Administrer StorageGRID

StorageGRID 11.9

NetApp
November 08, 2024

Sommaire

Administrer StorageGRID . . . 1
- Administrer StorageGRID . . . 1
- Lancez-vous avec Grid Manager . . . 1
- Contrôle de l’accès à StorageGRID . . . 33
- Utiliser la fédération de grille . . . 84
- Gérer la sécurité . . . 122
- Gérer les locataires . . . 191
- Configurer les connexions client . . . 211
- Gestion des réseaux et des connexions . . . 254
- Utiliser AutoSupport . . . 274
- Gérer des nœuds de stockage . . . 288
- Gérer les nœuds d’administration . . . 302

Administrer StorageGRID

Administrer StorageGRID

Suivez 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
- Créez des comptes de locataire pour permettre aux applications client S3 de stocker et de récupérer des objets
- Configurez et gérez les réseaux StorageGRID
- Configurez AutoSupport
- Gérer les paramètres du nœud

Avant de commencer

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

Lancez-vous avec Grid Manager

Navigateurs Web pris en charge

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 régler la fenêtre du navigateur sur une largeur recommandée.

Largeur du navigateur	Pixels
Minimum	1024
Optimale	1280

Connectez-vous au Grid Manager

Vous accédez à la page de connexion de Grid Manager en entrant le nom de domaine complet (FQDN) ou l'adresse IP d'un noeud 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 primaires. Vous pouvez vous connecter au Gestionnaire de grille sur n'importe quel noeud d'administration pour gérer le système StorageGRID. Toutefois, certaines procédures de maintenance ne peuvent être effectuées qu'à partir du nœud d'administration principal.

Se connecter au groupe haute disponibilité

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

Utiliser SSO

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

Connectez-vous à Grid Manager sur le premier nœud d'administration

Avant de commencer

- Vous disposez de 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 disposant d'au moins une autorisation.
- Vous avez l'URL du Gestionnaire de grille :

  `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 haute disponibilité de nœuds d'administration.

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

  `https://FQDN_or_Admin_Node_IP:port/`

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

Étapes

1. Lancez un navigateur Web pris en charge.
2. Dans la barre d'adresse du navigateur, entrez l'URL du Gestionnaire de grille.
3. Si vous êtes invité à recevoir une alerte de sécurité, installez le certificat à l'aide de l'assistant d'installation du navigateur. Voir "Gérer les certificats de sécurité".

4. Connectez-vous au Grid Manager.

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

Pas d'utilisation de SSO

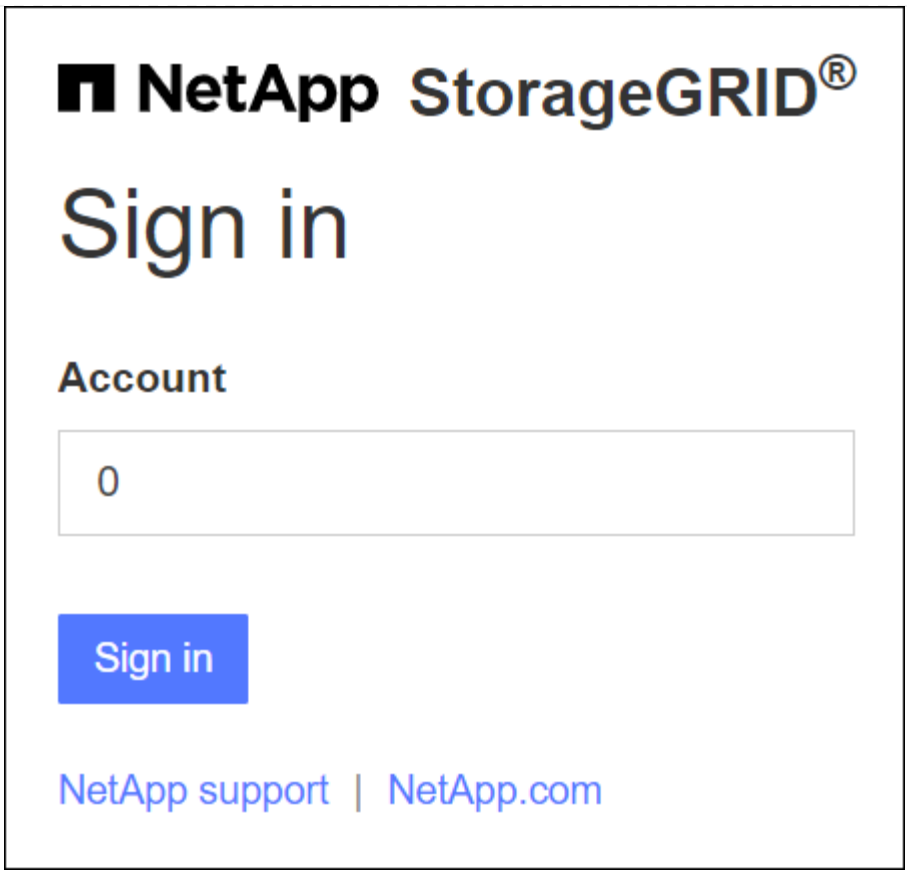
a. Saisissez votre nom d'utilisateur et votre mot de passe pour le Grid Manager.

b. Sélectionnez **connexion**.

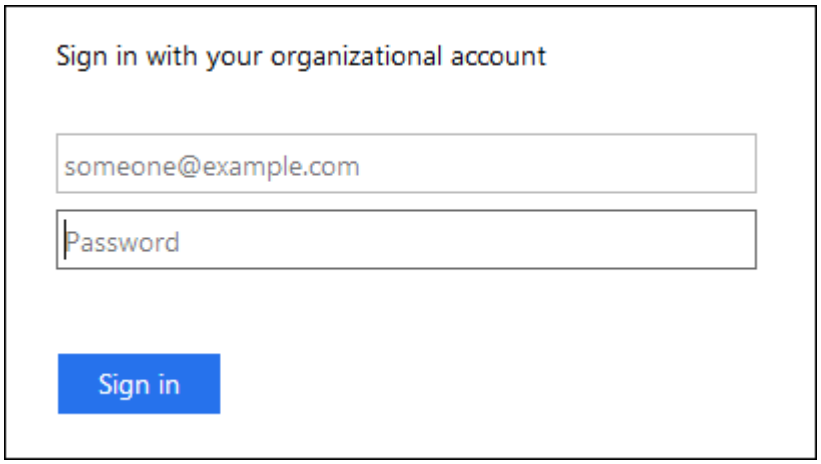
Utilisation de SSO

◦ Si StorageGRID utilise SSO pour la première fois que vous accédez à l'URL de ce navigateur :

i. Sélectionnez **connexion**. Vous pouvez laisser le 0 dans le champ compte.



ii. Saisissez vos identifiants SSO standard sur la page de connexion SSO de votre entreprise. Par exemple :



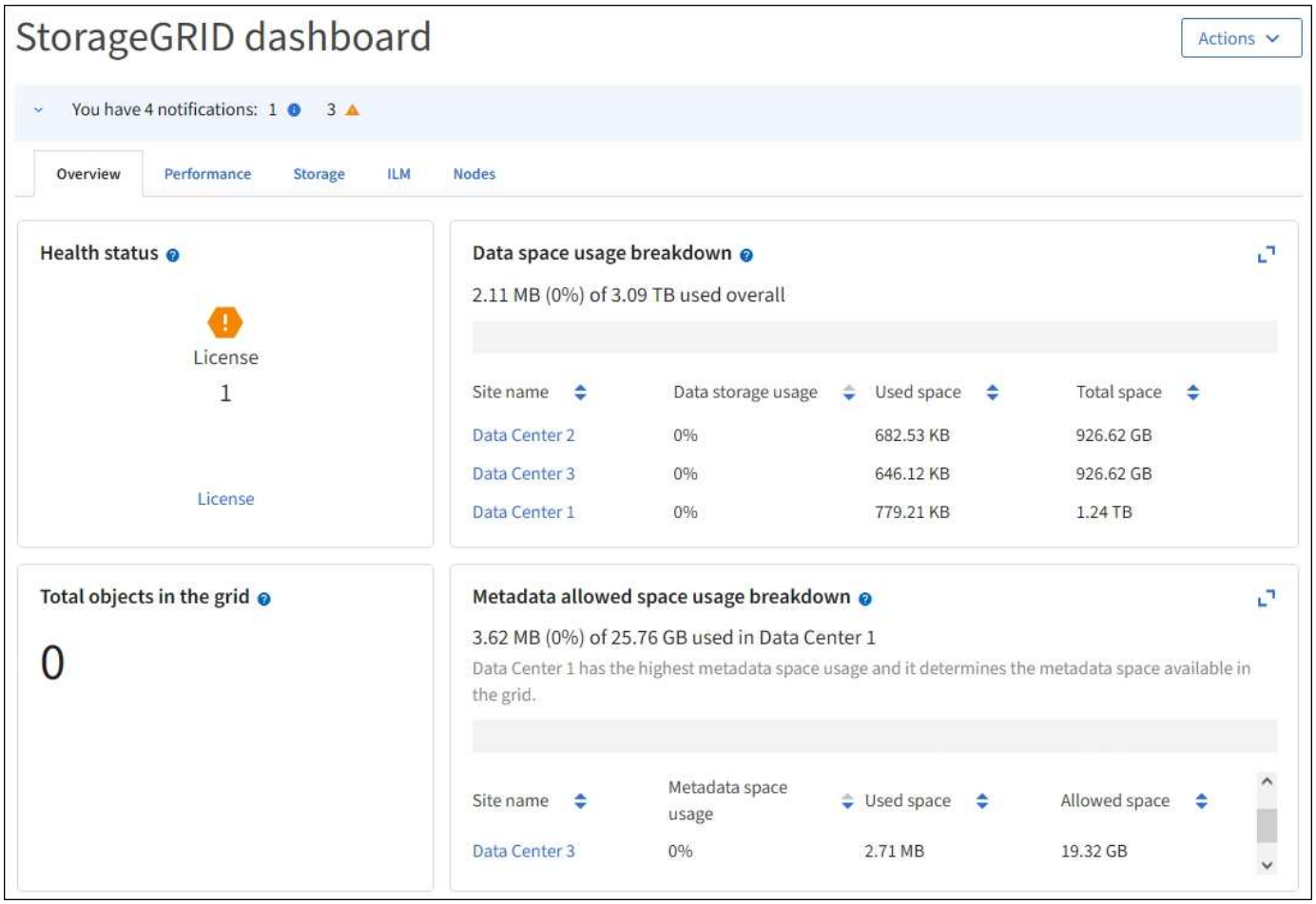
- Si StorageGRID utilise SSO et que vous avez déjà accédé au Gestionnaire de grille ou à un compte de locataire :

  i. Entrez **0** (l'ID de compte du gestionnaire de grille) ou sélectionnez **Grid Manager** s'il apparaît dans la liste des comptes récents.

ii. Sélectionnez **connexion**.

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

Lorsque vous êtes connecté, la page d'accueil du Gestionnaire de grille s'affiche, qui inclut le tableau de bord. Pour savoir quelles informations sont fournies, reportez-vous "Affichez et gérez le tableau de bord"à la section .



Connectez-vous à un autre nœud d'administration

Procédez comme suit pour vous connecter à un autre nœud d'administration.

Pas d'utilisation de SSO

Étapes

1. Dans la barre d'adresse du navigateur, entrez le nom de domaine complet ou l'adresse IP de l'autre noeud d'administration. Indiquez le numéro de port requis.
2. Saisissez 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 vous êtes connecté à un nœud d'administration, vous pouvez accéder à d'autres nœuds d'administration sans avoir à vous reconnecter.

Étapes

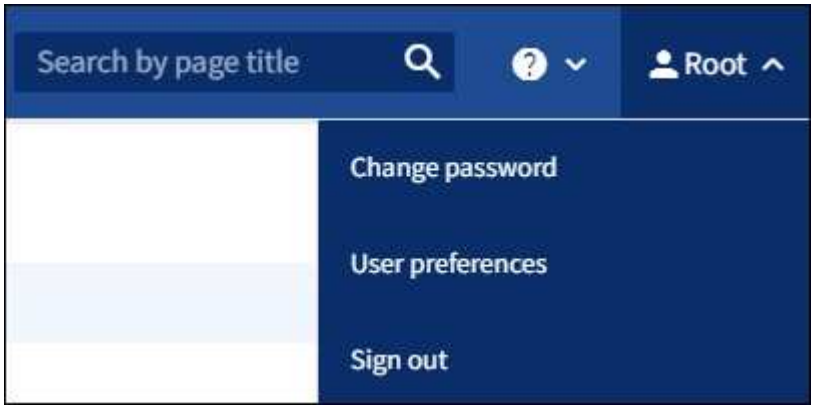
1. Entrez le nom de domaine complet ou l'adresse IP de l'autre noeud d'administration dans la barre d'adresse du navigateur.
2. Si votre session SSO a expiré, saisissez à nouveau vos informations d'identification.

Déconnectez-vous du Grid Manager

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

Étapes

1. 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 comme valeur par défaut dans la liste déroulante **comptes récents** et le champ **ID compte** affiche 0. **Remarque :** si SSO est activé et que vous êtes également connecté au gestionnaire de locataires, vous devez également vous "déconnectez-vous du compte du locataire"rendre à "Déconnectez-vous de SSO".

Changer votre mot de passe

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

Avant de commencer

Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".

Description de la 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 le Gestionnaire de grille. Vous devez plutôt modifier votre mot de passe dans le référentiel d'identité externe, par exemple Active Directory ou OpenLDAP.

Étapes

1. Dans l'en-tête de Grid Manager, sélectionnez ***votre nom*** > **changer mot de passe**.
2. Saisissez votre mot de passe actuel.
3. Saisissez un nouveau mot de passe.

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

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

Afficher les informations de licence StorageGRID

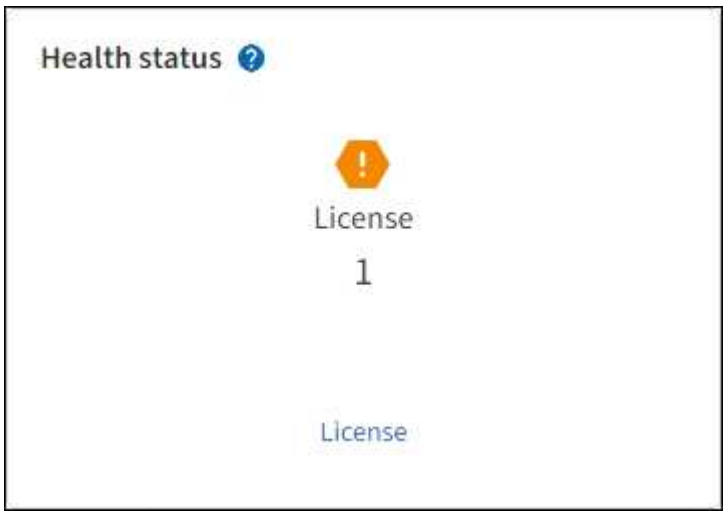
Vous pouvez afficher les informations relatives aux licences de votre système StorageGRID, comme la capacité de stockage maximale de votre réseau, si nécessaire.

Avant de commencer

Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".

Description de la tâche

En cas de problème avec la licence logicielle de ce système StorageGRID, la carte d'état d'intégrité du tableau de bord comprend une icône d'état de la licence et un lien **Licence**. Ce numéro indique le nombre de problèmes liés à la licence.



Étapes

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

Ce lien apparaît uniquement en cas de problème avec la licence.

2. Afficher les détails en lecture seule de la licence actuelle :
   - ID du système StorageGRID, qui est le numéro d'identification unique de cette installation StorageGRID
   - Numéro de série de la licence
   - Type de licence, soit **perpétuel** soit **abonnement**
   - Capacité de stockage sous licence de la grille
   - 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 de support après avoir obtenu le fichier de licence. Pour mettre à jour cette valeur, voir "Mettez à jour les informations de licence StorageGRID". Vous pouvez également afficher la date de fin réelle du contrat à l'aide de Active IQ.

   - Contenu du fichier texte de licence

Mettez à jour les informations de licence StorageGRID

Vous devez mettre à jour les informations de licence de votre système StorageGRID à tout moment que les conditions de votre modification de licence changent. Par exemple, vous devez mettre à jour les informations de licence si vous achetez de la capacité de stockage supplémentaire pour votre grid.

Avant de commencer

- Vous avez un nouveau fichier de licence à appliquer à votre système StorageGRID.
- Vous avez "autorisations d'accès spécifiques".
- Vous avez la phrase secrète pour le 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 pour le provisionnement.
5. Sélectionnez **Enregistrer**.

Utilisez l'API

Utilisez l'API de gestion du grid

Vous pouvez effectuer des tâches de gestion du système à l'aide de l'API REST Grid Management plutôt que de l'interface utilisateur Grid Manager. Par exemple, vous

pouvez utiliser l'API pour automatiser les opérations ou créer plusieurs entités plus rapidement (par exemple, les utilisateurs).

Ressources générales

L'API de gestion du grid fournit les ressources de premier niveau 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, voir "Utilisez un compte de 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 terminaux privés StorageGRID ignorent également la version API de la demande.

Émettre des requêtes API

L'API Grid Management utilise la plateforme d'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 swagger fournit des détails complets et de la documentation pour chaque opération API.

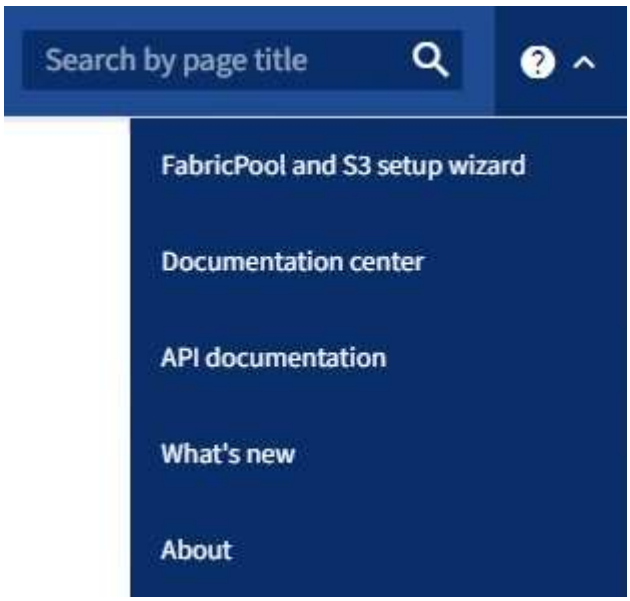
Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez "autorisations d'accès spécifiques".

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

Étapes

1. Dans l'en-tête Grid Manager, sélectionnez l'icône d'aide et sélectionnez **documentation API**.



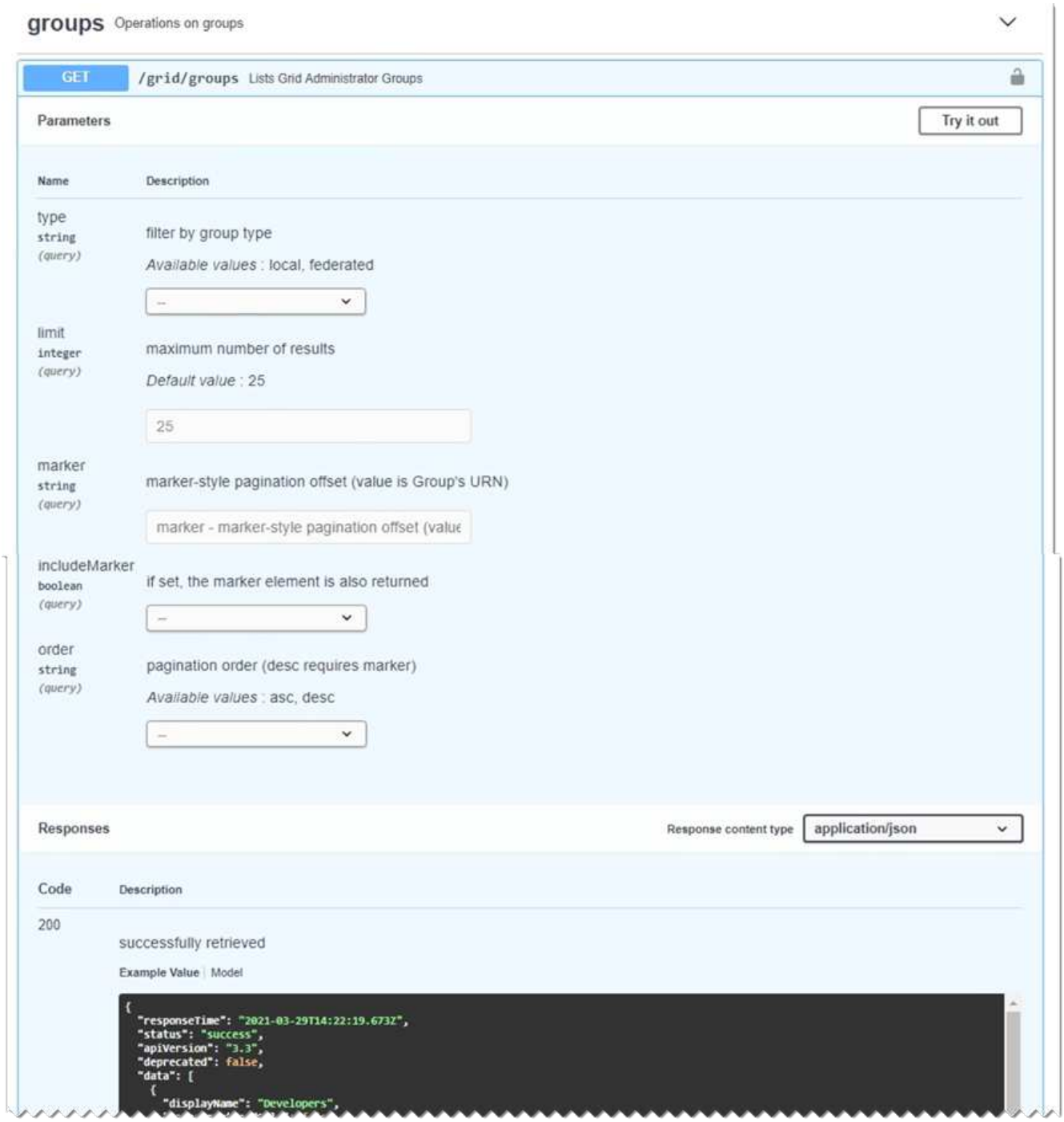
2. Pour effectuer une opération avec l'API privée, sélectionnez **accéder à la documentation API privée** sur la page API de gestion StorageGRID.

   Les API privées sont susceptibles d'être modifiées sans préavis. Les terminaux 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 ou DELETE.

4. Sélectionnez une action HTTP pour afficher les détails de la demande, notamment l'URL du noeud final, la liste de tous les paramètres obligatoires ou facultatifs, un exemple de l'organisme de 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, obtenir ces valeurs. Vous devrez peut-être d'abord lancer une autre demande d'API pour obtenir les informations dont vous avez besoin.
6. Déterminez si vous devez modifier l'exemple de corps de la demande. Si c'est le cas, vous pouvez sélectionner **modèle** pour connaître les exigences de chaque champ.
7. Sélectionnez **essayez-le**.
8. Fournir tous les paramètres requis ou modifier le corps de la demande selon les besoins.
9. Sélectionnez **Exécuter**.
10. Vérifiez le code de réponse pour déterminer si la demande a réussi.

Opérations de l'API de gestion du grid

L'API Grid Management 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.
- **Alerteurs** : opérations sur les récepteurs de notification d'alerte (e-mail).
- **Alert-rules** : opérations sur les règles d'alerte.
- **Silences d'alerte** : opérations sur les silences d'alerte.
- **Alertes** : opérations sur les alertes.
- **Audit** : opérations pour répertorier et mettre à jour la configuration de l'audit.
- **Auth** : opérations pour effectuer l'authentification de session utilisateur.

  L'API Grid Management prend en charge le schéma d'authentification par jeton Bearer. Pour vous connecter, vous devez fournir 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, un jeton de sécurité est renvoyé. Ce token doit être fourni dans l'en-tête des requêtes API suivantes (« autorisation : porteur *token* »). Le jeton expire au bout de 16 heures.

  Si l'authentification unique est activée pour le système StorageGRID, vous devez effectuer différentes étapes pour l'authentification. Reportez-vous à la section « authentification dans l'API si l'authentification unique est activée ».

  Pour plus d'informations sur l'amélioration de la sécurité de l'authentification, reportez-vous à la section « protection contre la falsification de demandes intersites ».

- **Certificats-client** : opérations permettant de configurer les certificats client 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 principales versions de l'API Grid Management prises en charge par cette version, et désactiver les versions obsolètes de l'API.
- **Désactivé-features** : opérations permettant d'afficher les fonctions qui auraient pu être désactivées.
- **dns-servers** : opérations permettant de répertorier et de modifier les serveurs DNS externes configurés.
- **Drive-details**: Opérations sur les lecteurs pour des modèles de dispositifs de stockage spécifiques.
- **Endpoint-domain-names** : opérations permettant de répertorier et de modifier les noms de domaine des noeuds finaux S3.
- **Code d'effacement** : opérations sur les profils de code d'effacement.
- **Expansion** : opérations d'expansion (au niveau de la procédure).
- **Noeuds-expansion**: Opérations sur expansion (niveau noeud).
- **Sites d'expansion** : opérations d'expansion (au niveau du site).
- **GRID-Networks** : opérations permettant de répertorier et de modifier la liste des réseaux de la grille.
- **GRID-mots de passe** : opérations pour la gestion des mots de passe de la grille.

- **Groupes** : opérations permettant de gérer les groupes d'administrateurs de grille locaux et de récupérer les groupes d'administrateurs de grille fédérés à partir d'un serveur LDAP externe.
- **Identity-source** : opérations permettant de configurer un référentiel d'identité externe et de synchroniser manuellement les informations relatives au groupe fédéré et à l'utilisateur.
- **ilm** : opérations sur la gestion du cycle de vie de l'information (ILM).
- **Procédures en cours** : récupère les procédures de maintenance en cours.
- **License** : opérations de récupération et de mise à jour de la licence StorageGRID.
- **Logs** : opérations de collecte et de téléchargement des fichiers journaux.v
- **Metrics** : opérations sur les métriques StorageGRID, y compris les requêtes métriques instantanées à un point dans le temps et les requêtes métriques de plage sur une plage de temps. L'API de gestion du grid utilise l'outil de contrôle des systèmes Prometheus comme source de données back-end. Pour plus d'informations sur la création de requêtes Prometheus, consultez le site Web Prometheus.

> Les mesures qui incluent `private` dans leur nom sont destinées à un usage interne uniquement. Ces metrics sont susceptibles d'être modifiés sans préavis entre les versions d'StorageGRID.

- **Node-details** : opérations sur les détails de noeud.
- **Node-Health** : opérations sur l'état d'intégrité du nœud.
- **État-stockage-noeud** : opérations sur l'état de stockage du noeud.
- **ntp-servers** : opérations de liste ou de mise à jour des 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 pour télécharger le progiciel de récupération.
- **Régions** : opérations pour afficher et créer des régions.
- **s3-object-lock** : opérations sur les paramètres globaux de verrouillage d'objet S3.
- **Server-certificate** : opérations pour afficher et mettre à jour les certificats de serveur Grid Manager.
- **snmp** : opérations sur la configuration SNMP actuelle.
- **Filigranes de stockage** : filigranes de nœuds de stockage.
- **Classes de trafic** : opérations pour les politiques de classification du trafic.
- **Ingest-client-network** : opérations sur la configuration réseau client non fiable.
- **Utilisateurs** : opérations permettant d'afficher et de gérer les utilisateurs de Grid Manager.

Gestion des versions de l'API de gestion du grid

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

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

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

La version majeure de l'API est incrémentée lorsque des modifications sont effectuées qui ne sont *pas compatibles* avec des versions plus anciennes. La version mineure de l'API est incrémentée lorsque des

modifications qui sont *compatibles* avec des versions plus anciennes sont effectuées. Les modifications compatibles incluent l'ajout de nouveaux noeuds finaux ou de nouvelles propriétés.

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

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

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

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

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

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

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

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

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

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

Spécifiez une version API pour une demande

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

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

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

Protection contre la contrefaçon de demandes intersites (CSRF)

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

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

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

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

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

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

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

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

Reportez-vous à la documentation en ligne de l'API pour obtenir des exemples et des détails supplémentaires.

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

Utilisez l'API si l'authentification unique est activée

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

Si vous avez "Authentification unique (SSO) configurée et activée" 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 de gestion de grille ou l'API de gestion des locataires.

Connectez-vous 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 appartenant à un groupe d'utilisateurs StorageGRID.
- Pour accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

Description de la tâche

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

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

- Un exemple de flux de travail des requêtes Curl.

  Le flux de travail de boucle risque de s'échapper si vous l'effectuez trop lentement. Vous pouvez voir l'erreur : `A valid SubjectConfirmation was not found on this Response`.

  > L'exemple de flux de travail Curl ne protège pas le mot de passe d'être vu par d'autres utilisateurs.

Si vous avez un problème de codage d'URL, vous pouvez 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.
   - Utiliser les demandes de gondoles. Passez à l'étape 3.
2. Si vous souhaitez utiliser le `storagegrid-ssoauth.py` script, transmettez-le à l'interpréteur Python et exécutez le script.

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

   - Méthode SSO. Entrez ADFS ou adfs.
   - Le nom d'utilisateur SSO
   - Domaine dans lequel StorageGRID est installé
   - L'adresse de StorageGRID
   - L'ID du compte de locataire, pour 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 maintenant utiliser le token pour d'autres requêtes, de la même manière que vous utilisiez l'API si SSO n'était pas utilisé.

3. Si vous souhaitez utiliser des requêtes Curl, suivez la procédure ci-dessous.

   a. Déclarez les variables nécessaires pour 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, envoyez une demande POST à `/api/v3/authorize-saml` et supprimez le codage JSON supplémentaire de la réponse.

Cet exemple montre une demande POST pour une URL d'authentification signée pour `TENANTACCOUNTID`. Les résultats seront transmis à `python -m json.tool` pour supprimer le codage 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 dans cet exemple inclut une URL signée codée par URL, mais n'inclut pas la couche supplémentaire de codage JSON.

```
{
    "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. Enregistrez la `SAMLRequest` à partir de la réponse pour l'utiliser dans les commandes suivantes.

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

d. Obtenir une URL complète incluant l'ID de demande client d'AD FS.

Une option consiste à demander le formulaire de connexion à l'aide de 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 demande 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 la demande client à partir de la réponse.

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

f. Envoyez vos informations d'identification à l'action de 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 post du formulaire 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. Enregistrez le `MSISAuth` cookie de la réponse.

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

h. Envoyez une demande 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 contiennent des informations sur la session AD FS pour une utilisation de déconnexion ultérieure et le corps de réponse contient SAMLResponse 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. Enregistrer le `SAMLResponse` à partir du champ masqué :

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

j. A l'aide de la commande enregistré `SAMLResponse`, faites une demande StorageGRID `/api/saml-response` pour générer un jeton d'authentification StorageGRID.

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

```
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, comme vous le feriez pour utiliser 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 de gestion Grid ou de l'API de gestion des locataires. Ces instructions s'appliquent si vous utilisez Active Directory comme fournisseur d'identité SSO

Description de la 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 de 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 rerediriger vers StorageGRID.

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

La réponse 302 est renvoyée. L'emplacement de redirection ne s'applique pas à la déconnexion 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 de support StorageGRID.

