pouvez créer des interfaces VLAN distinctes avec différents ensembles d'interfaces parentes sur chaque site. Cependant, deux interfaces VLAN avec le même ID ne peuvent pas partager la même interface sur un nœud. Si vous spécifiez un ID qui a déjà été utilisé, un message apparaît.

2. Vous pouvez également saisir une brève description de l'interface VLAN.
3. Sélectionnez **Continuer**.

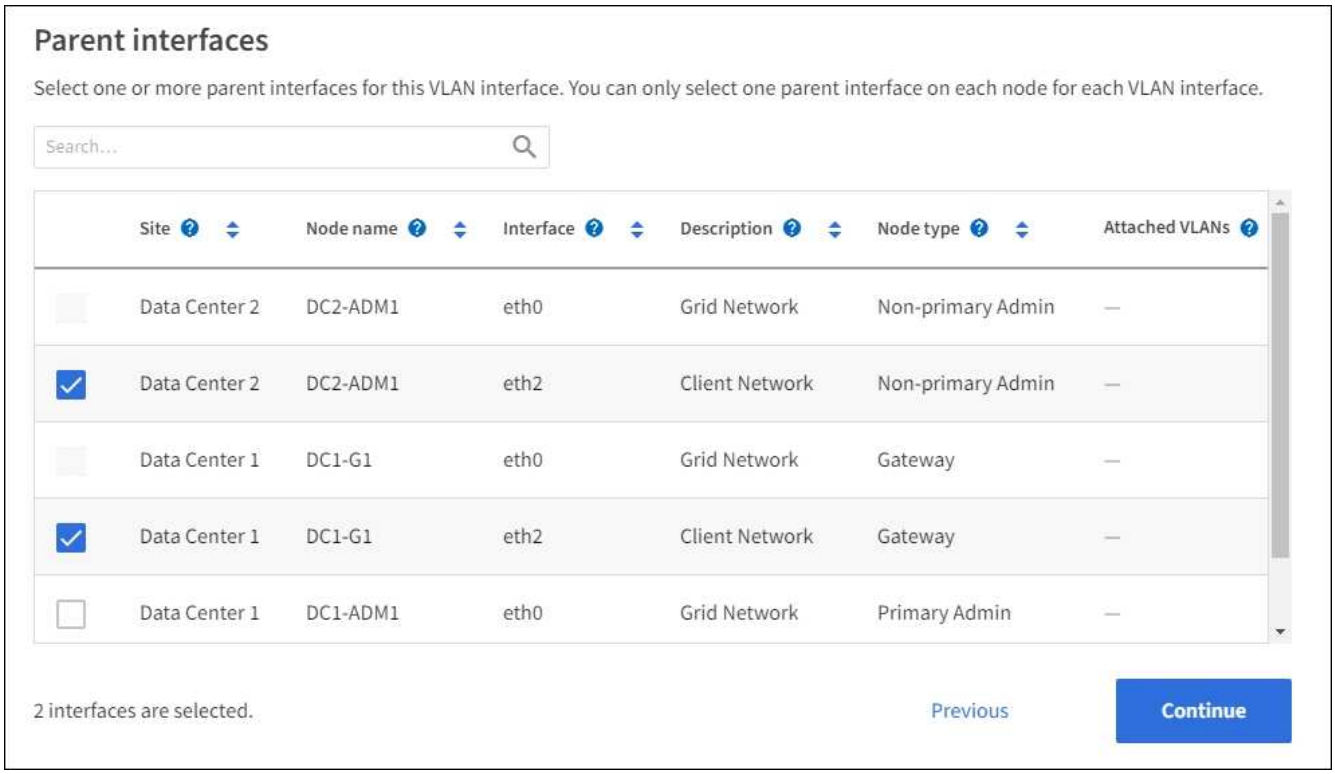
Choisir les interfaces parentes

Le tableau répertorie les interfaces disponibles pour tous les nœuds d'administration et les nœuds de passerelle sur chaque site de votre grille. Les interfaces réseau d'administration (eth1) ne peuvent pas être utilisées comme interfaces parentes et ne sont pas affichées.

Étapes

1. Sélectionnez une ou plusieurs interfaces parentes auxquelles attacher ce VLAN.

   Par exemple, vous souhaiterez peut-être attacher un VLAN à l'interface réseau client (eth2) pour un nœud de passerelle et un nœud d'administration.



2. Sélectionnez **Continuer**.

Confirmer les paramètres

Étapes

1. Vérifiez la configuration et apportez les modifications nécessaires.
   - Si vous devez modifier l'ID ou la description du VLAN, sélectionnez **Entrer les détails du VLAN** en haut de la page.
   - Si vous devez modifier une interface parente, sélectionnez **Choisir les interfaces parentes** en haut de la page ou sélectionnez **Précédent**.
   - Si vous devez supprimer une interface parent, sélectionnez la corbeille .
2. Sélectionnez **Enregistrer**.
3. Attendez jusqu'à 5 minutes pour que la nouvelle interface apparaisse comme sélection sur la page Groupes de haute disponibilité et soit répertoriée dans la table **Interfaces réseau** pour le nœud (**NODES** > ***parent interface node*** > **Network**).

Modifier une interface VLAN

Lorsque vous modifiez une interface VLAN, vous pouvez effectuer les types de modifications suivants :

- Modifiez l'ID ou la description du VLAN.
- Ajouter ou supprimer des interfaces parentes.

Par exemple, vous souhaiterez peut-être supprimer une interface parent d'une interface VLAN si vous prévoyez de mettre hors service le nœud associé.

Notez ce qui suit :

- Vous ne pouvez pas modifier un ID VLAN si l'interface VLAN est utilisée dans un groupe HA.
- Vous ne pouvez pas supprimer une interface parente si cette interface parente est utilisée dans un groupe HA.

  Par exemple, supposons que le VLAN 200 soit attaché aux interfaces parentes sur les nœuds A et B. Si un groupe HA utilise l'interface VLAN 200 pour le nœud A et l'interface eth2 pour le nœud B, vous pouvez supprimer l'interface parente inutilisée pour le nœud B, mais vous ne pouvez pas supprimer l'interface parente utilisée pour le nœud A.

Étapes

1. Sélectionnez **CONFIGURATION** > **Réseau** > **Interfaces VLAN**.
2. Cochez la case correspondant à l'interface VLAN que vous souhaitez modifier. Ensuite, sélectionnez **Actions** > **Modifier**.
3. Vous pouvez également mettre à jour l'ID VLAN ou la description. Ensuite, sélectionnez **Continuer**.

   Vous ne pouvez pas mettre à jour un ID VLAN si le VLAN est utilisé dans un groupe HA.

4. Vous pouvez également cocher ou décocher les cases pour ajouter des interfaces parentes ou pour supprimer les interfaces inutilisées. Ensuite, sélectionnez **Continuer**.
5. Vérifiez la configuration et apportez les modifications nécessaires.
6. Sélectionnez **Enregistrer**.

Supprimer une interface VLAN

Vous pouvez supprimer une ou plusieurs interfaces VLAN.

Vous ne pouvez pas supprimer une interface VLAN si elle est actuellement utilisée dans un groupe HA. Vous devez supprimer l'interface VLAN du groupe HA avant de pouvoir la supprimer.

Pour éviter toute interruption du trafic client, envisagez d'effectuer l'une des opérations suivantes :

- Ajoutez une nouvelle interface VLAN au groupe HA avant de supprimer cette interface VLAN.
- Créez un nouveau groupe HA qui n'utilise pas cette interface VLAN.
- Si l'interface VLAN que vous souhaitez supprimer est actuellement l'interface active, modifiez le groupe HA. Déplacez l'interface VLAN que vous souhaitez supprimer vers le bas de la liste des priorités. Attendez que la communication soit établie sur la nouvelle interface principale, puis supprimez l'ancienne interface du groupe HA. Enfin, supprimez l'interface VLAN sur ce nœud.

Étapes

1. Sélectionnez **CONFIGURATION** > **Réseau** > **Interfaces VLAN**.
2. Cochez la case correspondant à chaque interface VLAN que vous souhaitez supprimer. Ensuite, sélectionnez **Actions** > **Supprimer**.
3. Sélectionnez **Oui** pour confirmer votre sélection.

   Toutes les interfaces VLAN que vous avez sélectionnées sont supprimées. Une bannière de réussite verte apparaît sur la page des interfaces VLAN.

Gérer les politiques de classification du trafic

Quelles sont les politiques de classification du trafic ?

Les politiques de classification du trafic vous permettent d'identifier et de surveiller différents types de trafic réseau. Ces politiques peuvent vous aider à limiter et à surveiller le trafic afin d'améliorer vos offres de qualité de service (QoS).

Les stratégies de classification du trafic sont appliquées aux points de terminaison sur le service StorageGRID Load Balancer pour les nœuds de passerelle et les nœuds d'administration. Pour créer des politiques de classification du trafic, vous devez déjà avoir créé des points de terminaison d'équilibrage de charge.

Règles de correspondance

Chaque politique de classification du trafic contient une ou plusieurs règles de correspondance pour identifier le trafic réseau lié à une ou plusieurs des entités suivantes :

- Seaux
- Sous-réseau
- Locataire
- Points de terminaison de l'équilibreur de charge

StorageGRID surveille le trafic qui correspond à n'importe quelle règle de la politique en fonction des objectifs de la règle. Tout trafic correspondant à une règle d'une politique est géré par cette politique. À l'inverse, vous pouvez définir des règles pour correspondre à tout le trafic, à l'exception d'une entité spécifiée.

Limitation du trafic

En option, vous pouvez ajouter les types de limites suivants à une politique :

- Bande passante globale
- Bande passante par requête
- Demandes simultanées
- Taux de demande

Les valeurs limites sont appliquées pour chaque équilibreur de charge. Si le trafic est réparti simultanément sur plusieurs équilibreurs de charge, les débits maximum totaux sont un multiple des limites de débit que vous spécifiez.

> Vous pouvez créer des politiques pour limiter la bande passante globale ou pour limiter la bande passante par demande. Cependant, StorageGRID ne peut pas limiter les deux types de bande passante en même temps. Les limites de bande passante globales peuvent avoir un impact mineur supplémentaire sur les performances du trafic non limité.

Pour les limites de bande passante globales ou par demande, les demandes entrent ou sortent au débit que vous définissez. StorageGRID ne peut appliquer qu'une seule vitesse, donc la correspondance de politique la plus spécifique, par type de correspondance, est celle appliquée. La bande passante consommée par la demande n'est pas comptabilisée dans d'autres politiques de correspondance moins spécifiques contenant des politiques de limite de bande passante globale. Pour tous les autres types de limites, les demandes des clients sont retardées de 250 millisecondes et reçoivent une réponse 503 Slow Down pour les demandes qui dépassent toute limite de politique correspondante.

Dans le gestionnaire de grille, vous pouvez afficher les graphiques de trafic et vérifier que les politiques appliquent les limites de trafic que vous attendez.

Utiliser des politiques de classification du trafic avec des SLA

Vous pouvez utiliser des stratégies de classification du trafic conjointement avec des limites de capacité et la protection des données pour appliquer des accords de niveau de service (SLA) qui fournissent des détails sur la capacité, la protection des données et les performances.

L'exemple suivant montre trois niveaux d'un SLA. Vous pouvez créer des stratégies de classification du trafic pour atteindre les objectifs de performances de chaque niveau SLA.

Niveau de service	Capacité	Protection des données	Performances maximales autorisées	Coût
Or	1 Po de stockage autorisé	Règle ILM en 3 exemplaires	25 000 requêtes/sec Bande passante de 5 Go/s (40 Gbps)	$$$ par mois
Argent	250 To de stockage autorisé	Règle ILM en 2 exemplaires	10 000 requêtes/sec Bande passante de 1,25 Go/s (10 Gbps)	$$ par mois
Bronze	100 To de stockage autorisé	Règle ILM en 2 exemplaires	5 000 requêtes/s Bande passante de 1 Go/s (8 Gbps)	$ par mois

Créer des politiques de classification du trafic

Vous pouvez créer des stratégies de classification du trafic si vous souhaitez surveiller et éventuellement limiter le trafic réseau par bucket, regex de bucket, CIDR, point de terminaison d'équilibrage de charge ou locataire. Vous pouvez également définir des limites pour une politique en fonction de la bande passante, du nombre de demandes simultanées ou du taux de demande.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès root" .
- Vous avez créé tous les points de terminaison d'équilibrage de charge que vous souhaitez faire correspondre.
- Vous avez créé tous les locataires que vous souhaitez faire correspondre.

Étapes

1. Sélectionnez **CONFIGURATION** > **Réseau** > **Classification du trafic**.
2. Sélectionnez **Créer**.

3. Saisissez un nom et une description (facultatif) pour la politique et sélectionnez **Continuer**.

   Par exemple, décrivez à quoi s'applique cette politique de classification du trafic et ce qu'elle limitera.

4. Sélectionnez **Ajouter une règle** et spécifiez les détails suivants pour créer une ou plusieurs règles correspondantes pour la politique. Toute politique que vous créez doit avoir au moins une règle correspondante. Sélectionnez **Continuer**.

Champ	Description
Type	Sélectionnez les types de trafic auxquels la règle de correspondance s'applique. Les types de trafic sont les suivants : bucket, bucket regex, CIDR, point de terminaison de l'équilibreur de charge et locataire.
Valeur de correspondance	Saisissez la valeur qui correspond au type sélectionné. • Bucket : saisissez un ou plusieurs noms de bucket. • Expression régulière de compartiment : saisissez une ou plusieurs expressions régulières utilisées pour faire correspondre un ensemble de noms de compartiment. L'expression régulière n'est pas ancrée. Utilisez l'ancre ^ pour faire correspondre le début du nom du bucket et utilisez l'ancre $ pour faire correspondre la fin du nom. La correspondance d'expressions régulières prend en charge un sous-ensemble de la syntaxe PCRE (expression régulière compatible Perl). • CIDR : saisissez un ou plusieurs sous-réseaux IPv4, en notation CIDR, qui correspondent au sous-réseau souhaité. • Point de terminaison de l'équilibreur de charge : sélectionnez un nom de point de terminaison. Ce sont les points de terminaison de l'équilibreur de charge que vous avez définis sur le"Configurer les points de terminaison de l'équilibreur de charge" . • Locataire : la correspondance des locataires utilise l'ID de clé d'accès. Si la demande ne contient pas d'ID de clé d'accès (par exemple, un accès anonyme), la propriété du bucket consulté est utilisée pour déterminer le locataire.
Correspondance inverse	Si vous souhaitez faire correspondre tout le trafic réseau *à l'exception* du trafic cohérent avec le type et la valeur de correspondance qui viennent d'être définis, cochez la case **Correspondance inverse**. Sinon, laissez la case à cocher décochée. Par exemple, si vous souhaitez que cette stratégie s'applique à tous les points de terminaison de l'équilibreur de charge sauf un, spécifiez le point de terminaison de l'équilibreur de charge à exclure et sélectionnez **Correspondance inverse**. Pour une politique contenant plusieurs correspondances où au moins l'une d'elles est une correspondance inverse, veillez à ne pas créer une politique qui correspond à toutes les demandes.

5. Vous pouvez également sélectionner **Ajouter une limite** et sélectionner les détails suivants pour ajouter une ou plusieurs limites afin de contrôler le trafic réseau correspondant à une règle.

> StorageGRID collecte des métriques même si vous n'ajoutez aucune limite, afin que vous puissiez comprendre les tendances du trafic.

Champ	Description
Type	Le type de limite que vous souhaitez appliquer au trafic réseau correspondant à la règle. Par exemple, vous pouvez limiter la bande passante ou le débit de requête. **Remarque** : vous pouvez créer des politiques pour limiter la bande passante globale ou pour limiter la bande passante par requête. Cependant, StorageGRID ne peut pas limiter les deux types de bande passante en même temps. Lorsque la bande passante agrégée est utilisée, la bande passante par demande n'est pas disponible. À l'inverse, lorsque la bande passante par demande est utilisée, la bande passante globale n'est pas disponible. Les limites de bande passante globales peuvent avoir un impact mineur supplémentaire sur les performances du trafic non limité. Pour les limites de bande passante, StorageGRID applique la politique qui correspond le mieux au type de limite définie. Par exemple, si vous avez une politique qui limite le trafic dans une seule direction, le trafic dans la direction opposée sera illimité, même s'il existe du trafic correspondant à des politiques supplémentaires qui ont des limites de bande passante. StorageGRID implémente les « meilleures » correspondances pour les limites de bande passante dans l'ordre suivant : • Adresse IP exacte (masque /32) • Nom exact du bucket • Expression régulière de bucket • Locataire • Point final • Correspondances CIDR non exactes (pas /32) • Correspondances inverses
S'applique à	Si cette limite s'applique aux demandes de lecture client (GET ou HEAD) ou aux demandes d'écriture (PUT, POST ou DELETE).
Valeur	La valeur à laquelle le trafic réseau sera limité, en fonction de l'unité que vous sélectionnez. Par exemple, entrez 10 et sélectionnez Mio/s pour empêcher le trafic réseau correspondant à cette règle de dépasser 10 Mio/s. **Remarque** : Selon le paramètre des unités, les unités disponibles seront soit binaires (par exemple, Gio) soit décimales (par exemple, Go). Pour modifier le paramètre des unités, sélectionnez la liste déroulante utilisateur dans le coin supérieur droit du gestionnaire de grille, puis sélectionnez **Préférences utilisateur**.