La suppression du jeton de support 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
```

Une `204 No Content` 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 "Authentification unique (SSO) configurée et activée"utilisez et que vous utilisez Azure en tant que fournisseur SSO, vous pouvez utiliser deux exemples de scripts pour obtenir un jeton d'authentification valide pour l'API de gestion du grid ou l'API de gestion des locataires.

Connectez-vous 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 SSO et le mot de passe d'un utilisateur fédéré appartenant à un groupe d'utilisateurs StorageGRID.
- Pour accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

Description de la tâche

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

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

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

Pour écrire votre propre intégration d'API avec Azure, consultez le `storagegrid-ssoauth-azure.py` script. Le script Python fait deux requêtes directement à StorageGRID (d'abord pour obtenir la SAMLRequest et plus tard 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 d'API, mais cette opération n'est pas simple. Le module Puppeteer Node.js est utilisé pour gratter l'interface SSO Azure.

Si vous avez un problème de codage d'URL, vous pouvez voir l'erreur : `Unsupported SAML version`.

Étapes

1. Installez les dépendances requises comme suit :

a. Installez Node.js (voir "https://nodejs.org/en/download/").

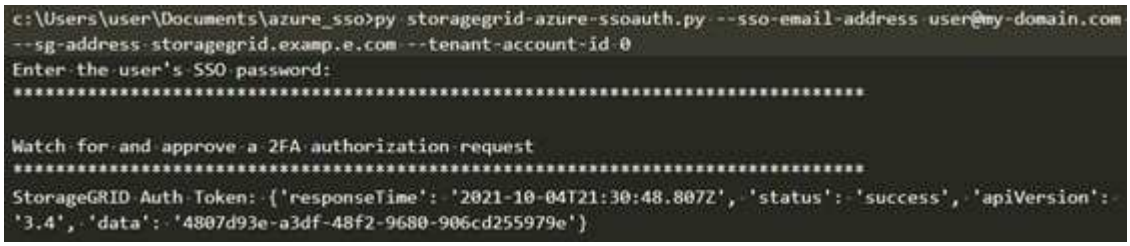
b. Installez les modules Node.js requis (maripeteer et jsdom) :

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

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

   Le script Python appelle ensuite le script Node.js correspondant pour exécuter les interactions SSO Azure.

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



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

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

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

Si vous avez "Authentification unique (SSO) configurée et activée" 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 de tenant.

Connectez-vous 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 appartenant à un groupe d'utilisateurs StorageGRID.
- Pour accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

Description de la tâche

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

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

  Le flux de travail de boucle risque de s'échapper si vous l'effectuez trop lentement. Vous pouvez voir l'erreur : `A valid SubjectConfirmation was not found on this Response`.

  > L'exemple de flux de travail Curl ne protège pas le mot de passe d'être vu par d'autres utilisateurs.

  Si vous avez un problème de codage d'URL, vous pouvez 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.
   - Utiliser les demandes de gondoles. Passez à l'étape 3.
2. Si vous souhaitez utiliser le `storagegrid-ssoauth.py` script, transmettez-le à l'interpréteur Python et exécutez le script.

   Lorsque vous y êtes invité, entrez des valeurs pour les arguments suivants :
   - Méthode SSO. Vous pouvez entrer n'importe quelle variation de "pingfederate" (PINGFEDERATE, pingfederate, et ainsi de suite).
   - Le nom d'utilisateur SSO
   - Domaine dans lequel StorageGRID est installé. Ce champ n'est pas utilisé pour PingFederate. Vous pouvez le laisser vide ou entrer n'importe quelle valeur.
   - L'adresse de StorageGRID
   - L'ID du compte de locataire, pour 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 maintenant utiliser le token pour d'autres requêtes, de la même manière que vous utilisiez l'API si SSO n'était pas utilisé.
3. Si vous souhaitez utiliser des requêtes Curl, suivez la procédure ci-dessous.

   a. Déclarez les variables nécessaires pour 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, envoyez une demande POST à `/api/v3/authorize-saml` et supprimez le codage JSON supplémentaire de la réponse.

Cet exemple montre une demande 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 dans cet exemple inclut une URL signée codée par URL, mais n'inclut pas la couche supplémentaire de codage JSON.

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

c. Enregistrez la `SAMLRequest` à partir de la réponse pour l'utiliser dans les commandes suivantes.

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

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

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

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

e. Exporter la valeur 'pf.adapterId' et réafficher la réponse :

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

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

f. Exporter la valeur « href » (supprimer la barre oblique inverse /) et afficher en écho 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 des 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. Enregistrer le `SAMLResponse` à partir du champ masqué :

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

j. A l'aide de la commande enregistré `SAMLResponse`, faites une demande StorageGRID`/api/saml-response` pour générer un jeton d'authentification StorageGRID.

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

```
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, comme vous le feriez pour utiliser 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 de gestion Grid ou de l'API de gestion des locataires. Ces instructions s'appliquent si vous utilisez PingFederate comme fournisseur d'identité SSO

Description de la 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 de 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 rerediriger vers StorageGRID.

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

La réponse 302 est renvoyée. L'emplacement de redirection ne s'applique pas à la déconnexion 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 de support StorageGRID.

La suppression du jeton de support 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
```

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

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

Désactivez les fonctions à l'aide de l'API

Vous pouvez utiliser l'API de gestion de grille pour désactiver complètement certaines fonctions du système StorageGRID. Lorsqu'une fonction est désactivée, aucune autorisation ne peut être attribuée pour effectuer les tâches associées à cette fonctionnalité.

Description de la tâche

Le système de fonctions désactivées vous permet d'empêcher l'accès à certaines fonctions du système StorageGRID. La désactivation d'une fonctionnalité est le seul moyen d'empêcher l'utilisateur racine ou les utilisateurs appartenant à des groupes d'administration disposant de l'autorisation **accès racine** d'utiliser cette fonctionnalité.

Pour comprendre l'utilité de cette fonctionnalité, prenez en compte 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 de tenant. Pour protéger la sécurité des objets de leurs détenteurs de bail, la Société A veut s'assurer que ses employés ne peuvent jamais accéder à un compte de locataire après le déploiement du compte.

*Société A peut atteindre cet objectif en utilisant le système Désactiver les fonctions dans l'API de gestion de grille. En désactivant complètement la fonction **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 Admin, y compris l'utilisateur root et les utilisateurs appartenant à des groupes avec l'autorisation **Root Access**, ne peuvent pas modifier le mot de passe de l'utilisateur root d'un compte de locataire.*

Étapes

1. Accédez à la documentation de swagger pour l'API Grid Management. Voir "Utilisez l'API de gestion du grid".
2. Localisez le point d'extrémité Désactiver les fonctions.
3. Pour désactiver une fonction, par exemple changer le mot de passe racine du locataire, envoyez un corps à l'API comme suit :

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

   Une fois la demande terminée, la fonction de modification du mot de passe racine du locataire est désactivée. L'autorisation de gestion **Modifier le mot de passe root** du locataire n'apparaît plus dans l'interface utilisateur et toute demande d'API qui tente de modifier le mot de passe root d'un locataire échoue avec "403 interdit".

Réactiver les fonctions désactivées

Par défaut, vous pouvez utiliser l'API Grid Management pour réactiver une fonction qui a été désactivée. Toutefois, si vous souhaitez empêcher la réactivation des fonctions désactivées, vous pouvez désactiver la fonction **activeFeatures** elle-même.

> La fonction **activateFeatures** ne peut pas être réactivée. Si vous décidez de désactiver cette fonction, sachez que vous perdrez définitivement la capacité de réactiver les autres fonctions désactivées. Vous devez contacter le support technique pour restaurer toute fonctionnalité perdue.

Étapes

1. Accédez à la documentation de swagger pour l'API Grid Management.
2. Localisez le point d'extrémité Désactiver les fonctions.
3. Pour réactiver toutes les fonctions, envoyez un corps à l'API comme suit :

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

   Lorsque cette demande est terminée, toutes les fonctions, y compris la fonction Modifier le mot de passe racine du locataire, sont réactivées. L'autorisation de gestion **Modifier le mot de passe racine** du locataire apparaît maintenant dans l'interface utilisateur et toute demande d'API qui tente de modifier le mot de passe racine d'un locataire va réussir, en supposant que l'utilisateur dispose de l'autorisation de gestion **accès racine** ou **changer le mot de passe racine du locataire**.

> L'exemple précédent provoque la réactivation des fonctions *All* DESACTIVE. Si d'autres fonctions doivent rester désactivées, vous devez les spécifier explicitement dans la demande PUT. Par exemple, pour réactiver la fonction Modifier le mot de passe root du locataire et continuer à désactiver l'autorisation de gestion storageAdmin, envoyez cette demande PUT: `{ "grid": {"storageAdmin": true} }`

Contrôle de l'accès à StorageGRID

Contrôlez l'accès au StorageGRID

Vous pouvez contrôler 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. Vous pouvez également activer l'authentification unique (SSO), créer des certificats client et modifier les mots de passe de la grille.

Contrôle de l'accès au Grid Manager

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

L'utilisation de "fédération des identités" rend la configuration "groupes"et "utilisateurs" plus rapide, et permet aux utilisateurs de se connecter à StorageGRID à l'aide des informations d'identification habituelles. Vous pouvez configurer la fédération des identités 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 affectant différentes tâches "autorisations"à chaque groupe. Par exemple, il peut être nécessaire que les utilisateurs d'un groupe puissent gérer les règles ILM et les utilisateurs d'un autre groupe pour effectuer les tâches de maintenance. Un utilisateur doit appartenir à au moins un groupe pour accéder au système.

Vous pouvez également 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 fonctions. Ils ne peuvent pas apporter de modifications ni effectuer d'opérations dans l'API Grid Manager ou Grid Management.

Activez l'authentification unique

Le système StorageGRID prend en charge la fonctionnalité SSO (Single Sign-on) en utilisant la 2.0 norme SAML 2.0 (Security assertion Markup Language). Après vous "Configurer et activer SSO", tous les utilisateurs doivent être authentifiés par un fournisseur d'identité externe avant de pouvoir accéder au Gestionnaire de grille, au Gestionnaire de locataires, à l'API de gestion de grille ou à l'API de gestion des locataires. Les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

Modifiez la phrase secrète du provisionnement

La phrase de passe de provisionnement est requise pour de nombreuses procédures d'installation et de maintenance, ainsi que pour le téléchargement du package de restauration StorageGRID. Une phrase secrète est également nécessaire pour télécharger les sauvegardes des informations de topologie de la grille et des clés de chiffrement pour le système StorageGRID. Vous pouvez le faire "modifiez la phrase de passe" selon vos besoins.

Changer les mots de passe de la console du nœud

Chaque nœud de votre grid dispose d'un mot de passe unique de console de nœud. Vous devez vous connecter au nœud en tant qu'administrateur via SSH ou à l'utilisateur root sur une connexion VM/console physique. En fonction des besoins, vous pouvez "modifiez le mot de passe de la console du nœud" pour chaque nœud.

Modifiez la phrase secrète de provisionnement

Utilisez cette procédure pour modifier la phrase secrète du provisionnement StorageGRID. La phrase de passe est requise pour les procédures de restauration, d'extension et de maintenance. La phrase de passe est également requise pour télécharger les sauvegardes du pack de récupération qui incluent les informations de topologie de la grille, les mots de passe de la console des nœuds grid et les clés de chiffrement pour le système StorageGRID.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès à la racine ou à la maintenance.
- Vous disposez de la phrase secrète pour le provisionnement.

Description de la tâche

La phrase secrète de provisionnement est requise pour de nombreuses procédures d'installation et de maintenance, et pour "Téléchargement du progiciel de restauration". La phrase de passe de provisionnement n'est pas répertoriée dans le `Passwords.txt` fichier. Veillez à documenter la phrase de passe de provisionnement et à la conserver dans un emplacement sûr et sécurisé.

Étapes

1. Sélectionnez **CONFIGURATION** > **contrôle d'accès**> **mots de passe de grille**.
2. Sous **Modifier la phrase de passe de provisionnement**, sélectionnez **faire une modification**
3. Saisissez votre phrase secrète pour le provisionnement.
4. Saisissez la nouvelle phrase de passe. La phrase de passe doit contenir au moins 8 caractères et pas plus de 32 caractères. Les phrases passe sont sensibles à la casse.

5. Stocker la nouvelle phrase secrète pour le provisionnement dans un emplacement sécurisé Elle est requise pour les procédures d'installation, d'extension et de maintenance.
6. Saisissez à nouveau la nouvelle phrase de passe et sélectionnez **Enregistrer**.

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

7. Sélectionnez **progiciel de récupération**.
8. Entrez la nouvelle phrase de passe de provisionnement pour télécharger le nouveau progiciel de restauration.

> Après avoir modifié la phrase de passe de provisionnement, vous devez télécharger immédiatement un nouveau progiciel de restauration. Le fichier du progiciel de récupération vous permet de restaurer le système en cas de défaillance.

Changer les mots de passe de la console du nœud

Chaque nœud de votre grid dispose d'un mot de passe de console de nœud unique que vous devez vous connecter au nœud. Procédez comme suit pour modifier chaque mot de passe de console de nœud unique pour chaque nœud de votre grille.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Maintenance ou autorisation d'accès racine".
- Vous disposez de la phrase secrète pour le provisionnement.

Description de la tâche

Utilisez le mot de passe de la console du nœud pour vous connecter à un nœud en tant qu'administrateur via SSH ou à l'utilisateur root sur une connexion de console physique/machine virtuelle. Le processus de modification du mot de passe de la console des nœuds 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` dans le module 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 grille**.
2. Sous **Modifier les mots de passe de la console de nœuds**, sélectionnez **faire une modification**.

Saisissez la phrase secrète pour le provisionnement

Étapes

1. Saisissez la phrase de passe de provisionnement pour votre grid.
2. Sélectionnez **Continuer**.

Téléchargez le package de récupération actuel

Avant de modifier les mots de passe de la console de nœuds, téléchargez le progiciel de récupération actuel. Vous pouvez utiliser les mots de passe de ce fichier si le processus de modification du mot de passe échoue pour un noeud quelconque.

Étapes

1. Sélectionnez **Télécharger le paquet de récupération**.
2. Copiez le fichier du package de récupération (`.zip`) dans deux emplacements sécurisés et séparés.

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

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

   Vous ne pouvez pas annuler ce processus après son démarrage.

Changer 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. Les mots de passe sont ensuite 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 nouveau paquet de récupération**.
3. Une fois le téléchargement terminé :

   a. Ouvrez le `.zip` fichier.

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

   c. Copiez le nouveau fichier de package de récupération (`.zip`) dans deux emplacements sécurisés et séparés.

      Ne remplacez pas l'ancien package de récupération.

   Le fichier du progiciel de récupération doit être sécurisé car il contient des clés de cryptage et des mots de passe qui peuvent être utilisés pour obtenir des données 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 de nœuds** et attendez que tous les nœuds soient mis à jour avec les nouveaux mots de passe. Cette opération peut prendre quelques minutes.

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

En cas d'erreur lors du processus de mise à jour, un message de bannière indique le nombre de nœuds dont les mots de passe n'ont pas été modifiés. Le système réexécute automatiquement le processus sur tout nœud dont le mot de passe n'a pas été modifié. Si le processus se termine avec certains nœuds qui n'ont toujours pas de mot de passe modifié, le bouton **Réessayer** s'affiche.

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

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

b. Résolvez les problèmes.

c. Sélectionnez **Réessayer**.

> ⓘ La tentative de nouveau modifie uniquement les mots de passe de la console de nœud sur les nœuds qui ont échoué lors des précédentes tentatives de changement de mot de passe.

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

Modifier les mots de passe d'accès SSH des 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 via une authentification sécurisée 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 VM ou une connexion à une console physique.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Maintenance ou autorisation d'accès racine".
- Vous disposez de la phrase secrète pour le provisionnement.

Description de la tâche

Les nouveaux mots de passe d'accès pour les nœuds d'administration et les nouvelles clés internes pour chaque nœud sont stockés dans `Passwords.txt` le fichier du 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. Celles-ci ne sont pas modifiées par cette procédure.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION** > **contrôle d'accès** > **mots de passe de grille**.

2. Sous **Modifier les clés SSH**, sélectionnez **faire une modification**.

Téléchargez le package de récupération actuel

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

Étapes

1. Saisissez la phrase de passe de provisionnement pour votre grid.
2. Sélectionnez **Télécharger le paquet de récupération**.
3. Copiez le fichier du package de récupération (`.zip`) dans deux emplacements sécurisés et séparés.

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

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

   Vous ne pouvez pas annuler ce processus après son démarrage.

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. Les clés sont ensuite 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 progiciel de récupération est activé, sélectionnez **Télécharger un nouveau progiciel de récupération** et enregistrez le nouveau fichier de progiciel de récupération (`.zip`) dans deux emplacements sécurisés, sécurisés et séparés.
3. Une fois le téléchargement terminé :

   a. Ouvrez le `.zip` fichier.

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

   c. Copiez le nouveau fichier de package de récupération (`.zip`) dans deux emplacements sécurisés et séparés.

      Ne remplacez pas l'ancien package de récupération.

   Le fichier du progiciel de récupération doit être sécurisé car il contient des clés de cryptage et des mots de passe qui peuvent être utilisés pour obtenir des données 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 s'affiche.

En cas d'erreur lors du processus de mise à jour, un message d'avertissement indique 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 pu être modifiée. Si le processus se termine alors que certains nœuds n'ont toujours pas de clé modifiée, le bouton **Réessayer** s'affiche.

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

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

b. Résolvez les problèmes.

c. Sélectionnez **Réessayer**.

La reconnexion ne modifie que les clés d'accès SSH sur les nœuds qui ont échoué lors des tentatives précédentes de changement de clé.

5. Une fois les clés d'accès SSH modifiées pour tous les nœuds, supprimez le Premier package de récupération que vous avez téléchargé.
6. Si vous le souhaitez, sélectionnez **MAINTENANCE** > **système** > **paquet de récupération** pour télécharger une copie supplémentaire du nouveau paquet de récupération.

Utiliser la fédération des identités

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

Configurer la fédération des identités pour Grid Manager

Vous pouvez configurer la fédération des identités dans Grid Manager si vous souhaitez que les groupes et les utilisateurs d'administration 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 Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez "autorisations d'accès spécifiques".
- Vous utilisez Active Directory, Azure AD, OpenLDAP ou Oracle Directory Server comme fournisseur d'identité.

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

- Si vous avez l'intention d'utiliser OpenLDAP, vous devez configurer le serveur OpenLDAP. Voir Instructions de configuration d'un serveur OpenLDAP.
- Si vous prévoyez d'activer l'authentification unique (SSO), vous avez consulté le "configuration requise et considérations pour l'authentification unique".
- Si vous prévoyez d'utiliser TLS (transport Layer Security) pour les communications avec le serveur LDAP, le fournisseur d'identités utilise TLS 1.2 ou 1.3. Voir "Chiffrement pris en charge pour les connexions TLS sortantes".

Description de la tâche

Vous pouvez configurer un référentiel d'identité pour Grid Manager si vous souhaitez importer des groupes à

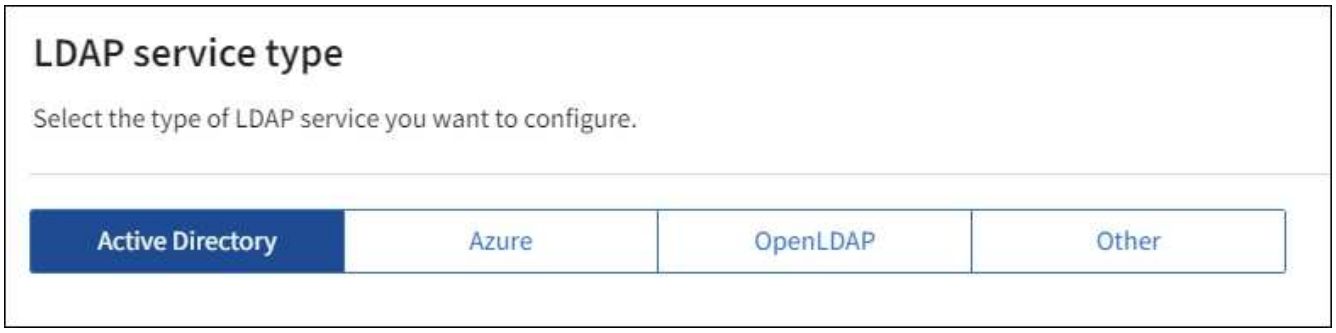
partir d'un autre système, tel qu'Active Directory, Azure AD, OpenLDAP ou Oracle Directory Server. Vous pouvez importer les types de groupes suivants :

- Groupes d'administration. Les utilisateurs des groupes admin 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 référentiel 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 de locataire" et "Utilisez un compte de locataire" pour plus de détails.

Entrez la configuration

Étapes

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



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

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

- **Nom d'hôte** : le nom de domaine complet (FQDN) ou l'adresse IP du serveur LDAP.
- **Port** : port utilisé pour se connecter au serveur LDAP.

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

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

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

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

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

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

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

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

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

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

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

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

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

  Entrez l'un des motifs suivants :

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

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

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

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

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

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

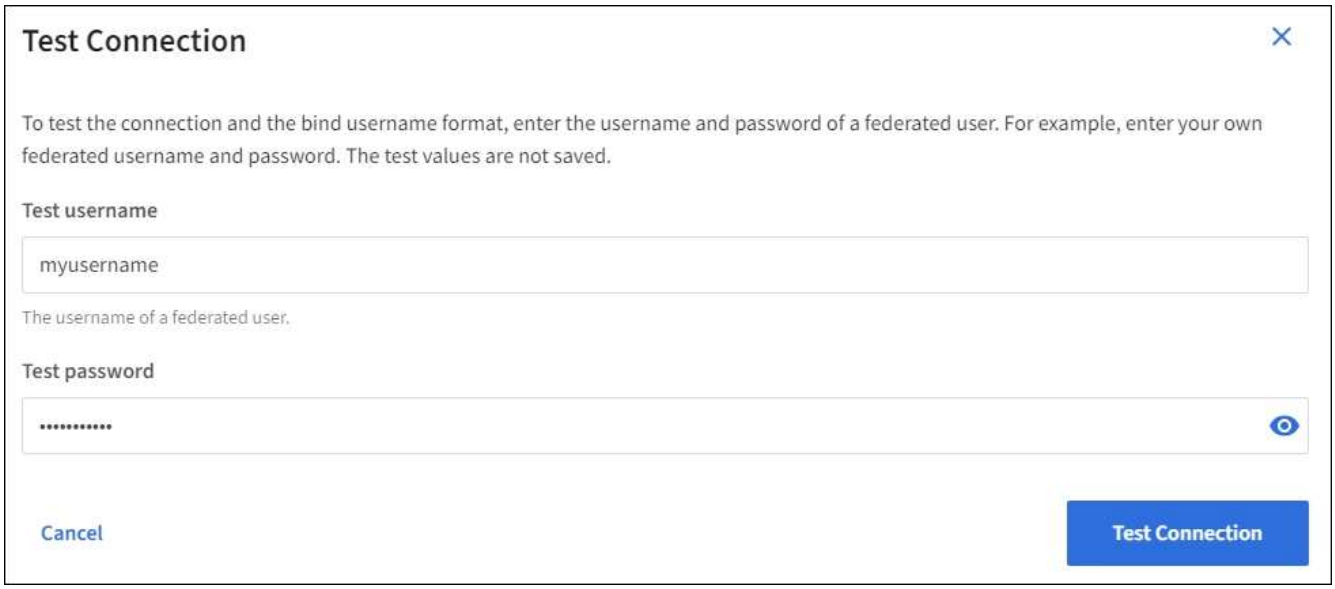
Testez la connexion et enregistrez la configuration

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

Étapes

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

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



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

Forcer la synchronisation avec le référentiel d'identité

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

Étapes

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

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

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

Désactiver la fédération des identités

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

Description de la tâche

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

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

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

- La synchronisation entre le système StorageGRID et le référentiel d'identité ne se fera pas et les alertes ne seront pas émises pour les comptes qui n'ont pas été synchronisés.
- La case **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 connexion unique doit être **désactivé** avant de pouvoir désactiver la fédération d'identités. Voir "Désactiver l'authentification unique".

Étapes

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

Instructions de configuration d'un serveur OpenLDAP

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

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

Recouvrements de memberOf et de raffint

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

Indexation

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

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

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

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

Gérez les groupes d'administration

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

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez "autorisations d'accès spécifiques".
- Si vous envisagez d'importer un groupe fédéré, vous avez configuré la fédération des identités et le groupe fédéré existe déjà dans le référentiel d'identité configuré.

Créer un groupe d'administration

Les groupes Admin vous permettent de déterminer quels utilisateurs peuvent accéder aux fonctions et opérations du gestionnaire de grille et de l'API Grid Management.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION** > **contrôle d'accès** > **groupes Admin**.
2. Sélectionnez **Créer 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 du référentiel 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. Entrez 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. Entrez le nom du groupe à importer, exactement tel qu'il apparaît dans le référentiel d'identité configuré.
   - 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 **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 ne peuvent afficher que 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 pas apporter de modifications ni effectuer d'opérations dans l'API Grid Manager ou 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 dispose d'un accès en lecture seule à tous les paramètres et fonctions sélectionnés.

2. Sélectionnez une ou plusieurs "autorisations de groupe d'administration".

   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 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 groupe** et **Terminer**.

Afficher et modifier les groupes d'administration

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 de 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 du groupe. b. Sélectionnez **actions** > **Afficher les détails du groupe**.	Sélectionnez le nom du groupe dans le tableau.
Modifier le nom d'affichage (groupes locaux uniquement)	a. Cochez la case du groupe. b. Sélectionnez **actions** > **Modifier le nom du groupe**. c. Saisissez le nouveau nom. d. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom du groupe pour afficher les détails. b. Sélectionnez l'icône Modifier . c. Saisissez le nouveau nom. d. Sélectionnez **Enregistrer les modifications**.

Tâche	Menu actions	Page de détails
Modifier le mode d'accès ou les autorisations	a. Cochez la case du groupe. b. Sélectionnez **actions** > **Afficher les détails du groupe**. c. Si vous le souhaitez, modifiez le mode d'accès du groupe. d. Si vous le souhaitez, sélectionnez ou désélectionnez "autorisations de groupe d'administration". e. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom du groupe pour afficher les détails. b. Si vous le souhaitez, modifiez le mode d'accès du groupe. c. Si vous le souhaitez, sélectionnez ou désélectionnez "autorisations de groupe d'administration". d. Sélectionnez **Enregistrer les modifications**.

Dupliquer un groupe

Étapes

1. Cochez la case du groupe.
2. Sélectionnez **actions** > **Dupliquer le groupe**.
3. Suivez l'assistant de duplication de groupe.

Supprimer un groupe

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

Étapes

1. Dans la page groupes, cochez la case correspondant à chaque groupe à supprimer.
2. Sélectionnez **actions** > **Supprimer le groupe**.
3. Sélectionnez **Supprimer les groupes**.

Autorisations de groupe d'administration

Lors de la création de groupes d'utilisateurs admin, vous sélectionnez une ou plusieurs autorisations pour contrôler l'accès à des fonctions spécifiques de Grid Manager. Vous pouvez ensuite affecter chaque utilisateur à un ou plusieurs de ces groupes d'administration pour déterminer les tâches que l'utilisateur peut effectuer.

Vous devez affecter au moins une autorisation à chaque groupe ; sinon, les utilisateurs appartenant à ce groupe ne pourront pas se connecter au Grid Manager ou à l'API Grid Management.

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

- Connectez-vous au Grid Manager
- Afficher le tableau de bord
- Affichez les pages nœuds

- Afficher les alertes actuelles et résolues
- Modifier son propre mot de passe (utilisateurs locaux uniquement)
- Afficher 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 ne peuvent afficher que les paramètres et les fonctionnalités associés. Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur **lecture seule**, l'utilisateur dispose d'un accès en lecture seule à tous les paramètres et fonctions sélectionnés.

Les sections suivantes décrivent les autorisations que vous pouvez attribuer lors de la création ou de la modification d'un groupe d'administration. Toute fonctionnalité qui n'est pas explicitement mentionnée requiert l'autorisation **accès racine**.

Accès racine

Cette autorisation donne accès à toutes les fonctions d'administration de la grille.

Modifier le mot de passe root du locataire

Cette autorisation donne accès à l'option **changer mot de passe root** de la page locataires, ce qui vous permet de contrôler qui peut modifier le mot de passe de l'utilisateur racine 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 **changer mot de passe racine**, attribuez également l'autorisation **comptes locataire**.

Configuration de la page de topologie grid

Cette autorisation permet d'accéder aux onglets Configuration de la page **SUPPORT** > **Outils** > **topologie de grille**.

> La page de topologie de la grille est obsolète et sera supprimée dans une version ultérieure.

ILM

Cette autorisation permet d'accéder aux options de menu **ILM** suivantes :

- Règles
- Stratégies
- Balises de stratégie
- Pools de stockage
- Niveaux de stockage
- Régions
- Recherche de métadonnées d'objet

Les utilisateurs doivent disposer des autorisations **autre configuration de grille** et **Configuration de page de topologie de grille** pour gérer les classes de stockage.

Maintenance

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

- **CONFIGURATION** > **contrôle d'accès** :
  - Mots de passe de grille
- **CONFIGURATION** > **réseau** :
  - Noms de domaine de terminaux S3
- **MAINTENANCE** > **tâches** :
  - Désaffectation
  - De développement
  - Vérification de l'existence d'objet
  - Reprise après incident
- **MAINTENANCE** > **système** :
  - Package de restauration
  - Mise à jour logicielle
- **SUPPORT** > **Outils** :
  - Journaux

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

- **MAINTENANCE** > **réseau** :
  - Serveurs DNS
  - Réseau Grid
  - Serveurs NTP
- **MAINTENANCE** > **système** :
  - Licence
- **CONFIGURATION** > **réseau** :
  - Noms de domaine de terminaux 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.

Interrogation de metrics

Cette autorisation permet d'accéder aux éléments suivants :

- **SUPPORT** > **Outils** > **métriques** page
- Requêtes de metrics Prometheus personnalisées à l'aide de la section **Metrics** de l'API de gestion de grille
- Cartes de tableau de bord de Grid Manager qui contiennent des metrics

Recherche de métadonnées d'objet

Cette autorisation permet d'accéder à la page **ILM** > **recherche de métadonnées objet**.

Autre configuration de grille

Cette autorisation donne accès à d'autres options de configuration de grille.

> Pour voir ces options supplémentaires, les utilisateurs doivent également disposer de l'autorisation **Grid topology page configuration**.

- **ILM** :
  - Niveaux de stockage
- **CONFIGURATION** > **système** :
- **SUPPORT** > **autre** :
  - Coût des liens

Administrateur de l'appliance de stockage

Cette autorisation permet :

- Accès à E-Series SANtricity System Manager sur les appliances de stockage via le gestionnaire de grid.
- Possibilité d'effectuer des tâches de dépannage et de maintenance dans l'onglet gérer les lecteurs pour les appliances prenant en charge ces opérations.

Comptes de locataires

Cette autorisation permet de :

- Accédez à la page tenants, où vous pouvez créer, modifier et supprimer des comptes de tenant
- Afficher les stratégies de classification du trafic existantes
- Affichez 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'administration locaux pour déterminer les fonctions de Grid Manager auxquelles ces utilisateurs peuvent accéder.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".

- Vous avez "autorisations d'accès spécifiques".

Créez un utilisateur local

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

Vous ne pouvez créer que des utilisateurs locaux. Utilisez le référentiel d'identité externe pour gérer des utilisateurs et des groupes fédérés.

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

> 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 Admin**.
2. Sélectionnez **Créer utilisateur**.

Saisissez 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. Vous pouvez également sélectionner **Oui** si cet utilisateur ne doit pas avoir accès à Grid Manager ou à l'API de gestion de grille.
3. Sélectionnez **Continuer**.

Affecter à des groupes

Étapes

1. Vous pouvez éventuellement attribuer 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 "Gérez les groupes d'administration" pour plus de détails.

2. Sélectionnez **Créer utilisateur** et **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 le référentiel d'identité externe pour gérer les

utilisateurs fédérés.

- Pour afficher les informations de base de tous les utilisateurs locaux et fédérés, consultez le tableau de la page utilisateurs.
- Pour afficher tous les détails d'un utilisateur spécifique, modifier un utilisateur local ou modifier 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 Grid Manager.

> Les utilisateurs locaux peuvent modifier leurs propres mots de passe à l'aide de l'option **Modifier le mot de passe** de la bannière Grid Manager.

Tâche	Menu actions	Page de détails
Afficher les détails de l'utilisateur	a. Cochez la case de 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 de l'utilisateur. b. Sélectionnez **actions** > **Modifier le nom complet**. c. Saisissez le nouveau nom. d. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'icône Modifier . c. Saisissez le nouveau nom. d. Sélectionnez **Enregistrer les modifications**.
Refuser ou autoriser l'accès StorageGRID	a. Cochez la case de 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 Grid Manager ou à l'API de gestion de la grille ou sélectionnez **non** pour permettre à l'utilisateur de 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 Grid Manager ou à l'API de gestion de la grille ou sélectionnez **non** pour permettre à l'utilisateur de se connecter. d. Sélectionnez **Enregistrer les modifications**.
Modifier le mot de passe (utilisateurs locaux uniquement)	a. Cochez la case de l'utilisateur. b. Sélectionnez **actions** > **Afficher les détails de l'utilisateur**. c. Sélectionnez l'onglet Mot de passe. d. Saisissez un nouveau mot de passe. e. Sélectionnez **changer mot de passe**.	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'onglet Mot de passe. c. Saisissez un nouveau mot de passe. d. Sélectionnez **changer mot de passe**.

Tâche	Menu actions	Page de détails
Modifier les groupes (utilisateurs locaux uniquement)	a. Cochez la case de 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 de 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 de 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 de l'utilisateur.
2. Sélectionnez **actions** > **Dupliquer utilisateur**.
3. Suivez l'assistant Dupliquer.

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. Dans la page utilisateurs, cochez la case correspondant à chaque utilisateur à supprimer.
2. Sélectionnez **actions** > **Supprimer l'utilisateur**.
3. Sélectionnez **Supprimer l'utilisateur**.

Utilisation de la connexion unique (SSO)

Configurer l'authentification unique

Lorsque l'authentification unique (SSO) est activée, les utilisateurs n'ont accès qu'au Grid Manager, au tenant Manager, à l'API Grid Management ou à l'API de gestion des locataires si leurs identifiants sont autorisés à l'aide du processus de connexion SSO mis en œuvre par votre entreprise. Les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

Fonctionnement de l'authentification unique

Le système StorageGRID prend en charge la fonctionnalité SSO (Single Sign-on) en utilisant la 2.0 norme SAML 2.0 (Security assertion Markup Language).

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

Connectez-vous lorsque SSO est activé

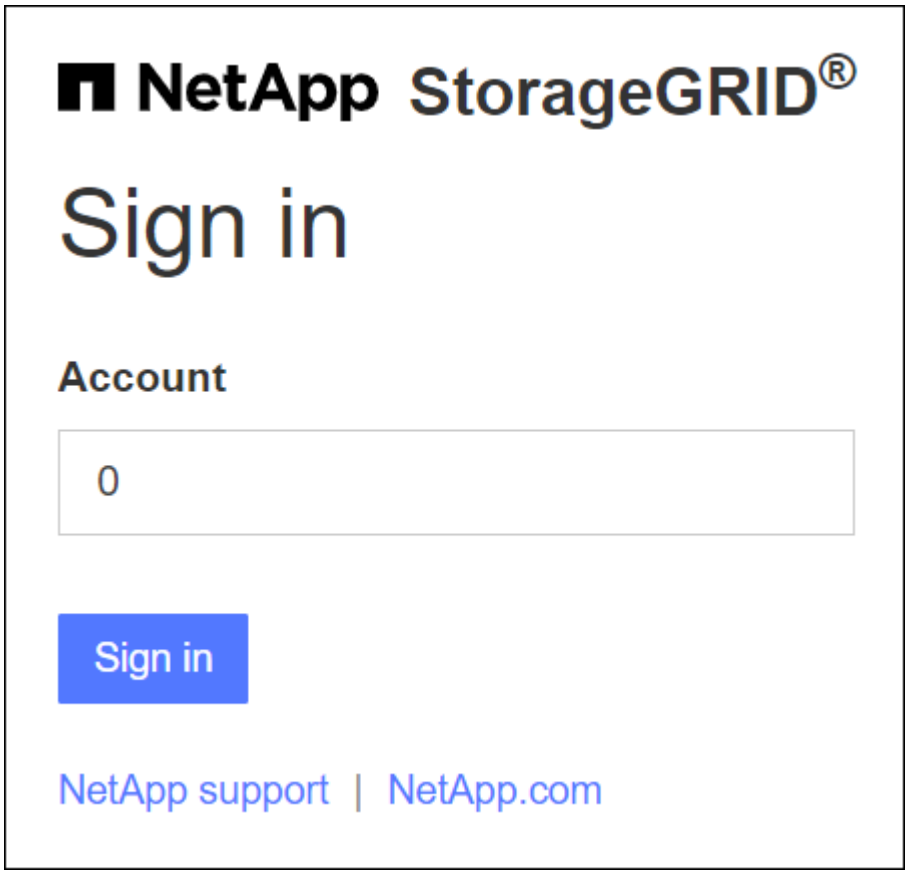
Lorsque l'authentification SSO est activée et que vous vous connectez à StorageGRID, vous êtes redirigé vers la page SSO de votre entreprise afin de valider vos identifiants.

Étapes

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

   La page de connexion StorageGRID s'affiche.

   - S'il s'agit de la première fois que vous accédez à l'URL sur ce navigateur, vous êtes invité à entrer un ID de compte :

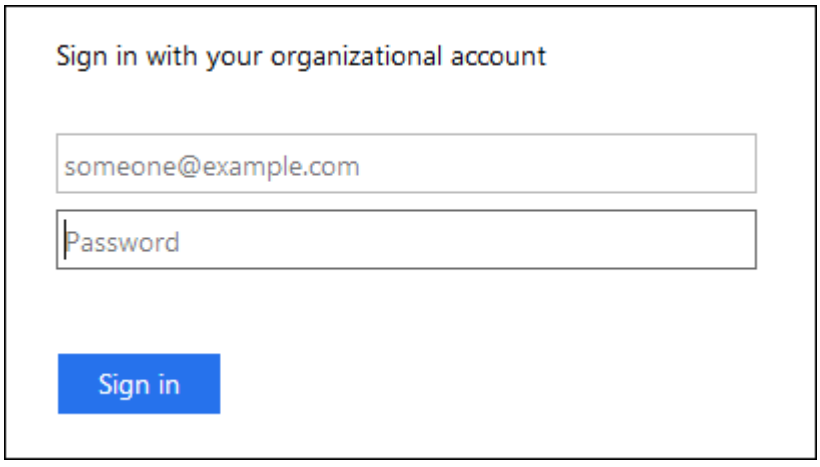


   - Si vous avez déjà accédé au Grid Manager ou au tenant Manager, vous êtes invité à sélectionner un compte récent ou à saisir un ID de compte :

La page de connexion StorageGRID n'apparaît pas lorsque vous entrez l'URL complète d'un compte de locataire (c'est-à-dire un nom de domaine complet ou une adresse IP suivie 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 pouvez Connectez-vous à l'aide de 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 **Grid Manager** si celui-ci apparaît dans la liste des comptes récents.
   - Pour accéder au Gestionnaire de locataires, entrez l'ID de compte de tenant à 20 chiffres ou sélectionnez un locataire par nom s'il apparaît dans la liste des comptes récents.
3. Sélectionnez **connexion**

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



4. Connectez-vous à l'aide de vos identifiants SSO.

Si vos informations d'identification SSO sont correctes :

a. Le fournisseur d'identités 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 Gestionnaire de grille ou au Gestionnaire des locataires, selon le compte que vous avez sélectionné.

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