Champ	Description
Unité	L'unité qui décrit la valeur que vous avez saisie.

Par exemple, si vous souhaitez créer une limite de bande passante de 40 Go/s pour un niveau SLA, créez deux limites de bande passante agrégées : GET/HEAD à 40 Go/s et PUT/POST/DELETE à 40 Go/s.

6. Sélectionnez **Continuer**.
7. Lisez et révisez la politique de classification du trafic. Utilisez le bouton **Précédent** pour revenir en arrière et apporter les modifications nécessaires. Lorsque vous êtes satisfait de la politique, sélectionnez **Enregistrer et continuer**.

   Le trafic client S3 est désormais géré conformément à la politique de classification du trafic.

Après avoir terminé

"Afficher les mesures du trafic réseau"pour vérifier que les policiers appliquent les limites de circulation que vous attendez.

Modifier la politique de classification du trafic

Vous pouvez modifier une politique de classification du trafic pour changer son nom ou sa description, ou pour créer, modifier ou supprimer des règles ou des limites pour la politique.

Avant de commencer

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

Étapes

1. Sélectionnez **CONFIGURATION** > **Réseau** > **Classification du trafic**.

   La page Stratégies de classification du trafic s'affiche et les stratégies existantes sont répertoriées dans un tableau.

2. Modifiez la politique en utilisant le menu Actions ou la page de détails. Voir"créer des politiques de classification du trafic" pour quoi entrer.

   Menu Actions

   a. Cochez la case correspondant à la politique.

   b. Sélectionnez **Actions** > **Modifier**.

   Page de détails

   a. Sélectionnez le nom de la politique.

   b. Sélectionnez le bouton **Modifier** à côté du nom de la politique.

3. Pour l'étape Saisir le nom de la politique, modifiez éventuellement le nom ou la description de la politique et sélectionnez **Continuer**.

4. Pour l'étape Ajouter des règles de correspondance, ajoutez éventuellement une règle ou modifiez le **Type** et la **Valeur de correspondance** de la règle existante, puis sélectionnez **Continuer**.
5. Pour l'étape Définir les limites, ajoutez, modifiez ou supprimez éventuellement une limite et sélectionnez **Continuer**.
6. Consultez la politique mise à jour et sélectionnez **Enregistrer et continuer**.

   Les modifications que vous avez apportées à la politique sont enregistrées et le trafic réseau est désormais géré conformément aux politiques de classification du trafic. Vous pouvez consulter les graphiques de circulation et vérifier que les politiques appliquent les limites de circulation que vous attendez.

Supprimer une politique de classification du trafic

Vous pouvez supprimer une politique de classification du trafic si vous n'en avez plus besoin. Assurez-vous de supprimer la bonne politique, car une politique ne peut pas être récupérée lorsqu'elle est supprimée.

Avant de commencer

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

Étapes

1. Sélectionnez **CONFIGURATION** > **Réseau** > **Classification du trafic**.

   La page Stratégies de classification du trafic s'affiche avec les stratégies existantes répertoriées dans un tableau.

2. Supprimez la politique en utilisant le menu Actions ou la page de détails.

   Menu Actions

   a. Cochez la case correspondant à la politique.

   b. Sélectionnez **Actions** > **Supprimer**.

   Page de détails de la politique

   a. Sélectionnez le nom de la politique.

   b. Sélectionnez le bouton **Supprimer** à côté du nom de la politique.

3. Sélectionnez **Oui** pour confirmer que vous souhaitez supprimer la politique.

   La politique est supprimée.

Afficher les mesures du trafic réseau

Vous pouvez surveiller le trafic réseau en affichant les graphiques disponibles sur la page Stratégies de classification du trafic.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Accès root ou autorisation des comptes locataires" .

À propos de cette tâche

Pour toute stratégie de classification du trafic existante, vous pouvez afficher les métriques du service d'équilibrage de charge afin de déterminer si la stratégie limite avec succès le trafic sur le réseau. Les données des graphiques peuvent vous aider à déterminer si vous devez ajuster la politique.

Même si aucune limite n'est définie pour une politique de classification du trafic, des mesures sont collectées et les graphiques fournissent des informations utiles pour comprendre les tendances du trafic.

Étapes

1. Sélectionnez **CONFIGURATION** > **Réseau** > **Classification du trafic**.

   La page Stratégies de classification du trafic s'affiche et les stratégies existantes sont répertoriées dans le tableau.

2. Sélectionnez le nom de la politique de classification du trafic pour laquelle vous souhaitez afficher les métriques.
3. Sélectionnez l'onglet **Métriques**.

   Les graphiques de la politique de classification du trafic apparaissent. Les graphiques affichent les métriques uniquement pour le trafic correspondant à la politique sélectionnée.

   Les graphiques suivants sont inclus sur la page.

   - Taux de demande : ce graphique fournit la quantité de bande passante correspondant à cette politique gérée par tous les équilibreurs de charge. Les données reçues incluent les en-têtes de demande pour toutes les demandes et la taille des données du corps pour les réponses contenant des données du corps. Sent inclut les en-têtes de réponse pour toutes les demandes et la taille des données du corps de la réponse pour les demandes qui incluent des données de corps dans la réponse.

     > Lorsque les demandes sont terminées, ce graphique affiche uniquement l'utilisation de la bande passante. Pour les demandes d'objets lentes ou volumineuses, la bande passante instantanée réelle peut différer des valeurs indiquées dans ce graphique.

   - Taux de réponse aux erreurs : ce graphique fournit un taux approximatif auquel les requêtes correspondant à cette politique renvoient des erreurs (code d'état HTTP >= 400) aux clients.
   - Durée moyenne des requêtes (sans erreur) : ce graphique fournit une durée moyenne des requêtes réussies correspondant à cette politique.
   - Utilisation de la bande passante de la politique : ce graphique fournit la quantité de bande passante correspondant à cette politique gérée par tous les équilibreurs de charge. Les données reçues incluent les en-têtes de demande pour toutes les demandes et la taille des données du corps pour les réponses contenant des données du corps. Sent inclut les en-têtes de réponse pour toutes les demandes et la taille des données du corps de la réponse pour les demandes qui incluent des données de corps dans la réponse.
4. Positionnez le curseur sur un graphique linéaire pour voir une fenêtre contextuelle de valeurs sur une partie spécifique du graphique.
5. Sélectionnez **Tableau de bord Grafana** juste en dessous du titre Métriques pour afficher tous les graphiques d'une politique. En plus des quatre graphiques de l'onglet **Metrics**, vous pouvez afficher deux autres graphiques :

- Taux de demande d'écriture par taille d'objet : taux de demandes PUT/POST/DELETE correspondant à cette politique. Le positionnement sur une cellule individuelle affiche les taux par seconde. Les taux affichés dans la vue de survol sont tronqués en nombres entiers et peuvent indiquer 0 lorsqu'il y a des demandes différentes de zéro dans le bucket.
- Taux de demande de lecture par taille d'objet : taux de demandes GET/HEAD correspondant à cette politique. Le positionnement sur une cellule individuelle affiche les taux par seconde. Les taux affichés dans la vue de survol sont tronqués en nombres entiers et peuvent indiquer 0 lorsqu'il y a des demandes différentes de zéro dans le bucket.

6. Vous pouvez également accéder aux graphiques à partir du menu **SUPPORT**.
   a. Sélectionnez **SUPPORT** > **Outils** > **Métriques**.
   b. Sélectionnez **Politique de classification du trafic** dans la section **Grafana**.
   c. Sélectionnez la politique dans le menu en haut à gauche de la page.
   d. Placez le curseur sur un graphique pour voir une fenêtre contextuelle indiquant la date et l'heure de l'échantillon, les tailles d'objets agrégées dans le décompte et le nombre de requêtes par seconde pendant cette période.

      Les politiques de classification du trafic sont identifiées par leur ID. Les identifiants de stratégie sont répertoriés sur la page Stratégies de classification du trafic.

7. Analysez les graphiques pour déterminer à quelle fréquence la politique limite le trafic et si vous devez ajuster la politique.

Chiffres pris en charge pour les connexions TLS sortantes

Le système StorageGRID prend en charge un ensemble limité de suites de chiffrement pour les connexions TLS (Transport Layer Security) aux systèmes externes utilisés pour la fédération d'identité et les pools de stockage cloud.

Versions prises en charge de TLS

StorageGRID prend en charge TLS 1.2 et TLS 1.3 pour les connexions aux systèmes externes utilisés pour la fédération d'identité et les pools de stockage cloud.

Les chiffrements TLS pris en charge pour une utilisation avec des systèmes externes ont été sélectionnés pour garantir la compatibilité avec une gamme de systèmes externes. La liste est plus longue que la liste des chiffrements pris en charge pour une utilisation avec les applications clientes S3. Pour configurer les chiffrements, accédez à **CONFIGURATION** > **Sécurité** > **Paramètres de sécurité** et sélectionnez **Politiques TLS et SSH**.

> Les options de configuration TLS telles que les versions de protocole, les chiffrements, les algorithmes d'échange de clés et les algorithmes MAC ne sont pas configurables dans StorageGRID. Contactez votre représentant de compte NetApp si vous avez des demandes spécifiques concernant ces paramètres.

Avantages des connexions HTTP actives, inactives et simultanées

La façon dont vous configurez les connexions HTTP peut avoir un impact sur les performances du système StorageGRID . Les configurations diffèrent selon que la connexion HTTP est active ou inactive ou que vous avez plusieurs connexions

simultanées.

Vous pouvez identifier les avantages en termes de performances pour les types de connexions HTTP suivants :

- Connexions HTTP inactives
- Connexions HTTP actives
- Connexions HTTP simultanées

Avantages de garder les connexions HTTP inactives ouvertes

Vous devez garder les connexions HTTP ouvertes même lorsque les applications clientes sont inactives pour permettre aux applications clientes d'effectuer des transactions ultérieures sur la connexion ouverte. Sur la base des mesures du système et de l'expérience d'intégration, vous devez maintenir une connexion HTTP inactive ouverte pendant 10 minutes maximum. StorageGRID peut fermer automatiquement une connexion HTTP maintenue ouverte et inactive pendant plus de 10 minutes.

Les connexions HTTP ouvertes et inactives offrent les avantages suivants :

- Latence réduite entre le moment où le système StorageGRID détermine qu'il doit effectuer une transaction HTTP et le moment où le système StorageGRID peut effectuer la transaction

  La latence réduite est le principal avantage, en particulier compte tenu du temps nécessaire à l'établissement des connexions TCP/IP et TLS.

- Augmentation du taux de transfert de données en amorçant l'algorithme de démarrage lent TCP/IP avec les transferts précédemment effectués
- Notification instantanée de plusieurs classes de conditions de panne qui interrompent la connectivité entre l'application cliente et le système StorageGRID

Déterminer la durée pendant laquelle maintenir une connexion inactive ouverte est un compromis entre les avantages d'un démarrage lent associé à la connexion existante et l'allocation idéale de la connexion aux ressources internes du système.

Avantages des connexions HTTP actives

Pour les connexions directes aux nœuds de stockage, vous devez limiter la durée d'une connexion HTTP active à un maximum de 10 minutes, même si la connexion HTTP effectue en continu des transactions.

Déterminer la durée maximale pendant laquelle une connexion doit rester ouverte est un compromis entre les avantages de la persistance de la connexion et l'allocation idéale de la connexion aux ressources internes du système.

Pour les connexions client aux nœuds de stockage, la limitation des connexions HTTP actives offre les avantages suivants :

- Permet un équilibrage de charge optimal sur le système StorageGRID .

  Au fil du temps, une connexion HTTP peut ne plus être optimale à mesure que les exigences d'équilibrage de charge changent. Le système réalise son meilleur équilibrage de charge lorsque les applications clientes établissent une connexion HTTP distincte pour chaque transaction, mais cela annule les gains bien plus précieux associés aux connexions persistantes.

- Permet aux applications clientes de diriger les transactions HTTP vers les services LDR disposant d'espace disponible.
- Permet de démarrer les procédures de maintenance.

  Certaines procédures de maintenance démarrent uniquement une fois toutes les connexions HTTP en cours terminées.

Pour les connexions client au service Load Balancer, limiter la durée des connexions ouvertes peut être utile pour permettre à certaines procédures de maintenance de démarrer rapidement. Si la durée des connexions client n'est pas limitée, la fin automatique des connexions actives peut prendre plusieurs minutes.

Avantages des connexions HTTP simultanées

Vous devez conserver plusieurs connexions TCP/IP au système StorageGRID ouvertes pour permettre le parallélisme, ce qui augmente les performances. Le nombre optimal de connexions parallèles dépend de divers facteurs.

Les connexions HTTP simultanées offrent les avantages suivants :

- Latence réduite

  Les transactions peuvent démarrer immédiatement au lieu d'attendre que d'autres transactions soient terminées.

- Augmentation du débit

  Le système StorageGRID peut effectuer des transactions parallèles et augmenter le débit global des transactions.

Les applications clientes doivent établir plusieurs connexions HTTP. Lorsqu'une application cliente doit effectuer une transaction, elle peut sélectionner et utiliser immédiatement toute connexion établie qui ne traite pas actuellement une transaction.

La topologie de chaque système StorageGRID présente un débit maximal différent pour les transactions et les connexions simultanées avant que les performances ne commencent à se dégrader. Le débit maximal dépend de facteurs tels que les ressources informatiques, les ressources réseau, les ressources de stockage et les liaisons WAN. Le nombre de serveurs et de services ainsi que le nombre d'applications prises en charge par le système StorageGRID sont également des facteurs.

Les systèmes StorageGRID prennent souvent en charge plusieurs applications client. Vous devez garder cela à l'esprit lorsque vous déterminez le nombre maximal de connexions simultanées utilisées par une application cliente. Si l'application cliente se compose de plusieurs entités logicielles qui établissent chacune des connexions au système StorageGRID , vous devez additionner toutes les connexions entre les entités. Vous devrez peut-être ajuster le nombre maximal de connexions simultanées dans les situations suivantes :

- La topologie du système StorageGRID affecte le nombre maximal de transactions et de connexions simultanées que le système peut prendre en charge.
- Les applications clientes qui interagissent avec le système StorageGRID sur un réseau à bande passante limitée peuvent devoir réduire le degré de concurrence pour garantir que les transactions individuelles sont terminées dans un délai raisonnable.
- Lorsque de nombreuses applications clientes partagent le système StorageGRID , vous devrez peut-être réduire le degré de concurrence pour éviter de dépasser les limites du système.

Séparation des pools de connexions HTTP pour les opérations de lecture et d'écriture

Vous pouvez utiliser des pools distincts de connexions HTTP pour les opérations de lecture et d'écriture et contrôler la quantité de pool à utiliser pour chacune. Des pools distincts de connexions HTTP vous permettent de mieux contrôler les transactions et d'équilibrer les charges.

Les applications clientes peuvent créer des charges à dominante de récupération (lecture) ou à dominante de stockage (écriture). Avec des pools distincts de connexions HTTP pour les transactions de lecture et d'écriture, vous pouvez ajuster la quantité de chaque pool à dédier aux transactions de lecture ou d'écriture.

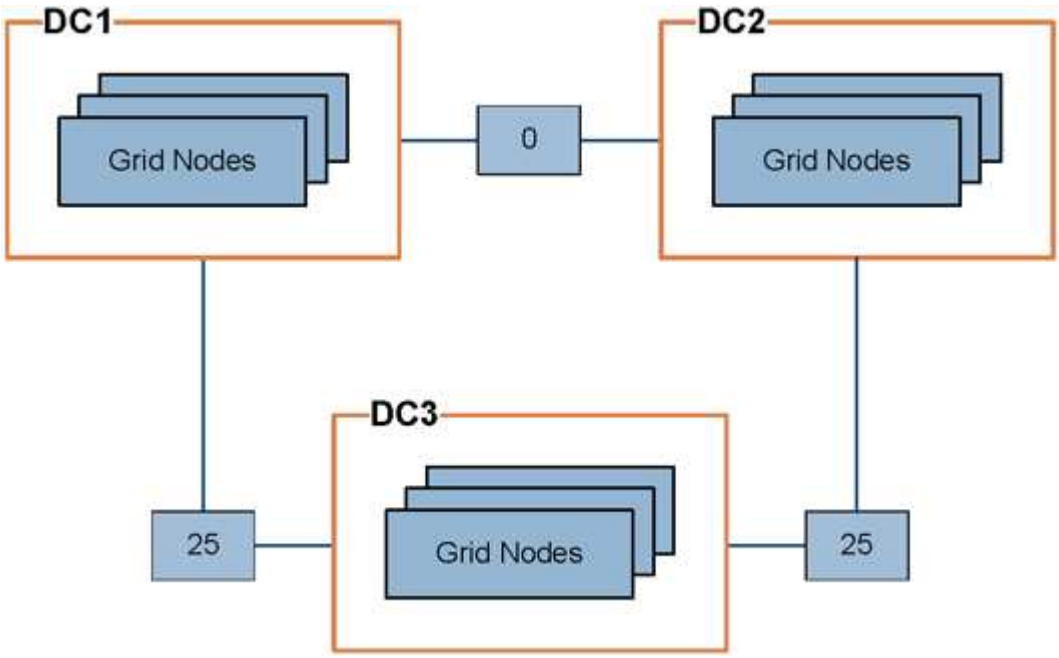
Gérer les coûts de liaison

Les coûts de liaison vous permettent de prioriser le site de centre de données qui fournit un service demandé lorsque deux sites de centre de données ou plus existent. Vous pouvez ajuster les coûts de liaison pour refléter la latence entre les sites.