5. Accédez éventuellement à d'autres nœuds d'administration ou à Grid Manager ou au tenant Manager, si vous disposez des autorisations adéquates.

   Il n'est pas nécessaire de saisir à nouveau vos informations d'identification SSO.

Déconnectez-vous lorsque SSO est activé

Lorsque l'authentification SSO est activée pour StorageGRID, le processus de déconnexion dépend de ce que vous êtes connecté et de l'endroit 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 connexion 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 plus rapidement à ces interfaces utilisateur à l'avenir.

Si vous êtes connecté à…	Et vous vous déconnectez de…	Vous êtes déconnecté de…
Grid Manager sur un ou plusieurs nœuds d'administration	Grid Manager sur n'importe quel nœud d'administration	Grid Manager sur tous les nœuds d'administration **Remarque :** si vous utilisez Azure pour SSO, la session 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
Grid Manager et tenant Manager	Gestionnaire de grille	Le Grid Manager uniquement. Vous devez également vous déconnecter du tenant Manager 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 à travers plusieurs sessions de navigateur, vous devez vous déconnecter de toutes les sessions de navigateur séparément.

Configuration requise et considérations pour l'authentification unique

Avant d'activer la signature unique (SSO) pour un système StorageGRID, consultez les conditions requises et les considérations à prendre en compte.

Exigences du fournisseur d'identités

StorageGRID prend en charge les fournisseurs d'identités SSO suivants :

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

Vous devez configurer la fédération des identités de votre système StorageGRID avant de pouvoir configurer un fournisseur d'identités SSO. Le type de service LDAP que vous utilisez pour la fédération des identités 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 • Azure • PingFederate
Azure	Azure

Exigences AD FS

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

- Système de fichiers AD Windows Server 2022
- Système de fichiers AD Windows Server 2019
- Système de fichiers AD Windows Server 2016

Windows Server 2016 doit utiliser le "Mise à jour KB3201845" ou une version ultérieure.

Supplémentaires requise

- TLS (transport Layer Security) 1.2 ou 1.3
- Microsoft .NET Framework, version 3.5.1 ou supérieure

Avantages d'Azure

Si vous utilisez Azure comme type SSO et que les utilisateurs ont des noms d'utilisateur principaux qui n'utilisent pas le préfixe sAMAccountName, des problèmes de connexion peuvent se produire si StorageGRID

perd sa connexion avec le serveur LDAP. Pour autoriser les utilisateurs à se connecter, vous devez restaurer la connexion au serveur LDAP.

Configuration requise pour le certificat de serveur

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

Si vous ne l'avez pas déjà "configuré un certificat personnalisé pour l'interface de gestion"fait, vous devriez 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 tiers StorageGRID, les applications d'entreprise ou les connexions SP.

> Il n'est pas recommandé d'utiliser le certificat de serveur par défaut d'un nœud d'administration dans une connexion de confiance, d'une application d'entreprise ou d'un SP. 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 restauré, vous devez mettre à jour la confiance de la partie utilisatrices, l'application d'entreprise ou la connexion SP avec le nouveau certificat.

Vous pouvez accéder au certificat de serveur d'un nœud d'administration en vous connectant au shell de commande du nœud et en allant dans le `/var/local/mgmt-api` répertoire. Un certificat de serveur personnalisé est nommé `custom-server.crt`. Le certificat de serveur par défaut du nœud est nommé `server.crt`.

Configuration requise pour les ports

L'authentification unique (SSO) n'est pas disponible sur les ports du gestionnaire de grille restreinte ou du gestionnaire de locataires. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec une connexion unique. Voir "Contrôler l'accès au niveau du pare-feu externe".

Confirmez 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 Grid Manager et au tenant Manager pour tout compte de tenant existant.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez "autorisations d'accès spécifiques".
- Vous avez déjà configuré la fédération des identités.

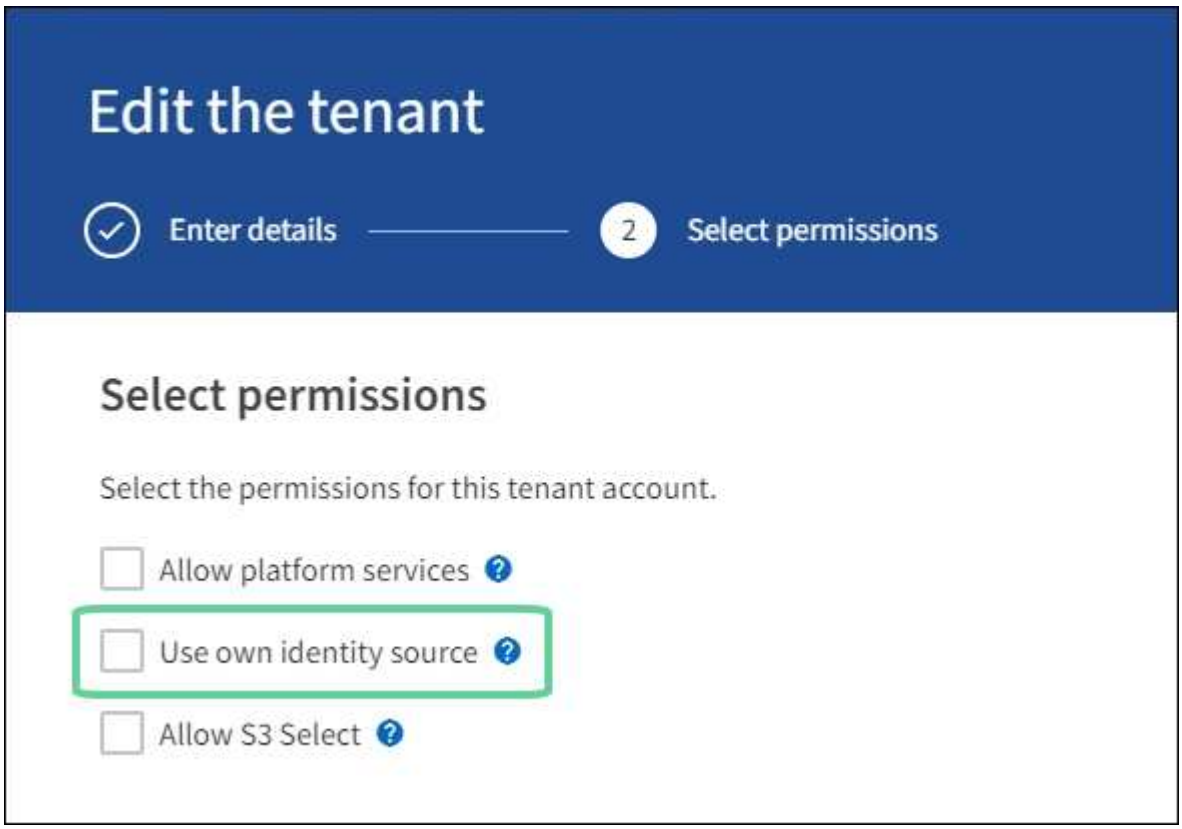
Étapes

1. S'il existe des comptes de tenant existants, vérifiez qu'aucun des locataires n'utilise son propre référentiel d'identité.

> Lorsque vous activez SSO, un référentiel d'identité configuré dans le Gestionnaire de locataires est remplacé par le référentiel d'identité configuré dans le Gestionnaire de grille. Les utilisateurs appartenant au référentiel d'identité du locataire ne pourront plus se connecter à moins qu'ils aient un compte avec le référentiel d'identité Grid Manager.

a. Connectez-vous au Gestionnaire de locataires pour chaque compte de locataire.
b. Sélectionnez **ACCESS MANAGEMENT** > **identity federation**.
c. Vérifiez que la case **Activer la fédération d'identité** n'est pas cochée.
d. Si c'est le cas, vérifiez que tous les groupes fédérés pouvant être utilisés pour ce compte de tenant ne sont plus nécessaires, décochez la case et sélectionnez **Enregistrer**.

2. Vérifiez qu'un utilisateur fédéré peut accéder au Grid Manager :
   a. Dans Grid Manager, sélectionnez **CONFIGURATION** > **contrôle d'accès** > **groupes d'administration**.
   b. Assurez-vous qu'au moins un groupe fédéré a été importé du référentiel d'identité Active Directory et qu'il a reçu l'autorisation d'accès racine.
   c. Se déconnecter.
   d. Confirmez que vous pouvez vous reconnecter au Grid Manager en tant qu'utilisateur dans le groupe fédéré.
3. S'il existe des comptes de tenant existants, confirmez qu'un utilisateur fédéré disposant d'une autorisation d'accès racine peut se connecter :
   a. Dans Grid Manager, sélectionnez **TENANTS**.
   b. Sélectionnez le compte locataire, puis sélectionnez **actions** > **Modifier**.
   c. Dans l'onglet entrer les détails, sélectionnez **Continuer**.
   d. Si la case **utiliser le propre référentiel d'identité** est cochée, décochez la case et sélectionnez **Enregistrer**.



La page tenant s'affiche.

a. Sélectionnez le compte de tenant, sélectionnez **connexion** et connectez-vous au compte de tenant en tant qu'utilisateur racine local.

b. Dans le Gestionnaire de locataires, sélectionnez **ACCESS MANAGEMENT** > **Groups**.

c. Assurez-vous qu'au moins un groupe fédéré du Grid Manager a reçu l'autorisation d'accès racine pour ce locataire.

d. Se déconnecter.

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

Informations associées

- "Configuration requise et considérations pour l'authentification unique"
- "Gérez les groupes d'administration"
- "Utilisez un compte de 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 SSO activé, vous pouvez revenir en mode sandbox chaque fois que vous devez modifier ou tester à nouveau la configuration.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine".
- Vous avez configuré la fédération des identités pour votre système StorageGRID.
- Pour le type de service LDAP * de fédération d'identités, vous avez sélectionné Active Directory ou Azure, en fonction du fournisseur d'identité SSO que vous envisagez d'utiliser.

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

Description de la 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. Le fournisseur d'identité SSO renvoie une réponse d'authentification à StorageGRID, indiquant si la demande d'authentification a réussi. Pour les demandes réussies :

- La réponse d'Active Directory ou 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 au sujet des demandes d'authentification des utilisateurs, vous devez configurer certains paramètres dans StorageGRID. Ensuite, vous devez utiliser le logiciel du fournisseur d'identités SSO pour créer une confiance de tiers 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 le SSO.

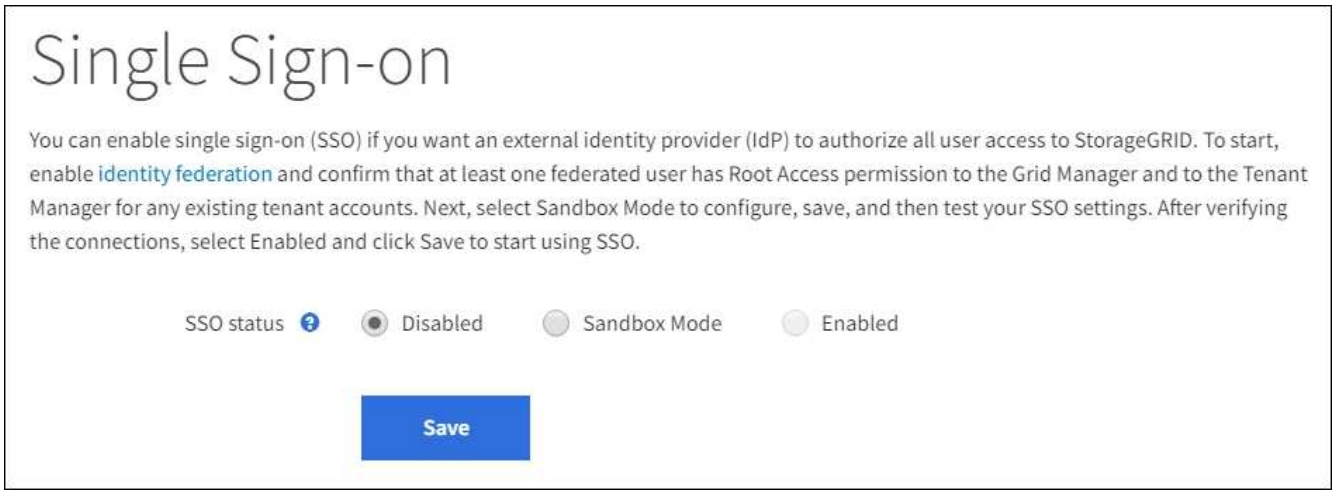
Le mode sandbox facilite l'exécution de cette configuration et le test de tous vos paramètres avant l'activation de SSO. Lorsque vous utilisez le mode sandbox, les utilisateurs ne peuvent pas se connecter à l'aide de SSO.

Accéder au mode sandbox

Étapes

1. Sélectionnez **CONFIGURATION** > **contrôle d'accès** > **connexion unique**.

   La page connexion unique s'affiche, avec l'option **Disabled** sélectionnée.



   Si les options Statut SSO ne s'affichent pas, vérifiez que vous avez configuré le fournisseur d'identité comme référentiel d'identité fédéré. Voir "Configuration requise et considérations pour l'authentification unique".

2. Sélectionnez **Sandbox mode**.

   La section fournisseur d'identité s'affiche.

Saisissez les détails du fournisseur d'identité

Étapes

1. Sélectionnez le **SSO type** dans la liste déroulante.
2. Renseignez les champs de la section Identity Provider en fonction du type SSO sélectionné.

Active Directory

a. Entrez le nom du service de fédération * pour le fournisseur d'identités, exactement comme il apparaît dans Active Directory Federation Service (AD FS).

> Pour localiser le nom du service de fédération, accédez à Windows Server Manager. Sélectionnez **Outils** > **AD FS Management**. Dans le menu action, sélectionnez **Modifier les propriétés du service de fédération**. Le nom du service de fédération est indiqué dans le second champ.

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

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

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

> Si vous modifiez le certificat de l'autorité de certification, testez immédiatement "Redémarrez le service mgmt-api sur les nœuds d'administration" et vérifiez si une authentification unique réussie est présente dans le gestionnaire de grille.

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

- Par exemple, si votre grid 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 grid inclut plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identifiant. Par exemple `SG-[HOSTNAME],` . Cette commande génère une table qui affiche l'identifiant de partie comptant pour chaque nœud d'administration de votre système, en fonction du nom d'hôte du nœud.

> Vous devez créer une confiance en tiers pour chaque nœud d'administration de votre système StorageGRID. Le fait d'avoir une confiance de partie de confiance pour chaque nœud d'administration permet aux utilisateurs de se connecter et de se déconnecter en toute sécurité à n'importe quel nœud d'administration.

d. Sélectionnez **Enregistrer**.

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

Azure

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

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

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

   > Si vous modifiez le certificat de l'autorité de certification, testez immédiatement "Redémarrez le service mgmt-api sur les nœuds d'administration" et vérifiez si une authentification unique réussie est présente dans le gestionnaire de grille.

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

   - Par exemple, si votre grid 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 grid inclut plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identifiant. Par exemple `SG-[HOSTNAME]`, . Cela génère une table qui indique le nom d'une application d'entreprise pour chaque noeud d'administration de votre système, en fonction du nom d'hôte du noeud.

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

c. Suivez les étapes de la section "Création d'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 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 **Save** pendant quelques secondes.

PingFederate

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

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

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

> Si vous modifiez le certificat de l'autorité de certification, testez immédiatement "Redémarrez le service mgmt-api sur les nœuds d'administration" et vérifiez si une authentification unique réussie est présente dans le gestionnaire de grille.

b. Dans la section SP (Service Provider), 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 grid 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 grid inclut plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identifiant. Par exemple `SG-[HOSTNAME],` . Ce tableau génère un 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. La présence d'une connexion SP pour chaque nœud d'administration permet aux utilisateurs de se connecter et de se déconnecter en toute sécurité à n'importe quel nœud d'administration.

c. Spécifiez l'URL des métadonnées de fédération pour chaque noeud d'administration dans le champ **URL des métadonnées de 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 **Save** pendant quelques secondes.

Configurez les approbations des parties utilisatrices, les applications d'entreprise ou les connexions SP

Lorsque la configuration est enregistrée, l'avis de confirmation du mode Sandbox s'affiche. Cet avis confirme

que le mode sandbox est désormais activé et fournit des instructions de présentation.

StorageGRID peut rester en mode sandbox tant que nécessaire. Toutefois, lorsque **Sandbox mode** est sélectionné sur la page connexion unique, SSO est désactivé pour tous les utilisateurs StorageGRID. Seuls les utilisateurs locaux peuvent se connecter.

Procédez comme suit pour configurer les approbations de tiers de confiance (Active Directory), les applications d’entreprise complètes (Azure) ou les connexions SP (PingFederate).

Active Directory

Étapes

1. Accédez à Active Directory Federation Services (AD FS).
2. Créez une ou plusieurs fiducies de tiers de confiance pour StorageGRID, en utilisant chaque identifiant de partie de confiance indiqué dans le tableau de la page authentification unique StorageGRID.

   Vous devez créer une confiance pour chaque noeud d'administration indiqué dans le tableau.

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

Azure

Étapes

1. Dans la page Single Sign-on du noeud d'administration auquel vous êtes actuellement connecté, sélectionnez le bouton pour télécharger et enregistrer les métadonnées SAML.
2. Ensuite, pour tout autre nœud d'administration de votre grid, répétez la procédure suivante :
   a. Connectez-vous au nœud.
   b. Sélectionnez **CONFIGURATION** > **contrôle d'accès** > **connexion unique**.
   c. Téléchargez et enregistrez les métadonnées SAML pour ce nœud.
3. Accédez au portail Azure.
4. Suivez les étapes de la section "Création d'applications d'entreprise dans Azure AD" pour télécharger le fichier de métadonnées SAML pour chaque nœud d'administration dans l'application d'entreprise Azure correspondante.

PingFederate

Étapes

1. Dans la page Single Sign-on du noeud d'administration auquel vous êtes actuellement connecté, sélectionnez le bouton pour télécharger et enregistrer les métadonnées SAML.
2. Ensuite, pour tout autre nœud d'administration de votre grid, répétez la procédure suivante :
   a. Connectez-vous au nœud.
   b. Sélectionnez **CONFIGURATION** > **contrôle d'accès** > **connexion unique**.
   c. Téléchargez et enregistrez les métadonnées SAML pour ce nœud.
3. Accédez à PingFederate.
4. "Créez une ou plusieurs connexions de fournisseur de services pour StorageGRID". Utilisez l'ID de connexion SP pour chaque nœud d'administration (indiqué 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 affiché 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

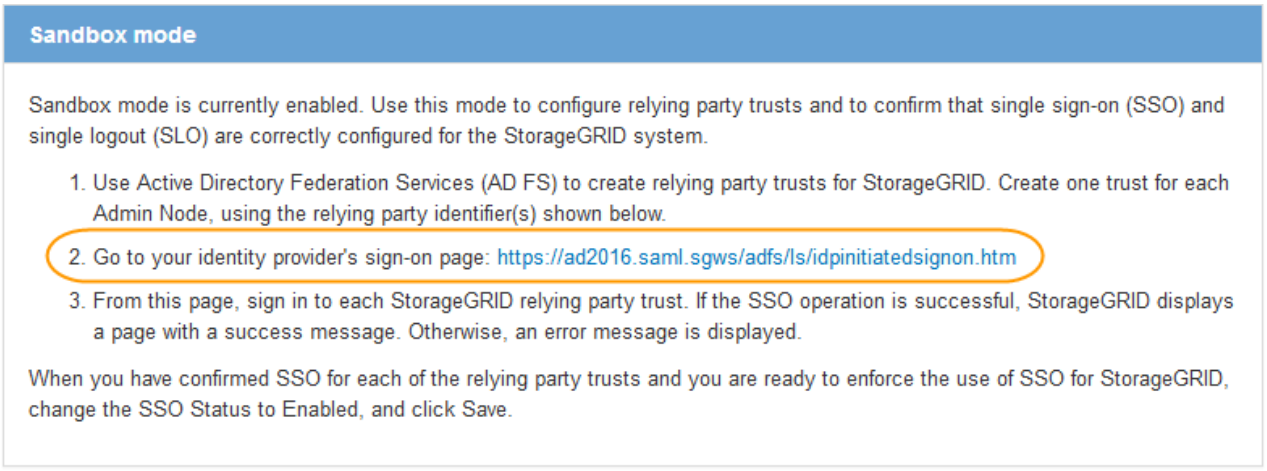
chaque nœud d’administration.

Active Directory

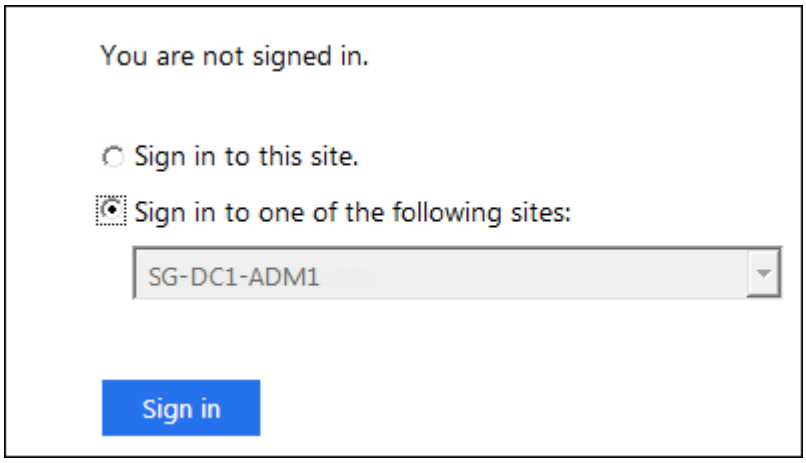
Étapes

1. Sur la page d'ouverture de session unique de StorageGRID, localisez le lien dans le message en mode Sandbox.

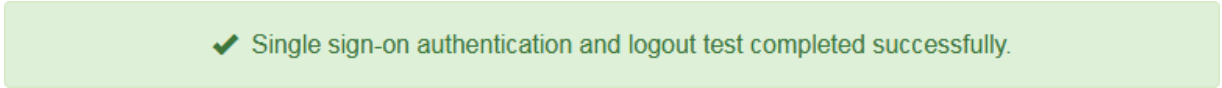
   L'URL est dérivée de la valeur que vous avez saisie dans le champ **Nom du service de fédération**.



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



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



   - Si l'opération SSO échoue, un message d'erreur s'affiche. Corrigez 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.

Azure

Étapes

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

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

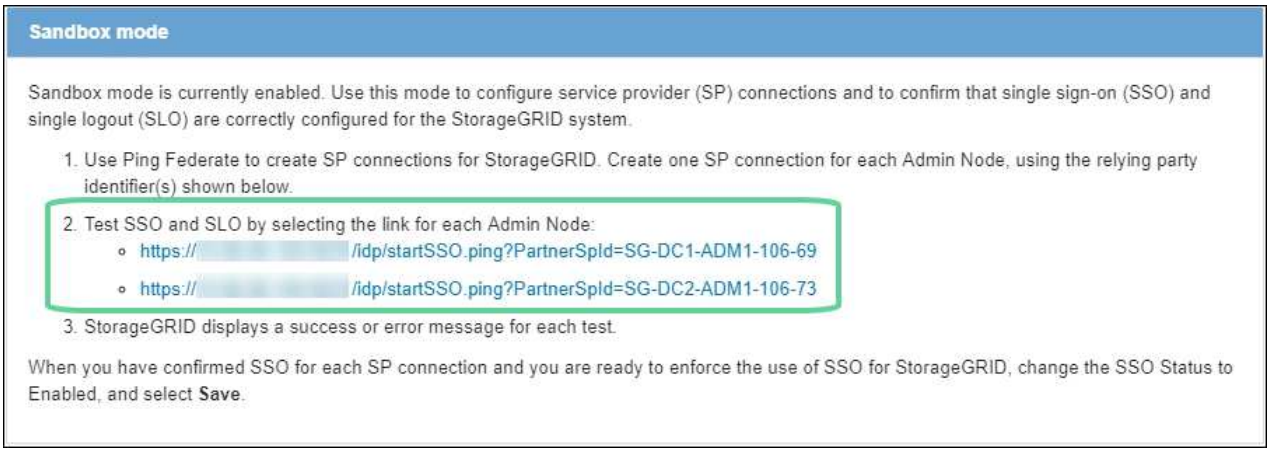
   - Si l'opération SSO échoue, un message d'erreur s'affiche. Corrigez le problème, effacez les cookies du navigateur et réessayez.
4. Répétez ces étapes pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

PingFederate

Étapes

1. Sur la page d'ouverture de session unique de StorageGRID, sélectionnez le premier lien dans le message en mode Sandbox.

   Sélectionnez et testez un lien à la fois.



2. Entrez les informations d'identification d'un utilisateur fédéré.
   - Si les opérations de connexion SSO et de déconnexion ont réussi, 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. Corrigez le problème, effacez les cookies du navigateur et réessayez.
3. Cliquez sur le lien suivant pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

Si un message page expirée s'affiche, sélectionnez le bouton **Retour** dans votre navigateur et soumettez à nouveau vos informations d'identification.

Activez l'authentification unique

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

Lorsque l'authentification SSO est activée, tous les utilisateurs doivent utiliser l'authentification SSO pour accéder au Grid Manager, au tenant Manager, à l'API Grid Management et à l'API tenant Management. Les utilisateurs locaux ne peuvent plus accéder à StorageGRID.

Étapes

1. Sélectionnez **CONFIGURATION** > **contrôle d'accès** > **connexion unique**.
2. Définissez l'état SSO sur **activé**.
3. Sélectionnez **Enregistrer**.
4. Vérifiez 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 (utilisateur d'un groupe fédéré importé dans StorageGRID) Ou déconnectez-vous du portail Azure avant de tenter de vous connecter à StorageGRID.

Créer des fiducies de tiers de confiance dans AD FS

Vous devez utiliser Active Directory Federation Services (AD FS) pour créer une confiance de partie de confiance pour chaque nœud d'administration de votre système. Vous pouvez créer des approbations tierces via les commandes PowerShell, en important les métadonnées SAML depuis StorageGRID ou en saisissant manuellement les données.

Avant de commencer

- Vous avez configuré l'authentification unique pour StorageGRID et sélectionné **AD FS** comme type SSO.
- **Sandbox mode** est sélectionné sur la page Single Sign-on dans Grid Manager. Voir "Utiliser le mode sandbox".
- Vous connaissez le nom de domaine complet (ou l'adresse IP) et l'identifiant de partie comptant pour chaque nœud d'administration de votre système. Ces valeurs sont disponibles dans le tableau des détails des nœuds d'administration de la page d'ouverture de session unique StorageGRID.

Vous devez créer une confiance en tiers pour chaque nœud d'administration de votre système StorageGRID. Le fait d'avoir une confiance de partie de confiance pour chaque nœud d'administration permet aux utilisateurs de se connecter et de se déconnecter en toute sécurité à n'importe quel nœud d'administration.

- Vous avez l'expérience de créer des approbations de tiers de confiance dans AD FS, ou vous avez accès à la documentation Microsoft AD FS.
- Vous utilisez le composant logiciel enfichable AD FS Management et vous appartenez au groupe administrateurs.
- Si vous créez manuellement la confiance de la partie utilisatrices, vous disposez du certificat personnalisé chargé pour l'interface de gestion StorageGRID, ou vous savez comment vous connecter à un nœud d'administration à partir du shell de commande.

Description de la 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. Pour toute question, consultez la documentation Microsoft AD FS.

Créez une confiance en vous appuyant sur Windows PowerShell

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

Étapes

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

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

   - Pour `Admin_Node_Identifier`, entrez l'identificateur de partie utilisatrice pour le noeud Admin, exactement comme il apparaît sur la page Single Sign-On. Par exemple `SG-DC1-ADM1`, .
   - Pour `Admin_Node_FQDN`, entrez le nom de domaine complet pour le même noeud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)
3. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils** > **AD FS Management**.

   L'outil de gestion AD FS s'affiche.
4. Sélectionnez **AD FS** > **confiance de la partie de confiance**.

   La liste des fiducies de tiers de confiance s'affiche.
5. Ajouter une stratégie de contrôle d'accès à la confiance de la partie qui vient d'être créée :
   a. Recherchez la confiance de la partie de confiance que vous venez de créer.
   b. Cliquez avec le bouton droit de la souris sur la confiance et sélectionnez **Modifier la stratégie de contrôle d'accès**.
   c. Sélectionnez une stratégie de contrôle d'accès.
   d. Sélectionnez **appliquer**, puis **OK**
6. Ajouter une politique d'émission de demandes de remboursement à la nouvelle fiducie de compte comptant :
   a. Recherchez la confiance de la partie de confiance que vous venez de créer.

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

c. Sélectionnez **Ajouter règle**.

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

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

   Par exemple, **objectGUID à ID de nom** ou **UPN à ID de nom**.

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

g. Dans la colonne attribut LDAP de la table mappage, tapez **objectGUID** ou sélectionnez **User-principal-Name**.

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

i. Sélectionnez **Terminer** et sélectionnez **OK**.

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

   a. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrices pour ouvrir ses propriétés.

   b. Vérifiez que les champs des onglets **Endpoints**, **identificateurs** et **Signature** sont renseignés.

      Si les métadonnées sont manquantes, vérifiez que l'adresse des métadonnées de fédération est correcte ou entrez les valeurs manuellement.

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

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

Créez une confiance de partie de confiance en vous important des métadonnées de fédération

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

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis **AD FS Management**.
2. Sous actions, sélectionnez **Ajouter la confiance de la partie de confiance**.
3. Sur la page de bienvenue, choisissez **revendications Aware** et sélectionnez **Démarrer**.
4. Sélectionnez **Importer les données concernant la partie de confiance publiée en ligne ou sur un réseau local**.
5. Dans **adresse de métadonnées de fédération (nom d'hôte ou URL)**, saisissez l'emplacement des métadonnées SAML pour ce noeud d'administration :

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

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

adresse IP change.)

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

> Lors de la saisie du nom d'affichage, utilisez l'identificateur de partie comptant pour le noeud d'administration, exactement comme il apparaît sur la page d'ouverture de session unique dans le Gestionnaire de grille. Par exemple `SG-DC1-ADM1,`.

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

      Par exemple, **objectGUID à ID de nom** ou **UPN à ID de nom**.

   e. Pour le magasin d'attributs, sélectionnez **Active Directory**.
   f. Dans la colonne attribut LDAP de la table mappage, tapez **objectGUID** ou sélectionnez **User-principal-Name**.
   g. Dans la colonne Type de demande sortante de la table mappage, sélectionnez **Nom ID** dans la liste déroulante.
   h. Sélectionnez **Terminer** et sélectionnez **OK**.
8. Confirmez que les métadonnées ont été importées avec succès.
   a. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrices pour ouvrir ses propriétés.
   b. Vérifiez que les champs des onglets **Endpoints**, **identificateurs** et **Signature** sont renseignés.

      Si les métadonnées sont manquantes, vérifiez que l'adresse des métadonnées de fédération est correcte ou entrez les valeurs manuellement.
9. Répétez ces étapes pour configurer une confiance de tiers pour tous les nœuds d'administration de votre système StorageGRID.
10. Lorsque vous avez terminé, revenez à StorageGRID et testez toutes les approbations de parties utilisatrices pour confirmer qu'elles sont correctement configurées. Voir "Utiliser le mode Sandbox" pour obtenir des instructions.

Créer une confiance de partie de confiance manuellement

Si vous choisissez de ne pas importer les données pour les approbations de pièces de confiance, vous pouvez entrer les valeurs manuellement.

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis **AD FS Management**.
2. Sous actions, sélectionnez **Ajouter la confiance de la partie de confiance**.
3. Sur la page de bienvenue, choisissez **revendications Aware** et sélectionnez **Démarrer**.

4. Sélectionnez **Entrez les données relatives à la partie de confiance manuellement** et sélectionnez **Suivant**.
5. Suivez l'assistant confiance de la partie de confiance :

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

      Pour plus de cohérence, utilisez l'identifiant de partie utilisatrices du nœud d'administration, exactement comme il apparaît sur la page Single Sign-On du Grid Manager. 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 noeud final du service SAML pour le noeud 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. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)

   e. Sur la page configurer les identificateurs, spécifiez l'identificateur de partie de confiance pour le même noeud d'administration :

      `Admin_Node_Identifier`

      Pour *`Admin_Node_Identifier`*, entrez l'identificateur de partie utilisatrice pour le noeud Admin, exactement comme il apparaît sur la page Single Sign-On. Par exemple `SG-DC1-ADM1`, .

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

      La boîte de dialogue Modifier la politique d'émission des demandes de remboursement s'affiche.

      > Si la boîte de dialogue ne s'affiche pas, cliquez avec le bouton droit de la souris sur la fiducie et sélectionnez **Modifier la politique d'émission des sinistres**.

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

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

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

      Par exemple, **objectGUID à ID de nom** ou **UPN à ID de nom**.

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

   d. Dans la colonne attribut LDAP de la table mappage, tapez **objectGUID** ou sélectionnez **User-principal-Name**.

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

   f. Sélectionnez **Terminer** et sélectionnez **OK**.

7. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrices pour ouvrir ses propriétés.
8. Dans l'onglet **Endpoints**, configurez le noeud final pour une déconnexion unique (SLO) :

   a. Sélectionnez **Ajouter SAML**.

   b. Sélectionnez **Endpoint Type** > **SAML Logout**.

   c. Sélectionnez **Redirect** > **Redirect**.

   d. Dans le champ **URL de confiance**, entrez l'URL utilisée pour la déconnexion unique (SLO) à partir de ce noeud 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. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)

   a. Sélectionnez **OK**.

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

   a. Ajouter le certificat personnalisé :

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

      > L'utilisation du certificat par défaut du nœud d'administration (`server.crt`) n'est pas recommandée. Si le nœud d'administration échoue, le certificat par défaut sera régénéré lorsque vous restaurez le nœud et vous devrez mettre à jour la confiance de l'organisme 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 confiance de tiers pour tous les nœuds d'administration de votre système StorageGRID.
11. Lorsque vous avez terminé, revenez à StorageGRID et testez toutes les approbations de parties utilisatrices pour confirmer qu'elles sont correctement configurées. Voir "Utiliser le mode sandbox" pour obtenir des instructions.

Création d'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 la connexion unique pour StorageGRID et vous avez sélectionné **Azure** comme type SSO.

- **Sandbox mode** est sélectionné sur la page Single Sign-on dans Grid Manager. Voir "Utiliser le mode sandbox".
- Vous disposez du **Nom d'application entreprise** pour chaque noeud 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. La présence d'une application d'entreprise pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité à 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 avez l'un des rôles suivants dans le compte Azure : administrateur global, administrateur des applications clouds, administrateur d'applications clouds ou propriétaire du principal du service.

Accéder à Azure AD

Étapes

1. Connectez-vous au "Portail Azure".
2. Accédez à "Azure Active Directory".
3. Sélectionnez "Les 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 afin de créer une application d'entreprise pour chaque nœud d'administration. Vous allez copier les URL de métadonnées de la fédération à partir d'Azure et les coller dans les champs URL* de métadonnées de la fédération correspondants sur la page d'ouverture de session unique de StorageGRID.

Étapes

1. Répétez les étapes suivantes pour chaque nœud d'administration.
   a. Dans le volet applications Azure Enterprise, sélectionnez **Nouvelle application**.
   b. Sélectionnez **Créez votre propre application**.
   c. Pour le nom, entrez le **nom de l'application entreprise** que vous avez copié à partir du tableau Détails du noeud d'administration sur la page connexion 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 **Get Started** dans **2. Configurez la case Single Sign On** ou sélectionnez le lien **Single Sign-on** dans la marge de gauche.
   g. Sélectionnez la case **SAML**.
   h. Copiez l'URL **App Federation Metadata URL**, que vous trouverez sous **étape 3 SAML Signing Certificate**.
   i. Accédez à la page d'ouverture de session unique StorageGRID et collez l'URL dans le champ **URL de métadonnées de fédération** qui correspond au nom de l'application **entreprise** que vous avez utilisée.

2. Une fois que vous avez 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'ouverture de session 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. Connectez-vous à StorageGRID à partir du nœud d'administration.
   b. Sélectionnez **CONFIGURATION** > **contrôle d'accès** > **connexion unique**.
   c. Sélectionnez le bouton pour télécharger les métadonnées SAML de ce nœud d'administration.
   d. Enregistrez le fichier que vous allez télécharger dans Azure AD.

Téléchargez les métadonnées SAML sur chaque application d'entreprise

Après le téléchargement d'un fichier de métadonnées SAML pour chaque nœud d'administration StorageGRID, effectuez les opérations suivantes dans Azure AD :

Étapes

1. Revenez au portail Azure.
2. Répétez cette procédure 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 séparément les affectations).
   c. Accédez à la page Single Sign-on.
   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 **X** pour fermer le volet. Vous revenez à la page configurer un Single Sign-on avec SAML.
3. Suivez les étapes de la section "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 noeud d'administration de votre système. Pour accélérer le processus, vous importez les métadonnées SAML à partir de StorageGRID.

Avant de commencer

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

- **Sandbox mode** est sélectionné sur la page Single Sign-on dans Grid Manager. Voir "Utiliser le mode sandbox".
- Vous disposez de l'ID de connexion * SP* pour chaque noeud d'administration de votre système. Ces valeurs sont disponibles dans le tableau des détails des nœuds d'administration de la page d'ouverture de session unique StorageGRID.
- Vous avez téléchargé les métadonnées **SAML** pour chaque noeud d'administration de votre système.
- Vous avez l'expérience de la création de connexions SP dans PingFederate Server.
- Vous avez le "Guide de référence de l'administrateur"serveur for PingFederate. La documentation PingFederate fournit des instructions détaillées étape par étape et des explications.
- Vous avez le "Autorisation d'administrateur"serveur for PingFederate.

Description de la 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 sur votre version.

Remplir les conditions préalables 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 lors de la configuration des connexions du processeur de service.

Créer un magasin de données

Si ce n'est pas déjà fait, créez un magasin de données pour connecter PingFederate au serveur LDAP AD FS. Utilisez les valeurs que vous avez utilisées "configuration de la fédération des identités"dans StorageGRID.

- **Type**: Répertoire (LDAP)
- **Type LDAP** : Active Directory
- **Nom d'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 ce n'est pas déjà fait, créez un validateur pour les informations d'identification du mot de passe.

- **Type**: LDAP Nom d'utilisateur Mot de passe validateur des informations d'identification
- **Magasin de données** : sélectionnez le magasin de données que vous avez créé.
- **Base de recherche** : saisissez des informations à partir de LDAP (par exemple, DC=saml,DC=sgws).
- **Filtre de recherche** : sAMAccountName=${username}
- **Portée** : sous-arbre

Créer une instance d'adaptateur IDP

Si ce n'est déjà fait, créez une instance de carte IDP.

Étapes

1. Accédez à **Authentication** > **Integration** > **IDP Adapters**.

2. Sélectionnez **Créer une nouvelle instance**.
3. Dans l'onglet Type, sélectionnez **HTML Form IDP adapter**.
4. Dans l'onglet carte IDP, sélectionnez **Ajouter une nouvelle ligne à 'Validators Credentials'**.
5. Sélectionnez le validateur des informations d'identification du mot de passe que vous avez créé.
6. Dans l'onglet attributs de l'adaptateur, sélectionnez l'attribut **nom d'utilisateur** pour **pseudonyme**.
7. Sélectionnez **Enregistrer**.

Créer ou importer un certificat de signature

Si ce n'est déjà fait, créez ou importez le certificat de signature.

Étapes

1. Accédez à **sécurité** > **clés 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 téléchargées depuis StorageGRID pour le noeud d'administration. Le fichier de métadonnées contient la plupart des 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 en toute sécurité à n'importe quel nœud et en dehors. Suivez ces instructions pour créer la première connexion du processeur de service. Ensuite, accédez à Créer des connexions SP supplémentaires pour créer les connexions supplémentaires dont vous avez besoin.

Choisissez le type de connexion SP

Étapes

1. Accédez à **applications** > **intégration** > **connexions SP**.
2. Sélectionnez **Créer connexion**.
3. Sélectionnez **ne pas utiliser de modèle pour cette connexion**.
4. Sélectionnez **Browser SSO Profiles** et **SAML 2.0** comme protocole.

Importation des métadonnées SP

Étapes

1. Dans l'onglet Importer les 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. Passez en revue le résumé des métadonnées et les informations fournies dans l'onglet Infos générales.

   L'ID d'entité du partenaire et le nom de connexion sont définis sur l'ID de connexion SP StorageGRID. (Par exemple, 10.96.105.200-DC1-ADM1-105-200). L'URL de base est l'adresse IP du nœud d'administration StorageGRID.

4. Sélectionnez **Suivant**.

Configurer SSO du navigateur IDP

Étapes

1. Dans l'onglet SSO du navigateur, sélectionnez **configurer SSO du navigateur**.
2. Dans l'onglet des profils SAML, sélectionnez les options **SSO** initiée par le SP, **SLO initial du SP**, **SSO initié par l'IDP** et **SLO** lancé par l'IDP.
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.

Mapper l'instance de l'adaptateur

Étapes

1. Dans l'onglet mappage de la source d'authentification, sélectionnez **mappage d'une nouvelle instance de carte**.
2. Dans l'onglet instance d'adaptateur, sélectionnez le instance d'adaptateur que vous avez 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 utilisateur, sélectionnez **Ajouter une source d'attribut**.
5. Dans l'onglet Data Store, indiquez une description et sélectionnez le magasin de données que vous avez ajouté.
6. Dans l'onglet LDAP Directory Search :
   - Saisissez le **DN de base**, qui doit correspondre exactement à la valeur que vous avez saisie dans StorageGRID pour le serveur LDAP.
   - Pour l'étendue de la recherche, sélectionnez **sous-arbre**.
   - Pour la classe d'objets racine, recherchez et ajoutez l'un de ces attributs : **objectGUID** ou **userPrincipalName**.
7. Dans l'onglet types d'encodage d'attribut binaire LDAP, sélectionnez **Base64** pour l'attribut **objectGUID**.
8. Dans l'onglet filtre LDAP, entrez **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 et enregistrez la source d'attribut.
11. Dans l'onglet Source de l'attribut FailSave, sélectionnez **abandonner la transaction SSO**.
12. Passez en revue le résumé et sélectionnez **Done**.
13. Sélectionnez **Done**.

Configurer les paramètres de protocole

Étapes

1. Dans l'onglet **connexion SP** > **connexion du navigateur SSO** > **Paramètres de protocole**, sélectionnez **configurer les paramètres de protocole**.
2. Dans l'onglet URL du service d'utilisateur d'assertion, acceptez les valeurs par défaut, qui ont été importées à partir des métadonnées StorageGRID SAML (**POST** pour la liaison et `/api/saml-response` pour l'URL du point final).
3. Dans l'onglet URL du service SLO, acceptez les valeurs par défaut, qui ont été importées à partir des métadonnées StorageGRID SAML (**REDIRECT** pour la liaison et `/api/saml-logout` pour l'URL du noeud final.
4. Dans l'onglet Allowable SAML Bindings, désactivez **ARTEFACT** et **SOAP**. Seuls **POST** et **REDIRECT** sont requis.
5. Dans l'onglet Signature Policy, laissez les cases **exiger la signature des requêtes Authn** et **toujours signer l'assertion** cochées.
6. Dans l'onglet Stratégie de cryptage, sélectionnez **aucun**.
7. Consultez le résumé et sélectionnez **Done** pour enregistrer les paramètres du protocole.
8. Consultez le résumé et sélectionnez **Done** 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 le signature du certificat que 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 de certificat de signature, qui ont été importées à partir des métadonnées SAML StorageGRID.
5. Passez en revue les écrans de résumé et sélectionnez **Enregistrer** pour enregistrer la connexion SP.

Créer des connexions SP supplémentaires

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

> Les connexions SP des 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 signature, Et l'URL de réponse SLO.

Étapes

1. Sélectionnez **action** > **copie** pour créer une copie de la connexion SP initiale pour chaque nœud d'administration supplémentaire.
2. Entrez l'ID de connexion et le nom de connexion de la copie, puis sélectionnez **Enregistrer**.
3. Choisissez le fichier de métadonnées correspondant au nœud d'administration :
   a. Sélectionnez **action** > **mettre à jour avec métadonnées**.
   b. Sélectionnez **Choisissez fichier** et chargez les métadonnées.

c. Sélectionnez **Suivant**.

d. Sélectionnez **Enregistrer**.

4. Résoudre l'erreur en raison de l'attribut inutilisé :

a. Sélectionnez la nouvelle connexion.

b. Sélectionnez **configurer le navigateur SSO > configurer la création d'assertion > 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 des identités.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez "autorisations d'accès spécifiques".

Étapes

1. Sélectionnez **CONFIGURATION** > **contrôle d'accès** > **connexion unique**.

   La page authentification unique s'affiche.

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

   Un message d'avertissement s'affiche pour indiquer que les utilisateurs locaux pourront maintenant se connecter.

4. Sélectionnez **OK**.

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

Désactivez et réactivez temporairement l'authentification unique pour un nœud d'administration

Il se peut que vous ne puissiez pas vous connecter à Grid Manager si le système d'authentification unique (SSO) est en panne. Dans ce cas, vous pouvez temporairement désactiver et réactiver SSO pour un noeud d'administration. Pour désactiver puis réactiver SSO, vous devez accéder au shell de commande du nœud.

Avant de commencer

- Vous avez "autorisations d'accès spécifiques".
- Vous avez le `Passwords.txt` fichier.
- Vous connaissez le mot de passe de l'utilisateur racine local.

Description de la tâche

Après avoir désactivé SSO pour un noeud d'administration, vous pouvez vous connecter à Grid Manager en tant qu'utilisateur racine local. Pour sécuriser votre système StorageGRID, vous devez utiliser le shell de commande 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 pour les autres nœuds d'administration de la grille. La case **Activer SSO** de la page ouverture de session unique du gestionnaire de grille reste cochée 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. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour basculer en root : `su -`
   d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

      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 l'authentification SSO.

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

4. À partir d'un navigateur Web, accédez à Grid Manager sur le même nœud d'administration.

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

5. Connectez-vous avec le nom d'utilisateur root et le mot de passe de l'utilisateur root local.
6. Si vous avez désactivé l'authentification SSO temporairement car vous avez besoin de corriger la configuration SSO :
   a. Sélectionnez **CONFIGURATION** > **contrôle d'accès** > **connexion unique**.
   b. Modifiez les paramètres SSO incorrects ou obsolètes.
   c. Sélectionnez **Enregistrer**.

      La sélection de **Enregistrer** sur la page ouverture de session unique permet de réactiver automatiquement SSO pour l'ensemble de la grille.

7. Si vous avez désactivé l'authentification SSO temporairement car vous devez accéder au Grid Manager pour une autre raison :
   a. Effectuez les tâches que vous souhaitez effectuer.
   b. Sélectionnez **se déconnecter** et fermez le Gestionnaire de grille.
   c. Réactivez SSO sur le nœud d'administration. Vous pouvez effectuer l'une des opérations 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 le SSO.

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

- Redémarrer le nœud grid : `reboot`

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

Utiliser la fédération de grille

Qu'est-ce que la fédération de grille ?

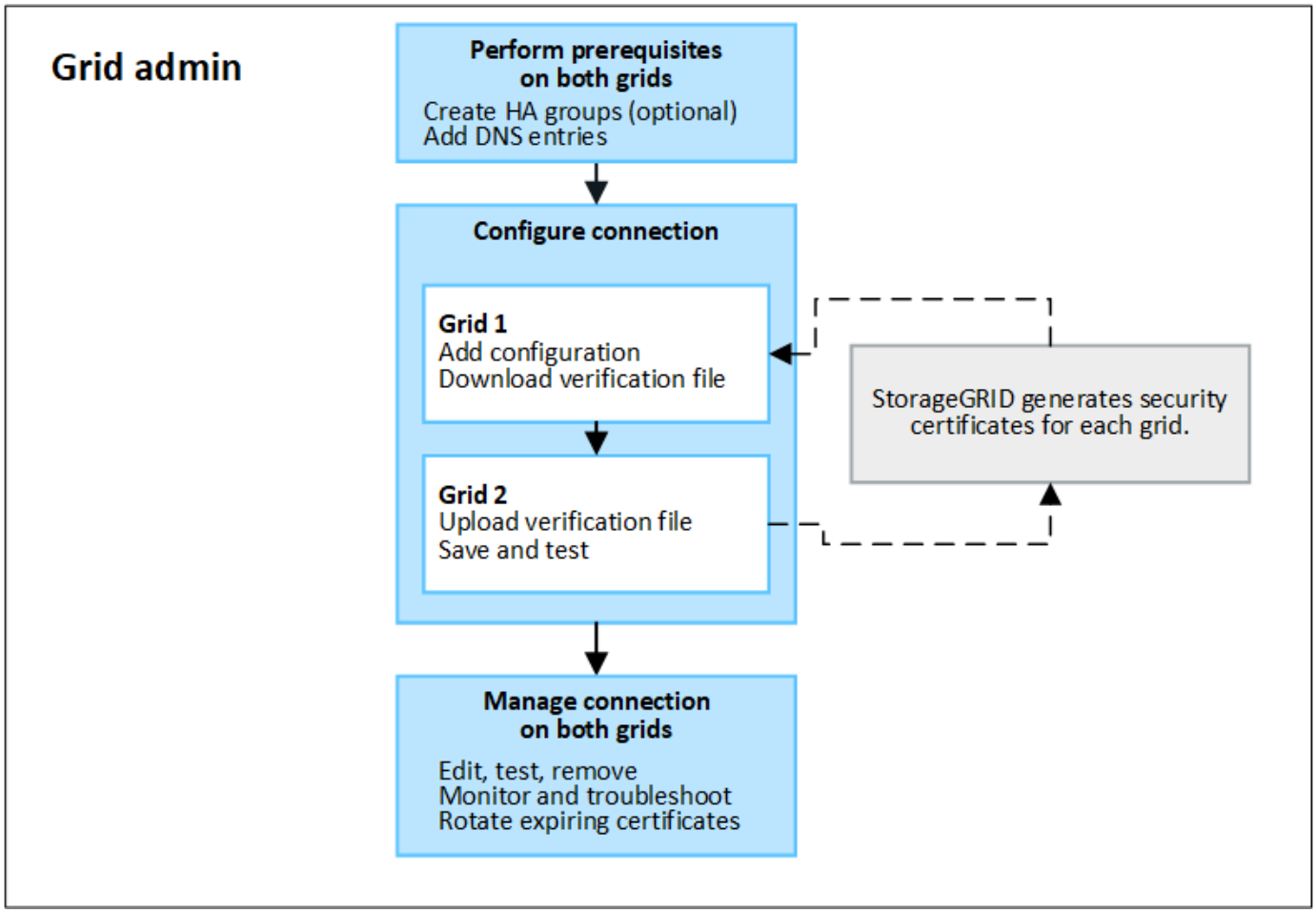
Vous pouvez utiliser la fédération de grid pour cloner les locataires et répliquer leurs objets entre deux systèmes StorageGRID à des fins de reprise après incident.

Qu'est-ce qu'une connexion de fédération de grille ?

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

Flux de travail pour la fédération de grille

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



Considérations et conditions requises pour les connexions de fédération de grille

- Les grilles utilisées pour la fédération de grille doivent exécuter des versions StorageGRID identiques ou ne doivent pas avoir plus d'une différence de version majeure entre elles.

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

- Une grille peut avoir une ou plusieurs connexions de fédération de grille à d'autres grilles. Chaque connexion de fédération de grille est indépendante des autres connexions. Par exemple, si la grille 1 a une connexion avec la grille 2 et une seconde connexion avec la grille 3, il n'y a pas de connexion implicite entre la grille 2 et la grille 3.
- Les connexions de 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 grille.
- Au moins une connexion de fédération de grille doit exister avant de pouvoir utiliser "clone de compte" ou "réplication entre plusieurs grilles".

Exigences en matière de mise en 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 grid sur l'autre grille composé de nœuds d'administration, de nœuds de passerelle ou des deux.
- Il est recommandé de connecter les "Groupes haute disponibilité (HA)"nœuds de passerelle et

d'administration sur chaque grid. L'utilisation des groupes haute disponibilité permet de s'assurer que les connexions de fédération du grid resteront en ligne si les nœuds ne sont plus disponibles. En cas de défaillance de l'interface active de l'un ou l'autre groupe haute disponibilité, 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 nœud d'administration ou d'un nœud de passerelle unique. Si le nœud devient indisponible, la connexion de fédération de grille devient également indisponible.
- "Réplication entre plusieurs grilles" D'objets exige que les nœuds de stockage de chaque grid puissent accéder aux nœuds d'administration et de passerelle configurés sur l'autre grid. Pour chaque grid, vérifiez que tous les nœuds de stockage disposent d'une route à large bande passante vers en tant que nœuds d'administration ou nœuds de passerelle utilisés pour la connexion.

Utilisez des FQDN 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. Créez ensuite les entrées DNS appropriées, comme suit :

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

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

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

Configuration requise pour les ports

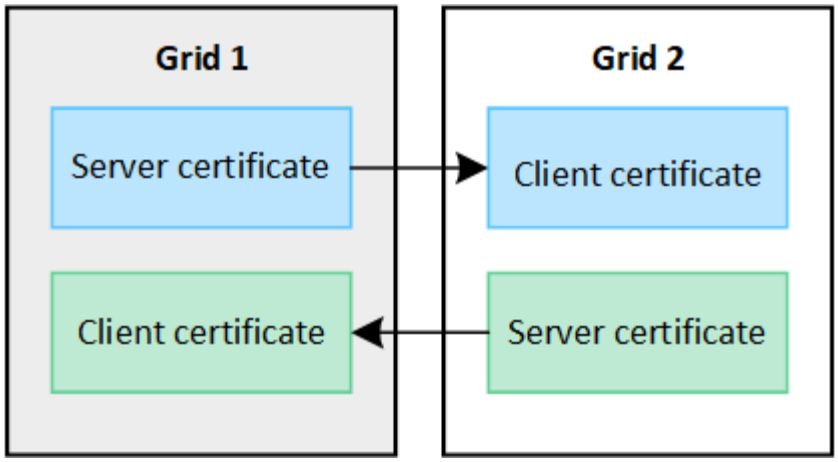
Lors de la création d'une connexion de fédération de grille, vous pouvez spécifier tout numéro de port inutilisé compris entre 23000 et 23999. Les deux grilles de cette connexion utilisent le même port.

Vous devez vous assurer qu'aucun nœud d'une 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 de serveur et de client pour authentifier et crypter les informations envoyées de la grille 1 à la grille 2
- Certificats de serveur et de client pour authentifier et crypter les informations envoyées de la grille 2 à la grille 1



Par défaut, les certificats sont valides pendant 730 jours (2 ans). Lorsque ces certificats sont proches de leur date d'expiration, l'alerte **expiration du certificat de fédération GRID** vous rappelle de faire pivoter les certificats, ce que vous pouvez faire à l'aide de Grid Manager.

> Si les certificats à l'une des extrémités de la connexion expirent, la connexion cesse de fonctionner. La réplication des données sera en attente jusqu'à la mise à jour des certificats.

En savoir plus >>

- "Créer des connexions de fédération de grille"
- "Gérer les connexions de fédération de grille"
- "Dépanner les erreurs de fédération de grille"

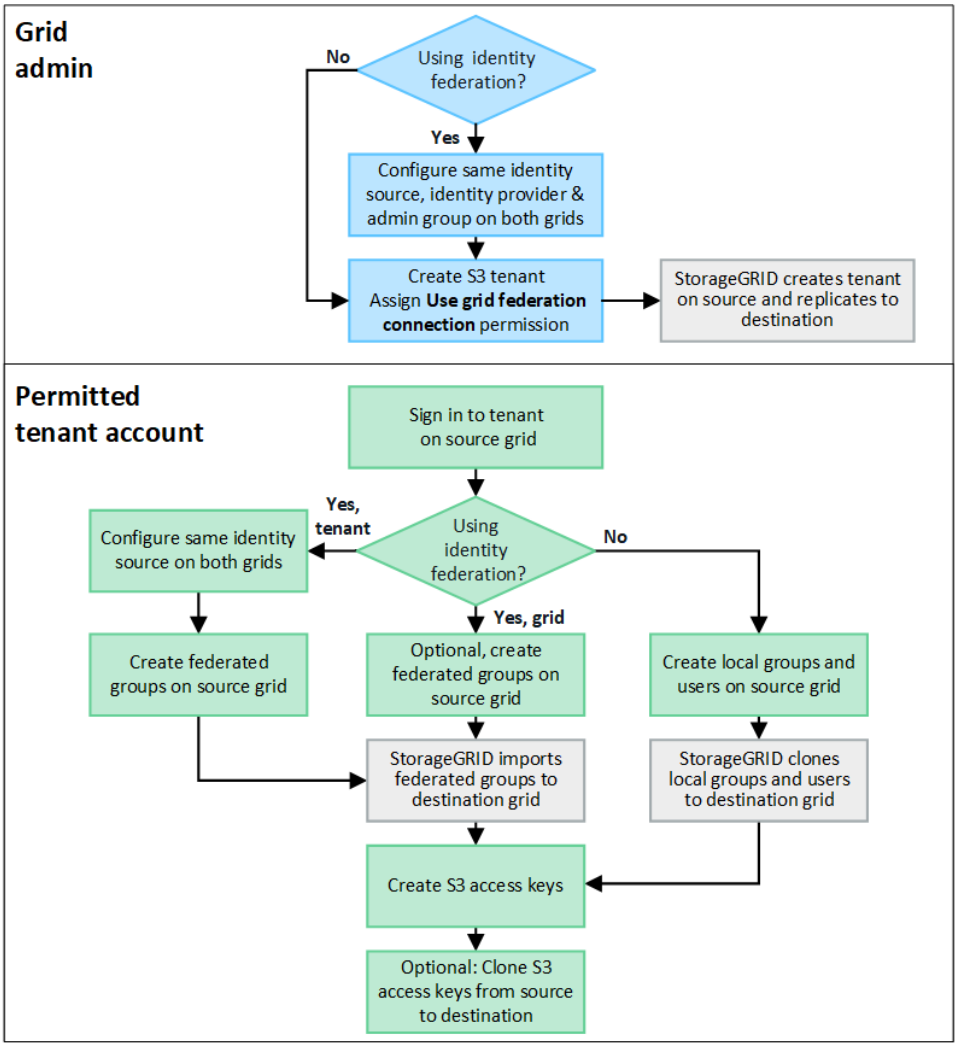
Qu'est-ce que le clone du compte ?

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

Le clone de compte est requis pour "réplication entre plusieurs grilles". Le clonage des informations de compte d'un système StorageGRID source vers un système StorageGRID de destination permet de s'assurer que les utilisateurs et groupes de locataires peuvent accéder aux compartiments et objets correspondants dans les deux grilles.

Workflow de clonage de compte

Le schéma de workflow présente les étapes que les administrateurs du grid et les locataires autorisés doivent suivre pour configurer le clone de compte. Ces étapes sont effectuées après "la connexion de fédération de grille est configurée".



Workflow d'administration du grid

Les étapes que les administrateurs du grid effectuent dépendent du type d'authentification unique (SSO) ou de fédération des identités des systèmes StorageGRID"connexion de fédération de grille".

configurer SSO pour le clone 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 tenant 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 le même référentiel d'identité pour les deux grilles. Voir "Utiliser la fédération des identités".
2. Configurez le même fournisseur d'identité SSO pour les deux grilles. Voir "Configurer l'authentification unique".
3. "Créez le même groupe d'administration" sur les deux grilles en important le même groupe fédéré.

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

Si ce groupe d'administration n'existe pas sur les deux grilles avant la création du tenant, celui-ci n'est pas répliqué vers la destination.

configurer la fédération des identités au niveau de la grille pour le clone de compte (facultatif)

Si l'un ou l'autre des systèmes StorageGRID utilise la fédération des identités sans SSO, les deux grilles doivent utiliser la fédération des identités. Avant de créer les comptes de tenant 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 le même référentiel d'identité pour les deux grilles. Voir "Utiliser la fédération des identités".
2. Si un groupe fédéré dispose d'une autorisation d'accès racine initiale pour les comptes de tenant source et de destination, "créez le même groupe d'administration" 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 tenant 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 racine initiale pour les deux comptes, spécifiez un mot de passe pour l'utilisateur root local.

Créez un compte de locataire S3 autorisé

Après avoir configuré éventuellement une SSO ou une fédération d'identités, un administrateur du grid effectue ces étapes pour déterminer quels locataires peuvent répliquer des objets de compartiment vers d'autres systèmes StorageGRID.

Étapes

1. Déterminez la grille source du locataire pour les opérations de clonage de compte.

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

2. Dans cette grille, créez un compte de locataire S3 ou modifiez un compte existant.
3. Attribuez l'autorisation **utiliser la connexion de fédération de grille**.
4. Si le compte de tenant gère ses propres utilisateurs fédérés, attribuez l'autorisation **utiliser son propre référentiel d'identité**.

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

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

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

   - Les deux comptes de tenant possèdent les mêmes ID de compte, nom, quota de stockage et autorisations attribuées.

- Si vous avez sélectionné un groupe fédéré pour obtenir l'autorisation d'accès racine pour le tenant, ce groupe est cloné vers le tenant de destination.
- Si vous avez sélectionné un utilisateur local pour obtenir l'autorisation d'accès racine pour le locataire, cet utilisateur est cloné vers le locataire de destination. Toutefois, le mot de passe de cet utilisateur n'est pas cloné.

Pour plus de détails, voir "Gestion des locataires autorisés pour la fédération dans le grid".

Workflow de compte de locataire autorisé

Après la réplication d'un locataire doté de l'autorisation **utiliser la connexion de fédération GRID** dans la grille de destination, les comptes de locataires autorisés peuvent effectuer ces étapes pour cloner des groupes de locataires, des utilisateurs et des clés d'accès S3.

Étapes

1. Connectez-vous au compte du locataire sur la grille source du locataire.
2. Si vous êtes autorisé, configurez la fédération d'identification sur les comptes de locataire 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 dans le locataire de destination, mais aucun clonage n'a lieu de la destination vers la source.

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

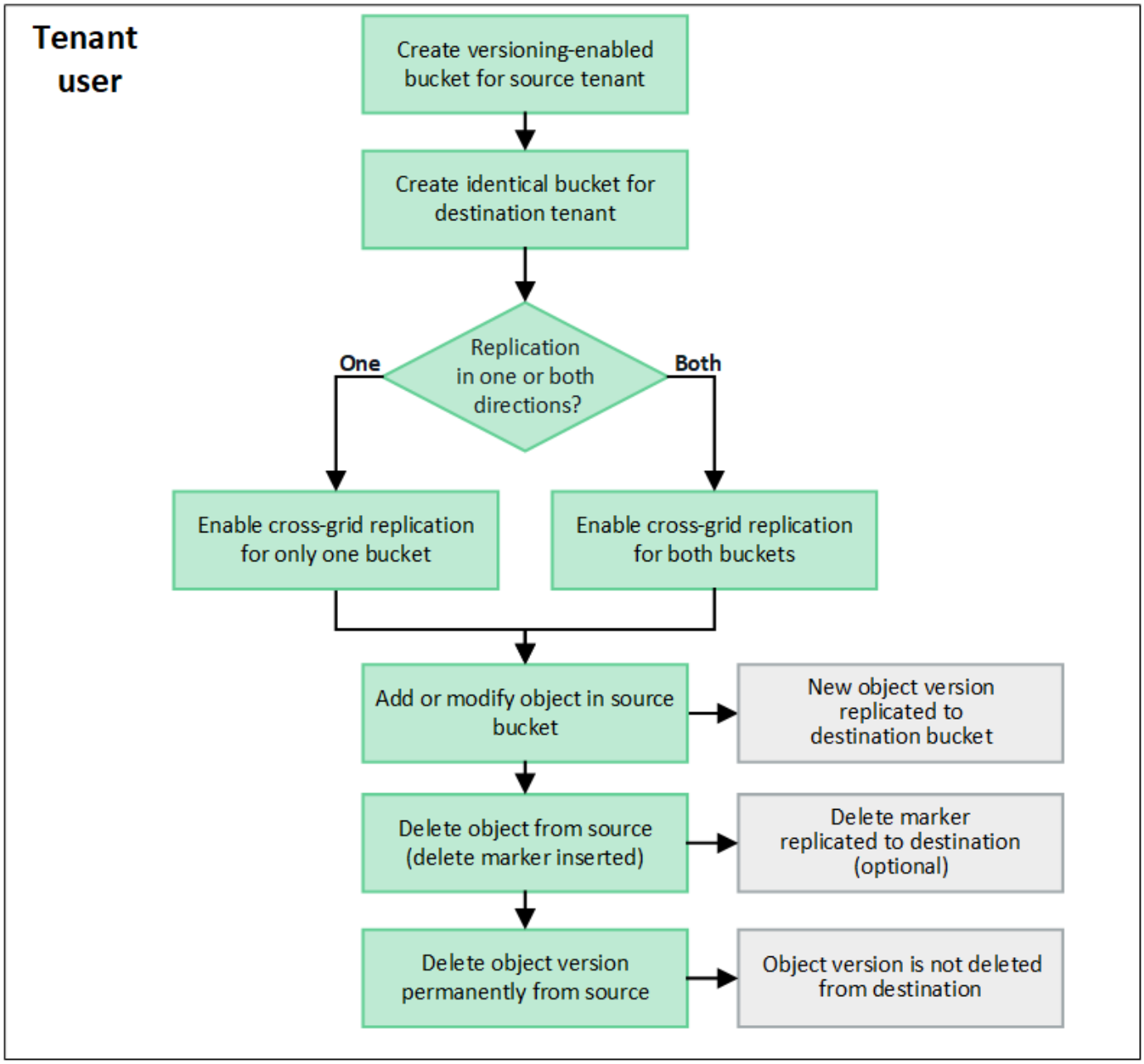
Pour en savoir plus sur le workflow des comptes de locataires autorisés et sur le clonage des groupes, des utilisateurs et des clés d'accès S3, reportez-vous aux sections "Cloner des groupes de locataires et des utilisateurs" et "Cloner les clés d'accès S3 à l'aide de l'API".

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

La réplication inter-grid est la réplication automatique des objets entre des compartiments S3 sélectionnés dans deux systèmes StorageGRID connectés dans un "connexion de fédération de grille". "Clone de compte" est nécessaire pour la réplication entre les grilles.

Flux de production pour la réplication entre les grilles

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



Conditions requises pour la réplication entre les grilles

Si un compte de locataire dispose de l'autorisation **utiliser la connexion de fédération de grille** pour utiliser un ou plusieurs "connexions de fédération de grille", un utilisateur de tenant avec l'autorisation d'accès racine peut créer des compartiments identiques dans les comptes de tenant correspondants sur chaque grille. Ces compartiments :

- Doit avoir le même nom mais peut avoir des régions différentes
- La gestion des versions doit être activée
- Le verrouillage d'objet S3 doit être désactivé
- Doit être vide

Une fois les deux compartiments créés, la réplication inter-grid peut être configurée pour l'un ou l'autre des compartiments, ou pour les deux.

En savoir plus >>

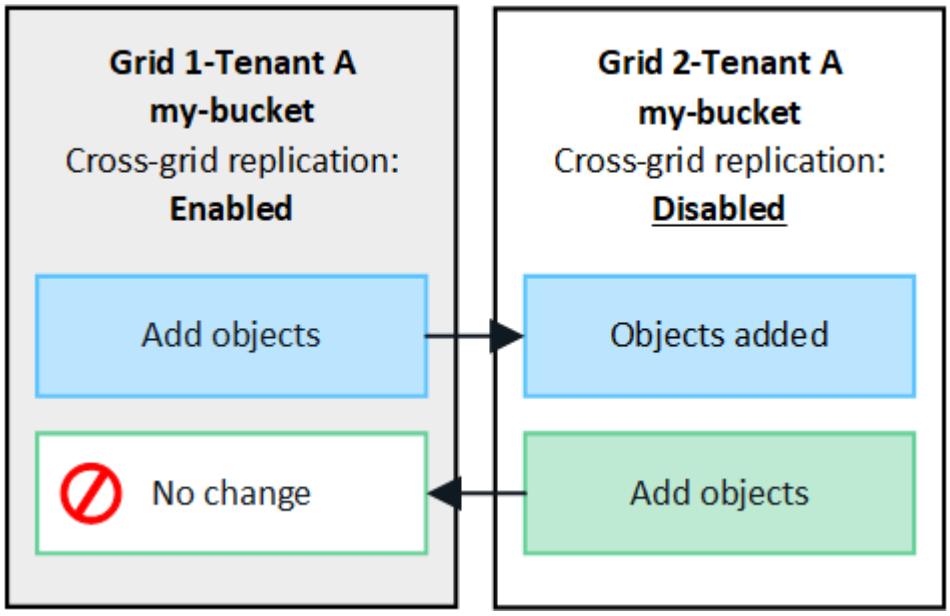
"Gérer la réplication entre les grilles"

Fonctionnement de la réplication entre les grilles

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

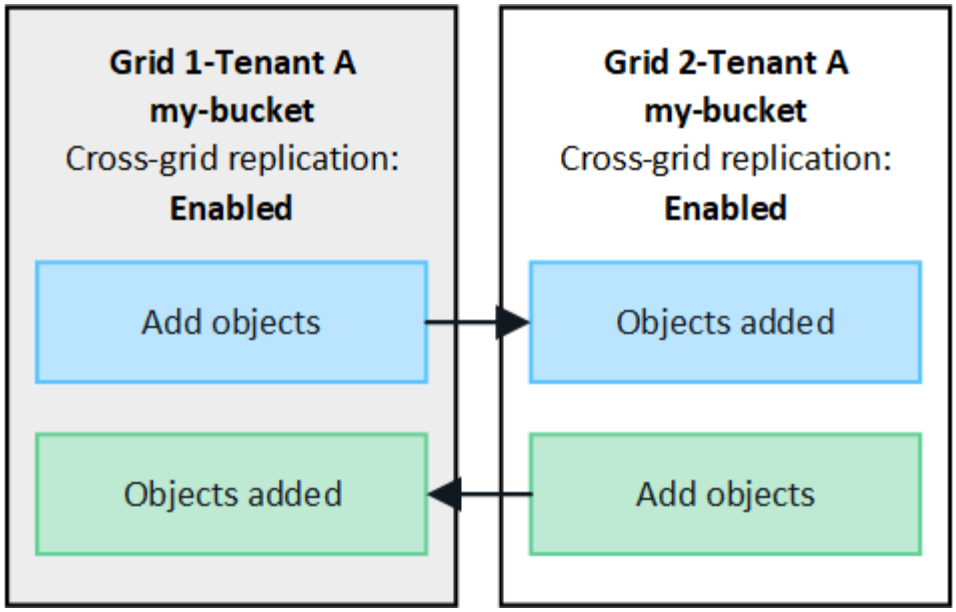
Réplication dans une direction

Si vous activez la réplication inter-grid pour un compartiment sur une seule grille, les objets ajoutés à ce compartiment (le compartiment source) sont répliqués dans le compartiment correspondant de l'autre grille (le compartiment de destination). Toutefois, les objets ajoutés au compartiment de destination ne sont pas répliqués à nouveau 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-grid pour le même compartiment sur les deux grilles, les objets ajoutés à l'un des compartiments 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 compartiment pour lequel la réplication inter-grid est activée, les événements suivants se produisent :

1. StorageGRID réplique automatiquement l'objet depuis le compartiment source vers le compartiment de destination. Le temps nécessaire pour effectuer cette opération de réplication en arrière-plan dépend de plusieurs facteurs, dont le 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 en-tête de réponse spécifique à StorageGRID `x-ntap-sg-cgr-replication-status`, 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 en-tête de réponse spécifique à StorageGRID `x-ntap-sg-cgr-replication-status`, qui aura l'une des valeurs suivantes :

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

   > StorageGRID ne prend pas en charge la `x-amz-replication-status` barre de coupe.

2. StorageGRID utilise les règles ILM actives de chaque grille pour gérer les objets, comme n'importe quel autre objet. Par exemple, l'objet A sur la grille 1 peut être stocké sous forme de deux copies répliquées et conservé indéfiniment, tandis que la copie de l'objet A répliqué sur la grille 2 peut être stockée avec un code 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 tenant Manager sélectionne l'"'Supprime les objets du compartiment"option de suppression de tous les objets d'un compartiment.
- Le compartiment dispose d'une configuration en 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 compartiment, d'expiration du cycle de vie du compartiment ou d'expiration du placement ILM, l'objet répliqué n'est jamais supprimé d'une autre grille d'une connexion de fédération de grid. Toutefois, les marqueurs de suppression ajoutés au compartiment source par les suppressions du client S3 peuvent éventuellement être répliqués dans le compartiment de destination.

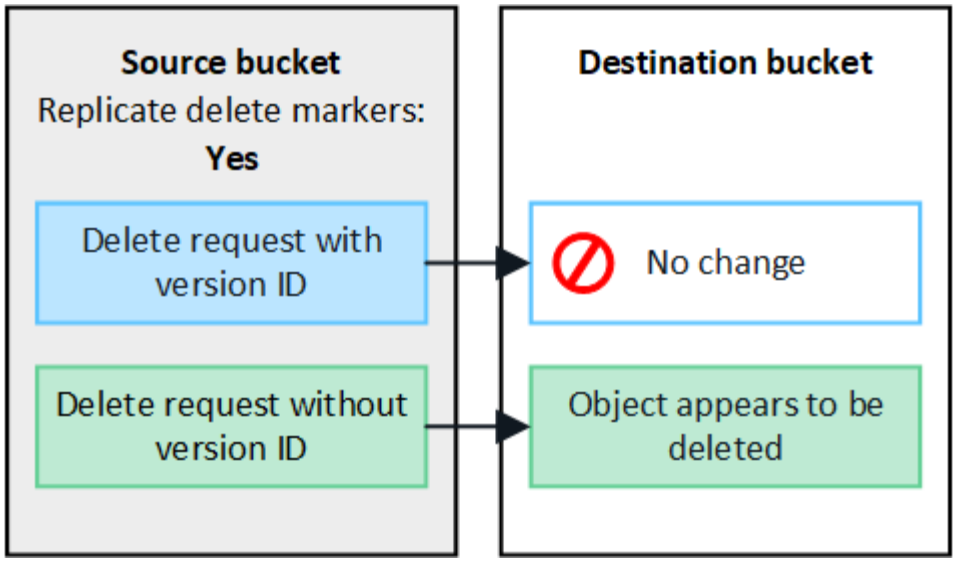
Pour comprendre ce qui se passe lorsqu'un client S3 supprime des objets d'un compartiment dans lequel la réplication inter-grid est activée, vérifiez comment les clients S3 suppriment des objets des compartiments pour lesquels la gestion de version est activée, comme suit :

- 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 godet.
- 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 godet. Avec le marqueur de suppression, StorageGRID agit comme si l'objet avait été supprimé :
  - Une demande GetObject sans ID de version échoue avec `404 No Object Found`
  - Une demande GetObject avec un ID de version valide réussit et renvoie la version d'objet demandée.

Lorsqu'un client S3 supprime un objet d'un compartiment pour lequel la réplication inter-grid 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-grid pour le compartiment :
  - Si vous choisissez de répliquer les marqueurs de suppression (par défaut), un marqueur de suppression est ajouté au compartiment source et répliqué vers le compartiment 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 compartiment source, mais il n'est pas répliqué vers le compartiment de destination. En effet, les objets supprimés de la grille source ne sont pas supprimés de la grille de destination.

Dans la figure, **replicate delete marqueurs** a été défini sur **Yes** lorsque "la réplication inter-grid a été activée". Les demandes de suppression du compartiment source qui incluent un ID de version ne supprimera pas les objets du compartiment de destination. Les demandes de suppression pour le compartiment source qui n'incluent pas d'ID de version apparaissent pour supprimer des objets dans le compartiment de destination.



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

Mode de réplication des objets chiffrés

Lorsque vous répliquez les objets entre les grilles à l'aide de la réplication multigrille, vous pouvez chiffrer des objets individuels, utiliser le chiffrement de compartiment par défaut ou configurer le chiffrement au niveau de la grille. Vous pouvez ajouter, modifier ou supprimer les paramètres de chiffrement de compartiment ou de grille par défaut avant ou après l'activation de la réplication entre plusieurs grilles pour un compartiment.

Pour chiffrer des objets individuels, vous pouvez utiliser SSE (chiffrement côté serveur avec des clés gérées par StorageGRID) lors de l'ajout des objets au compartiment source. Utilisez l' `x-amz-server-side-encryption`en-tête de la requête et spécifiez `AES256`. Voir "Utilisez 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'acquisition échoue.

Pour utiliser le cryptage par défaut pour un compartiment, utilisez une requête PutBucketEncryption et définissez le `SSEAlgorithm` paramètre sur `AES256`. Le chiffrement au niveau du compartiment s'applique à tous les objets ingérés sans l' `x-amz-server-side-encryption`en-tête de la demande. Voir "Opérations sur les compartiments".

Pour utiliser le cryptage au niveau de la grille, définissez l'option **Stored object Encryption** sur **AES-256**. Le chiffrement au niveau du grid s'applique aux objets qui ne sont pas chiffrés au niveau du compartiment ou qui sont ingérés sans l'en-tête de la `x-amz-server-side-encryption` demande. Voir "Configurez les options réseau et objet".

SSE ne prend pas en charge AES-128. Si l'option **Stored object Encryption** 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. À la place, l'objet répliqué utilisera le paramètre de chiffrement par défaut du compartiment ou de la grille de destination, le cas échéant.

Lors de la détermination du mode de chiffrement des objets source, StorageGRID applique les règles suivantes :

1. Utilisez l' `x-amz-server-side-encryption`en-tête d'ingestion, le cas échéant.
2. Si aucun en-tête d'ingestion n'est présent, utilisez le paramètre de chiffrement par défaut du compartiment, s'il est configuré.
3. Si aucun paramètre de compartiment n'est configuré, utilisez le paramètre de chiffrement au niveau de la grille, si celui-ci est configuré.
4. Si aucun paramètre de grille n'est présent, ne chiffrez pas l'objet source.

Pour déterminer comment chiffrer les objets répliqués, StorageGRID applique les règles suivantes dans l'ordre suivant :

1. Utilisez le même chiffrement que l'objet source, sauf si cet objet utilise le chiffrement AES-128.
2. Si l'objet source n'est pas chiffré ou utilise la norme AES-128, utilisez le paramètre de chiffrement par défaut du compartiment de destination, s'il est configuré.
3. Si le compartiment de destination ne possède pas de paramètre de chiffrement, utilisez le paramètre de chiffrement de la grille de destination, si celui-ci est configuré.
4. Si aucun paramètre de grille n'est présent, ne chiffrez 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 compartiments pour lesquels la réplication inter-grid est activée.

Si un client S3 émet une requête PutObjectTagging ou DeleteObjectTagging, `501 Not Implemented` est renvoyée. 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 dans une autre grille, le paramètre **taille de segment maximale** (**CONFIGURATION** > **système** > **Options de stockage**) de la grille source sera utilisé sur les deux grilles. Par exemple, supposons que la taille de segment maximale de la grille source soit de 1 Go, alors que la taille de segment maximale de la grille de destination est de 50 Mo. Si vous ingérer un objet de 2 Go sur la grille source, cet objet est enregistré en tant que 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 de segment de cette grille est de 50 Mo.

Comparez la réplication entre les grilles et la réplication CloudMirror

Lorsque vous commencez à utiliser la fédération de grille, examinez les similarités et les différences entre "réplication entre plusieurs grilles" et "Service de réplication StorageGRID CloudMirror".

	Réplication entre plusieurs grilles	Service de réplication CloudMirror
Quel est l'objectif principal ?	Un système StorageGRID agit comme un système de reprise après incident. Les objets d'un compartiment peuvent être répliqués entre les grilles dans une ou les deux directions.	Permet à un locataire de répliquer automatiquement les objets à partir d'un compartiment dans StorageGRID (source) vers un compartiment 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 elle est souvent traitée dans le cloud.
Comment est-il configuré ?	1. Configurer une connexion de fédération de grille entre deux grilles. 2. Ajoutez de nouveaux comptes de locataires, qui sont automatiquement clonés dans l'autre grid. 3. Ajoutez de nouveaux groupes de locataires et utilisateurs qui sont également clonés. 4. Créez les compartiments correspondants sur chaque grille et activez la réplication inter-grille dans une ou les deux directions.	1. Un utilisateur de locataire configure la réplication CloudMirror en définissant un terminal CloudMirror (adresse IP, identifiants, etc.) à l'aide du Gestionnaire des locataires ou de l'API S3. 2. Tout compartiment appartenant à ce compte de locataire peut être configuré de manière à pointer vers le terminal CloudMirror.
Qui est responsable de sa configuration ?	• Un administrateur du grid configure la connexion et les locataires. • Les utilisateurs locataires configurent les groupes, les utilisateurs, les clés et les compartiments.	Généralement, un utilisateur locataire.
Quelle est la destination ?	Un compartiment S3 correspondant et identique sur l'autre système StorageGRID dans la connexion de fédération du grid.	• Toute infrastructure S3 compatible (y compris Amazon S3) • Google Cloud Platform (GCP)
La gestion des versions d'objets est-elle requise ?	Oui, la gestion des versions d'objet doit être activée dans les compartiments source et de destination.	Non, la réplication CloudMirror prend en charge toute combinaison de compartiments sans version et avec version sur la source et la destination.

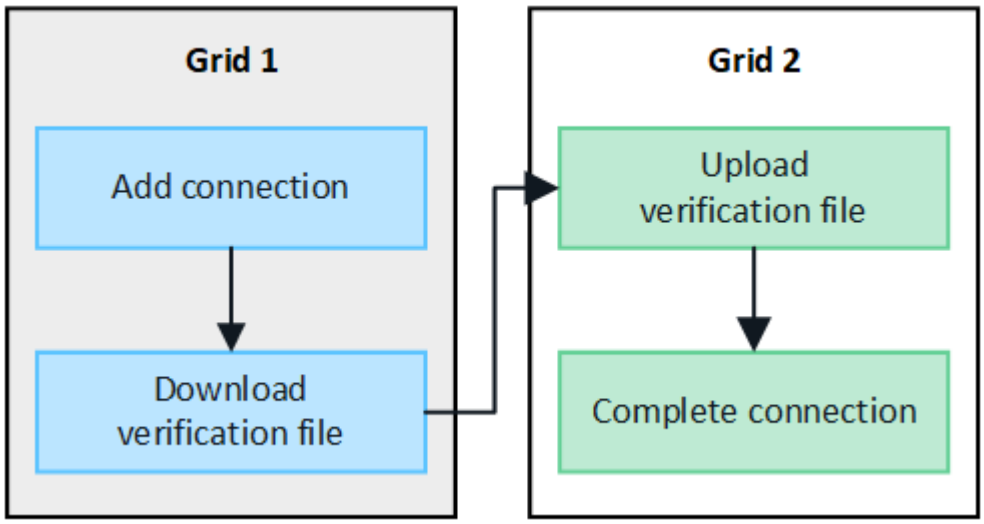
	Réplication entre plusieurs grilles	Service de réplication CloudMirror
Pourquoi déplacer des objets vers la destination ?	Les objets sont automatiquement répliqués lorsque ceux-ci sont ajoutés à un compartiment sur lequel la réplication inter-grid est activée.	Les objets sont automatiquement répliqués lorsqu'ils sont ajoutés à un compartiment qui a été configuré avec un terminal CloudMirror. Les objets qui existaient dans le compartiment source avant la configuration du compartiment avec le point de terminaison CloudMirror ne sont pas répliqués, sauf s'ils ont été modifiés.
Comment les objets sont-ils répliqués ?	La réplication inter-grid crée des objets versionnés et réplique l'ID de version du compartiment source vers le compartiment de destination. Cela permet de maintenir l'ordre des versions sur les deux grilles.	La réplication CloudMirror ne nécessite pas de compartiments prenant en charge la gestion des versions. CloudMirror peut donc uniquement gérer les commandes d'une clé au sein d'un site. Il n'y a aucune garantie que la commande sera maintenue pour les demandes à un objet sur un site différent.
Que se passe-t-il si un objet ne peut pas être répliqué ?	L'objet est placé dans la file d'attente de réplication, en fonction des limites de stockage des métadonnées.	L'objet est mis en file d'attente pour la réplication, sous réserve des limites des services de plate"Recommandations relatives à l'utilisation des services de plate-forme" -forme (voir).
Les métadonnées système de l'objet sont-elles répliquées ?	Oui, lorsqu'un objet est répliqué sur l'autre grille, les métadonnées de son système sont également répliquées. Les métadonnées seront identiques sur les deux grilles.	Non. Lorsqu'un objet est répliqué vers un compartiment externe, les métadonnées de son système sont mises à jour. Les métadonnées diffèrent d'un emplacement à l'autre, selon le moment de l'ingestion et le comportement de l'infrastructure S3 indépendante.
Comment les objets sont-ils récupérés ?	Les applications peuvent récupérer ou lire les objets en faisant une demande au compartiment sur les deux grilles.	Les applications peuvent récupérer ou lire les objets en faisant une requête vers StorageGRID ou vers la destination S3. Supposons, par exemple, que vous utilisiez la réplication CloudMirror pour mettre en miroir les objets dans une organisation partenaire. Le partenaire peut utiliser ses propres applications pour lire ou mettre à jour les objets directement à partir de la destination S3. Utiliser StorageGRID n'est pas nécessaire.

	Réplication entre plusieurs grilles	Service de réplication CloudMirror
Que se passe-t-il si un objet est supprimé ?	• Les demandes de suppression comprenant un ID de version ne sont jamais répliquées dans la grille de destination. • Les demandes de suppression qui n'incluent pas d'ID de version ajoutent un marqueur de suppression au compartiment source, qui peut éventuellement être répliqué vers la grille de destination. • Si la réplication inter-grid 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 gestion des versions des compartiments source et destination (qui ne doivent pas nécessairement être identiques) : • Si les deux compartiments sont versionnés, une demande de suppression ajoute un marqueur de suppression aux deux emplacements. • Si seul le compartiment source est versionné, une demande de suppression ajoute un marqueur de suppression à la source, mais pas à la destination. • Si aucun compartiment n'est versionné, une demande de suppression supprime l'objet de la source mais pas de la destination. De même, les objets du compartiment 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 d'objet.

Comme illustré dans la figure, la création d'une connexion de fédération de grille inclut des étapes sur les deux grilles. Vous ajoutez la connexion sur une grille et la remplissez sur l'autre grille. Vous pouvez commencer à partir de n'importe quelle 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 complets (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 contient les entrées appropriées.
- Vous utilisez un "navigateur web pris en charge".
- Vous disposez des droits d'accès racine et de la phrase de passe de provisionnement pour les deux grilles.

Ajouter une connexion

Effectuez ces étapes sur l'un des deux systèmes StorageGRID.

Étapes

1. Connectez-vous au Grid Manager à partir du nœud d'administration principal de l'une des grilles.
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'une des options suivantes : • Nom de domaine complet de la grille dans laquelle vous êtes actuellement connecté • Adresse VIP d'un groupe haute disponibilité sur cette grille • Adresse IP d'un nœud d'administration ou d'un nœud de passerelle sur cette grille. L'adresse IP peut se trouver sur n'importe quel réseau que la grille de destination peut atteindre.
Port	Le port que vous souhaitez utiliser pour cette connexion. Vous pouvez entrer n'importe quel numéro de port inutilisé compris entre 23000 et 23999. Les deux grilles de cette connexion utilisent le même port. Vous devez vous assurer qu'aucun nœud d'une grille n'utilise ce port pour d'autres connexions.