Quels sont les coûts de liaison ?

- Les coûts de lien sont utilisés pour prioriser la copie d'objet utilisée pour effectuer les récupérations d'objet.
- Les coûts de liaison sont utilisés par l'API Grid Management et l'API Tenant Management pour déterminer les services StorageGRID internes à utiliser.
- Les coûts de liaison sont utilisés par le service Load Balancer sur les nœuds d'administration et les nœuds de passerelle pour diriger les connexions client. Voir "Considérations relatives à l'équilibrage de charge" .

Le diagramme montre une grille à trois sites avec des coûts de liaison configurés entre les sites :



- Le service d'équilibrage de charge sur les nœuds d'administration et les nœuds de passerelle distribue de manière égale les connexions client à tous les nœuds de stockage du même site de centre de données et à tous les sites de centre de données avec un coût de liaison de 0.

  Dans l'exemple, un nœud de passerelle sur le site de centre de données 1 (DC1) distribue de manière égale les connexions client aux nœuds de stockage de DC1 et aux nœuds de stockage de DC2. Un nœud de passerelle sur DC3 envoie des connexions client uniquement aux nœuds de stockage sur DC3.

- Lors de la récupération d'un objet qui existe sous forme de plusieurs copies répliquées, StorageGRID récupère la copie dans le centre de données qui a le coût de liaison le plus bas.

  Dans l'exemple, si une application cliente sur DC2 récupère un objet stocké à la fois sur DC1 et DC3, l'objet est récupéré à partir de DC1, car le coût de liaison de DC1 à DC2 est de 0, ce qui est inférieur au coût de liaison de DC3 à DC2 (25).

Les coûts de liaison sont des nombres relatifs arbitraires sans unité de mesure spécifique. Par exemple, un coût de lien de 50 est utilisé de manière moins préférentielle qu'un coût de lien de 25. Le tableau montre les coûts des liens couramment utilisés.

Lien	Coût du lien	Remarques
Entre les sites de centres de données physiques	25 (par défaut)	Centres de données connectés par une liaison WAN.
Entre les sites de centres de données logiques au même emplacement physique	0	Centres de données logiques dans le même bâtiment physique ou campus connectés par un réseau local.

Coûts de mise à jour des liens

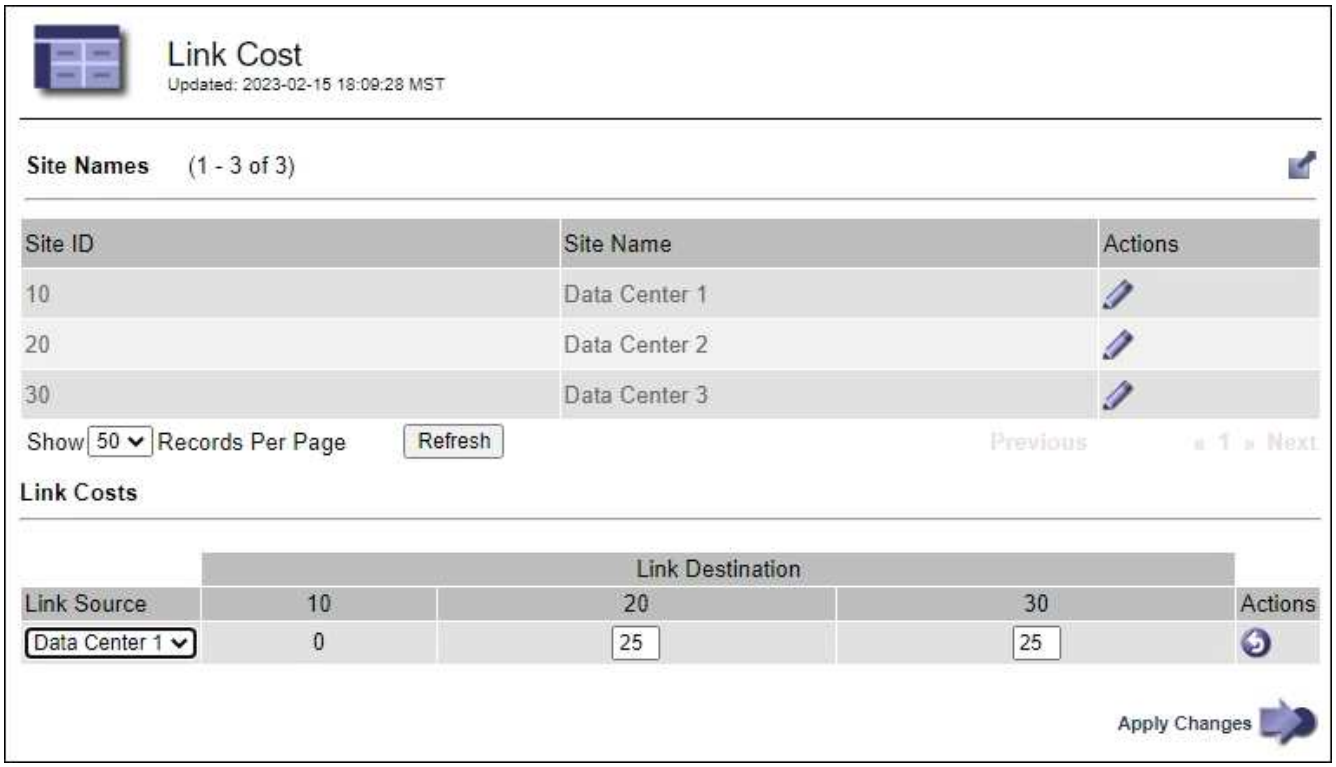
Vous pouvez mettre à jour les coûts de liaison entre les sites du centre de données pour refléter la latence entre les sites.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation de configuration de la page de topologie de grille" .

Étapes

1. Sélectionnez **SUPPORT** > **Autre** > **Coût du lien**.



2. Sélectionnez un site sous **Source du lien** et entrez une valeur de coût comprise entre 0 et 100 sous **Destination du lien**.

   Vous ne pouvez pas modifier le coût du lien si la source est la même que la destination.

   Pour annuler les modifications, sélectionnez **Revenir**.

3. Sélectionnez **Appliquer les modifications**.

Utiliser AutoSupport

Qu’est-ce AutoSupport?

La fonctionnalité AutoSupport permet à StorageGRID d’envoyer des packages d’état et de santé au support technique NetApp .

L’utilisation AutoSupport peut considérablement accélérer la détermination et la résolution des problèmes. Le support technique peut également surveiller les besoins de stockage de votre système et vous aider à déterminer si vous devez ajouter de nouveaux nœuds ou sites. En option, vous pouvez configurer les packages AutoSupport pour qu’ils soient envoyés vers une destination supplémentaire.

StorageGRID dispose de deux types d' AutoSupport:

- * StorageGRID AutoSupport* signale des problèmes logiciels StorageGRID . Activé par défaut lors de la première installation de StorageGRID. Tu peux"modifier la configuration par défaut AutoSupport" si nécessaire.

Si StorageGRID AutoSupport n'est pas activé, un message apparaît sur le tableau de bord du Grid Manager. Le message inclut un lien vers la page de configuration AutoSupport . Si vous fermez le message, il n'apparaîtra plus tant que le cache de votre navigateur n'aura pas été vidé, même si AutoSupport reste désactivé.

- **Appliance hardware AutoSupport** signale des problèmes liés à l'appliance StorageGRID . Vous devez"configurer le matériel AutoSupport sur chaque appareil" .

Qu'est-ce que Active IQ?

Active IQ est un conseiller numérique basé sur le cloud qui exploite l'analyse prédictive et la sagesse de la communauté de la base installée de NetApp. Ses évaluations continues des risques, ses alertes prédictives, ses conseils prescriptifs et ses actions automatisées vous aident à prévenir les problèmes avant qu'ils ne surviennent, ce qui améliore la santé du système et sa disponibilité.

Si vous souhaitez utiliser les tableaux de bord et les fonctionnalités Active IQ sur le site de support NetApp , vous devez activer AutoSupport.

"Documentation du Digital Advisor Active IQ"

Informations incluses dans le package AutoSupport

Un package AutoSupport contient les fichiers et les détails suivants.

Nom des fichiers	Champs	Description
AUTOSUPPORT-HISTORY.XML	Numéro de séquence AutoSupport + Destination pour cet AutoSupport + Statut de livraison + Tentatives de livraison + Objet AutoSupport + URI de livraison + Dernière erreur + Nom de fichier PUT AutoSupport + Heure de génération + Taille compressée AutoSupport + Taille décompressée AutoSupport + Durée totale de collecte (ms)	Fichier historique AutoSupport .
AUTOSUPPORT.XML	Nœud + Protocole pour contacter le support + URL de support pour HTTP/HTTPS + Adresse de support + État AutoSupport OnDemand + URL du serveur AutoSupport OnDemand + Intervalle d'interrogation AutoSupport OnDemand	Fichier d'état AutoSupport . Fournit des détails sur le protocole utilisé, l'URL et l'adresse du support technique, l'intervalle d'interrogation et OnDemand AutoSupport s'il est activé ou désactivé.

Nom des fichiers	Champs	Description
BUCKETS.XML	ID de compartiment + ID de compte + Version de build + Configuration des contraintes d'emplacement + Conformité activée + Configuration de la conformité + Verrouillage d'objet S3 activé + Configuration du verrouillage d'objet S3 + Configuration de la cohérence + CORS activé + Configuration CORS + Heure du dernier accès activée + Politique activée + Configuration de la politique + Notifications activées + Configuration des notifications + Miroir Cloud activé + Configuration Miroir Cloud + Recherche activée + Configuration de la recherche + Balisage de compartiment activé + Configuration du balisage de compartiment + Configuration du contrôle de version	Fournit des détails de configuration et des statistiques au niveau du bucket. Les exemples de configurations de bucket incluent les services de plateforme, la conformité et la cohérence des buckets.
GRID-CONFIGURATIONS.XML	ID d'attribut + Nom d'attribut + Valeur + Index + ID de table + Nom de table	Fichier d'informations de configuration à l'échelle de la grille. Contient des informations sur les certificats de grille, l'espace réservé aux métadonnées, les paramètres de configuration à l'échelle de la grille (conformité, verrouillage d'objet S3, compression d'objet, alertes, syslog et configuration ILM), les détails du profil de codage d'effacement, le nom DNS et"Nom du NMS" .
GRID-SPEC.XML	Spécifications de la grille, XML brut	Utilisé pour configurer et déployer StorageGRID. Contient les spécifications de la grille, l'IP du serveur NTP, l'IP du serveur DNS, la topologie du réseau et les profils matériels des nœuds.
GRID-TASKS.XML	Nœud + Chemin de service + ID d'attribut + Nom d'attribut + Valeur + Index + ID de table + Nom de table	Fichier d'état des tâches de la grille (procédures de maintenance). Fournit des détails sur les tâches actives, terminées, terminées, échouées et en attente de la grille.

Nom des fichiers	Champs	Description
GRILLE.JSON	Grille + Révision + Version du logiciel + Description + Licence + Mots de passe + DNS + NTP + Sites + Nœuds	Informations sur la grille.
ILM-CONFIGURATION.XML	ID d'attribut + Nom d'attribut + Valeur + Index + ID de table + Nom de table	Liste des attributs pour les configurations ILM.
ILM-STATUT.XML	Nœud + Chemin de service + ID d'attribut + Nom d'attribut + Valeur + Index + ID de table + Nom de table	Fichier d'informations sur les métriques ILM. Contient les taux d'évaluation ILM pour chaque nœud et les mesures à l'échelle de la grille.
ILM.XML	XML brut ILM	Fichier de politique active ILM. Contient des détails sur les politiques ILM actives, telles que l'ID du pool de stockage, le comportement d'ingestion, les filtres, les règles et la description.
LOG.TGZ	*n / A*	Fichier journal téléchargeable. Contient `bycast-err.log` et `servermanager.log` de chaque nœud.
MANIFEST.XML	Ordre de collecte + Nom du fichier de contenu AutoSupport pour ces données + Description de cet élément de données + Nombre d'octets collectés + Temps passé à collecter + Statut de cet élément de données + Description de l'erreur + Type de contenu AutoSupport pour ces données	Contient les métadonnées AutoSupport et de brèves descriptions de tous les fichiers AutoSupport .
NMS-ENTITÉS.XML	Index d'attribut + OID d'entité + ID de nœud + ID de modèle d'appareil + Version du modèle d'appareil + Nom d'entité	Entités de groupe et de service dans le"arbre NMS" . Fournit des détails sur la topologie de la grille. Le nœud peut être déterminé en fonction des services exécutés sur le nœud.

Nom des fichiers	Champs	Description
OBJETS-STATUS.XML	Nœud + Chemin de service + ID d'attribut + Nom d'attribut + Valeur + Index + ID de table + Nom de table	État de l'objet, y compris l'état de l'analyse en arrière-plan, le transfert actif, le taux de transfert, le nombre total de transferts, le taux de suppression, les fragments corrompus, les objets perdus, les objets manquants, la tentative de réparation, le taux d'analyse, la période d'analyse estimée et l'état d'achèvement de la réparation.
SERVER-STATUS.XML	Nœud + Chemin de service + ID d'attribut + Nom d'attribut + Valeur + Index + ID de table + Nom de table	Configurations du serveur. Contient ces détails pour chaque nœud : type de plate-forme, système d'exploitation, mémoire installée, mémoire disponible, connectivité de stockage, numéro de série du châssis du dispositif de stockage, nombre de disques défaillants du contrôleur de stockage, température du châssis du contrôleur de calcul, matériel de calcul, numéro de série du contrôleur de calcul, alimentation, taille du disque et type de disque.
SERVICE-STATUS.XML	Nœud + Chemin de service + ID d'attribut + Nom d'attribut + Valeur + Index + ID de table + Nom de table	Fichier d'informations sur le nœud de service. Contient des détails tels que l'espace table alloué, l'espace table libre, les métriques Reaper de la base de données, la durée de réparation du segment, la durée du travail de réparation, les redémarrages automatiques du travail et l'arrêt automatique du travail.
NIVEAUX DE STOCKAGE.XML	ID de niveau de stockage + Nom de niveau de stockage + ID de nœud de stockage + Chemin du nœud de stockage	Fichier de définitions de qualité de stockage pour chaque nœud de stockage.
RÉSUMÉ-ATTRIBUTS.XML	OID du groupe + Chemin du groupe + ID de l'attribut récapitulatif + Nom de l'attribut récapitulatif + Valeur + Index + ID de la table + Nom de la table	Données d'état du système de haut niveau qui résument les informations d'utilisation de StorageGRID . Fournit des détails tels que le nom de la grille, les noms des sites, le nombre de nœuds de stockage par grille et par site, le type de licence, la capacité et l'utilisation de la licence, les conditions de support logiciel et les détails des opérations S3.

Nom des fichiers	Champs	Description
ALERTES-SYSTEME.XML	Nom + Gravité + Nom du nœud + État de l'alerte + Nom du site + Heure de déclenchement de l'alerte + Heure de résolution de l'alerte + ID de règle + ID du nœud + ID du site + Silencieux + Autres annotations + Autres étiquettes	Alertes système actuelles indiquant des problèmes potentiels dans le système StorageGRID .
USERAGENTS.XML	Agent utilisateur + Nombre de jours + Nombre total de requêtes HTTP + Nombre total d'octets ingérés + Nombre total d'octets récupérés + Requêtes PUT + Requêtes GET + Requêtes DELETE + Requêtes HEAD + Requêtes POST + Requêtes OPTIONS + Temps moyen de requête (ms) + Temps moyen de requête PUT (ms) + Temps moyen de requête GET (ms) + Temps moyen de requête DELETE (ms) + Temps moyen de requête HEAD (ms) + Temps moyen de requête POST (ms) + Temps moyen de requête OPTIONS (ms)	Statistiques basées sur les agents utilisateurs de l'application. Par exemple, le nombre d'opérations PUT/GET/DELETE/HEAD par agent utilisateur et la taille totale en octets de chaque opération.
X-HEADER-DATA	X-Netapp-asup-generated-on + X-Netapp-asup-hostname + X-Netapp-asup-os-version + X-Netapp-asup-serial-num + X-Netapp-asup-subject + X-Netapp-asup-system-id + X-Netapp-asup-model-name	Données d'en-tête AutoSupport .

Configurer AutoSupport

Par défaut, la fonctionnalité StorageGRID AutoSupport est activée lors de la première installation de StorageGRID. Cependant, vous devez configurer le matériel AutoSupport sur chaque appareil. Selon vos besoins, vous pouvez modifier la configuration AutoSupport .