Jours de validité du certificat pour cette grille	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 730 jours (2 ans), mais vous pouvez entrer une valeur comprise entre 1 et 762 jours. StorageGRID génère automatiquement des certificats client et serveur pour chaque grille lorsque vous enregistrez la connexion.

Champ	Description
Phrase secrète de provisionnement pour cette grille	Phrase secrète de provisionnement de la grille à laquelle vous êtes connecté.
FQDN ou IP pour l'autre grille	L'une des options suivantes : • Nom de domaine complet de la grille à laquelle vous souhaitez vous connecter • Adresse VIP d'un groupe HA sur l'autre grid • Adresse IP d'un nœud d'administration ou d'un nœud de passerelle sur l'autre grille. L'adresse 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 terminée sur l'autre grille, vous ne pouvez plus télécharger le fichier de vérification depuis l'une ou l'autre grille.

7. Localisez le fichier téléchargé (*connection-name*`.grid-federation`) et enregistrez-le dans un emplacement sûr.

   Ce fichier contient des secrets (masqués en tant que *****) et d'autres détails sensibles et doit être stocké et transmis en toute sécurité.

8. Sélectionnez **Fermer** pour revenir à la page de fédération de grille.
9. Vérifiez que la nouvelle connexion est affichée et que son **état de connexion** est **en attente de connexion**.
10. Fournissez le *connection-name*`.grid-federation` fichier à l'administrateur de grille pour l'autre grille.

Connexion complète

Procédez comme suit sur le système StorageGRID auquel vous vous connectez (l'autre grille).

Étapes

1. Connectez-vous au Grid Manager 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 Télécharger.
4. Sélectionnez **Télécharger le fichier de vérification**. Ensuite, naviguez jusqu'au fichier téléchargé à partir de la première grille et sélectionnez(*connection-name*`.grid-federation`-le.

   Les détails de la connexion sont affichés.

5. Vous pouvez également saisir un nombre différent de jours valides pour les certificats de sécurité de cette grille. Par défaut, l'entrée **Certificate valid Days** correspond à la valeur que vous avez entrée sur 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 des extrémités de la connexion expirent, la connexion cesse de fonctionner et les réplications sont en attente jusqu'à ce que les certificats soient mis à jour.

6. Saisissez la phrase de passe 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 apparaît sur la page de fédération de grille. **État de la connexion** sera **connecté**.

   Si un message d'erreur s'affiche, résoudre les problèmes éventuels. Voir "Dépanner les erreurs de fédération de grille".

8. Accédez à la page grid federation sur la première grille et actualisez le navigateur. Vérifiez que l'état de la **connexion** est maintenant **connecté**.
9. Une fois la connexion établie, supprimez de manière sécurisée toutes les copies du fichier de vérification.

   Si vous modifiez cette connexion, un nouveau fichier de vérification sera créé. Le fichier d'origine ne peut pas être réutilisé.

Une fois que vous avez terminé

- Passez en revue les considérations relatives à "gestion des locataires autorisés".
- "Créez un ou plusieurs nouveaux comptes de locataire", Attribuez l'autorisation **utiliser la connexion de 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 de surveillance StorageGRID normales.
- "Dépanner la connexion", y compris la résolution des alertes et erreurs liées au clone de compte et à la réplication inter-grille.

Gérer les connexions de fédération de grille

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 de locataire et la suppression des connexions inutilisées.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille sur l'une des grilles à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine" pour la grille à laquelle vous êtes connecté.

modifiez une connexion de fédération de grille

Vous pouvez modifier une connexion de fédération de grille en vous connectant au nœud d'administration principal sur l'une des grilles de la connexion. Après avoir apporté des modifications à la première grille, vous devez télécharger un nouveau fichier de vérification et le télécharger sur l'autre grille.

Pendant la modification de la connexion, les demandes de réplication de clone de compte ou de grille croisée continueront à utiliser les paramètres de connexion existants. Toutes les modifications apportées à la première grille sont enregistrées localement, mais ne sont utilisées qu'après avoir été téléchargées sur la deuxième grille, enregistrées et testées.

Commencez à modifier la connexion

Étapes

1. Connectez-vous au Grid Manager à partir du nœud d'administration principal de l'une des grilles.
2. Sélectionnez **NODES** et confirmez que tous les autres noeuds Admin de votre système sont en ligne.

   Lorsque vous modifiez une connexion de fédération de grille, StorageGRID tente d'enregistrer un fichier de configuration de candidat 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 s'affiche 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** de la page de fédération de la grille ou de la page de détails d'une connexion spécifique. Reportez-vous à la section "Créer des connexions de fédération de grille" pour savoir ce que vous devez saisir.

   Menu actions

   a. Sélectionnez le bouton radio de 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 de passe 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, rendez-vous sur la page de détails de la connexion.

8. Localisez le fichier téléchargé (`connection-name.grid-federation`) et enregistrez-le dans un emplacement 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 fédération de grille.
10. Vérifiez que l'état de la **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 **modification en attente**.

11. Fournissez le *`connection-name`*`.grid-federation` fichier à l'administrateur de 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. Connectez-vous au Grid Manager 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 téléchargé à partir de la première grille.
5. Saisissez la phrase de passe 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 s'affiche. Passez en revue le message et répondez à tout problème.

7. Fermez l'assistant pour revenir à la page de fédération de grille.
8. Vérifiez que l'état de la **connexion** est **connecté**.
9. Accédez à la page grid federation sur la première grille et actualisez le navigateur. Vérifiez que l'état de la **connexion** est maintenant **connecté**.
10. Une fois la connexion établie, supprimez de manière sécurisée toutes les copies du fichier de vérification.

Tester une connexion de fédération de grille

Étapes

1. Connectez-vous au Grid Manager à partir du nœud d'administration principal.
2. Sélectionnez **CONFIGURATION** > **système** > **fédération de grille**.
3. Testez la connexion à l'aide du menu **actions** de la page de fédération de la grille ou de la page de détails d'une connexion spécifique.

Menu actions

a. Sélectionnez le bouton radio de 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 grilles sont connectées et communiquent normalement.
Erreur	La connexion est en état d'erreur. Par exemple, un certificat a expiré ou une valeur de configuration n'est plus valide.
Modification en attente	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 sur l'autre grille.
En attente de connexion	Vous avez configuré la connexion sur cette grille, mais la connexion n'a pas été effectuée sur l'autre grille. Téléchargez le fichier de vérification à partir 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 mise en réseau ou d'un nœud hors ligne.

5. Si l'état de la connexion est **Error**, résolvez les problèmes éventuels. Ensuite, sélectionnez de nouveau **Tester la connexion** pour confirmer que le problème a été résolu.

faire pivoter les certificats de connexion

Chaque connexion de fédération de grille utilise quatre certificats SSL générés automatiquement pour sécuriser la connexion. Lorsque les deux certificats de chaque grille sont proches de leur date d'expiration, l'alerte **expiration du certificat de fédération GRID** vous rappelle de faire pivoter les certificats.

> ⚠ Si les certificats à l'une des extrémités de la connexion expirent, la connexion cesse de fonctionner et les réplications sont en attente jusqu'à ce que les certificats soient mis à jour.

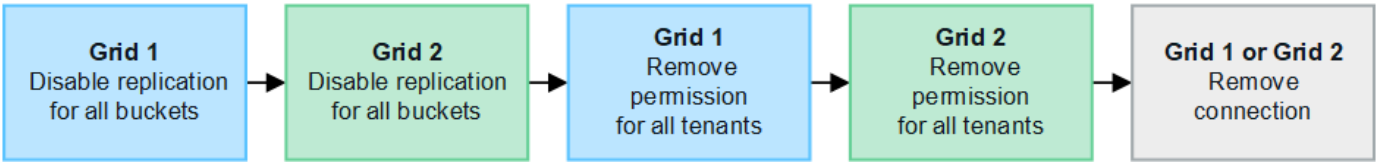
Étapes

1. Connectez-vous au Grid Manager à partir du nœud d'administration principal de l'une des grilles.
2. Sélectionnez **CONFIGURATION** > **système** > **fédération de grille**.
3. Dans l'un des onglets de la page fédération de grille, sélectionnez le nom de la connexion pour afficher ses détails.
4. Sélectionnez l'onglet **certificats**.
5. Sélectionnez **faire pivoter les certificats**.
6. Spécifiez le nombre de jours pendant lesquels les nouveaux certificats doivent être valides.
7. Saisissez la phrase de passe de provisionnement pour la grille à laquelle vous êtes connecté.
8. Sélectionnez **faire pivoter 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.

supprime une connexion de fédération de grille

Vous pouvez supprimer une connexion de fédération de grille de l'une 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 pas utilisée par un locataire sur l'une ou l'autre des grilles.



Avant de supprimer une connexion, notez les points suivants :

- La suppression d'une connexion ne supprime pas les éléments qui ont déjà été copiés entre les grilles. Par exemple, les utilisateurs de tenant, les groupes et les objets qui existent sur les deux grilles ne sont pas supprimés de l'une ou l'autre de ces grilles lorsque l'autorisation du tenant 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.

Désactivez la réplication pour tous les compartiments de locataires

Étapes

1. À partir de l'une 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 un locataire.
5. Si des locataires sont répertoriés, demandez à tous les locataires de "désactiver la réplication entre les grilles" pour tous leurs compartiments sur les deux grilles de la connexion.

> Vous ne pouvez pas supprimer l'autorisation **utiliser la connexion de fédération de grille** si une réplication de type cross-grid est activée dans des compartiments de tenant. Chaque compte de locataire doit désactiver la réplication inter-grid pour ses compartiments sur les deux grilles.

Supprimer l'autorisation pour chaque locataire

Une fois la réplication multigrille désactivée pour tous les compartiments de tenant, supprimez l'autorisation **utiliser la fédération de grid** 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 de fédération de grille** de chaque locataire. Voir "Gérer les locataires autorisés".
4. Répétez ces étapes pour les locataires autorisés sur l'autre grille.

Déposer la connexion

Étapes

1. Lorsqu'aucun locataire de l'une ou l'autre grille 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 de fédération de grille est maintenant supprimée des deux grilles.
   - Si la connexion ne peut pas être supprimée (par exemple, elle est toujours en cours d'utilisation ou si une erreur de connexion s'est produite), un message d'erreur s'affiche. Vous pouvez effectuer l'une des opérations suivantes :
     - Résolvez l'erreur (recommandé). Voir "Dépanner les erreurs de fédération de grille".
     - Déposer la connexion par la force. Voir la section suivante.

supprime une connexion de fédération de grille par force

Si nécessaire, vous pouvez forcer la suppression d'une connexion qui n'a pas l'état **Connected**.

La suppression forcée supprime uniquement la connexion de la grille locale. 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 s'affiche. Cette connexion de fédération de grille ne peut plus être utilisée. Cependant, la réplication entre les compartiments de locataires peut toujours être activée et certaines copies d'objet peuvent avoir déjà été répliquées entre les grilles dans 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 dans le grid

Vous pouvez autoriser les comptes de locataires S3 à utiliser une connexion de fédération de grid entre deux systèmes StorageGRID. Lorsque les locataires sont autorisés à utiliser une connexion, des étapes spéciales sont requises 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 des grilles à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine" pour la grille à laquelle vous êtes connecté.
- Vous avez "créé une connexion de fédération de grille" entre deux grilles.

- Vous avez examiné les flux de travail pour "clone de compte" et "réplication entre plusieurs grilles".
- 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 clone de compte".

Créez un locataire autorisé

Si vous souhaitez autoriser un compte de locataire nouveau ou existant à utiliser une connexion de fédération de grille pour le clone de compte et la réplication inter-grille, suivez les instructions générales à "Créer un locataire S3" ou "modifier un compte de locataire" et notez les points suivants :

- Vous pouvez créer le locataire à partir de l'une ou l'autre grille dans la connexion. La grille dans laquelle un locataire est créé est la *grille source du locataire*.
- L'état de la connexion doit être **connecté**.
- Lorsque le locataire est créé ou modifié pour activer l'autorisation **utiliser la connexion de fédération de grille**, puis enregistré sur la première grille, un locataire identique est automatiquement répliqué sur l'autre grille. La grille dans laquelle le locataire est répliqué est la grille de destination du locataire_.
- Les locataires des deux grilles auront les mêmes ID de compte, nom, description, quota et autorisations à 20 chiffres. 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 s'affiche également pour le locataire répliqué dans 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.

> Pour qu'un utilisateur root local puisse se connecter au tenant répliqué sur la grille de destination, un administrateur de grille pour cette grille doit "modifiez le mot de passe de l'utilisateur root local".

- Une fois que le nouveau locataire ou le locataire modifié est disponible sur les deux grilles, les utilisateurs du tenant peuvent effectuer les opérations suivantes :
  - Dans la grille source du locataire, créez des groupes et des utilisateurs locaux qui sont automatiquement clonés dans la grille de destination du locataire. Voir "Cloner des groupes de locataires et des utilisateurs".
  - Créez de nouvelles clés d'accès S3, qui peuvent être clonées sur la grille de destination du locataire. Voir "Cloner les clés d'accès S3 à l'aide de l'API".
  - Créez des compartiments identiques sur les deux grilles dans la connexion et activez la réplication de type grille dans une direction ou dans les deux directions. Voir "Gérer la réplication entre les grilles".

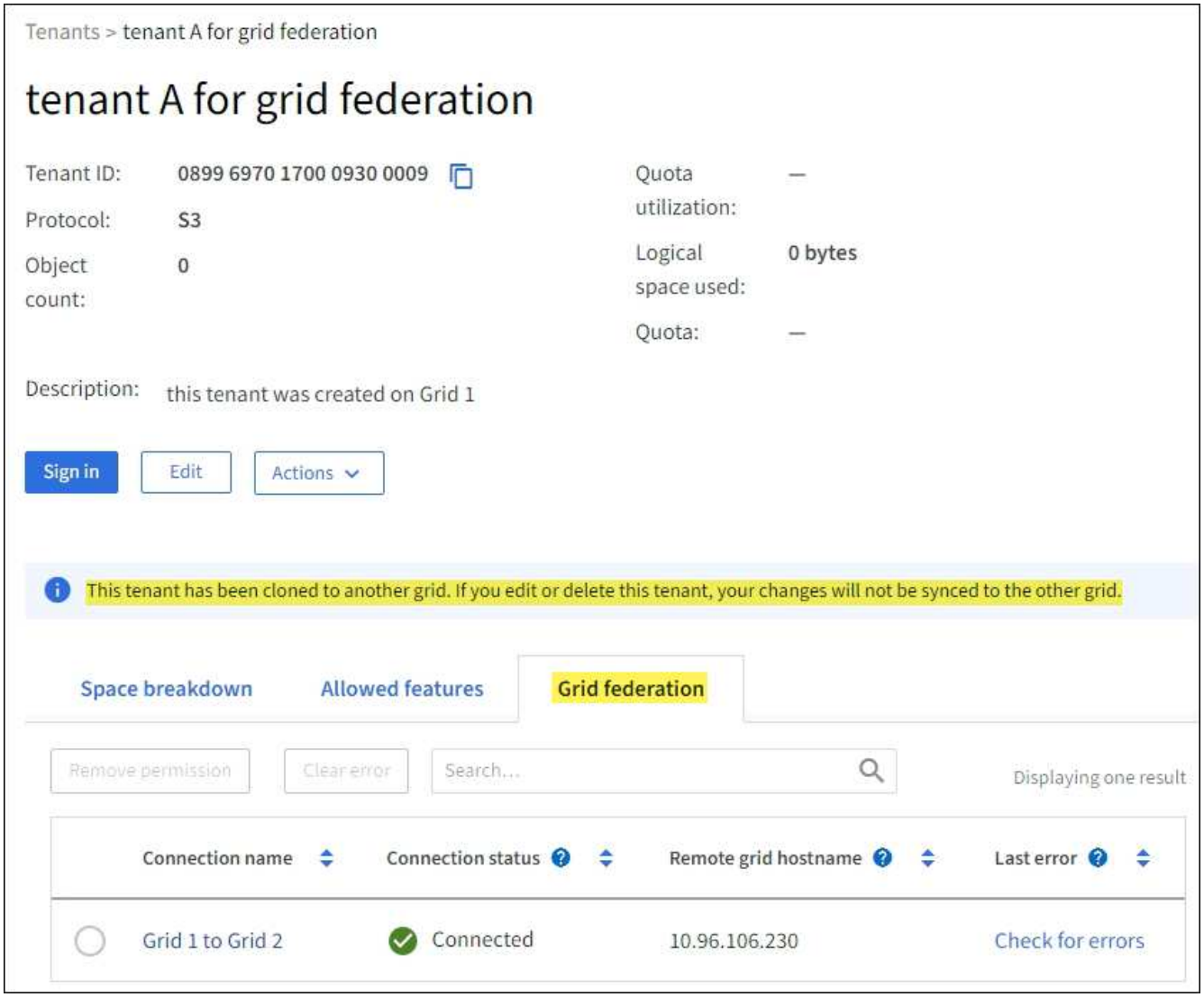
Afficher un locataire autorisé

Vous pouvez afficher les détails d'un locataire autorisé à utiliser une connexion de fédération de grille.

Étapes

1. Sélectionnez **LOCATAIRES**.
2. Sur la page tenants, 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 dans 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 **Grid federation** à "surveillez la connexion de fédération de grille".

Modifier un locataire autorisé

Si vous devez modifier un locataire doté de l'autorisation **utiliser la connexion de fédération de grille**, suivez les instructions générales pour "modification d'un compte de locataire" et notez ce qui suit :

- Si un locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, vous pouvez modifier les détails du locataire à partir de l'une des grilles de la connexion. Toutefois, les modifications que vous apportez ne seront pas copiées dans l'autre grille. Si vous souhaitez que les détails du locataire restent synchronisés entre les grilles, vous devez effectuer les mêmes modifications sur les deux grilles.
- Vous ne pouvez pas effacer l'autorisation **utiliser la connexion de fédération de grille** lorsque vous modifiez un locataire.
- Vous ne pouvez pas sélectionner une autre connexion de fédération de grille lorsque vous modifiez un locataire.

Supprimer un locataire autorisé

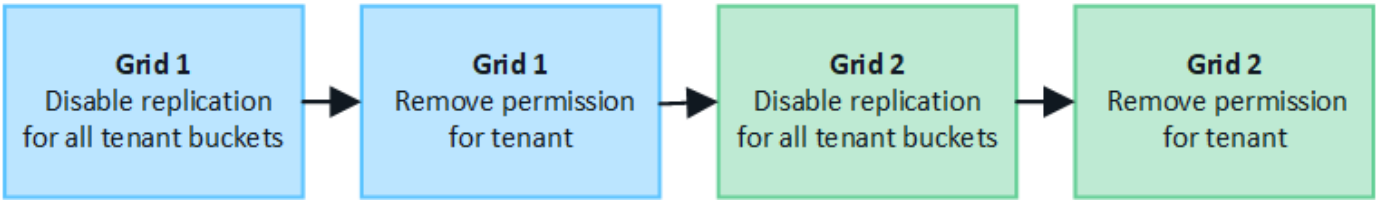
Si vous devez supprimer un locataire doté de l'autorisation **utiliser la connexion de fédération de grille**, suivez les instructions générales pour "suppression d'un compte de locataire" et notez ce qui suit :

- Avant de pouvoir supprimer le locataire d'origine sur la grille source, vous devez supprimer toutes les rubriques du compte sur la grille source.
- Avant de supprimer le locataire cloné sur la grille de destination, vous devez supprimer tous les compartiments du compte de la grille de destination.
- Si vous supprimez le locataire d'origine ou cloné, le compte ne peut plus être utilisé pour la réplication entre les grilles.
- Si vous supprimez le locataire d'origine sur la grille source, tous les groupes de locataires, utilisateurs ou clés clonés dans 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 compartiments.
- Si vous supprimez le locataire cloné sur la grille de destination, des erreurs de clonage se produisent 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 de fédération de grille avant de supprimer le locataire de cette grille.

Supprimer l'autorisation de connexion utiliser 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 de fédération de grille, notez ce qui suit :

- Vous ne pouvez pas supprimer l'autorisation **utiliser la connexion de fédération de grille** si la réplication inter-grille est activée pour l'un des compartiments du locataire. Le compte de locataire doit d'abord désactiver la réplication inter-grid pour tous ses compartiments.
- La suppression de l'autorisation **utiliser la connexion de fédération de grille** ne supprime pas les éléments qui ont déjà été répliqués entre les grilles. Par exemple, les utilisateurs, groupes et objets de tenant qui existent sur les deux grilles ne sont pas supprimés de l'une ou l'autre des grilles lorsque l'autorisation du tenant 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 de fédération de grille** fait de la grille locale la grille source et déclenche le clonage vers la grille distante spécifiée par la connexion de fédération de grille sélectionnée. Si le compte de tenant existe déjà sur la grille distante, le clonage entraîne une erreur de conflit.

Avant de commencer

- Vous utilisez un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine" pour les deux grilles.

Désactivez la réplication pour les compartiments de locataires

Dans un premier temps, désactivez la réplication inter-grid pour tous les compartiments de locataires.

Étapes

1. À partir de l'une 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 vous indiquer "désactiver la réplication entre les grilles"tous ses compartiments sur les deux grilles de la connexion.

> Vous ne pouvez pas supprimer l'autorisation **utiliser la connexion de fédération de grille** si une réplication de type cross-grid est activée dans des compartiments de tenant. Le locataire doit désactiver la réplication inter-grid pour ses compartiments sur les deux grilles.

Supprimer l'autorisation pour le locataire

Une fois la réplication multigrille désactivée pour les compartiments de tenant, vous pouvez supprimer l'autorisation du locataire d'utiliser la connexion de fédération GRID.

Étapes

1. Connectez-vous au Grid Manager à partir du nœud d'administration principal.
2. Supprimez l'autorisation de la page grid federation ou de la page tenants.

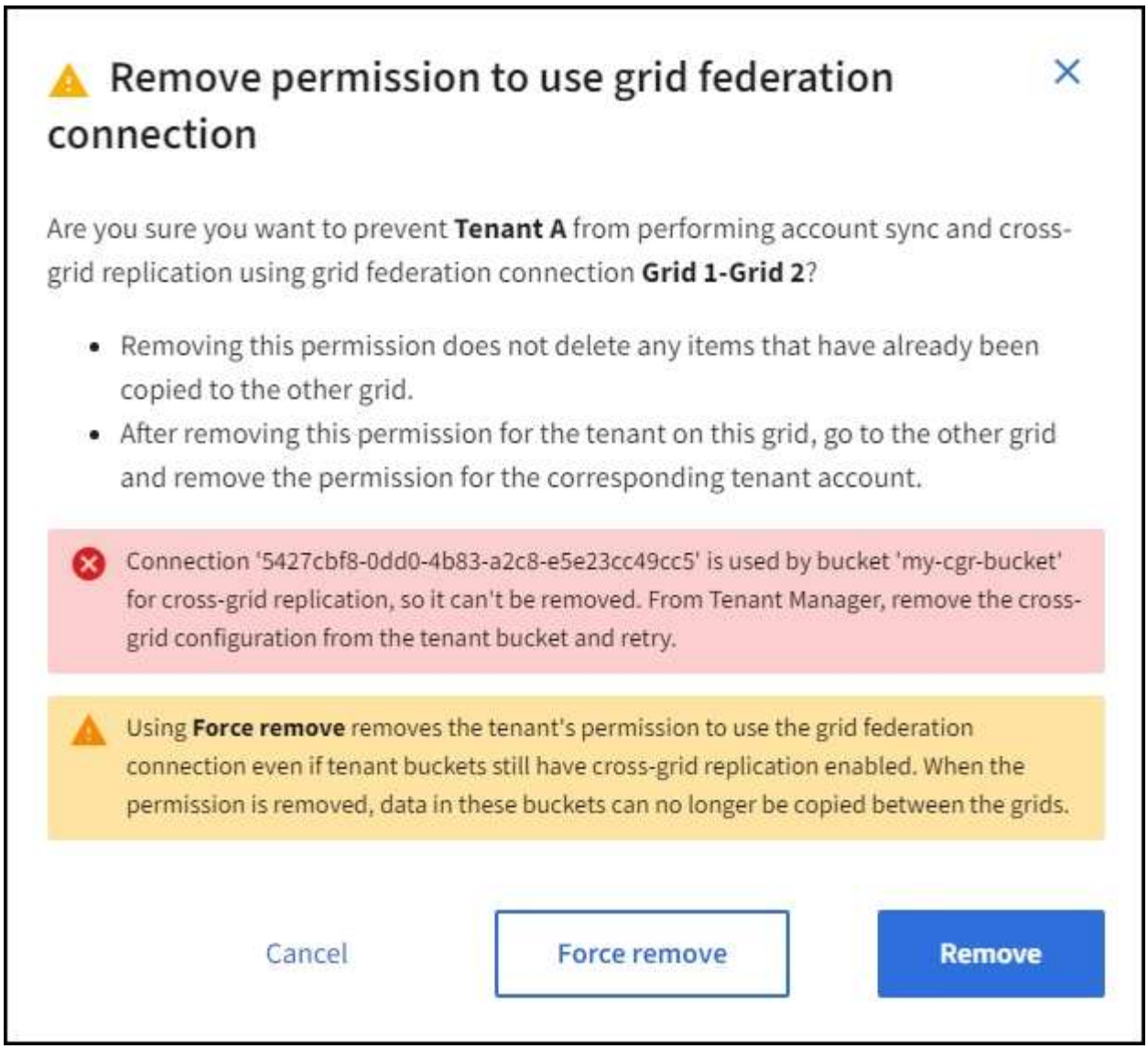
Page de fédération de grille

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 du locataire.
d. Sélectionnez **Supprimer l'autorisation**.

Page locataires

a. Sélectionnez **LOCATAIRES**.
b. Sélectionnez le nom du locataire pour afficher la page de détails.
c. Dans l'onglet **grid federation**, sélectionnez le bouton radio de la connexion.
d. Sélectionnez **Supprimer l'autorisation**.

3. Passez en revue les avertissements dans la boîte de dialogue de confirmation et sélectionnez **Supprimer**.
   - Si l'autorisation peut être supprimée, vous êtes renvoyé à la page des détails et un message de réussite s'affiche. Ce locataire ne peut plus utiliser la connexion de fédération de grille.
   - Si la réplication entre plusieurs compartiments de tenant est toujours activée, une erreur s'affiche.



Vous pouvez effectuer l'une des opérations suivantes :

- (Recommandé.) Connectez-vous au gestionnaire de locataires et désactivez la réplication pour chaque compartiments du locataire. Voir "Gérer la réplication entre les grilles". Répétez ensuite les étapes pour supprimer l'autorisation **utiliser la connexion grille**.
- Supprimez l'autorisation par force. Voir la section suivante.

4. Accédez à l'autre grille et répétez ces étapes pour supprimer l'autorisation pour le même locataire sur l'autre grille.

supprimez l'autorisation par la 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-grid est activée dans les compartiments de locataires.

Avant de supprimer l'autorisation d'un locataire par la force, notez les considérations générales suppression de l'autorisationet les considérations supplémentaires suivantes :

- Si vous supprimez l'autorisation **utiliser la connexion de fédération de grille** par force, 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 compartiment de destination, vous devez

également supprimer l'autorisation du locataire sur l'autre grille.

- Tous les objets ingérés dans le compartiment source après la suppression de l'autorisation **utiliser la connexion de fédération de grille** ne seront jamais répliqués dans le compartiment de destination.

Étapes

1. Connectez-vous au Grid Manager 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 du locataire.
5. Sélectionnez **Supprimer l'autorisation**.
6. Passez en revue les avertissements dans la boîte de dialogue de confirmation et sélectionnez **forcer la suppression**.

   Un message de réussite s'affiche. Ce locataire ne peut plus utiliser la connexion de 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 de tenant sur l'autre grille. Par exemple, vous devez répéter ces étapes sur l'autre grille pour empêcher les objets en cours d'atteindre le compartiment de destination.

Dépanner les erreurs de fédération de grille

Vous devrez peut-être résoudre les problèmes liés aux alertes et aux erreurs liées aux connexions de fédération du grid, au clone de compte et à la réplication intergrille.

alertes et erreurs de connexion de fédération de grille

Vous pouvez recevoir des alertes ou rencontrer des erreurs avec vos connexions de fédération de grille.

Après avoir effectué des modifications pour résoudre un problème de connexion, testez la connexion pour vous assurer que l'état de la connexion revient à **connecté**. Pour obtenir des instructions, reportez-vous à la section "Gérer les connexions de fédération de grille".

Alerte d'échec de la connexion de fédération de grille

Problème

L'alerte **échec de la connexion de 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 de la page de fédération de grille pour les deux grilles. Vérifier que toutes les valeurs sont correctes. Voir "Gérer les connexions de fédération de grille".
2. Vérifiez les certificats utilisés pour la connexion. Assurez-vous qu'il n'y a pas d'alertes pour les certificats de fédération de grille expirés et que les détails de chaque certificat sont valides. Reportez-vous aux instructions relatives à la rotation "Gérer les connexions de fédération de grille"des certificats de connexion dans .
3. Vérifiez que tous les nœuds d'administration et de passerelle des deux grilles sont en ligne et disponibles. Résolvez 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, vérifiez que le serveur DNS est en ligne et disponible. Reportez-vous à la section "Qu'est-ce que la fédération de grille ?" pour connaître la configuration réseau, l'adresse IP et DNS requise.

Expiration de l'alerte de certificat de fédération de grille

Problème

L'alerte **expiration du certificat de 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

Reportez-vous aux instructions relatives à la rotation "Gérer les connexions de fédération de grille"des certificats de connexion dans .

Erreur lors de la modification d'une connexion de fédération de grille

Problème

Lors de la modification d'une connexion de fédération de grille, le message d'avertissement suivant s'affiche lorsque vous sélectionnez **Enregistrer et tester** : "Echec de la création d'un fichier de configuration de candidat sur un ou plusieurs nœuds."

Détails

Lorsque vous modifiez une connexion de fédération de grille, StorageGRID tente d'enregistrer un fichier de configuration de candidat 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. Vérifiez que tous les nœuds d'administration de ce grid sont en ligne.
3. Si des nœuds sont hors ligne, remettez-les en ligne et réessayez de modifier la connexion.

Erreurs de clonage de compte

Impossible de se connecter à un compte de locataire cloné

Problème

Vous ne pouvez pas vous connecter à un compte de 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 depuis la grille source du locataire vers la grille de destination du locataire, le mot de passe que vous définissez pour l'utilisateur root local du locataire n'est pas cloné. De même, lorsqu'un locataire crée des utilisateurs locaux dans sa grille source, les mots de passe des utilisateurs locaux ne sont pas clonés dans la grille de destination.

Actions recommandées

Pour que l'utilisateur root puisse se connecter à la grille de destination du locataire, l'administrateur de la grille doit d'abord se connecter "modifiez le mot de passe de l'utilisateur root local"à la grille de destination.

Pour 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 obtenir des instructions, reportez-vous à la section "Gérez les utilisateurs locaux" dans les instructions d'utilisation du Gestionnaire de locataires.

Locataire créé sans clone

Problème

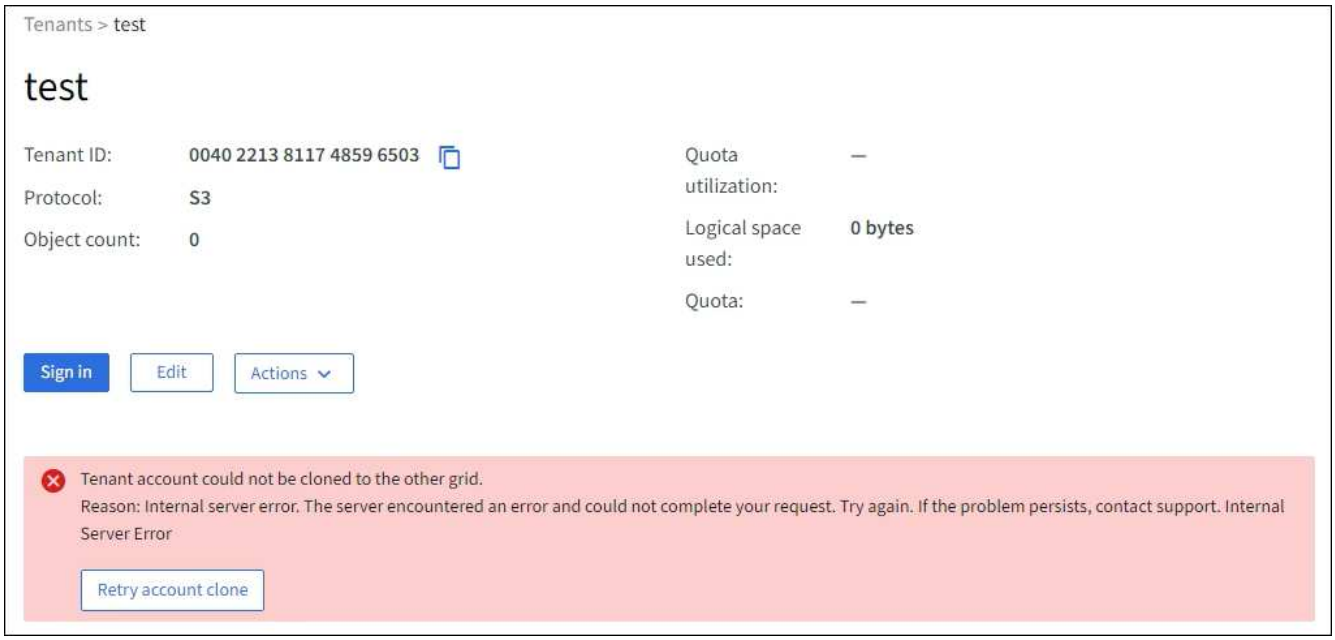
Le message "tenant créé sans clone" s'affiche après la création d'un nouveau tenant avec l'autorisation **utiliser la connexion de fédération de grille**.

Détails

Ce problème peut se produire si les mises à jour de l'état de la connexion sont retardées, ce qui peut entraîner la liste d'une connexion défectueuse sous le nom **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 de fédération de grille.
2. Suivez les instructions pour tester une connexion de fédération de grille dans "Gérer les connexions de fédération de grille" pour vérifier que le problème a été résolu.
3. Dans la grille source du locataire, sélectionnez **TENANTS**.
4. Recherchez le compte de locataire qui n'a pas pu être cloné.
5. Sélectionnez le nom du locataire pour afficher la page de détails.
6. Sélectionnez **Réessayer le clone de compte**.



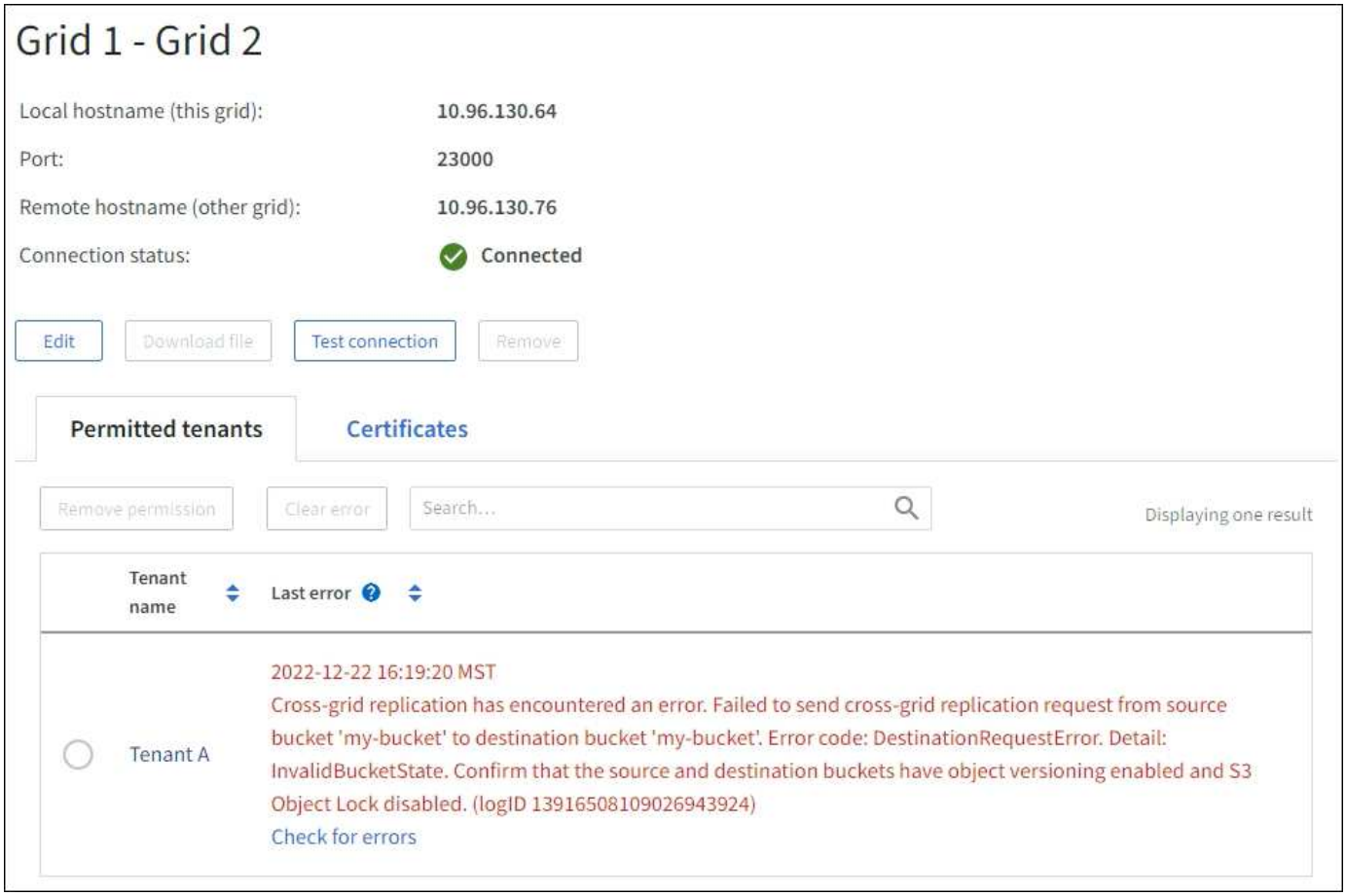
Si l'erreur a été résolue, le compte locataire sera cloné dans l'autre grille.

Alertes et erreurs de réplication intergrid

Dernière erreur affichée pour la connexion ou le locataire

Problème

Quand "affichage d'une connexion de fédération de grille" (ou quand "gestion des locataires autorisés" pour une connexion), vous remarquez une erreur dans la colonne **dernière erreur** de la page des détails de la connexion. Par exemple :



Détails

Pour chaque connexion de fédération de grille, la colonne **dernière erreur** indique l'erreur la plus récente à se produire, le cas échéant, lors de la réplication des données d'un locataire vers l'autre grille. Cette colonne affiche uniquement la dernière erreur de réplication inter-grille à se produire ; les erreurs précédentes qui se sont peut-être produites ne seront pas affichées. Une erreur dans cette colonne peut se produire pour l'une des raisons suivantes :

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

Actions recommandées

Si un message d'erreur apparaît dans la colonne **dernière erreur**, procédez comme suit :

1. Vérifiez le texte du message.
2. Effectuez toutes les actions recommandées. Par exemple, si la gestion des versions a été suspendue dans le compartiment de destination pour la réplication inter-grid, réactivez la gestion des versions pour ce compartiment.
3. Sélectionnez le compte de connexion ou de locataire dans le tableau.
4. Sélectionnez **Effacer erreur**.
5. Sélectionnez **Oui** pour effacer le message et mettre à jour l'état du système.
6. Patientez 5-6 minutes, puis ingérer un nouvel objet dans le compartiment. Vérifiez que le message d'erreur ne réapparaît pas.

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

   Après avoir dégagé l'erreur, une nouvelle **dernière erreur** peut apparaître si des objets sont ingérés dans un autre compartiment qui présente également une erreur.

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

Alerte de défaillance permanente de la réplication multi-grid

Problème

L'alerte **échec permanent de la réplication Cross-grid** a été déclenchée.

Détails

Cette alerte indique que les objets tenant ne peuvent pas être répliqués entre les compartiments de deux grilles pour une raison qui nécessite une intervention de l'utilisateur. Cette alerte est généralement causée par une modification du compartiment source ou de destination.

Actions recommandées

1. Connectez-vous à la grille dans laquelle l'alerte a été déclenchée.
2. Accédez à **CONFIGURATION** > **système** > **fédération de grille** et localisez le nom de connexion indiqué dans l'alerte.
3. Dans l'onglet locataires autorisés, consultez la colonne **dernière erreur** pour déterminer quels comptes de locataires ont des erreurs.
4. Pour en savoir plus sur l'échec, reportez-vous aux instructions de la section "Surveiller les connexions de fédération de grille" pour consulter les mesures de réplication entre les grilles.
5. Pour chaque compte de locataire concerné :
   a. Reportez-vous aux instructions de la "Surveillez l'activité des locataires" pour vérifier que le locataire n'a pas dépassé son quota sur la grille de destination pour la réplication inter-grid.
   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 au Gestionnaire de locataires sur les deux grilles afin de comparer la liste des compartiments.
7. Pour chaque compartiment pour lequel la réplication inter-grid est activée, vérifiez les points suivants :
   - Il existe un compartiment correspondant pour le même locataire sur l'autre grille (doit utiliser le nom

exact).

- La gestion des versions des objets est activée dans les deux compartiments (la gestion des versions ne peut pas être suspendue sur les deux grilles).
- Le verrouillage d'objet S3 est désactivé dans les deux compartiments.
- Aucun compartiment n'est à l'état **Suppression d'objets : lecture seule**.

8. Pour vérifier que le problème a été résolu, reportez-vous aux instructions de la section "Surveiller les connexions de fédération de grille" pour vérifier les mesures de réplication inter-grille ou effectuez les opérations suivantes :

   a. Retournez à la page Grid federation.
   b. Sélectionnez le locataire affecté et sélectionnez **Effacer erreur** dans la colonne **dernière erreur**.
   c. Sélectionnez **Oui** pour effacer le message et mettre à jour l'état du système.
   d. Patientez 5-6 minutes, puis ingérer un nouvel objet dans le compartiment. Vérifiez que le message d'erreur ne réapparaît pas.

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

   > Une fois l'alerte résolue, il peut s'écouler jusqu'à un jour avant que l'alerte ne s'efface.

   a. Accédez 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 de ressource de réplication inter-grid indisponible

Problème

L'alerte **ressource de réplication multigrille indisponible** a été déclenchée.

Détails

Cette alerte indique que les demandes de réplication inter-grid sont en attente car une ressource n'est pas disponible. Par exemple, une erreur réseau peut se produire.

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 a une alerte **échec de la connexion de fédération de grille** pour la même connexion ou une alerte **Impossible de communiquer avec le nœud** pour un nœud. Cette alerte peut être résolue lorsque vous résolvez ces alertes.
3. Pour en savoir plus sur l'échec, reportez-vous aux instructions de la section "Surveiller les connexions de fédération de grille" pour consulter les mesures de réplication entre les grilles.
4. Si vous ne parvenez pas à résoudre l'alerte, contactez le support technique.

La réplication inter-grid 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 Cross-grid**, 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 multigrille** indique que les objets tenant ne peuvent pas être répliqués entre les compartiments de deux grilles pour une raison qui nécessite une intervention de l'utilisateur pour la résoudre. Cette alerte est généralement causée par une modification du compartiment source ou de destination. Pour plus de détails, voir "Dépanner les erreurs de fédération de grille".

Déterminez 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 des messages dans le journal d'audit"CGRR (demande de réplication multigrille)". Ce message est ajouté au journal lorsque StorageGRID ne parvient pas à répliquer un objet, un objet en plusieurs parties ou un marqueur de suppression vers le compartiment de destination.

Vous pouvez utiliser pour traduire les "outil d'audit-explication"résultats dans un format plus facile à lire.

Avant de commencer

- Vous disposez de l'autorisation d'accès racine.
- Vous avez le `Passwords.txt` fichier.
- 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. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour basculer en root : `su -`
   d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

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

2. Recherchez les messages du CRGR sur le site audit.log et utilisez l'outil audit-explication pour formater les résultats.

   Par exemple, cette commande gronde 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 ressemblent à cet exemple, qui contient des entrées pour six messages CGRR. Dans l'exemple, toutes les demandes de réplication inter-grid ont renvoyé une erreur générale car l'objet n'a pas pu être répliqué. Les trois premières erreurs concernent les opérations « Replicate object » et les trois dernières sont pour les opérations « Replicate delete marker ».

```
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 croisée CGRR	Nom de la demande
locataire	ID de compte du locataire
connexion	ID de la connexion de fédération de grille
fonctionnement	Type d'opération de réplication en cours de tentative : • répliquer l'objet • répliquer le marqueur de suppression • répliquer un objet multipièce
godet	Nom du compartiment
objet	Nom de l'objet
version	ID de version de l'objet

Champ	Description
erreur	Type d'erreur. Si la réplication de la grille croisée a échoué, l'erreur est « erreur générale ».

Réessayer les réplications ayant échoué

Après avoir généré une liste d'objets et supprimé des marqueurs qui n'ont pas été répliqués dans le compartiment de destination et résolu les problèmes sous-jacents, vous pouvez réessayer la réplication de l'une des deux manières suivantes :

- Réintégrez chaque objet dans le compartiment 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 **aller à la documentation privée de l'API**.

> Les terminaux de l'API StorageGRID marqués « privé » sont susceptibles d'être modifiés sans préavis. Les terminaux privés StorageGRID ignorent également la version API de la demande.

3. Dans la section **cross-grid-Replication-Advanced**, sélectionnez le noeud final suivant :

   ```
   POST /private/cross-grid-replication-retry-failed
   ```

4. Sélectionnez **essayez-le**.
5. Dans la zone de texte **body**, remplacez l'exemple de **versionID** par un ID de version du fichier audit.log correspondant à une demande de réplication croisée ayant échoué.

   Veillez à conserver les guillemets doubles autour de la chaîne.

6. Sélectionnez **Exécuter**.
7. Vérifiez que le code de réponse du serveur est **204**, indiquant que l'objet ou le marqueur de suppression a été marqué comme en attente pour la réplication de la grille transversale 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 nouvelles tentatives de réplication

Vous devez surveiller les opérations de nouvelle tentative de réplication pour vous assurer qu'elles sont terminées.

> La réplication d'un objet ou d'un marqueur de suppression vers une autre grille peut prendre plusieurs heures, voire plus.

Vous pouvez surveiller les nouvelles tentatives de deux manières :

- Utilisation d'un S3 ou d'"GetObject"une "Objet principal"demande. La réponse inclut l'en-tête de réponse spécifique à StorageGRID `x-ntap-sg-cgr-replication-status`, qui aura l'une des valeurs suivantes :

Grille	État de la réplication
Source	• **TERMINÉ** : la réplication a réussi. • **EN ATTENTE** : l'objet n'a pas encore été répliqué. • **ÉCHEC** : la réplication a échoué avec une défaillance permanente. L'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 noeud final suivant :

   ```
   GET /private/cross-grid-replication-object-status/{id}
   ```

2. Sélectionnez **essayez-le**.
3. Dans la section paramètre, entrez l'ID de version que vous avez utilisé dans la `cross-grid-replication-retry-failed` demande.
4. Sélectionnez **Exécuter**.
5. Vérifiez que le code de réponse du serveur est **200**.
6. Vérifiez l'état de la 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 une défaillance permanente. L'utilisateur doit résoudre l'erreur.

Gérer la sécurité

Gérer la sécurité

Vous pouvez configurer différents paramètres de sécurité à partir du Gestionnaire de grille pour sécuriser votre système StorageGRID.

Gestion du chiffrement

StorageGRID propose plusieurs options pour le chiffrement des données. Vous devez "consultez les méthodes de cryptage disponibles"déterminer lesquelles répondent à vos exigences en matière de protection des données.

Gérer les certificats

Vous pouvez "configurer et gérer les certificats de serveur"l'utiliser pour les connexions HTTP ou les certificats

client utilisés pour authentifier l'identité d'un client ou d'un utilisateur sur le serveur.

Configurer les serveurs de gestion des clés

L'utilisation d'un "serveur de gestion des clés"vous permet de protéger vos données StorageGRID même si une appliance est retirée du data Center. Une fois les volumes de l'appliance chiffrés, vous ne pouvez accéder aux données de l'appliance que si le nœud peut communiquer avec le KMS.

> Pour utiliser la gestion des clés de chiffrement, vous devez activer le paramètre **Node Encryption** pour chaque appliance au cours de l'installation, avant d'ajouter l'appliance à la grille.

Gérer les paramètres proxy

Si vous utilisez les 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 terminaux 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.

Contrôle des 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 sur le "pare-feu externe". Vous pouvez également contrôler l'accès réseau à chaque nœud en configurant son "pare-feu interne". Vous pouvez empêcher l'accès à tous les ports, à l'exception de ceux nécessaires à votre déploiement.

Étudiez les méthodes de cryptage StorageGRID

StorageGRID propose plusieurs options pour le chiffrement des données. Consultez les méthodes disponibles pour identifier les méthodes qui répondent à vos exigences en matière de protection des données.

Le tableau fournit un récapitulatif détaillé des méthodes de cryptage disponibles dans StorageGRID.

Option de chiffrement	Comment cela fonctionne	S'applique à
Serveur de gestion des clés (KMS) dans Grid Manager	Vous "configurer un serveur de gestion des clés" pour le site StorageGRID et "activez le chiffrement des nœuds pour l'appliance". Ensuite, un nœud d'appliance se connecte au KMS pour demander une clé de chiffrement (KEK). Cette clé chiffre et décrypte la clé de chiffrement des données (DEK) sur chaque volume.	Nœuds d'appliance sur lesquels **Node Encryption** est activé pendant l'installation. Toutes les données de l'appliance sont protégées contre les pertes ou les suppressions physiques du data Center. **Remarque** : la gestion des clés de chiffrement avec un KMS n'est prise en charge que pour les nœuds de stockage et les appliances de services.

Option de chiffrement	Comment cela fonctionne	S'applique à
Page chiffrement de lecteur dans le programme d'installation de l'appliance StorageGRID	Si l'appliance contient des disques qui prennent en charge le chiffrement matériel, vous pouvez définir une phrase secrète de lecteur lors de l'installation. Lorsque vous définissez une phrase de passe pour un disque, il est impossible à quiconque de récupérer des données valides sur les disques qui ont été supprimés du système, sauf s'il connaît la phrase de passe. Avant de commencer l'installation, accédez à **Configure Hardware** > **Drive Encryption** pour définir une phrase de passe de lecteur qui s'applique à tous les disques à chiffrement automatique gérés par StorageGRID d'un nœud.	Les appliances contiennent des disques à chiffrement automatique. Toutes les données des disques sécurisés sont protégées contre les pertes ou suppressions physiques du data Center. Le chiffrement de disque ne s'applique pas aux disques gérés par SANtricity. Si vous disposez d'une appliance de stockage avec disques à chiffrement automatique et contrôleurs SANtricity, vous pouvez activer la sécurité des disques dans SANtricity.
Sécurité des disques dans SANtricity System Manager	Si la fonction de sécurité des lecteurs est activée pour votre appliance StorageGRID, vous pouvez utiliser "SANtricity System Manager" pour créer et gérer la clé de sécurité. La clé est requise pour accéder aux données sur les disques sécurisés.	Dispositifs de stockage équipés de disques Full Disk Encryption (FDE) ou de disques à autocryptage. Toutes les données des disques sécurisés sont protégées contre les pertes ou suppressions physiques du data Center. Utilisation avec certaines appliances de stockage ou avec des appliances de services impossible.
Chiffrement des objets stockés	Vous activez l'"Chiffrement des objets stockés"option dans le Gestionnaire de grille. Lorsqu'il est activé, tout nouvel objet non chiffré au niveau du compartiment ou de l'objet est chiffré lors de l'ingestion.	Données d'objet S3 récemment ingérées. Les objets stockés existants ne sont pas chiffrés. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées.
Chiffrement de compartiment S3	Vous lancez une demande PutBucketEncryption pour activer le cryptage du compartiment. Tout nouvel objet non chiffré au niveau de l'objet est chiffré lors de l'ingestion.	Données d'objet S3 récemment ingérées uniquement. Le chiffrement doit être spécifié pour le compartiment. Les objets de compartiment existants ne sont pas chiffrés. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées. "Opérations sur les compartiments"

Option de chiffrement	Comment cela fonctionne	S'applique à
Chiffrement côté serveur d'objets S3 (SSE)	Vous exécutez une demande S3 pour stocker un objet et inclure l'en- `x-amz-server-side-encryption`tête de la demande.	Données d'objet S3 récemment ingérées uniquement. Le chiffrement doit être spécifié pour l'objet. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées. StorageGRID gère les clés. "Utilisez le cryptage côté serveur"
Chiffrement côté serveur objet S3 avec clés fournies par le client (SSE-C)	Vous émettez une demande 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 récemment ingérées uniquement. Le chiffrement doit être spécifié pour l'objet. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées. Les clés sont gérées en dehors du StorageGRID. "Utilisez le cryptage côté serveur"
Chiffrement de volume ou de datastore externe	Vous utilisez une méthode de chiffrement autres que StorageGRID pour chiffrer un volume ou un datastore entier, si votre plateforme de déploiement le prend en charge.	Toutes les données d'objet, de métadonnées et de configuration du système, en supposant que chaque volume ou datastore est chiffré. Une méthode de chiffrement externe permet un contrôle plus précis des clés et des algorithmes de chiffrement. Peut être combiné avec les autres méthodes répertoriées.

Option de chiffrement	Comment cela fonctionne	S'applique à
Chiffrement d'objet en dehors de StorageGRID	Vous utilisez une méthode de chiffrement à l'extérieur de StorageGRID pour chiffrer les données d'objet et les métadonnées avant leur ingestion dans StorageGRID.	Données et métadonnées d'objet uniquement (les données de configuration du système ne sont pas chiffrées). Une méthode de chiffrement externe permet un contrôle plus précis des clés et des algorithmes de chiffrement. 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"

Utilisez plusieurs méthodes de chiffrement

Selon vos besoins, vous pouvez utiliser plusieurs méthodes de chiffrement à la fois. Par exemple :

- Vous pouvez utiliser un KMS pour protéger les nœuds de l'appliance et utiliser la fonctionnalité de sécurité des disques de SANtricity System Manager pour « double chiffrement » des données sur les disques à chiffrement automatique des mêmes appliances.
- Vous pouvez utiliser un KMS pour sécuriser les données des nœuds de l'appliance et utiliser l'option de chiffrement des objets stockés pour chiffrer tous les objets lors de leur ingestion.

Si seule une petite partie de vos objets doit être cryptée, pensez à contrôler le chiffrement au niveau du compartiment ou de l'objet au niveau individuel. L'activation de plusieurs niveaux de chiffrement a un coût supplémentaire en termes de performance.

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 permettent d'établir des connexions sécurisées entre les clients et les serveurs, d'authentifier l'identité d'un serveur pour ses clients et de fournir un chemin de communication sécurisé pour les données. Le serveur et le client ont chacun une copie du certificat.
- **Certificats client** authentifiez une identité client ou utilisateur au serveur, fournissant une authentification plus sécurisée que les mots de passe seuls. Les certificats client ne chiffrent 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

figurant 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 (par exemple, le point de terminaison de l'équilibreur de charge) ou comme client pour d'autres connexions (par exemple, le service de réplication CloudMirror).

Certificat CA grille par défaut

StorageGRID inclut une autorité de certification intégrée qui génère un certificat d'autorité de certification interne Grid lors de l'installation du système. Par défaut, le certificat de l'autorité de certification Grid est utilisé pour sécuriser le trafic StorageGRID interne. Une autorité de certification externe peut émettre des certificats personnalisés qui sont entièrement conformes aux politiques de sécurité des informations de votre entreprise. Bien que vous puissiez utiliser le certificat d'autorité de certification Grid pour un environnement non productif, 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 d'autorité de certification personnalisée 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 au "instructions 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 bundle de certificats d'autorité de certification).

> ⓘ StorageGRID inclut également des certificats CA du système d'exploitation identiques 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 d'autorité de certification du système d'exploitation.

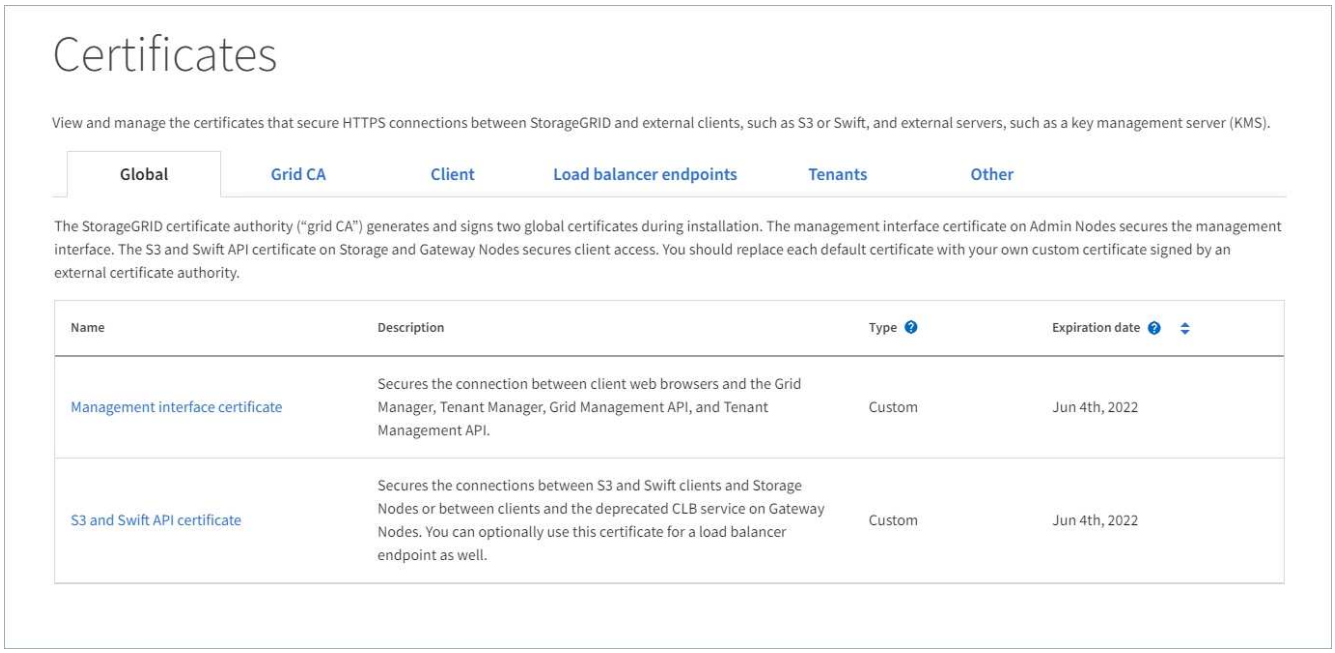
Les variantes du serveur et des types de certificats client sont mises en œuvre de plusieurs façons. Avant de configurer le système, tous les certificats nécessaires à votre configuration StorageGRID spécifique doivent être prêts.

Accéder aux certificats de sécurité

Vous pouvez accéder aux informations relatives à tous les certificats StorageGRID dans un seul emplacement, ainsi qu'aux liens vers le flux de travail de configuration de chaque certificat.

Étapes

1. Dans Grid Manager, 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 de navigateurs Web et de 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.
   - **Noeuds finaux 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'identités ou des terminaux de service de plate-forme 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 StorageGRID à partir de navigateurs Web et de 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 de l'interface de gestion: Sécurise les connexions du navigateur Web client aux interfaces de gestion StorageGRID.
- Certificat d'API S3: Sécurise les connexions API client aux nœuds de stockage, nœuds d'administration et nœuds de passerelle, que les applications client S3 utilisent pour télécharger et télécharger les données d'objet.

Les informations sur les certificats globaux installés comprennent :

- **Nom** : nom du certificat avec lien vers la gestion du certificat.
- **Description**
- **Type** : personnalisé ou par défaut. + vous devez toujours utiliser un certificat personnalisé pour améliorer la sécurité de la grille.
- **Date d'expiration** : si vous utilisez le certificat par défaut, aucune date d'expiration n'est affichée.

Vous pouvez :

- Remplacez les certificats par défaut par des certificats personnalisés signés par une autorité de certification externe pour améliorer la sécurité de la grille :
  - "Remplacez le certificat d'interface de gestion généré par défaut par StorageGRID" Utilisé pour les connexions Grid Manager et tenant Manager.
  - "Remplacez le certificat de l'API S3" Utilisé pour les connexions de nœuds de stockage et de terminaux d'équilibrage de la charge (en option).
- "Restaurez le certificat de l'interface de gestion par défaut".
- "Restaurez le certificat d'API S3 par défaut".
- "Utilisez un script pour générer un nouveau certificat d'interface de gestion auto-signé".
- Copiez ou téléchargez le ou le "certificat de l'interface de gestion""Certificat d'API S3".

CA grille

Le Certificat CA de la grille, généré par l'autorité de certification StorageGRID lors de l'installation de StorageGRID, sécurise tout le trafic StorageGRID interne.

Les informations sur le certificat comprennent la date d'expiration du certificat et son contenu.

Vous pouvez "Copiez ou téléchargez le certificat d'autorité de certification Grid", mais vous ne pouvez pas le modifier.

Client

Certificats client, Générée par une autorité de certification externe, sécurise les connexions entre les outils de contrôle externes et la base de données StorageGRID Prometheus.

La table de certificats possède 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.

Vous pouvez :

- "Téléchargez ou générez un nouveau certificat client."
- Sélectionnez un nom de certificat pour afficher les détails du certificat où vous pouvez :
  - "Modifiez le nom du certificat client."
  - "Définissez l'autorisation d'accès Prometheus."
  - "Téléchargez et remplacez le certificat client."
  - "Copiez ou téléchargez le certificat client."
  - "Supprimez le certificat client."
- Sélectionnez **actions** pour rapidement "modifier", "attacher"ou "déposer" un certificat client. Vous pouvez sélectionner jusqu'à 10 certificats client et les supprimer en une seule fois en utilisant **actions** > **Supprimer**.

Terminaux d'équilibrage de charge

Certificats de noeud final de l'équilibreur de charge Sécurisez les connexions entre les clients S3 et le service StorageGRID Load Balancer sur les nœuds de passerelle et les nœuds d'administration.

Le tableau des terminaux d'équilibrage de la charge comporte une ligne pour chaque terminal d'équilibrage de la charge configuré et indique si le certificat d'API S3 global ou le certificat de terminal d'équilibreur de charge personnalisé est utilisé pour le terminal. La date d'expiration de chaque certificat s'affiche également.

> Les modifications apportées à un certificat de point final peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

Vous pouvez :

- "Afficher un point d'extrémité d'équilibreur de charge", y compris les détails de son certificat.
- "Spécifiez un certificat de noeud final de l'équilibreur de charge pour FabricPool."
- "Utilisez le certificat d'API S3 global" au lieu de générer un nouveau certificat de point de terminaison d'équilibreur de charge.

Locataires

Les locataires peuvent utiliser certificats de serveur de fédération des identités ou certificats de terminal du service de plate-forme pour sécuriser leurs connexions avec StorageGRID.

La table de tenant dispose d'une ligne pour chaque locataire et indique si chaque locataire a l'autorisation d'utiliser ses propres services de référentiel d'identité ou de plate-forme.

Vous pouvez :

- "Sélectionnez un nom de locataire pour vous connecter au Gestionnaire de tenant"
- "Sélectionnez un nom de locataire pour afficher les détails de la fédération des identités du locataire"
- "Sélectionnez un nom de locataire pour afficher les détails des services de plateforme du locataire"
- "Spécifiez un certificat de noeud final du service de plate-forme pendant la création du noeud final"

Autre

StorageGRID utilise d'autres certificats de sécurité pour des fins spécifiques. Ces certificats sont répertoriés par leur nom fonctionnel. Voici d'autres certificats de sécurité :

- Certificats de pool de stockage cloud
- Certificats de notification d'alerte par e-mail
- Certificats de serveur syslog externe
- Certificats de connexion de fédération de grille
- Certificats de fédération des identités
- Certificats de serveur de gestion des clés (KMS)
- Certificats d'authentification unique

Informations indique le type de certificat utilisé par une fonction et ses dates d'expiration de certificat de serveur et de 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 relatives aux autres certificats que si vous disposez du "autorisation appropriée".

Vous pouvez :

- "Spécification d'un certificat de pool de stockage cloud pour S3, C2S S3 ou Azure"
- "Spécifiez un certificat pour les notifications par e-mail d'alerte"
- "Utilisez un certificat pour un serveur syslog externe"
- "Faire pivoter les certificats de connexion de fédération de grille"
- "Afficher et modifier un certificat de fédération d'identités"
- "Télécharger les certificats du serveur de gestion des clés (KMS) et du client"
- "Spécifiez manuellement un certificat SSO pour une confiance de partie utilisatrice"

Détails du certificat de sécurité

Chaque type de certificat de sécurité est décrit ci-dessous, avec des liens vers les instructions d'implémentation.

Certificat de l'interface de gestion

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les navigateurs Web client et l'interface de gestion StorageGRID, permettant aux utilisateurs d'accéder à Grid Manager et au gestionnaire de locataires sans avertissement de sécurité. Ce certificat authentifie également les connexions de l'API de gestion du grid et de l'API de gestion des locataires. 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 **certificat d'interface de gestion**	"Configurer les certificats d'interface de gestion"

Certificat d'API S3

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie les connexions client S3 sécurisées vers un nœud de stockage et les terminaux d'équilibrage de la charge (facultatif).	**CONFIGURATION** > **sécurité** > **certificats**, sélectionnez l'onglet **Global**, puis sélectionnez **certificat API S3**	"Configurer les certificats d'API S3"

Certificat CA de la grille

Voir la Description du certificat CA de la grille par défaut.

Certificat du 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. • Contrôle sécurisé de StorageGRID à l'aide d'outils externes.	**CONFIGURATION** > **sécurité** > **certificats**, puis sélectionnez l'onglet **client**	"Configurer les certificats client"

Certificat de terminal de l'équilibreur de charge

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les clients S3 et le service StorageGRID Load Balancer 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 noeud final d'équilibreur de charge. Les applications client utilisent le certificat d'équilibreur de charge lors de la connexion à StorageGRID pour enregistrer et récupérer les données d'objet. Vous pouvez également utiliser une version personnalisée du certificat global Certificat d'API S3pour 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 noeud final 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 l'StorageGRID.	**CONFIGURATION** > **réseau** > **points d'extrémité de l'équilibreur de charge**	• "Configurer les terminaux de l'équilibreur de charge" • "Créez un noeud final d'équilibrage de charge pour FabricPool"

Certificat de terminal Cloud Storage Pool

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion à partir d'un pool de stockage cloud StorageGRID vers un emplacement de stockage externe, tel que S3 Glacier ou Microsoft Azure Blob Storage. Un certificat différent est requis pour chaque type de fournisseur cloud.	**ILM** > **pools de stockage**	"Création d'un pool de stockage cloud"

Certificat de notification d'alerte par e-mail

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 TLS (transport Layer Security), vous devez spécifier le certificat AC du serveur de messagerie. • Spécifiez un certificat client uniquement si le serveur de messagerie SMTP nécessite des certificats client pour l'authentification.	**ALERTES** > **Configuration de la messagerie**	"Configurez les 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 consigne 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 de fédération de grille

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifier et crypter 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 pivoter les certificats de connexion"

Certificat de fédération des identités

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 des identités, ce qui permet de gérer les groupes et les utilisateurs d'administration par un système externe.	**CONFIGURATION** > **contrôle d'accès** > **fédération d'identités**	"Utiliser la fédération des identités"

Certificat de serveur de gestion des clés (KMS)

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifie la connexion entre StorageGRID et un serveur de gestion des clés (KMS) externe qui fournit les clés de chiffrement aux nœuds d'appliance StorageGRID.	**CONFIGURATION** > **sécurité** > **serveur de gestion des clés**	"Ajout d'un serveur de gestion des clés (KMS)"

Certificat de terminal des services de plate-forme

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentification de la connexion depuis le service de la plateforme StorageGRID vers une ressource de stockage S3	**Tenant Manager** > **STORAGE (S3)** > **Platform services Endpoints**	"Créer un terminal de services de plate-forme" "Modifier le point final des services de plate-forme"

Certificat SSO (Single Sign-on)

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les services de fédération d'identités, tels que Active Directory Federation Services (AD FS) et StorageGRID utilisés pour les demandes SSO (Single Sign-on).	**CONFIGURATION** > **contrôle d'accès** > **Single Sign-on**	"Configurer l'authentification unique"

Exemples de certificats

Exemple 1 : service Load Balancer

Dans cet exemple, StorageGRID sert de serveur.

1. Vous configurez un noeud final de l'équilibreur de charge et téléchargez ou générez un certificat de serveur dans StorageGRID.
2. Vous configurez une connexion client S3 avec le terminal de l'équilibreur de charge et téléchargez le même certificat vers 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 une signature basée

sur la clé privée.

5. Le client vérifie ce certificat en comparant la signature du serveur à la signature figurant sur sa copie du certificat. Si les signatures correspondent, le client lance une session à l'aide de la même clé publique.
6. Le client envoie des données d'objet à StorageGRID.

Exemple 2 : serveur de gestion externe des clés (KMS)

Dans cet exemple, StorageGRID agit comme client.

1. À l'aide du logiciel serveur de gestion de clés externe, vous configurez StorageGRID en tant que client KMS et obtenez un certificat de serveur signé par l'autorité de certification, un certificat de client public et la clé privée pour le certificat client.
2. À l'aide de Grid Manager, 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 requête 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 à l'aide de la connexion validée.

Types de certificat de serveur pris en charge

Le système StorageGRID prend en charge les certificats personnalisés chiffrés avec RSA ou ECDSA (algorithme de signature numérique de courbe elliptique).

> Le type de chiffrement de la stratégie de sécurité doit correspondre au type de certificat du serveur. Par exemple, les chiffrements RSA nécessitent des certificats RSA et les chiffrements ECDSA requièrent des certificats ECDSA. Voir "Gérer les certificats de sécurité". Si vous configurez une stratégie de sécurité personnalisée qui n'est pas compatible avec le certificat de serveur, vous pouvez "rétablir temporairement la stratégie de sécurité par défaut".

Pour plus d'informations sur la façon dont StorageGRID sécurise les connexions client, reportez-vous à la section "Sécurité pour les clients S3".

Configurer les certificats d'interface de gestion

Vous pouvez remplacer le certificat de l'interface de gestion par défaut par un certificat personnalisé unique qui permet aux utilisateurs d'accéder à Grid Manager et au Gestionnaire de locataires sans rencontrer d'avertissement de sécurité. Vous pouvez également revenir au certificat d'interface de gestion par défaut ou en générer un nouveau.

Description de la tâche

Par défaut, chaque nœud d'administration est doté d'un certificat signé par l'autorité de certification de la grille. Ces certificats signés par l'autorité de certification peuvent être remplacés par un seul certificat d'interface de gestion personnalisée commun et une clé privée correspondante.

Étant donné qu'un seul certificat d'interface de gestion personnalisée est utilisé pour tous les nœuds d'administration, vous devez spécifier le certificat en tant que certificat générique ou multidomaine si les clients doivent vérifier le nom d'hôte lors de la connexion à Grid Manager et au tenant Manager. 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 (AC) que vous utilisez, les utilisateurs peuvent également avoir besoin d'installer le certificat d'autorité de certification Grid dans le navigateur Web qu'ils utiliseront pour accéder au Grid Manager et au Gestionnaire de locataires.

Pour garantir que les opérations ne sont pas interrompues 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 afficher le moment où le certificat en cours expire en sélectionnant **CONFIGURATION** > **sécurité** > **certificats** et en consultant la date d'expiration du certificat de l'interface de gestion dans l'onglet Global.

Si vous accédez à Grid Manager ou au Gestionnaire de locataires 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'un des cas suivants se produit :

- Votre certificat d'interface de gestion personnalisée expire.
- Vous restaurez le certificat de serveur par défaut à partir d'un certificat d'interface de gestion personnalisée.

Ajoutez un certificat d'interface de gestion personnalisée

Pour ajouter un certificat d'interface de gestion personnalisée, vous pouvez fournir votre propre certificat ou en générer un à l'aide de Grid Manager.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**.
2. Dans l'onglet **Global**, sélectionnez **Management interface certificate**.
3. Sélectionnez **utiliser le certificat personnalisé**.
4. Chargez 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** : fichier de certificat de serveur personnalisé (codé PEM).
- **Clé privée de certificat** : fichier de clé privée de certificat de serveur personnalisé (`.key`).

> Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2048 bits ou plus.

- **Paquet CA** : un fichier facultatif unique contenant les certificats de chaque autorité de certification intermédiaire (AC). Le fichier doit contenir chacun des fichiers de certificat d'autorité de certification codés au PEM, concaténés dans l'ordre de la chaîne de certificats.

c. Développez **Détails du certificat** pour afficher 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 paquet CA** pour enregistrer le lot 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 **Copy certificate PEM** ou **Copy CA bundle PEM** pour copier le contenu du certificat pour le coller ailleurs.

d. Sélectionnez **Enregistrer**. + le certificat d'interface de gestion personnalisée est utilisé pour toutes les nouvelles connexions ultérieures à Grid Manager, tenant Manager, l'API Grid Manager ou l'API tenant Manager.

Générez un certificat

Générez les fichiers de certificat du serveur.

> La meilleure pratique pour un environnement de production consiste à utiliser un certificat d'interface de gestion personnalisée signé par une autorité de certification externe.

a. Sélectionnez **générer certificat**.

b. Spécifiez les informations de certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine complets à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.

Champ	Description
IP	Une ou plusieurs adresses IP à inclure dans le certificat.
Objet (facultatif)	Objet 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 l'adresse IP comme nom commun de l'objet (CN).
Jours valides	Nombre de jours après la création, pendant lesquels le certificat expire.
Ajouter des extensions d'utilisation de clé	Si cette option est sélectionnée (par défaut et recommandée), l'utilisation des clés et les extensions d'utilisation des clés étendues sont ajoutées au certificat généré. Ces extensions définissent l'objectif de la clé contenue dans le certificat. **Remarque** : ne cochez pas cette case si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **generate**.

d. Sélectionnez **Détails du certificat** pour afficher 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 pour le coller ailleurs.

e. Sélectionnez **Enregistrer**. + le certificat d'interface de gestion personnalisée est utilisé pour toutes les nouvelles connexions ultérieures à Grid Manager, tenant Manager, l'API Grid Manager ou l'API tenant Manager.

5. Actualisez la page pour vous assurer que le navigateur Web est mis à jour.

> Après avoir téléchargé ou généré un nouveau certificat, autorisez jusqu'à un jour l'effacement des alertes d'expiration de certificat associées.

6. Une fois que vous avez ajouté un certificat d'interface de gestion personnalisé, la page de certificat de l'interface de gestion affiche des informations détaillées sur le certificat pour les certificats en cours d'utilisation. + vous pouvez télécharger ou copier le certificat PEM selon vos besoins.

Restaurez le certificat de l'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 **Management interface certificate**.
3. Sélectionnez **utiliser le certificat par défaut**.

   Lorsque vous restaurez le certificat d'interface de gestion par défaut, les fichiers de certificat de serveur personnalisés que vous avez configurés sont supprimés et ne peuvent pas être récupérés du système. Le certificat d'interface de gestion par défaut est utilisé pour toutes les nouvelles connexions client suivantes.

4. Actualisez la page pour vous assurer que le navigateur Web est mis à jour.

Utilisez 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

- Vous avez "autorisations d'accès spécifiques".
- Vous avez le `Passwords.txt` fichier.