Si vous souhaitez modifier la configuration de StorageGRID AutoSupport, effectuez vos modifications uniquement sur le nœud d'administration principal. Vous devezconfigurer le matériel AutoSupport sur chaque appareil.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès root" .
- Si vous utilisez HTTPS pour envoyer des packages AutoSupport , vous avez fourni un accès Internet sortant au nœud d'administration principal, soit directement, soit"en utilisant un serveur proxy" (connexions entrantes non requises).
- Si HTTP est sélectionné sur la page StorageGRID AutoSupport , vous avez"configuré un serveur proxy" pour transférer les packages AutoSupport en HTTPS. Les serveurs AutoSupport de NetApp rejetteront les packages envoyés via HTTP.
- Si vous utilisez SMTP comme protocole pour les packages AutoSupport , vous avez configuré un serveur de messagerie SMTP.

À propos de cette tâche

Vous pouvez utiliser n'importe quelle combinaison des options suivantes pour envoyer des packages AutoSupport au support technique :

- **Hebdomadaire** : envoie automatiquement des packages AutoSupport une fois par semaine. Paramètre par défaut : Activé.
- **Déclenché par événement** : envoyez automatiquement des packages AutoSupport toutes les heures ou lorsque des événements système importants se produisent. Paramètre par défaut : Activé.
- **À la demande** : autorisez le support technique à demander à votre système StorageGRID d'envoyer automatiquement des packages AutoSupport , ce qui est utile lorsqu'ils travaillent activement sur un problème (nécessite le protocole de transmission HTTPS AutoSupport). Paramètre par défaut : désactivé.
- **Déclenché par l'utilisateur** : envoyez manuellement des packages AutoSupport à tout moment.

Spécifiez le protocole pour les packages AutoSupport

Vous pouvez utiliser l'un des protocoles suivants pour envoyer des packages AutoSupport :

- **HTTPS** : il s'agit du paramètre par défaut et recommandé pour les nouvelles installations. Ce protocole utilise le port 443. Si tu veuxactiver la fonctionnalité AutoSupport à la demande , vous devez utiliser HTTPS.
- **HTTP** : si vous sélectionnez HTTP, vous devez configurer un serveur proxy pour transférer les packages AutoSupport en HTTPS. Les serveurs AutoSupport de NetApp rejettent les packages envoyés via HTTP. Ce protocole utilise le port 80.
- **SMTP** : utilisez cette option si vous souhaitez que les packages AutoSupport soient envoyés par courrier électronique.

Le protocole que vous définissez est utilisé pour envoyer tous les types de packages AutoSupport .

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > * AutoSupport* > **Paramètres**.
2. Sélectionnez le protocole que vous souhaitez utiliser pour envoyer des packages AutoSupport .
3. Si vous avez sélectionné **HTTPS**, indiquez si vous souhaitez utiliser un certificat de support NetApp (certificat TLS) pour sécuriser la connexion au serveur de support technique.
   - **Vérifier le certificat** (par défaut) : garantit que la transmission des packages AutoSupport est sécurisée. Le certificat de support NetApp est déjà installé avec le logiciel StorageGRID .
   - **Ne pas vérifier le certificat** : sélectionnez cette option uniquement lorsque vous avez une bonne raison de ne pas utiliser la validation de certificat, par exemple en cas de problème temporaire avec un

certificat.

4. Sélectionnez **Enregistrer**. Tous les packages hebdomadaires, déclenchés par l'utilisateur et déclenchés par un événement sont envoyés à l'aide du protocole sélectionné.

Désactiver AutoSupport hebdomadaire

Par défaut, le système StorageGRID est configuré pour envoyer un package AutoSupport au support technique une fois par semaine.

Pour déterminer quand le package AutoSupport hebdomadaire sera envoyé, accédez à l'onglet * AutoSupport* > **Résultats**. Dans la section **Weekly AutoSupport**, regardez la valeur de **Next Scheduled Time**.

Vous pouvez désactiver l'envoi automatique des packages AutoSupport hebdomadaires à tout moment.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > * AutoSupport* > **Paramètres**.
2. Décochez la case **Activer AutoSupport hebdomadaire**.
3. Sélectionnez **Enregistrer**.

Désactiver AutoSupport déclenché par un événement

Par défaut, le système StorageGRID est configuré pour envoyer un package AutoSupport au support technique toutes les heures.

Vous pouvez désactiver AutoSupport déclenché par un événement à tout moment.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > * AutoSupport* > **Paramètres**.
2. Décochez la case **Activer AutoSupport déclenchée par événement**.
3. Sélectionnez **Enregistrer**.

Activer AutoSupport à la demande

AutoSupport on Demand peut vous aider à résoudre les problèmes sur lesquels le support technique travaille activement.

Par défaut, AutoSupport on Demand est désactivé. L'activation de cette fonctionnalité permet au support technique de demander à votre système StorageGRID d'envoyer automatiquement les packages AutoSupport . Le support technique peut également définir l'intervalle de temps d'interrogation pour les requêtes AutoSupport à la demande.

Le support technique ne peut pas activer ou désactiver AutoSupport à la demande.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > * AutoSupport* > **Paramètres**.
2. Sélectionnez **HTTPS** pour le protocole.
3. Cochez la case **Activer AutoSupport hebdomadaire**.
4. Cochez la case **Activer AutoSupport à la demande**.
5. Sélectionnez **Enregistrer**.

AutoSupport on Demand est activé et le support technique peut envoyer des demandes AutoSupport on Demand à StorageGRID.

Désactiver les vérifications des mises à jour logicielles

Par défaut, StorageGRID contacte NetApp pour déterminer si des mises à jour logicielles sont disponibles pour votre système. Si un correctif ou une nouvelle version de StorageGRID est disponible, la nouvelle version est affichée sur la page de mise à niveau de StorageGRID .

Si nécessaire, vous pouvez éventuellement désactiver la vérification des mises à jour logicielles. Par exemple, si votre système ne dispose pas d'accès WAN, vous devez désactiver la vérification pour éviter les erreurs de téléchargement.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > * AutoSupport* > **Paramètres**.
2. Décochez la case **Vérifier les mises à jour logicielles**.
3. Sélectionnez **Enregistrer**.

Ajouter une destination AutoSupport supplémentaire

Lorsque vous activez AutoSupport, les packages de santé et d'état sont envoyés au support technique. Vous pouvez spécifier une destination supplémentaire pour tous les packages AutoSupport .

Pour vérifier ou modifier le protocole utilisé pour envoyer les packages AutoSupport , consultez les instructions pourspécifier le protocole pour les packages AutoSupport .

> Vous ne pouvez pas utiliser le protocole SMTP pour envoyer des packages AutoSupport vers une destination supplémentaire.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > * AutoSupport* > **Paramètres**.
2. Sélectionnez **Activer la destination AutoSupport supplémentaire**.
3. Précisez les éléments suivants :

Nom d'hôte

Le nom d'hôte du serveur ou l'adresse IP d'un serveur de destination AutoSupport supplémentaire.

> Vous ne pouvez saisir qu'une seule destination supplémentaire.

Port

Le port utilisé pour se connecter à un serveur de destination AutoSupport supplémentaire. La valeur par défaut est le port 80 pour HTTP ou le port 443 pour HTTPS.

Validation du certificat

Si un certificat TLS est utilisé pour sécuriser la connexion à la destination supplémentaire.

- Sélectionnez **Vérifier le certificat** pour utiliser la validation du certificat.
- Sélectionnez **Ne pas vérifier le certificat** pour envoyer vos packages AutoSupport sans validation de certificat.

Sélectionnez cette option uniquement lorsque vous avez une bonne raison de ne pas utiliser la validation de certificat, par exemple en cas de problème temporaire avec un certificat.

4. Si vous avez sélectionné **Vérifier le certificat**, procédez comme suit :
   a. Accédez à l'emplacement du certificat CA.
   b. Téléchargez le fichier de certificat CA.

      Les métadonnées du certificat CA s'affichent.

5. Sélectionnez **Enregistrer**.

   Tous les futurs packages AutoSupport hebdomadaires, déclenchés par des événements et déclenchés par l'utilisateur seront envoyés vers la destination supplémentaire.

Configurer AutoSupport pour les appareils

AutoSupport pour les appliances signale les problèmes matériels StorageGRID et StorageGRID AutoSupport signale les problèmes logiciels StorageGRID , à une exception près : pour le SGF6112, StorageGRID AutoSupport signale les problèmes matériels et logiciels. Vous devez configurer AutoSupport sur chaque appareil, à l'exception du SGF6112, qui ne nécessite pas de configuration supplémentaire. AutoSupport est implémenté différemment pour les appliances de services et les appliances de stockage.

Vous utilisez SANtricity pour activer AutoSupport pour chaque appliance de stockage. Vous pouvez configurer SANtricity AutoSupport lors de la configuration initiale de l'appliance ou après l'installation d'une appliance :

- Pour les appareils SG6000 et SG5700, "configurer AutoSupport dans SANtricity System Manager"

Les packages AutoSupport des appliances de la série E peuvent être inclus dans StorageGRID AutoSupport si vous configurez la livraison AutoSupport par proxy dans"Gestionnaire de système SANtricity" .

StorageGRID AutoSupport ne signale pas les problèmes matériels, tels que les défauts de DIMM ou de carte d'interface hôte (HIC). Cependant, certaines défaillances de composants peuvent déclencher"alertes matérielles" . Pour les appliances StorageGRID avec un contrôleur de gestion de la carte mère (BMC), vous pouvez configurer des interruptions de messagerie et SNMP pour signaler les pannes matérielles :

- "Configurer des notifications par e-mail pour les alertes BMC"
- "Configurer les paramètres SNMP pour BMC"

Informations connexes

"Assistance NetApp"

Déclencher manuellement un package AutoSupport

Pour aider le support technique à résoudre les problèmes liés à votre système StorageGRID , vous pouvez déclencher manuellement l'envoi d'un package AutoSupport .

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous devez disposer de l'accès root ou de l'autorisation de configuration d'une autre grille.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > * AutoSupport*.
2. Dans l'onglet **Actions**, sélectionnez **Envoyer AutoSupport déclenchée par l'utilisateur**.

   StorageGRID tente d'envoyer un package AutoSupport au site de support NetApp . Si la tentative réussit, les valeurs **Résultat le plus récent** et **Dernière heure de réussite** dans l'onglet **Résultats** sont mises à jour. En cas de problème, la valeur **Résultat le plus récent** est mise à jour sur « Échec » et StorageGRID n'essaie pas d'envoyer à nouveau le package AutoSupport .

   Après avoir envoyé un package AutoSupport déclenché par l'utilisateur, actualisez la page AutoSupport dans votre navigateur après 1 minute pour accéder aux résultats les plus récents.

Dépannage des packages AutoSupport

Si une tentative d'envoi d'un package AutoSupport échoue, le système StorageGRID entreprend différentes actions selon le type de package AutoSupport . Vous pouvez vérifier l'état des packages AutoSupport en sélectionnant **SUPPORT** > **Outils** > * AutoSupport* > **Résultats**.

Lorsque le package AutoSupport ne parvient pas à être envoyé, « Échec » s'affiche dans l'onglet **Résultats** de la page * AutoSupport*.

Si vous avez configuré un serveur proxy pour transférer les packages AutoSupport vers NetApp, vous devez"vérifier que les paramètres de configuration du serveur proxy sont corrects" .

Échec hebdomadaire du package AutoSupport

Si un package AutoSupport hebdomadaire ne parvient pas à être envoyé, le système StorageGRID prend les mesures suivantes :

1. Met à jour l'attribut Résultat le plus récent sur Nouvelle tentative.
2. Tente de renvoyer le package AutoSupport 15 fois toutes les quatre minutes pendant une heure.
3. Après une heure d'échecs d'envoi, met à jour l'attribut Résultat le plus récent sur Échec.
4. Tente d'envoyer à nouveau un package AutoSupport à la prochaine heure programmée.
5. Maintient le calendrier AutoSupport régulier si le package échoue parce que le service NMS n'est pas disponible et si un package est envoyé avant sept jours.
6. Lorsque le service NMS est à nouveau disponible, il envoie immédiatement un package AutoSupport si aucun package n'a été envoyé pendant sept jours ou plus.

Échec du package AutoSupport déclenché par l'utilisateur ou par un événement

Si un package AutoSupport déclenché par un utilisateur ou un événement ne parvient pas à être envoyé, le système StorageGRID exécute les actions suivantes :

1. Affiche un message d'erreur si l'erreur est connue. Par exemple, si un utilisateur sélectionne le protocole SMTP sans fournir les paramètres de configuration de messagerie corrects, l'erreur suivante s'affiche : `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

2. N'essayez pas de renvoyer le colis.
3. Enregistre l'erreur dans `nms.log` .

Si une panne se produit et que SMTP est le protocole sélectionné, vérifiez que le serveur de messagerie du système StorageGRID est correctement configuré et que votre serveur de messagerie est en cours d'exécution (**SUPPORT** > **Alarmes (héritées)** > **Configuration de la messagerie héritée**). Le message d'erreur suivant peut apparaître sur la page AutoSupport : `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Découvrez comment "configurer les paramètres du serveur de messagerie" .

Corriger une défaillance du package AutoSupport

Si une panne se produit et que SMTP est le protocole sélectionné, vérifiez que le serveur de messagerie du système StorageGRID est correctement configuré et que votre serveur de messagerie est en cours d'exécution. Le message d'erreur suivant peut apparaître sur la page AutoSupport : `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Envoyer des packages AutoSupport de la série E via StorageGRID

Vous pouvez envoyer des packages E-Series SANtricity System Manager AutoSupport au support technique via un nœud d'administration StorageGRID plutôt que via le port de gestion du dispositif de stockage.

Voir "AutoSupport du matériel de la série E" pour plus d'informations sur l'utilisation AutoSupport avec les appareils de la série E.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Administrateur de l'appareil de stockage ou autorisation d'accès root" .
- Vous avez configuré SANtricity AutoSupport:
  - Pour les appareils SG6000 et SG5700, "configurer AutoSupport dans SANtricity System Manager"

> Vous devez disposer du micrologiciel SANtricity 8.70 ou supérieur pour accéder à SANtricity System Manager à l'aide de Grid Manager.

À propos de cette tâche

Les packages AutoSupport de la série E contiennent des détails sur le matériel de stockage et sont plus spécifiques que les autres packages AutoSupport envoyés par le système StorageGRID .

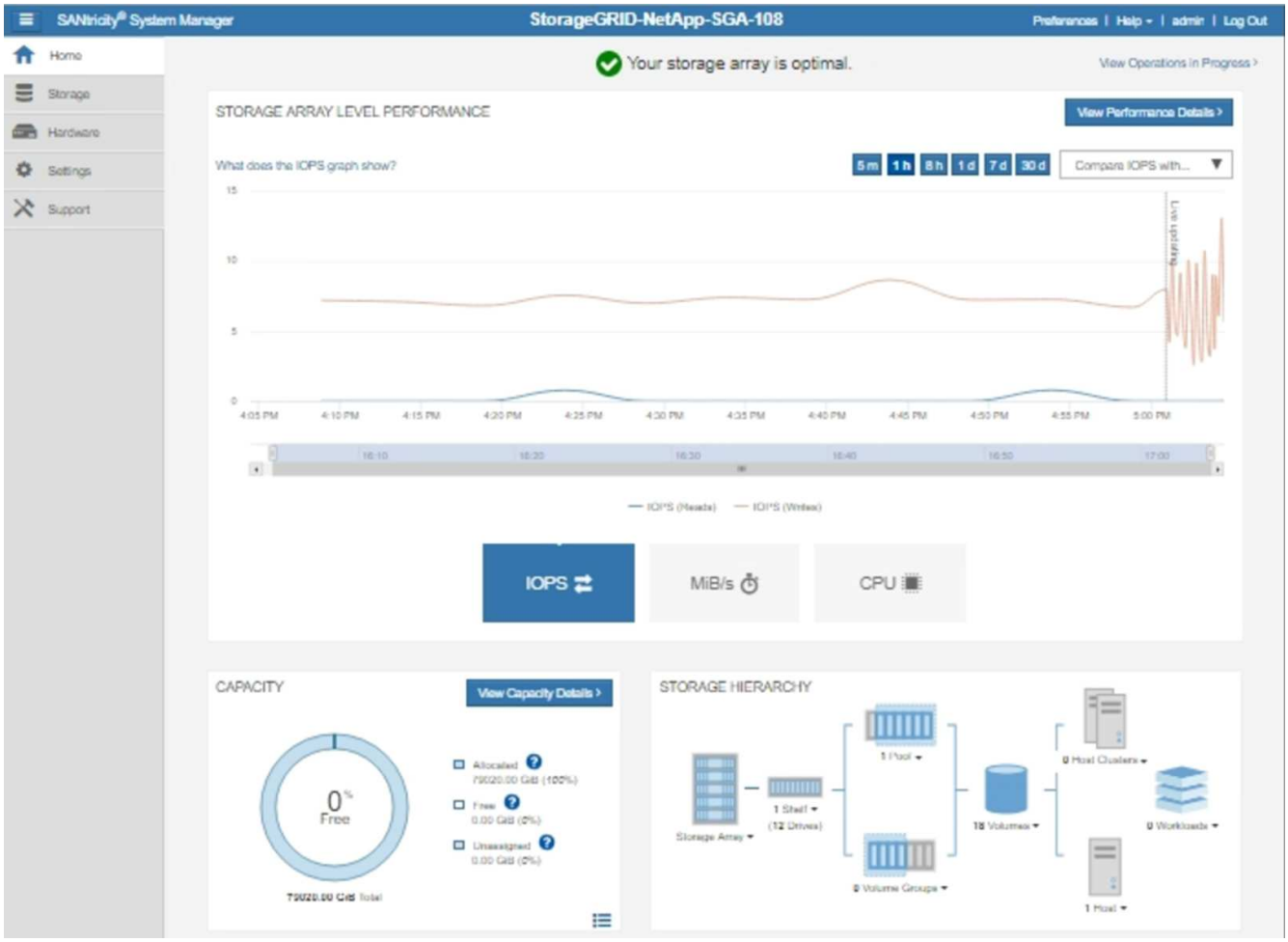
Vous pouvez configurer une adresse de serveur proxy spéciale dans SANtricity System Manager pour transmettre des packages AutoSupport via un nœud d'administration StorageGRID sans utiliser le port de gestion de l'appliance. Les packages AutoSupport transmis de cette manière sont envoyés par le"nœud d'administration de l'expéditeur préféré" , et ils utilisent n'importe quel"paramètres de proxy d'administration" qui ont été configurés dans le Grid Manager.

> Cette procédure concerne uniquement la configuration d'un serveur proxy StorageGRID pour les packages AutoSupport de la série E. Pour plus de détails sur la configuration AutoSupport de la série E, consultez le "Documentation NetApp E-Series et SANtricity" .

Étapes

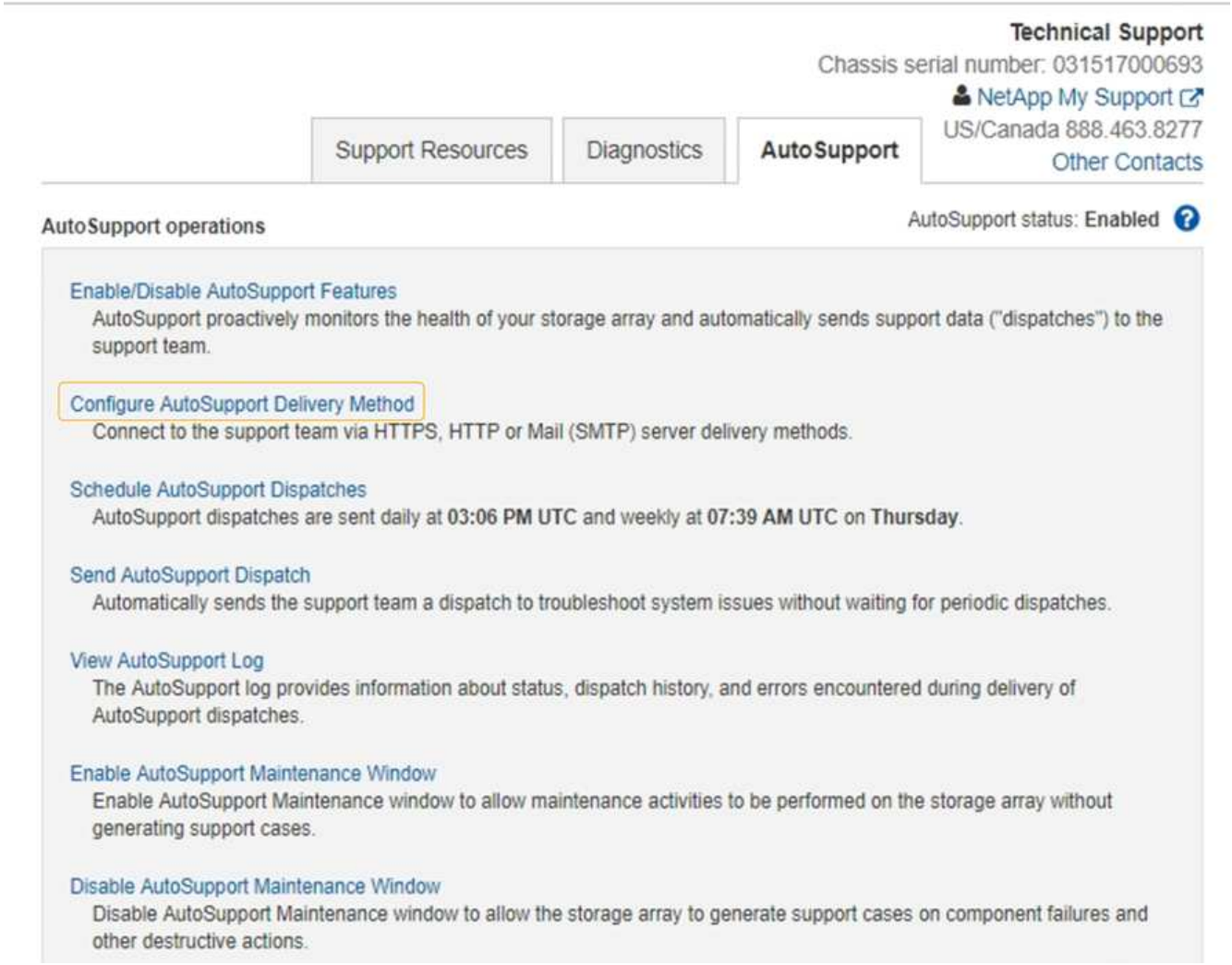
1. Dans le gestionnaire de grille, sélectionnez **NODES**.
2. Dans la liste des nœuds sur la gauche, sélectionnez le nœud du dispositif de stockage que vous souhaitez configurer.
3. Sélectionnez * SANtricity System Manager*.

   La page d'accueil de SANtricity System Manager apparaît.



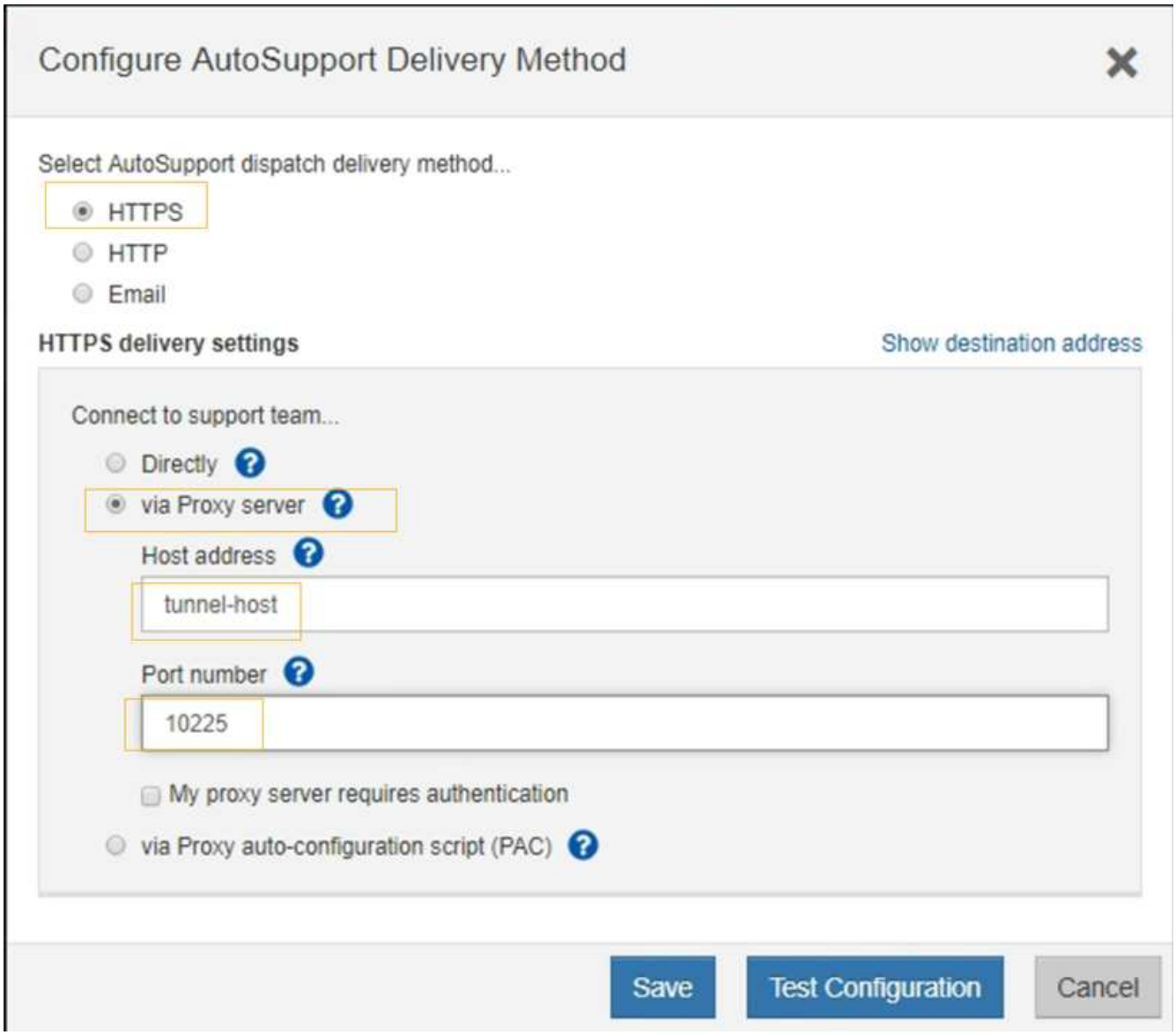
4. Sélectionnez **SUPPORT** > **Centre d'assistance** > * AutoSupport*.

   La page des opérations AutoSupport s'affiche.



5. Sélectionnez *Configurer la méthode de livraison AutoSupport *.

   La page Configurer la méthode de livraison AutoSupport s’affiche.



6. Sélectionnez **HTTPS** comme méthode de livraison.

   Le certificat qui active HTTPS est préinstallé.

7. Sélectionnez **via le serveur proxy**.
8. Entrer `tunnel-host` pour l'**adresse de l'hôte**.

   `tunnel-host`est l'adresse spéciale à utiliser pour un nœud d'administration afin d'envoyer des packages AutoSupport de la série E.

9. Entrer `10225` pour le **Numéro de port**.

   `10225`est le numéro de port sur le serveur proxy StorageGRID qui reçoit les packages AutoSupport du contrôleur E-Series de l'appliance.

10. Sélectionnez **Tester la configuration** pour tester le routage et la configuration de votre serveur proxy AutoSupport .

    Si c'est correct, un message dans une bannière verte apparaît : « Votre configuration AutoSupport a été

vérifiée. »

Si le test échoue, un message d'erreur apparaît dans une bannière rouge. Vérifiez vos paramètres DNS et votre réseau StorageGRID , assurez-vous que"nœud d'administration de l'expéditeur préféré" peut se connecter au site de support NetApp et réessayer le test.

11. Sélectionnez **Enregistrer**.

    La configuration est enregistrée et un message de confirmation s'affiche : « La méthode de livraison AutoSupport a été configurée. »

Gérer les nœuds de stockage

Gérer les nœuds de stockage

Les nœuds de stockage fournissent une capacité de stockage sur disque et des services. La gestion des nœuds de stockage implique les opérations suivantes :

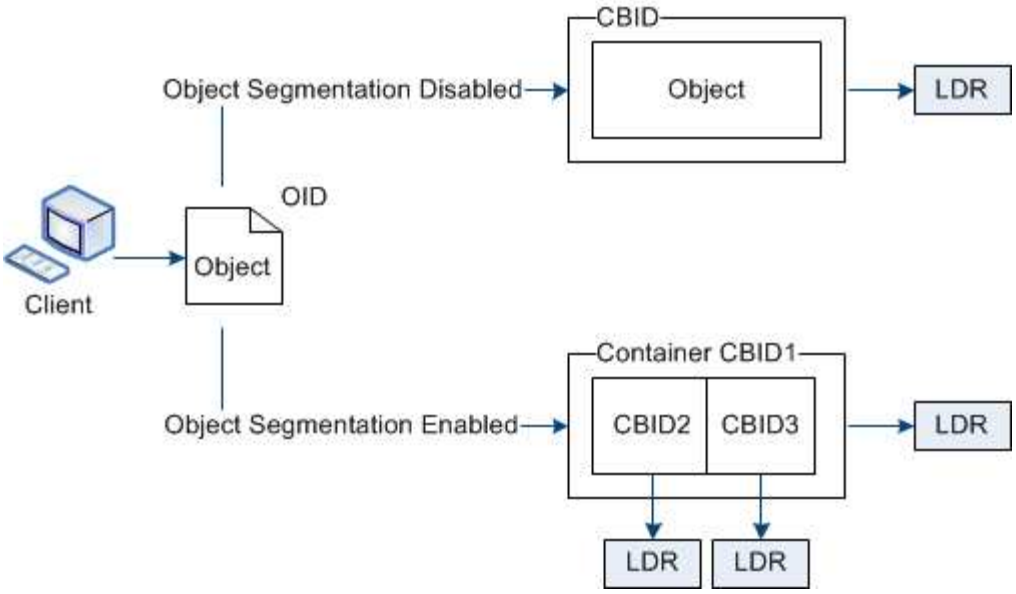
- Gestion des options de stockage
- Comprendre ce que sont les filigranes de volume de stockage et comment vous pouvez utiliser les remplacements de filigrane pour contrôler le moment où les nœuds de stockage deviennent en lecture seule
- Surveillance et gestion de l'espace utilisé pour les métadonnées des objets
- Configuration des paramètres globaux pour les objets stockés
- Application des paramètres de configuration du nœud de stockage
- Gestion des nœuds de stockage complets

Utiliser les options de stockage

Qu'est-ce que la segmentation d'objets ?

La segmentation d'objets est le processus de division d'un objet en une collection d'objets plus petits de taille fixe pour optimiser le stockage et l'utilisation des ressources pour les objets volumineux. Le téléchargement multi-parties S3 crée également des objets segmentés, avec un objet représentant chaque partie.

Lorsqu'un objet est ingéré dans le système StorageGRID , le service LDR divise l'objet en segments et crée un conteneur de segments qui répertorie les informations d'en-tête de tous les segments en tant que contenu.



Lors de la récupération d'un conteneur de segments, le service LDR assemble l'objet d'origine à partir de ses segments et renvoie l'objet au client.

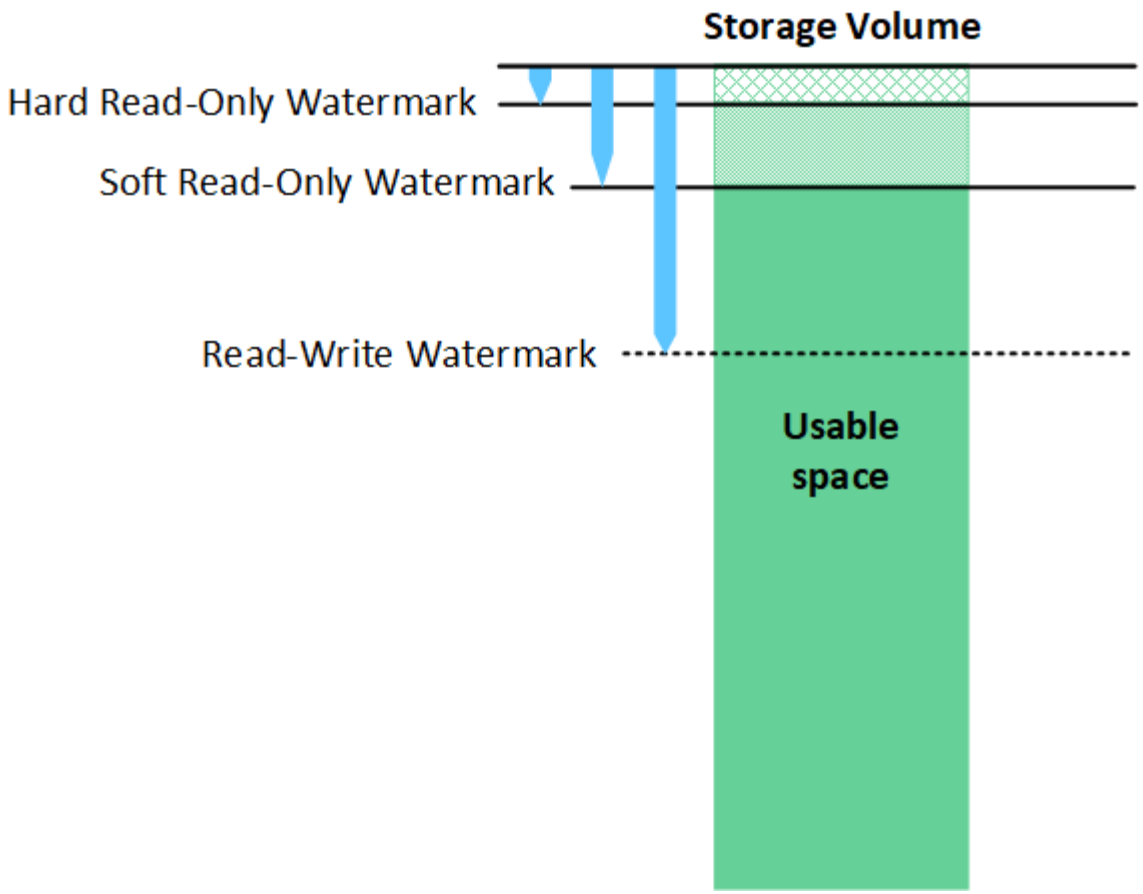
Le conteneur et les segments ne sont pas nécessairement stockés sur le même nœud de stockage. Le conteneur et les segments peuvent être stockés sur n'importe quel nœud de stockage au sein du pool de stockage spécifié dans la règle ILM.

Chaque segment est traité indépendamment par le système StorageGRID et contribue au nombre d'attributs tels que les objets gérés et les objets stockés. Par exemple, si un objet stocké dans le système StorageGRID est divisé en deux segments, la valeur des objets gérés augmente de trois une fois l'ingestion terminée, comme suit :

```
segment container + segment 1 + segment 2 = three stored objects
```

Que sont les filigranes de volume de stockage ?

StorageGRID utilise trois filigranes de volume de stockage pour garantir que les nœuds de stockage sont transférés en toute sécurité vers un état de lecture seule avant de manquer d'espace de manière critique et pour permettre aux nœuds de stockage qui sont passés à un état de lecture seule de redevenir en lecture-écriture.



Les filigranes de volume de stockage s'appliquent uniquement à l'espace utilisé pour les données d'objet répliquées et codées par effacement. Pour en savoir plus sur l'espace réservé aux métadonnées des objets sur le volume 0, rendez-vous sur"Gérer le stockage des métadonnées des objets" .

Qu'est-ce que le filigrane souple en lecture seule ?

Le **filigrane en lecture seule du volume de stockage** est le premier filigrane à indiquer que l'espace utilisable d'un nœud de stockage pour les données d'objet est en train de devenir plein.

Si chaque volume d'un nœud de stockage dispose de moins d'espace libre que le filigrane en lecture seule de ce volume, le nœud de stockage passe en mode lecture seule. Le mode lecture seule signifie que le nœud de stockage annonce les services en lecture seule au reste du système StorageGRID , mais répond à toutes les demandes d'écriture en attente.

Par exemple, supposons que chaque volume d'un nœud de stockage possède un filigrane en lecture seule souple de 10 Go. Dès que chaque volume dispose de moins de 10 Go d'espace libre, le nœud de stockage passe en mode lecture seule logicielle.

Qu'est-ce que le filigrane en lecture seule ?

Le **filigrane de lecture seule du volume de stockage** est le prochain filigrane à indiquer que l'espace utilisable d'un nœud pour les données d'objet est en train de devenir plein.

Si l'espace libre sur un volume est inférieur au filigrane en lecture seule de ce volume, les écritures sur le volume échoueront. Toutefois, les écritures sur d'autres volumes peuvent continuer jusqu'à ce que l'espace libre sur ces volumes soit inférieur à leurs filigranes en lecture seule.

Par exemple, supposons que chaque volume d'un nœud de stockage possède un filigrane en lecture seule de 5 Go. Dès que chaque volume dispose de moins de 5 Go d'espace libre, le nœud de stockage n'accepte plus aucune demande d'écriture.

Le filigrane en lecture seule dur est toujours inférieur au filigrane en lecture seule souple.

Qu'est-ce que le filigrane en lecture-écriture ?

Le **filigrane de lecture-écriture du volume de stockage** s'applique uniquement aux nœuds de stockage qui sont passés en mode lecture seule. Il détermine quand le nœud peut redevenir en lecture-écriture. Lorsque l'espace libre sur un volume de stockage d'un nœud de stockage est supérieur au filigrane de lecture-écriture de ce volume, le nœud revient automatiquement à l'état de lecture-écriture.

Par exemple, supposons que le nœud de stockage soit passé en mode lecture seule. Supposons également que chaque volume possède un filigrane de lecture-écriture de 30 Go. Dès que l'espace libre pour un volume augmente à 30 Go, le nœud redevient en lecture-écriture.

Le filigrane en lecture-écriture est toujours plus grand que le filigrane en lecture seule souple et que le filigrane en lecture seule rigide.

Afficher les filigranes du volume de stockage

Vous pouvez afficher les paramètres de filigrane actuels et les valeurs optimisées pour le système. Si des filigranes optimisés ne sont pas utilisés, vous pouvez déterminer si vous pouvez ou devez ajuster les paramètres.

Avant de commencer

- Vous avez terminé la mise à niveau vers StorageGRID 11.6 ou supérieur.
- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès root" .

Afficher les paramètres de filigrane actuels

Vous pouvez afficher les paramètres de filigrane de stockage actuels dans le gestionnaire de grille.

Étapes

1. Sélectionnez **SUPPORT** > **Autre** > **Filigranes de stockage**.
2. Sur la page Filigranes de stockage, cochez la case Utiliser des valeurs optimisées.
   - Si la case à cocher est sélectionnée, les trois filigranes sont optimisés pour chaque volume de stockage sur chaque nœud de stockage, en fonction de la taille du nœud de stockage et de la capacité relative du volume.

     Il s'agit du paramètre par défaut et recommandé. Ne mettez pas à jour ces valeurs. En option, vous pouvezAfficher les filigranes de stockage optimisés .
   - Si la case à cocher Utiliser les valeurs optimisées n'est pas sélectionnée, des filigranes personnalisés (non optimisés) sont utilisés. L'utilisation de paramètres de filigrane personnalisés n'est pas recommandée. Utilisez les instructions pour"dépannage des alertes de remplacement du filigrane en lecture seule faible" pour déterminer si vous pouvez ou devez ajuster les paramètres.

     Lorsque vous spécifiez des paramètres de filigrane personnalisés, vous devez saisir des valeurs supérieures à 0.

Afficher les filigranes de stockage optimisés

StorageGRID utilise deux mesures Prometheus pour afficher les valeurs optimisées qu'il a calculées pour le filigrane en lecture seule du volume de stockage. Vous pouvez afficher les valeurs optimisées minimales et maximales pour chaque nœud de stockage de votre grille.

1. Sélectionnez **SUPPORT** > **Outils** > **Métriques**.
2. Dans la section Prometheus, sélectionnez le lien pour accéder à l'interface utilisateur de Prometheus.
3. Pour voir le filigrane en lecture seule minimal recommandé, entrez la métrique Prometheus suivante et sélectionnez **Exécuter** :

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   La dernière colonne affiche la valeur optimisée minimale du filigrane en lecture seule souple pour tous les volumes de stockage sur chaque nœud de stockage. Si cette valeur est supérieure au paramètre personnalisé pour le filigrane en lecture seule logicielle du volume de stockage, l'alerte **Remplacement du filigrane en lecture seule faible** est déclenchée pour le nœud de stockage.

4. Pour voir le filigrane en lecture seule maximal recommandé, entrez la métrique Prometheus suivante et sélectionnez **Exécuter** :

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   La dernière colonne affiche la valeur optimisée maximale du filigrane en lecture seule pour tous les volumes de stockage sur chaque nœud de stockage.

Gérer le stockage des métadonnées des objets

La capacité des métadonnées d'objet d'un système StorageGRID contrôle le nombre maximal d'objets pouvant être stockés sur ce système. Pour garantir que votre système StorageGRID dispose de suffisamment d'espace pour stocker de nouveaux objets, vous devez comprendre où et comment StorageGRID stocke les métadonnées des objets.

Que sont les métadonnées d'objet ?

Les métadonnées d'objet sont toutes les informations qui décrivent un objet. StorageGRID utilise les métadonnées des objets pour suivre les emplacements de tous les objets sur la grille et pour gérer le cycle de vie de chaque objet au fil du temps.

Pour un objet dans StorageGRID, les métadonnées de l'objet incluent les types d'informations suivants :

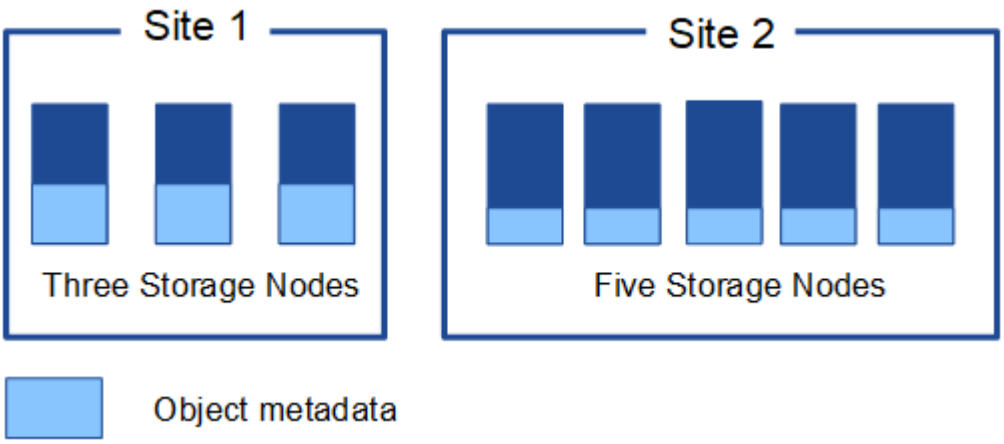
- Métadonnées système, y compris un ID unique pour chaque objet (UUID), le nom de l'objet, le nom du compartiment S3, le nom ou l'ID du compte locataire, la taille logique de l'objet, la date et l'heure de la première création de l'objet et la date et l'heure de la dernière modification de l'objet.
- Toutes les paires clé-valeur de métadonnées utilisateur personnalisées associées à l'objet.
- Pour les objets S3, toutes les paires clé-valeur de balise d'objet associées à l'objet.
- Pour les copies d'objets répliquées, l'emplacement de stockage actuel de chaque copie.
- Pour les copies d'objets codées par effacement, l'emplacement de stockage actuel de chaque fragment.
- Pour les copies d'objet dans un pool de stockage Cloud, l'emplacement de l'objet, y compris le nom du bucket externe et l'identifiant unique de l'objet.

- Pour les objets segmentés et les objets en plusieurs parties, identifiants de segment et tailles de données.

Comment les métadonnées des objets sont-elles stockées ?

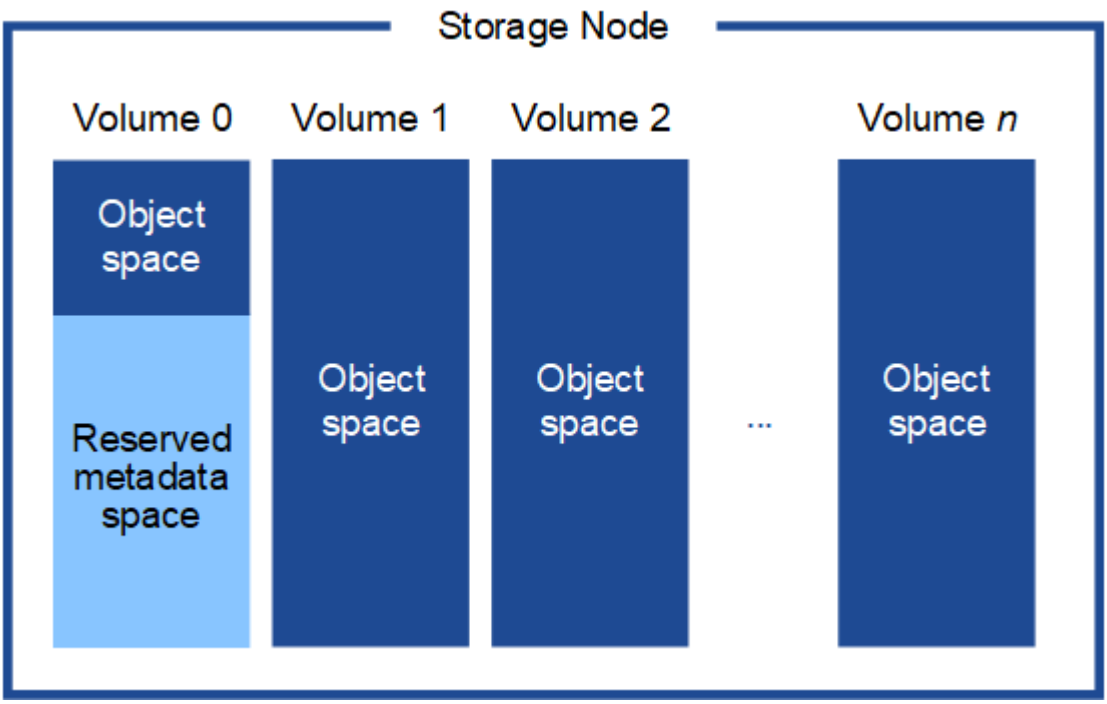
StorageGRID conserve les métadonnées des objets dans une base de données Cassandra, qui sont stockées indépendamment des données des objets. Pour assurer la redondance et protéger les métadonnées des objets contre la perte, StorageGRID stocke trois copies des métadonnées de tous les objets du système sur chaque site.

Cette figure représente les nœuds de stockage sur deux sites. Chaque site possède la même quantité de métadonnées d'objet, et les métadonnées de chaque site sont subdivisées entre tous les nœuds de stockage de ce site.



Où sont stockées les métadonnées des objets ?

Cette figure représente les volumes de stockage pour un seul nœud de stockage.



Comme indiqué dans la figure, StorageGRID réserve de l'espace pour les métadonnées d'objet sur le volume de stockage 0 de chaque nœud de stockage. Il utilise l'espace réservé pour stocker les métadonnées des

objets et effectuer les opérations essentielles de la base de données. Tout espace restant sur le volume de stockage 0 et tous les autres volumes de stockage du nœud de stockage sont utilisés exclusivement pour les données d'objet (copies répliquées et fragments codés par effacement).

La quantité d'espace réservée aux métadonnées d'objet sur un nœud de stockage particulier dépend de plusieurs facteurs, décrits ci-dessous.

Paramètre d'espace réservé aux métadonnées

L'espace réservé aux métadonnées est un paramètre à l'échelle du système qui représente la quantité d'espace qui sera réservée aux métadonnées sur le volume 0 de chaque nœud de stockage. Comme indiqué dans le tableau, la valeur par défaut de ce paramètre est basée sur :

- La version du logiciel que vous utilisiez lors de l'installation initiale de StorageGRID.
- La quantité de RAM sur chaque nœud de stockage.

Version utilisée pour l'installation initiale de StorageGRID	Quantité de RAM sur les nœuds de stockage	Paramètre d'espace réservé aux métadonnées par défaut
11,5 à 11,9	128 Go ou plus sur chaque nœud de stockage de la grille	8 To (8 000 Go)
	Moins de 128 Go sur n'importe quel nœud de stockage de la grille	3 To (3 000 Go)
11,1 à 11,4	128 Go ou plus sur chaque nœud de stockage sur un site donné	4 To (4 000 Go)
	Moins de 128 Go sur n'importe quel nœud de stockage sur chaque site	3 To (3 000 Go)
11.0 ou version antérieure	N'importe quel montant	2 To (2 000 Go)

Afficher le paramètre d'espace réservé aux métadonnées

Suivez ces étapes pour afficher le paramètre d'espace réservé aux métadonnées pour votre système StorageGRID .

Étapes

1. Sélectionnez **CONFIGURATION** > **Système** > **Paramètres de stockage**.
2. Sur la page Paramètres de stockage, développez la section **Espace réservé aux métadonnées**.

Pour StorageGRID 11.8 ou supérieur, la valeur de l'espace réservé aux métadonnées doit être d'au moins 100 Go et d'au plus 1 Po.

Le paramètre par défaut pour une nouvelle installation de StorageGRID 11.6 ou supérieure dans laquelle chaque nœud de stockage dispose de 128 Go ou plus de RAM est de 8 000 Go (8 To).

Espace réservé réel pour les métadonnées

Contrairement au paramètre d'espace réservé aux métadonnées à l'échelle du système, l'espace réservé réel pour les métadonnées d'objet est déterminé pour chaque nœud de stockage. Pour tout nœud de stockage donné, l'espace réservé réel pour les métadonnées dépend de la taille du volume 0 pour le nœud et du paramètre d'espace réservé aux métadonnées à l'échelle du système.

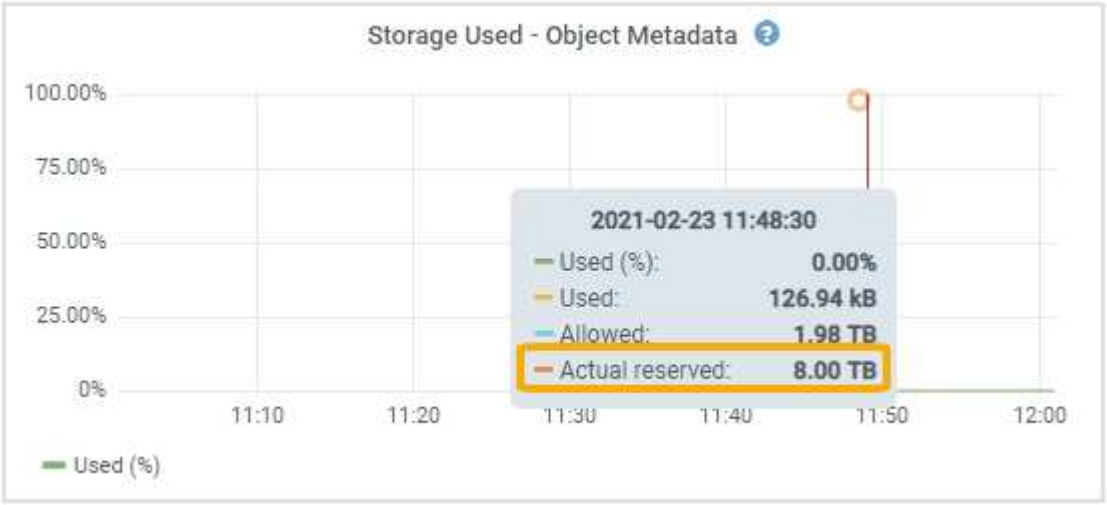
Taille du volume 0 pour le nœud	Espace réservé réel pour les métadonnées
Moins de 500 Go (utilisation hors production)	10% du volume 0
500 Go ou plus + ou + Nœuds de stockage de métadonnées uniquement	La plus petite de ces valeurs : • Volume 0 • Paramètre d'espace réservé aux métadonnées **Remarque** : un seul rangedb est requis pour les nœuds de stockage contenant uniquement des métadonnées.

Afficher l'espace réservé réel pour les métadonnées

Suivez ces étapes pour afficher l'espace réservé réel pour les métadonnées sur un nœud de stockage particulier.

Étapes

1. Dans le gestionnaire de grille, sélectionnez **NODES** > ***Storage Node***.
2. Sélectionnez l'onglet **Stockage**.
3. Placez votre curseur sur le graphique Stockage utilisé - Métadonnées de l'objet et recherchez la valeur **Réservée réelle**.



Dans la capture d'écran, la valeur **Réservée réelle** est de 8 To. Cette capture d'écran concerne un grand nœud de stockage dans une nouvelle installation de StorageGRID 11.6. Étant donné que le paramètre d'espace réservé aux métadonnées à l'échelle du système est inférieur au volume 0 pour ce nœud de stockage, l'espace réservé réel pour ce nœud est égal au paramètre d'espace réservé aux métadonnées.

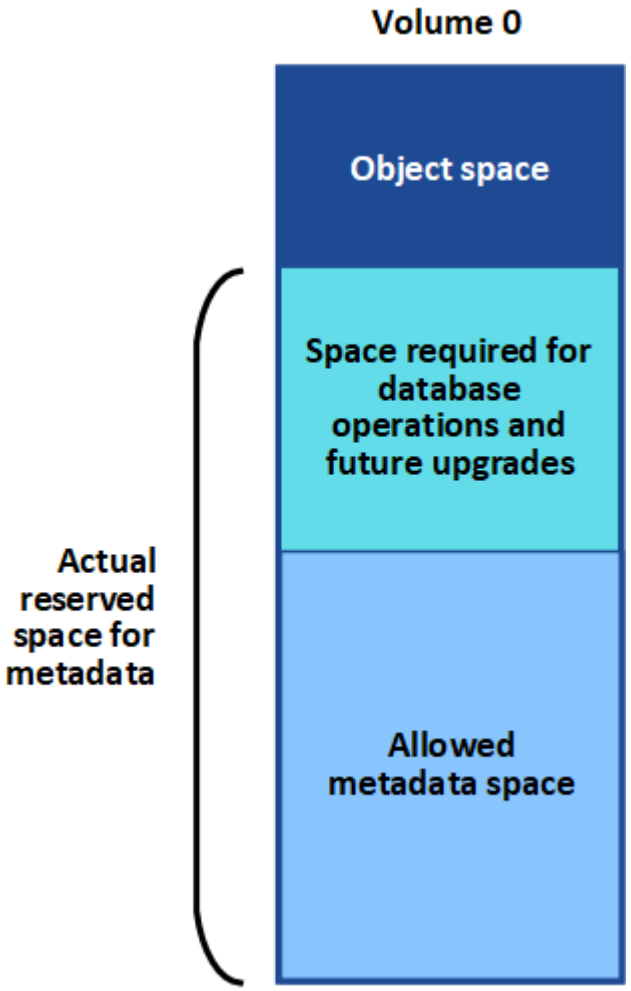
Exemple d’espace de métadonnées réservé réel

Supposons que vous installiez un nouveau système StorageGRID utilisant la version 11.7 ou ultérieure. Pour cet exemple, supposons que chaque nœud de stockage dispose de plus de 128 Go de RAM et que le volume 0 du nœud de stockage 1 (SN1) est de 6 To. Sur la base de ces valeurs :

- L’espace réservé aux métadonnées à l’échelle du système est défini sur 8 To. (Il s’agit de la valeur par défaut pour une nouvelle installation de StorageGRID 11.6 ou supérieure si chaque nœud de stockage dispose de plus de 128 Go de RAM.)
- L’espace réservé réel pour les métadonnées pour SN1 est de 6 To. (Le volume entier est réservé car le volume 0 est plus petit que le paramètre **Espace réservé aux métadonnées**.)

Espace de métadonnées autorisé

L’espace réservé réel de chaque nœud de stockage pour les métadonnées est subdivisé en espace disponible pour les métadonnées d’objet (l’espace de métadonnées autorisé) et l’espace requis pour les opérations de base de données essentielles (telles que le compactage et la réparation) et les futures mises à niveau matérielles et logicielles. L’espace de métadonnées autorisé régit la capacité globale de l’objet.



Le tableau suivant montre comment StorageGRID calcule l'**espace de métadonnées autorisé** pour différents nœuds de stockage, en fonction de la quantité de mémoire du nœud et de l’espace réservé réel pour les métadonnées.

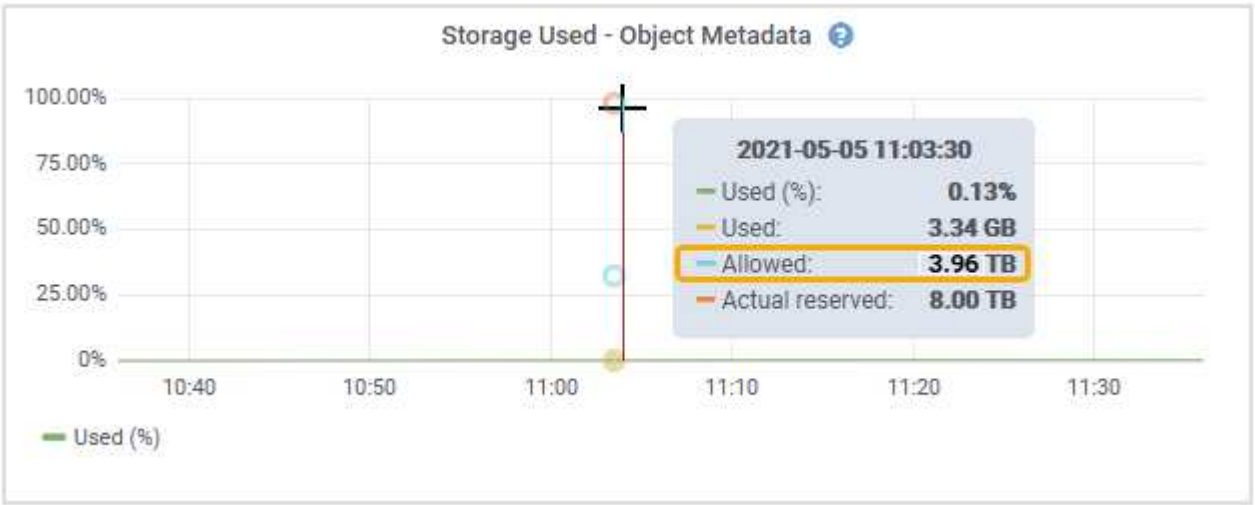
		Quantité de mémoire sur le nœud de stockage	
	< 128 Go	>= 128 Go	**Espace réservé réel pour les métadonnées**
⇐ 4 To	60 % de l'espace réel réservé aux métadonnées, jusqu'à un maximum de 1,32 To	60 % de l'espace réel réservé aux métadonnées, jusqu'à un maximum de 1,98 To	4 To

Afficher l'espace de métadonnées autorisé

Suivez ces étapes pour afficher l'espace de métadonnées autorisé pour un nœud de stockage.

Étapes

1. Dans le gestionnaire de grille, sélectionnez **NODES**.
2. Sélectionnez le nœud de stockage.
3. Sélectionnez l'onglet **Stockage**.
4. Placez votre curseur sur le graphique Stockage utilisé - métadonnées de l'objet et recherchez la valeur **Autorisée**.



Dans la capture d'écran, la valeur **Autorisée** est de 3,96 To, ce qui correspond à la valeur maximale pour un nœud de stockage dont l'espace réservé réel pour les métadonnées est supérieur à 4 To.

La valeur **Autorisée** correspond à cette métrique Prometheus :

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Exemple d'espace de métadonnées autorisé

Supposons que vous installiez un système StorageGRID utilisant la version 11.6. Pour cet exemple, supposons que chaque nœud de stockage dispose de plus de 128 Go de RAM et que le volume 0 du nœud de stockage 1 (SN1) est de 6 To. Sur la base de ces valeurs :

- L'espace réservé aux métadonnées à l'échelle du système est défini sur 8 To. (Il s'agit de la valeur par défaut pour StorageGRID 11.6 ou supérieur lorsque chaque nœud de stockage dispose de plus de 128 Go de RAM.)
- L'espace réservé réel pour les métadonnées pour SN1 est de 6 To. (Le volume entier est réservé car le volume 0 est plus petit que le paramètre **Espace réservé aux métadonnées**.)
- L'espace autorisé pour les métadonnées sur SN1 est de 3 To, sur la base du calcul indiqué dans letableau pour l'espace autorisé pour les métadonnées : (Espace réservé réel pour les métadonnées − 1 To) × 60 %, jusqu'à un maximum de 3,96 To.

Comment les nœuds de stockage de différentes tailles affectent la capacité des objets

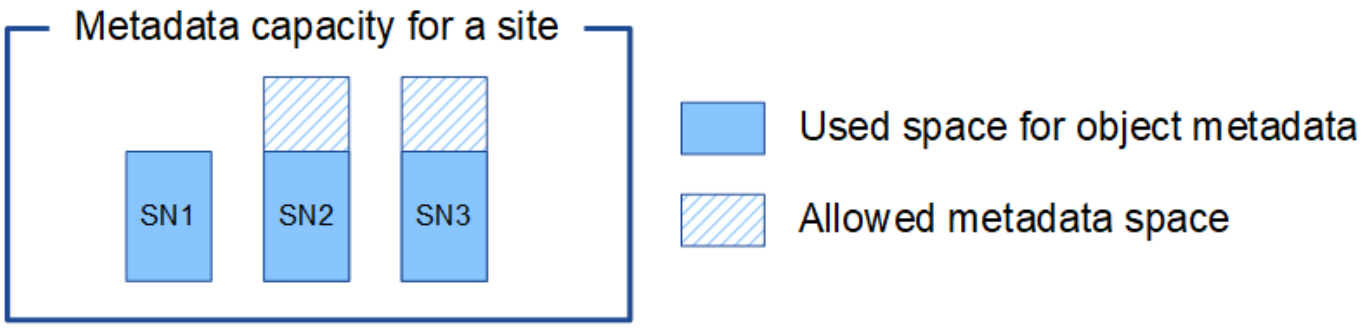
Comme décrit ci-dessus, StorageGRID répartit uniformément les métadonnées des objets sur les nœuds de stockage de chaque site. Pour cette raison, si un site contient des nœuds de stockage de différentes tailles, le plus petit nœud du site détermine la capacité de métadonnées du site.

Considérez l'exemple suivant :

- Vous disposez d'une grille à site unique contenant trois nœuds de stockage de tailles différentes.
- Le paramètre **Espace réservé aux métadonnées** est de 4 To.
- Les nœuds de stockage ont les valeurs suivantes pour l'espace de métadonnées réservé réel et l'espace de métadonnées autorisé.

Nœud de stockage	Taille du volume 0	Espace de métadonnées réservé réel	Espace de métadonnées autorisé
SN1	2,2 To	2,2 To	1,32 To
SN2	5 To	4 To	1,98 To
SN3	6 To	4 To	1,98 To

Étant donné que les métadonnées d'objet sont réparties uniformément sur les nœuds de stockage d'un site, chaque nœud de cet exemple ne peut contenir que 1,32 To de métadonnées. L'espace de métadonnées supplémentaire autorisé de 0,66 To pour SN2 et SN3 ne peut pas être utilisé.



De même, étant donné que StorageGRID conserve toutes les métadonnées d'objet pour un système StorageGRID sur chaque site, la capacité globale des métadonnées d'un système StorageGRID est déterminée par la capacité des métadonnées d'objet du plus petit site.

Et comme la capacité des métadonnées d'objet contrôle le nombre maximal d'objets, lorsqu'un nœud n'a plus de capacité de métadonnées, la grille est effectivement pleine.

Informations connexes

- Pour savoir comment surveiller la capacité des métadonnées d'objet pour chaque nœud de stockage, consultez les instructions de"Surveillance de StorageGRID" .
- Pour augmenter la capacité des métadonnées d'objets de votre système,"étendre une grille" en ajoutant de nouveaux nœuds de stockage.

Augmenter le paramètre d'espace réservé aux métadonnées

Vous pourrez peut-être augmenter le paramètre système Espace réservé aux métadonnées si vos nœuds de stockage répondent à des exigences spécifiques en matière de RAM et d'espace disponible.

Ce dont vous aurez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès racine ou configuration de la page de topologie de la grille et autres autorisations de configuration de la grille" .

La page Topologie de grille est obsolète et sera supprimée dans une prochaine version.

À propos de cette tâche

Vous pourrez peut-être augmenter manuellement le paramètre d'espace réservé aux métadonnées à l'échelle du système jusqu'à 8 To.

Vous ne pouvez augmenter la valeur du paramètre Espace réservé aux métadonnées à l'échelle du système que si ces deux affirmations sont vraies :

- Les nœuds de stockage de n'importe quel site de votre système disposent chacun de 128 Go ou plus de RAM.
- Les nœuds de stockage de n'importe quel site de votre système disposent chacun d'un espace disponible suffisant sur le volume de stockage 0.

Sachez que si vous augmentez ce paramètre, vous réduirez simultanément l'espace disponible pour le stockage d'objets sur le volume de stockage 0 de tous les nœuds de stockage. Pour cette raison, vous préférerez peut-être définir l'espace réservé aux métadonnées sur une valeur inférieure à 8 To, en fonction de

vos besoins en métadonnées d'objet attendus.

> En général, il est préférable d'utiliser une valeur supérieure plutôt qu'une valeur inférieure. Si le paramètre Espace réservé aux métadonnées est trop grand, vous pouvez le diminuer ultérieurement. En revanche, si vous augmentez la valeur ultérieurement, le système devra peut-être déplacer les données de l'objet pour libérer de l'espace.

Pour une explication détaillée de la manière dont le paramètre Espace réservé aux métadonnées affecte l'espace autorisé pour le stockage des métadonnées d'objet sur un nœud de stockage particulier, voir"Gérer le stockage des métadonnées des objets" .

Étapes

1. Déterminez le paramètre actuel de l'espace réservé aux métadonnées.
   a. Sélectionnez **CONFIGURATION** > **Système** > **Options de stockage**.
   b. Dans la section Filigranes de stockage, notez la valeur de **Espace réservé aux métadonnées**.
2. Assurez-vous de disposer de suffisamment d'espace disponible sur le volume de stockage 0 de chaque nœud de stockage pour augmenter cette valeur.
   a. Sélectionnez **NODES**.
   b. Sélectionnez le premier nœud de stockage dans la grille.
   c. Sélectionnez l'onglet Stockage.
   d. Dans la section Volumes, recherchez l'entrée **/var/local/rangedb/0**.
   e. Confirmez que la valeur disponible est égale ou supérieure à la différence entre la nouvelle valeur que vous souhaitez utiliser et la valeur actuelle de l'espace réservé aux métadonnées.

      Par exemple, si le paramètre Espace réservé aux métadonnées est actuellement de 4 To et que vous souhaitez l'augmenter à 6 To, la valeur Disponible doit être de 2 To ou plus.

   f. Répétez ces étapes pour tous les nœuds de stockage.
      - Si un ou plusieurs nœuds de stockage ne disposent pas de suffisamment d'espace disponible, la valeur de l'espace réservé aux métadonnées ne peut pas être augmentée. Ne continuez pas cette procédure.
      - Si chaque nœud de stockage dispose de suffisamment d'espace disponible sur le volume 0, passez à l'étape suivante.
3. Assurez-vous d'avoir au moins 128 Go de RAM sur chaque nœud de stockage.
   a. Sélectionnez **NODES**.
   b. Sélectionnez le premier nœud de stockage dans la grille.
   c. Sélectionnez l'onglet **Matériel**.
   d. Passez votre curseur sur le graphique d'utilisation de la mémoire. Assurez-vous que la **mémoire totale** est d'au moins 128 Go.
   e. Répétez ces étapes pour tous les nœuds de stockage.
      - Si un ou plusieurs nœuds de stockage ne disposent pas de suffisamment de mémoire totale disponible, la valeur de l'espace réservé aux métadonnées ne peut pas être augmentée. Ne continuez pas cette procédure.
      - Si chaque nœud de stockage dispose d'au moins 128 Go de mémoire totale, passez à l'étape suivante.

4. Mettre à jour le paramètre Espace réservé aux métadonnées.

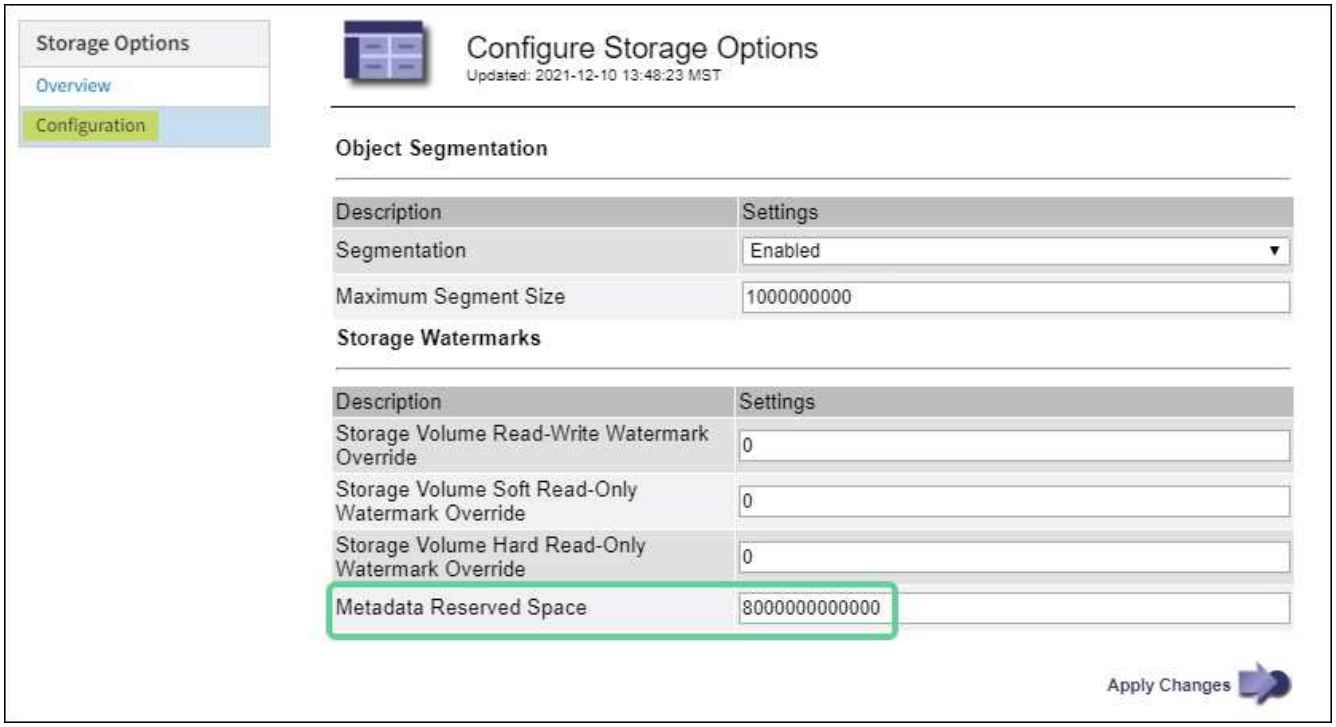
   a. Sélectionnez **CONFIGURATION** > **Système** > **Options de stockage**.

   b. Sélectionnez l'onglet Configuration.

   c. Dans la section Filigranes de stockage, sélectionnez **Espace réservé aux métadonnées**.

   d. Entrez la nouvelle valeur.

      Par exemple, pour saisir 8 To, qui est la valeur maximale prise en charge, saisissez **8000000000000** (8, suivi de 12 zéros)



   a. Sélectionnez **Appliquer les modifications**.

Compresser les objets stockés

Vous pouvez activer la compression d'objets pour réduire la taille des objets stockés dans StorageGRID, afin que les objets consomment moins de stockage.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .

À propos de cette tâche

Par défaut, la compression d'objet est désactivée. Si vous activez la compression, StorageGRID tente de compresser chaque objet lors de son enregistrement, en utilisant une compression sans perte.

> Si vous modifiez ce paramètre, l'application du nouveau paramètre prendra environ une minute. La valeur configurée est mise en cache pour les performances et la mise à l'échelle.

Avant d'activer la compression d'objet, tenez compte des points suivants :

- Vous ne devez pas sélectionner **Compresser les objets stockés** à moins que vous ne sachiez que les données stockées sont compressibles.
- Les applications qui enregistrent des objets dans StorageGRID peuvent compresser les objets avant de les enregistrer. Si une application cliente a déjà compressé un objet avant de l'enregistrer dans StorageGRID, la sélection de cette option ne réduira pas davantage la taille de l'objet.
- Ne sélectionnez pas **Compresser les objets stockés** si vous utilisez NetApp FabricPool avec StorageGRID.
- Si **Compresser les objets stockés** est sélectionné, les applications clientes S3 doivent éviter d'effectuer des opérations GetObject qui spécifient une plage d'octets à renvoyer. Ces opérations de « lecture de plage » sont inefficaces car StorageGRID doit décompresser efficacement les objets pour accéder aux octets demandés. Les opérations GetObject qui demandent une petite plage d'octets à partir d'un très grand objet sont particulièrement inefficaces ; par exemple, il est inefficace de lire une plage de 10 Mo à partir d'un objet compressé de 50 Go.

  Si les plages sont lues à partir d'objets compressés, les demandes des clients peuvent expirer.

> Si vous devez compresser des objets et que votre application cliente doit utiliser des lectures de plage, augmentez le délai d'expiration de lecture pour l'application.

Étapes

1. Sélectionnez **CONFIGURATION** > **Système** > **Paramètres de stockage** > **Compression d'objet**.
2. Cochez la case **Compresser les objets stockés**.
3. Sélectionnez **Enregistrer**.

Gérer des nœuds de stockage complets

À mesure que les nœuds de stockage atteignent leur capacité, vous devez étendre le système StorageGRID en ajoutant un nouveau stockage. Trois options sont disponibles : l'ajout de volumes de stockage, l'ajout d'étagères d'extension de stockage et l'ajout de nœuds de stockage.

Ajouter des volumes de stockage

Chaque nœud de stockage prend en charge un nombre maximal de volumes de stockage. Le maximum défini varie selon la plateforme. Si un nœud de stockage contient moins de volumes de stockage que le nombre maximal, vous pouvez ajouter des volumes pour augmenter sa capacité. Voir les instructions pour"extension d'un système StorageGRID" .

Ajouter des étagères d'extension de stockage

Certains nœuds de stockage d'appliance StorageGRID , tels que le SG6060 ou le SG6160, peuvent prendre en charge des étagères de stockage supplémentaires. Si vous disposez d'appliances StorageGRID avec des capacités d'extension qui n'ont pas déjà été étendues à leur capacité maximale, vous pouvez ajouter des étagères de stockage pour augmenter la capacité. Voir les instructions pour"extension d'un système StorageGRID" .

Ajouter des nœuds de stockage

Vous pouvez augmenter la capacité de stockage en ajoutant des nœuds de stockage. Une attention particulière doit être portée aux règles ILM actuellement actives et aux exigences de capacité lors de l'ajout de

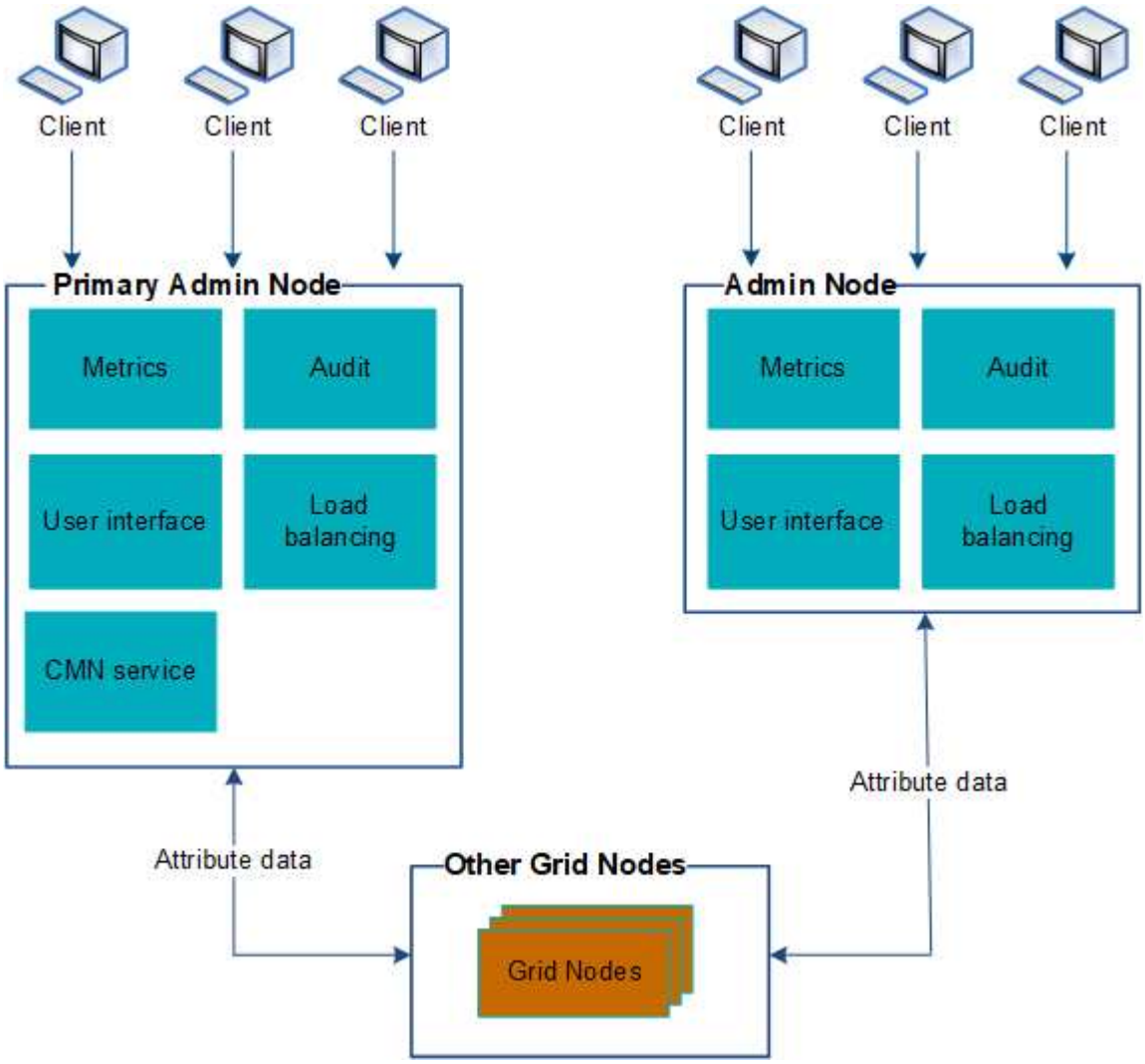
stockage. Voir les instructions pour"extension d'un système StorageGRID" .

Gérer les nœuds d'administration

Utiliser plusieurs nœuds d'administration

Un système StorageGRID peut inclure plusieurs nœuds d'administration pour vous permettre de surveiller et de configurer en continu votre système StorageGRID même si un nœud d'administration tombe en panne.

Si un nœud d'administration devient indisponible, le traitement des attributs continue, les alertes sont toujours déclenchées et les notifications par e-mail et les packages AutoSupport sont toujours envoyés. Cependant, le fait d'avoir plusieurs nœuds d'administration n'offre pas de protection de basculement, à l'exception des notifications et des packages AutoSupport .



Il existe deux options pour continuer à afficher et à configurer le système StorageGRID en cas de défaillance d'un nœud d'administration :

- Les clients Web peuvent se reconnecter à n'importe quel autre nœud d'administration disponible.
- Si un administrateur système a configuré un groupe haute disponibilité de nœuds d'administration, les clients Web peuvent continuer à accéder au gestionnaire de grille ou au gestionnaire de locataires à l'aide

de l’adresse IP virtuelle du groupe HA. Voir "Gérer les groupes de haute disponibilité" .

> Lors de l’utilisation d’un groupe HA, l’accès est interrompu si le nœud d’administration actif échoue. Les utilisateurs doivent se reconnecter après que l’adresse IP virtuelle du groupe HA bascule vers un autre nœud d’administration du groupe.

Certaines tâches de maintenance ne peuvent être effectuées qu’à l’aide du nœud d’administration principal. Si le nœud d’administration principal échoue, il doit être récupéré avant que le système StorageGRID soit à nouveau entièrement fonctionnel.

Identifier le nœud d’administration principal

Le nœud d’administration principal fournit plus de fonctionnalités que les nœuds d’administration non principaux. Par exemple, certaines procédures de maintenance doivent être effectuées à l’aide du nœud d’administration principal.

Pour plus d’informations sur les nœuds d’administration, voir"Qu’est-ce qu’un nœud d’administration" .

Avant de commencer

- Vous êtes connecté au Grid Manager à l’aide d’un"navigateur Web pris en charge" .
- Tu as"autorisations d’accès spécifiques" .

Étapes

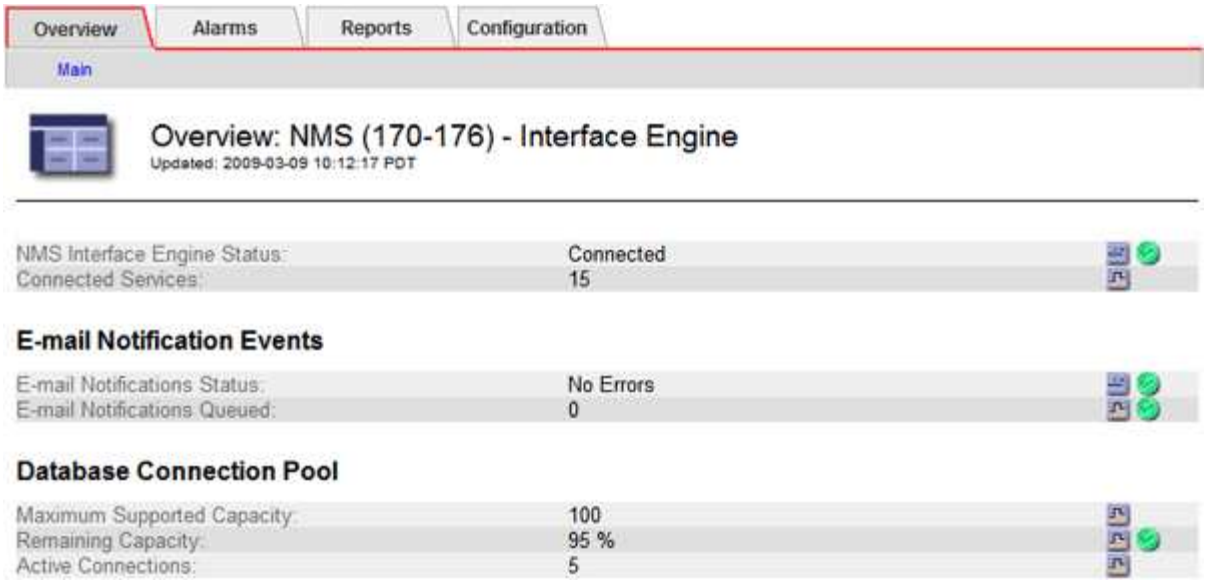
1. Sélectionnez **NODES**.
2. Saisissez **primaire** dans le champ de recherche.

   Dans les résultats de la recherche, identifiez le nœud avec « Nœud d’administration principal » affiché dans la colonne Type. Un nœud d’administration principal doit être répertorié.

Afficher l’état des notifications et les files d’attente

Le service du système de gestion de réseau (NMS) sur les nœuds d’administration envoie des notifications au serveur de messagerie. Vous pouvez afficher l’état actuel du service NMS et la taille de sa file d’attente de notifications sur la page Moteur d’interface.

Pour accéder à la page Moteur d’interface, sélectionnez **SUPPORT** > **Outils** > **Topologie de grille**. Sélectionnez ensuite ***site*** > ***Admin Node*** > **NMS** > **Interface Engine**.



Les notifications sont traitées via la file d'attente des notifications par e-mail et sont envoyées au serveur de messagerie l'une après l'autre dans l'ordre dans lequel elles sont déclenchées. S'il y a un problème (par exemple, une erreur de connexion réseau) et que le serveur de messagerie n'est pas disponible lorsque la tentative d'envoi de la notification est effectuée, une tentative de renvoi de la notification au serveur de messagerie se poursuit pendant une période de 60 secondes. Si la notification n'est pas envoyée au serveur de messagerie après 60 secondes, la notification est supprimée de la file d'attente des notifications et une tentative d'envoi de la notification suivante dans la file d'attente est effectuée.

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.