Description de la 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. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour basculer en root : `su -`
   d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

      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`.
   - Définissez `--type` sur `management` pour configurer le certificat de l'interface de gestion, utilisé par Grid Manager et tenant Manager.
   - Par défaut, les certificats générés sont valables pendant un an (365 jours) et doivent être recréés avant leur expiration. Vous pouvez utiliser l' `--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 peut rejeter le certificat.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 720
```

Le résultat contient le certificat public requis par votre client de l'API de gestion.

4. Sélectionnez et copiez le certificat.

   Incluez les étiquettes DE DÉBUT et DE FIN dans votre sélection.

5. Déconnectez-vous du shell de commande. `$ exit`
6. Vérifiez que le certificat a été configuré :
   a. Accédez au Grid Manager.
   b. Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**
   c. Dans l'onglet **Global**, sélectionnez **Management interface certificate**.
7. Configurez votre client de gestion pour utiliser le certificat public que vous avez copié. Incluez les balises DE DÉBUT et DE FIN.

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 **Management interface certificate**.
3. Sélectionnez l'onglet **Server** ou **CA bundle**, puis téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat ou le bundle CA

Téléchargez le fichier de certificat ou de bundle CA `.pem`. Si vous utilisez un bundle CA facultatif, chaque certificat du bundle s'affiche dans son propre sous-onglet.

a. Sélectionnez **Télécharger le certificat** ou **Télécharger le paquet CA**.

   Si vous téléchargez un bundle CA, tous les certificats des onglets secondaires de l'offre CA sont téléchargés en un seul fichier.

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 ou pack CA PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un bundle CA facultatif, chaque certificat du bundle s'affiche dans son propre sous-onglet.

a. Sélectionnez **Copy Certificate PEM** ou **Copy CA bundle PEM**.

   Si vous copiez un bundle CA, tous les certificats des onglets secondaires de l'offre CA 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 d'API S3

Vous pouvez remplacer ou restaurer le certificat du serveur utilisé pour les connexions client S3 avec les nœuds de stockage ou pour les terminaux d'équilibrage 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 doc. Voir "StorageGRID 11.8 : configurez les certificats d'API S3 et Swift".

Description de la tâche

Par défaut, chaque nœud de stockage est doté d'un certificat de serveur X.509 signé par l'autorité de certification de la grille. Ces certificats signés par l'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 un certificat générique ou multidomaine si les clients doivent vérifier le nom d'hôte lors de la connexion au noeud final de stockage. Définissez le certificat personnalisé de sorte qu'il corresponde à tous les nœuds de stockage de la grille.

Une fois la configuration terminée sur le serveur, vous devrez peut-être installer le certificat de l'autorité de certification Grid dans le client de l'API S3 que vous utiliserez pour accéder au système, selon l'autorité de

certification racine (CA) que vous utilisez.

> Pour garantir que les opérations ne sont pas interrompues par un certificat de serveur défaillant, l'alerte **expiration du certificat de serveur global pour l'API S3** est déclenchée lorsque le certificat de serveur racine est sur le point d'expirer. Si nécessaire, vous pouvez afficher la date d'expiration du certificat en cours 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 d'API S3 personnalisé.

Ajoutez un certificat d'API S3 personnalisé

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**.
2. Dans l'onglet **Global**, sélectionnez **S3 API Certificate**.
3. Sélectionnez **utiliser le certificat personnalisé**.
4. Chargez 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** : fichier de certificat de serveur personnalisé (codé PEM).
- **Clé privée de certificat** : fichier de clé privée de certificat de serveur personnalisé (`.key`).

> Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2048 bits ou plus.

- **Paquet CA** : un fichier facultatif unique contenant les certificats de chaque autorité de délivrance de certificat intermédiaire. Le fichier doit contenir chacun des fichiers de certificat d'autorité de certification codés au 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 d'API S3 personnalisé 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 paquet CA** pour enregistrer le lot 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 **Copy certificate PEM** ou **Copy CA bundle PEM** pour copier le contenu du certificat pour le coller ailleurs.

d. Sélectionnez **Enregistrer**.

Le certificat de serveur personnalisé est utilisé pour les nouvelles connexions client S3 suivantes.

Générez un certificat

Générez les fichiers de certificat du serveur.

a. Sélectionnez **générer certificat**.

b. Spécifiez les informations de certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine complets à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.
IP	Une ou plusieurs adresses IP à inclure dans le certificat.

Champ	Description
Objet (facultatif)	Objet 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 l'adresse IP comme nom commun de l'objet (CN).
Jours valides	Nombre de jours après la création, pendant lesquels le certificat expire.
Ajouter des extensions d'utilisation de clé	Si cette option est sélectionnée (par défaut et recommandée), l'utilisation des clés et les extensions d'utilisation des clés étendues sont ajoutées au certificat généré. Ces extensions définissent l'objectif de la clé contenue dans le certificat. **Remarque** : ne cochez pas cette case si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **generate**.

d. Sélectionnez **Détails du certificat** pour afficher les métadonnées et le PEM du certificat API S3 personnalisé 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 pour le coller ailleurs.

e. Sélectionnez **Enregistrer**.

Le certificat de serveur personnalisé est utilisé pour les nouvelles connexions client S3 suivantes.

5. Sélectionnez un onglet pour afficher les métadonnées du certificat de serveur StorageGRID par défaut, un certificat signé par l'autorité de certification qui a été chargé ou un certificat personnalisé qui a été généré.

> Après avoir téléchargé ou généré un nouveau certificat, autorisez jusqu'à un jour l'effacement des alertes d'expiration de certificat associées.

6. Actualisez la page pour vous assurer que le navigateur Web est mis à jour.
7. Après avoir ajouté un certificat d'API S3 personnalisé, la page de certificat d'API S3 affiche des informations détaillées sur le certificat d'API S3 personnalisé en cours d'utilisation. + vous pouvez télécharger ou copier le certificat PEM selon vos besoins.

Restaurez le certificat d'API S3 par défaut

Vous pouvez revenir à l'utilisation du certificat d'API S3 par défaut pour les connexions client S3 aux nœuds de stockage. Toutefois, vous ne pouvez pas utiliser le certificat d'API S3 par défaut pour un terminal d'équilibreur de charge.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**.
2. Dans l'onglet **Global**, sélectionnez **S3 API Certificate**.
3. Sélectionnez **utiliser le certificat par défaut**.

   Lorsque vous restaurez la version par défaut du certificat d'API S3 global, les fichiers de certificat de serveur personnalisé que vous avez configurés sont supprimés et ne peuvent pas être récupérés du système. Le certificat d'API S3 par défaut sera utilisé pour les nouvelles connexions client S3 suivantes 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 d'API S3 personnalisé a été utilisé pour les connexions de terminaux d'équilibrage de charge, une liste s'affiche indiquant les terminaux d'équilibrage de charge qui ne seront plus accessibles à l'aide du certificat d'API S3 par défaut. Accédez à "Configurer les terminaux de l'équilibreur de charge" pour modifier ou supprimer les points finaux affectés.

5. Actualisez la page pour vous assurer que le navigateur Web est mis à jour.

Téléchargez ou copiez le certificat d'API S3

Vous pouvez enregistrer ou copier le contenu du certificat de l'API S3 pour l'utiliser ailleurs.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**.
2. Dans l'onglet **Global**, sélectionnez **S3 API Certificate**.
3. Sélectionnez l'onglet **Server** ou **CA bundle**, puis téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat ou le bundle CA

Téléchargez le fichier de certificat ou de bundle CA `.pem`. Si vous utilisez un bundle CA facultatif, chaque certificat du bundle s'affiche dans son propre sous-onglet.

a. Sélectionnez **Télécharger le certificat** ou **Télécharger le paquet CA**.

   Si vous téléchargez un bundle CA, tous les certificats des onglets secondaires de l'offre CA sont téléchargés en un seul fichier.

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 ou pack CA PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un bundle CA facultatif, chaque certificat du bundle s'affiche dans son propre sous-onglet.

a. Sélectionnez **Copy Certificate PEM** ou **Copy CA bundle PEM**.

   Si vous copiez un bundle CA, tous les certificats des onglets secondaires de l'offre CA 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 associées

- "UTILISEZ L'API REST S3"
- "Configuration des noms de domaine de terminaux S3"

Copiez le certificat de l'autorité de certification Grid

StorageGRID utilise une autorité de certification interne pour sécuriser le trafic interne, Ce certificat ne change pas si vous téléchargez vos propres certificats.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez "autorisations d'accès spécifiques".

Description de la tâche

Si un certificat de serveur personnalisé a été configuré, les applications client doivent vérifier le serveur à l'aide du certificat de serveur personnalisé. Ils ne doivent pas copier le certificat de l'autorité de certification depuis le système StorageGRID.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**, puis sélectionnez l'onglet **Grid CA**.

2. Dans la section **Certificate PEM**, téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat

Téléchargez le fichier de certificat `.pem`.

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`

Configurez les certificats StorageGRID pour FabricPool

Pour les clients S3 qui valident rigoureusement le nom d'hôte et ne prennent pas en charge la désactivation de la validation stricte du nom d'hôte, comme les clients ONTAP qui utilisent FabricPool, vous pouvez générer ou télécharger un certificat de serveur lorsque vous configurez le terminal de l'équilibreur de charge.

Avant de commencer

- Vous avez "autorisations d'accès spécifiques".
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".

Description de la tâche

Lorsque vous créez un noeud final d'équilibreur de charge, vous pouvez générer un certificat de serveur auto-signé ou télécharger un certificat signé par une autorité de certification 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 pivotés sans interruption. Elles sont également plus sécurisées parce qu'elles offrent une meilleure protection contre les attaques de l'homme au milieu.

Les étapes suivantes fournissent des instructions d'ordre général pour les clients S3 qui utilisent FabricPool. Pour plus d'informations et de procédures, voir "Configuration de StorageGRID pour FabricPool".

Étapes

1. Configurez également un groupe haute disponibilité (HA) pour FabricPool à utiliser.
2. Créez un terminal d'équilibrage de charge S3 pour FabricPool.

   Lorsque vous créez un noeud final d'équilibreur de charge HTTPS, vous êtes invité à télécharger votre certificat de serveur, votre clé privée de certificat et votre bundle CA facultatif.

3. Association de StorageGRID en tant que Tier cloud dans ONTAP

   Spécifiez le port de point final de l'équilibreur de charge et le nom de domaine complet utilisé dans le certificat de l'autorité de certification que vous avez téléchargé. Ensuite, indiquez le certificat de l'autorité de certification.

> Si une autorité de certification intermédiaire a émis le certificat StorageGRID, vous devez fournir le certificat CA intermédiaire. Si le certificat StorageGRID a été émis directement par l'autorité de certification racine, vous devez fournir le certificat d'autorité de certification racine.

Configurer les certificats client

Les certificats client permettent aux clients externes autorisés d'accéder à la base de données StorageGRID Prometheus, ce qui fournit un moyen sécurisé aux outils externes de surveillance 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 de Grid Manager et copier les informations de certificat dans l'outil externe.

Voir "Gérer les certificats de sécurité" et "Configurer des certificats de serveur personnalisés".

> Pour garantir que les opérations ne sont pas interrompues par un certificat de serveur défaillant, l'alerte **expiration des certificats client configurés sur la page certificats** est déclenchée lorsque ce certificat de serveur est sur le point d'expirer. Si nécessaire, vous pouvez afficher le moment où le certificat en cours expire en sélectionnant **CONFIGURATION** > **sécurité** > **certificats** et en consultant la date d'expiration du certificat client dans l'onglet client.

> Si vous utilisez un serveur de gestion des clés (KMS) pour protéger les données sur les nœuds d'appliance spécialement configurés, consultez les informations spécifiques à la section "Téléchargement d'un certificat client KMS".

Avant de commencer

- Vous disposez de l'autorisation d'accès racine.
- Vous êtes connecté au Gestionnaire de grille 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 de l'interface de gestion StorageGRID, l'autorité de certification, le certificat client et la clé privée sont utilisés pour configurer le certificat de l'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 enregistrée ou enregistrée au moment de sa création. Si vous ne possédez pas 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 client

Pour ajouter le certificat client, utilisez l'une des procédures suivantes :

- Certificat d'interface de gestion déjà configuré
- CERTIFICAT client émis
- Certificat généré par 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 fournie par le client, d'un certificat client et d'une clé privée.

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 metrics Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser prometheus**.
5. Sélectionnez **Continuer**.
6. Pour l'étape **Attach certificates**, téléchargez le certificat de l'interface de gestion.
   a. Sélectionnez **Télécharger le certificat**.
   b. Sélectionnez **Browse** 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 certificat PEM.
      - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.
   c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

      Le nouveau certificat apparaît sur l'onglet client.
7. Configurer un outil de surveillance externe, Comme Grafana.

CERTIFICAT client émis

Utilisez cette procédure pour ajouter un certificat client d'administrateur si un certificat d'interface de gestion n'a pas été configuré et que vous prévoyez d'ajouter un certificat client pour Prometheus qui utilise un certificat client émis par l'autorité de certification et une clé privée.

Étapes

1. Effectuez les étapes à "configurez 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 metrics Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser prometheus**.

6. Sélectionnez **Continuer**.
7. Pour l'étape **joindre des certificats**, téléchargez le certificat client, la clé privée et les fichiers de bundle CA :
   a. Sélectionnez **Télécharger le certificat**.
   b. Sélectionnez **Browse** et sélectionnez le certificat client, la clé privée et les fichiers de bundle CA (`.pem`).
      - Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le certificat PEM.
      - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.
   c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

      Les nouveaux certificats apparaissent sur l'onglet client.
8. Configurer un outil de surveillance externe, Comme Grafana.

Certificat généré par Grid Manager

Utilisez cette procédure pour ajouter un certificat client d'administrateur si un certificat d'interface de gestion n'a pas été configuré et que vous prévoyez d'ajouter un certificat client pour Prometheus qui utilise la fonction générer 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 metrics 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 de certificat :
   - **Sujet** (facultatif) : sujet X.509 ou nom distinctif (DN) du propriétaire du certificat.
   - **Jours valides** : nombre de jours pendant lesquels le certificat généré est valide, à partir du moment où il est généré.
   - **Ajouter des extensions d'utilisation de clé** : si cette option est sélectionnée (par défaut et recommandée), l'utilisation de clé et les extensions 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 cochée sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.
8. Sélectionnez **generate**.
9. sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le certificat PEM.

Vous ne pourrez pas afficher la clé privée du certificat après avoir fermé la boîte de dialogue. Copiez ou téléchargez la clé dans un endroit sûr.

- Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour 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 de certificat pour coller ailleurs.
- Sélectionnez **Télécharger la clé privée** pour enregistrer la clé privée en tant que 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 sur 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 le certificat personnalisé**.
14. Téléchargez les fichiers certificate.pem et private_key.pem à partir de détails du certificat clientl'étape. Il n'est pas nécessaire de télécharger le pack CA.
    a. Sélectionnez **Télécharger le certificat**, puis **Continuer**.
    b. Télécharger chaque fichier de certificat (`.pem`).
    c. Sélectionnez **Enregistrer** pour enregistrer le certificat dans Grid Manager.

       Le nouveau certificat apparaît sur la page de certificat de l'interface de gestion.
15. Configurer un outil de surveillance externe, Comme Grafana.

configurez un outil de surveillance externe

Étapes

1. Configurez les paramètres suivants sur votre outil de surveillance externe, tels que Grafana.
   a. **Nom** : saisissez un nom pour la connexion.

      StorageGRID ne requiert 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 noeud d'administration. Spécifiez HTTPS et le port 9091.

      Par exemple : `https://admin-node.example.com:9091`

   c. Activez **TLS client Auth** et **avec CA Cert**.

d. Sous TLS/SSL Auth Details, copiez et collez :
   - Le certificat CA de l'interface de gestion à **CA Cert**
   - Le certificat client à **Cert client**
   - La clé privée pour **clé client**

e. **NomServeur** : saisissez le nom de domaine du noeud d'administration.

   Le nom de serveur 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 avez désormais accès aux metrics Prometheus à partir de StorageGRID grâce à votre outil de surveillance externe.

   Pour plus d'informations sur les mesures, reportez-vous au "Instructions de surveillance de StorageGRID".

Modifier les certificats client

Vous pouvez modifier un certificat de client d'administrateur pour changer son nom, activer ou désactiver l'accès 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 à modifier.
3. Sélectionnez **Modifier**, puis **Modifier le nom et l'autorisation**
4. Entrez un nom de certificat.
5. Pour accéder aux metrics Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser prometheus**.
6. Sélectionnez **Continuer** pour enregistrer le certificat dans Grid Manager.

   Le certificat mis à jour s'affiche dans l'onglet client.

Joindre un nouveau certificat client

Vous pouvez télécharger un nouveau certificat lorsque celui 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 à modifier.

3. Sélectionnez **Modifier**, puis sélectionnez une option d’édition.

Télécharger le certificat

Copiez le texte du certificat pour le coller ailleurs.

a. Sélectionnez **Télécharger le certificat**, puis **Continuer**.

b. Téléchargez le nom du certificat client (`.pem`).

   Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le certificat PEM.

   - 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 pour 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.

Générez un certificat

Générez le texte du certificat pour le coller ailleurs.

a. Sélectionnez **générer certificat**.

b. Spécifiez les informations de certificat :

   - **Sujet** (facultatif) : sujet X.509 ou nom distinctif (DN) du propriétaire du certificat.
   - **Jours valides** : nombre de jours pendant lesquels le certificat généré est valide, à partir du moment où il est généré.
   - **Ajouter des extensions d'utilisation de clé** : si cette option est sélectionnée (par défaut et recommandée), l'utilisation de clé et les extensions 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 cochée sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **generate**.

d. Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le certificat PEM.

   Vous ne pourrez pas afficher la clé privée du certificat après avoir fermé la boîte de dialogue. Copiez ou téléchargez la clé dans un endroit sûr.

   - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour 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 de certificat pour coller ailleurs.
- Sélectionnez **Télécharger la clé privée** pour enregistrer la clé privée en tant que 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 sur l'onglet client.

Téléchargez ou copiez les certificats client

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.

Téléchargez le fichier de certificat

Téléchargez le fichier de certificat `.pem`.

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`

Copier le 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 client

Si vous n'avez plus besoin d'un certificat de client administrateur, vous pouvez le supprimer.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**, puis sélectionnez l'onglet **client**.
2. Sélectionnez le certificat à 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**.

Après la suppression d'un certificat, les clients qui ont utilisé le certificat doivent spécifier un nouveau certificat client pour accéder à la base de données StorageGRID Prometheus.

Configurez les paramètres de sécurité

Gestion des règles TLS et SSH

La règle TLS et SSH détermine les protocoles et les chiffrements utilisés pour établir des connexions TLS sécurisées avec les applications client et des connexions SSH sécurisées avec les services StorageGRID internes.

La règle de sécurité contrôle la façon dont TLS et SSH chiffrent les données en mouvement. En général, utilisez la règle 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 le chiffrement inclus dans ces règles.

Avant de commencer

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

Sélectionnez une stratégie de sécurité

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **Paramètres de sécurité**.

   L'onglet **TLS et SSH policies** affiche les stratégies disponibles. La règle actuellement active est indiquée par une coche verte sur la vignette de la police.

2. Consultez les vignettes pour en savoir plus sur les stratégies disponibles.

Politique	Description
Compatibilité moderne (par défaut)	Utilisez la stratégie par défaut si vous avez besoin d'un cryptage fort et si vous ne disposez pas d'exigences particulières. Cette règle est compatible avec la plupart des clients TLS et SSH.
Compatibilité avec les systèmes existants	Utilisez cette stratégie si vous avez besoin d'options de compatibilité supplémentaires pour les anciens clients. Les options supplémentaires de cette politique pourraient la rendre moins sécurisée que la politique de compatibilité moderne.
Critères communs	Utilisez cette règle si vous avez besoin de la certification critères communs.
Norme FIPS stricte	Utilisez cette règle si vous avez besoin de la certification critères communs et que vous devez utiliser le module de sécurité cryptographique NetApp 3.0.8 pour les connexions de clients externes aux terminaux d'équilibrage de charge, au gestionnaire de locataires et au gestionnaire de grille. L'utilisation de cette règle peut réduire les performances. **Remarque** : après avoir sélectionné cette stratégie, tous les nœuds doivent être "redémarrés de manière mobile" pour activer le module de sécurité cryptographique NetApp. Utilisez **Maintenance** > **redémarrage en roulant** pour lancer et surveiller les redémarrages.
Personnalisées	Créez une stratégie personnalisée si vous devez appliquer vos propres chiffrements.

3. Pour afficher des détails sur les chiffrements, les protocoles et les algorithmes de chaque stratégie, sélectionnez **Afficher les détails**.
4. Pour modifier la stratégie actuelle, sélectionnez **utiliser la stratégie**.

   Une coche verte apparaît en regard de **police actuelle** sur la mosaïque de police.

Créez une stratégie de sécurité personnalisée

Vous pouvez créer une stratégie personnalisée si vous devez appliquer vos propres chiffrements.

Étapes

1. Dans la mosaïque de la stratégie la plus similaire à la stratégie personnalisée que vous souhaitez créer, sélectionnez **Afficher les détails**.
2. Sélectionnez **Copier dans le presse-papiers**, puis sélectionnez **Annuler**.

3. Dans la mosaïque **Personnaliser la stratégie**, sélectionnez **configurer et utiliser**.
4. Collez le fichier JSON que vous avez copié et apportez les modifications nécessaires.
5. Sélectionnez **utiliser la stratégie**.

   Une coche verte apparaît en regard de **politique actuelle** sur la mosaïque de stratégie personnalisée.

6. Si vous le souhaitez, sélectionnez **Modifier la configuration** pour apporter d'autres modifications à la nouvelle stratégie personnalisée.

Rétablir temporairement la stratégie de sécurité par défaut

Si vous avez configuré une stratégie de sécurité personnalisée, il se peut que vous ne puissiez pas vous connecter à Grid Manager si la stratégie TLS configurée est incompatible avec "certificat de serveur configuré".

Vous pouvez rétablir temporairement la stratégie de sécurité par défaut.

Étapes

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

      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 à Grid Manager sur le même nœud d'administration.
4. Suivez les étapes de la section Sélectionnez une stratégie de sécurité pour reconfigurer la stratégie.

Configurer la sécurité du réseau et des objets

Vous pouvez configurer la sécurité du réseau et des objets pour chiffrer les objets stockés, empêcher certaines requêtes S3 ou autoriser les connexions client aux nœuds de stockage à utiliser le protocole HTTP au lieu du protocole HTTPS.

Chiffrement des objets stockés

Le chiffrement des objets stockés permet de chiffrer toutes les données d'objet lors de leur ingestion via S3. Par défaut, les objets stockés ne sont pas chiffrés, mais vous pouvez choisir de chiffrer les objets à l'aide de l'algorithme de cryptage AES-128 ou AES-256. Lorsque vous activez le paramètre, tous les objets récemment acquis sont chiffrés, mais aucun changement n'est apporté 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 des objets stockés s'applique uniquement aux objets S3 qui n'ont pas été chiffrés par chiffrement au niveau du compartiment ou de l'objet.

Pour plus d'informations sur les méthodes de cryptage StorageGRID, reportez-vous à "Étudiez les méthodes de cryptage StorageGRID"la section .

Empêcher toute 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.

L'API REST S3

- Demandes DeleteBucket
- Toute demande de modification des données d'un objet existant, des métadonnées définies par l'utilisateur ou du balisage d'objets S3

Activez HTTP pour les connexions de nœud 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 autre que la production.

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 (parce que vous pouvez "configurez chaque point d'extrémité de l'équilibreur de charge"utiliser HTTP ou HTTPS).

Reportez-vous à la section "Résumé : adresses IP et ports pour les connexions client" pour connaître les ports utilisés par les clients S3 lors de la connexion aux nœuds de stockage via HTTP ou HTTPS.

Sélectionnez les options

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine.

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 **None** (par défaut) si vous ne souhaitez pas que les objets stockés soient cryptés, ou sélectionnez **AES-128** ou **AES-256** pour crypter les objets stockés.
4. Vous pouvez sélectionner **empêcher la modification du client** si vous voulez empêcher les clients S3 de faire des demandes spécifiques.

   Si vous modifiez ce paramètre, il faudra environ une minute pour appliquer le nouveau paramètre. La valeur configurée est mise en cache pour les performances et l'évolutivité.

5. Sélectionnez **Activer HTTP pour les connexions de noeud de stockage** si les clients se connectent directement aux noeuds de stockage et que vous souhaitez utiliser les connexions HTTP.

   Soyez prudent lorsque vous activez HTTP pour une grille de production car les requêtes seront envoyées de manière non chiffrée.

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 temps que spécifié et si une trace de pile est incluse dans les réponses d'erreur de l'API.

Avant de commencer

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

Description de la tâche

La page **Paramètres de sécurité** inclut les paramètres **délai d'inactivité du navigateur** et **trace de pile de l'API de gestion**.

Délai d'inactivité du navigateur dépassé

Indique la durée pendant laquelle le navigateur d'un utilisateur peut être inactif avant que l'utilisateur ne soit déconnecté. La valeur par défaut est 15 minutes.

Le délai d'inactivité du navigateur est également contrôlé par les éléments suivants :

- Un minuteur StorageGRID séparé 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'inactivité 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 la fonction SSO est activée et que le navigateur d'un utilisateur arrive à expiration, l'utilisateur doit saisir à nouveau ses informations d'identification SSO pour accéder à StorageGRID à nouveau. Voir "Configurer l'authentification unique".

Trace de la 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 pouvez 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 logiciels internes en cas d'erreurs d'API.

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 la période de temporisation, spécifiez une valeur comprise entre 60 secondes et 7 jours. Le délai par défaut est de 15 minutes.
   c. Pour désactiver cette fonction, décochez la case.
   d. Sélectionnez **Enregistrer**.

      Le nouveau paramètre n'affecte pas les utilisateurs qui sont actuellement connectés. Les utilisateurs doivent se reconnecter ou actualiser leur navigateur pour que le nouveau paramètre de délai d'attente prenne effet.
4. Pour modifier le paramètre de trace de pile de l'API de gestion :
   a. Développez l'accordéon.
   b. Cochez cette 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 logiciels internes en cas d'erreur d'API.

   c. Sélectionnez **Enregistrer**.

Configurer les serveurs de gestion des clés

Qu'est-ce qu'un serveur de gestion des clés (KMS) ?

Un serveur de gestion des 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 KMIP (Key Management Interoperability Protocol).

StorageGRID prend uniquement en charge certains serveurs de gestion des clés. Pour obtenir la liste des produits et versions pris en charge, utilisez le "Matrice d'interopérabilité NetApp (IMT)".

Vous pouvez utiliser un ou plusieurs serveurs de gestion des clés pour gérer les clés de cryptage de nœud pour tous les nœuds d'appliance StorageGRID dont le paramètre **Node Encryption** est activé pendant l'installation. L'utilisation de serveurs de gestion des clés avec ces nœuds de dispositif permet de protéger vos données même en cas de retrait d'une appliance du data Center. Une fois les volumes de l'appliance chiffrés, vous ne pouvez accéder aux données de l'appliance que si le nœud peut communiquer avec le KMS.

StorageGRID ne crée ni ne gère pas les clés externes utilisées pour chiffrer et décrypter les nœuds des systèmes. Si vous prévoyez d'utiliser un serveur de gestion externe des clés pour protéger les données StorageGRID, vous devez comprendre comment configurer ce serveur et savoir comment gérer les clés de cryptage. Ces instructions ne sont pas uniquement destinées à effectuer des tâches de gestion clés. Si vous avez besoin d'aide, consultez la documentation de votre serveur de gestion des clés ou contactez le support technique.

KM et configuration de l'appliance

Avant d'utiliser un serveur de gestion des clés (KMS) afin de 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 est automatique.

L'organigramme présente les étapes générales permettant d'utiliser un KMS pour sécuriser les données StorageGRID sur les nœuds du dispositif.

L'organigramme présente la configuration du KMS et l'appliance en parallèle. Toutefois, vous pouvez configurer les serveurs de gestion des clés avant ou après avoir activé le chiffrement des nœuds pour les nouveaux nœuds d'appliance, selon vos besoins.

Configuration du serveur de gestion des clés (KMS)

La configuration d'un serveur de gestion des clés comprend les étapes générales suivantes.

Étape	Reportez-vous à la section
Accédez au logiciel KMS et ajoutez un client pour StorageGRID à chaque cluster KMS ou KMS.	"Configurer StorageGRID en tant que client dans le KMS"
Obtenir les informations requises pour le client StorageGRID sur le KMS.	"Configurer StorageGRID en tant que client dans le KMS"
Ajoutez le KMS à Grid Manager, attribuez-le à un seul site ou à un groupe de sites par défaut, téléchargez les certificats requis et enregistrez la configuration KMS.	"Ajout d'un serveur de gestion des clés (KMS)"

Configurez l'appareil

La configuration d'un nœud d'appliance pour l'utilisation de KMS comprend les étapes générales suivantes.

1. Pendant l'étape de configuration matérielle de l'installation de l'appliance, utilisez le programme d'installation de l'appliance StorageGRID pour activer le paramètre **Node Encryption** pour l'appliance.

Vous ne pouvez pas activer le paramètre **Node Encryption** après l'ajout d'une appliance à la grille, et vous ne pouvez pas utiliser la gestion de clés externe pour les appliances pour lesquelles 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 aléatoire des données (DEK) est attribuée à chaque volume de dispositif, comme suit :
   - Les clés de licence sont utilisées pour chiffrer les données sur chaque volume. Ces clés sont générées à l'aide du chiffrement de disque LUKS (Unified Key Setup) Linux dans le système d'exploitation de l'appliance et ne peuvent pas être modifiées.
   - Chaque DEK individuel est chiffré par une clé de cryptage principale (KEK). La KEK initiale est une clé temporaire qui chiffre les clés de fin de séjour jusqu'à ce que l'appareil puisse se connecter au KMS.
3. Ajoutez le nœud d'appliance à StorageGRID.

Voir "Activez le chiffrement de nœud" pour plus de détails.

Processus de chiffrement de la gestion des clés (automatique)

Le chiffrement de la gestion des clés inclut les étapes générales suivantes qui sont automatiquement effectuées.

1. Lorsque vous installez une appliance sur laquelle le chiffrement de nœud est activé dans le grid, 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 de l'appliance continuent d'être cryptées 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'appliance utilise la configuration KMS pour vous connecter au KMS et demander une clé de chiffrement.
3. Le KMS envoie une clé de chiffrement à l'appliance. La nouvelle clé du KMS remplace la KEK temporaire et est maintenant utilisée pour crypter et décrypter les clés de fin de séjour des volumes d'appliance.

> ⚠ Toutes les données qui existent avant que le nœud d'appliance chiffré ne se connecte au KMS configuré sont chiffrées à l'aide d'une clé temporaire. Cependant, les volumes de l'appliance ne doivent pas être considérés comme protégés de leur retrait du data Center tant que la clé temporaire n'est pas remplacée par la clé de cryptage KMS.

4. Si l'appliance est sous tension ou redémarrée, elle se reconnecte au KMS pour demander la clé. La clé, enregistrée dans la mémoire volatile, ne peut pas survivre à une perte de puissance ou à un redémarrage.

Considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés

Avant de configurer un serveur de gestion des clés externe (KMS), vous devez connaître les considérations et les exigences requises.

Quelle version de KMIP est prise en charge ?

StorageGRID prend en charge KMIP version 1.4.

"Spécification du protocole d'interopérabilité de gestion des clés version 1.4"

Quelles sont les considérations relatives au réseau ?

Les paramètres de pare-feu réseau doivent permettre à chaque nœud de l'appliance de communiquer via le port utilisé pour les communications 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 cluster KMS ou KMS que vous avez configuré pour le site.

Quelles sont les versions de TLS prises en charge ?

Les communications entre les nœuds d'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 des éléments pris en charge par KMS et que "Règles 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 lors de la connexion. Pour connaître les versions de protocole et les suites de chiffrement/chiffrement disponibles, consultez la `tlsOutbound` section de la stratégie TLS et SSH active de la grille (**CONFIGURATION** > **sécurité Paramètres de sécurité**).

Quels dispositifs sont pris en charge ?

Vous pouvez utiliser un serveur de gestion des clés (KMS) pour gérer les clés de cryptage de n'importe quelle appliance StorageGRID de la grille dont le paramètre **Node Encryption** est activé. Ce paramètre ne peut être activé que lors de l'étape de configuration matérielle de l'installation de l'appliance à l'aide du programme d'installation de l'appliance StorageGRID.

> ⓘ Le chiffrement des nœuds ne peut pas être activé après l'ajout d'une appliance à la grille. De plus, vous ne pouvez pas utiliser la gestion externe des clés pour les appliances pour lesquelles le chiffrement des nœuds n'est pas activé.

Vous pouvez utiliser le KMS configuré pour les appliances et les nœuds StorageGRID.

Vous ne pouvez pas utiliser le KMS configuré pour les nœuds logiciels (non liés à l'appliance) :

- Nœuds déployés en tant que machines virtuelles
- Nœuds déployés dans les moteurs de mise en conteneurs sur les hôtes Linux

Les nœuds déployés sur ces autres plateformes peuvent utiliser le cryptage en dehors de StorageGRID au niveau du datastore ou du disque.

Quand dois-je configurer les serveurs de gestion des clés ?

Dans le cadre d'une nouvelle installation, vous devez généralement configurer un ou plusieurs serveurs de gestion des clés dans Grid Manager avant de créer des locataires. Cette commande garantit que les nœuds sont protégés avant que des données d'objet ne soient stockées sur ces nœuds.

Vous pouvez configurer les serveurs de gestion des clés dans Grid Manager avant ou après l'installation des nœuds de l'appliance.

Combien de serveurs de gestion des clés ai-je besoin ?

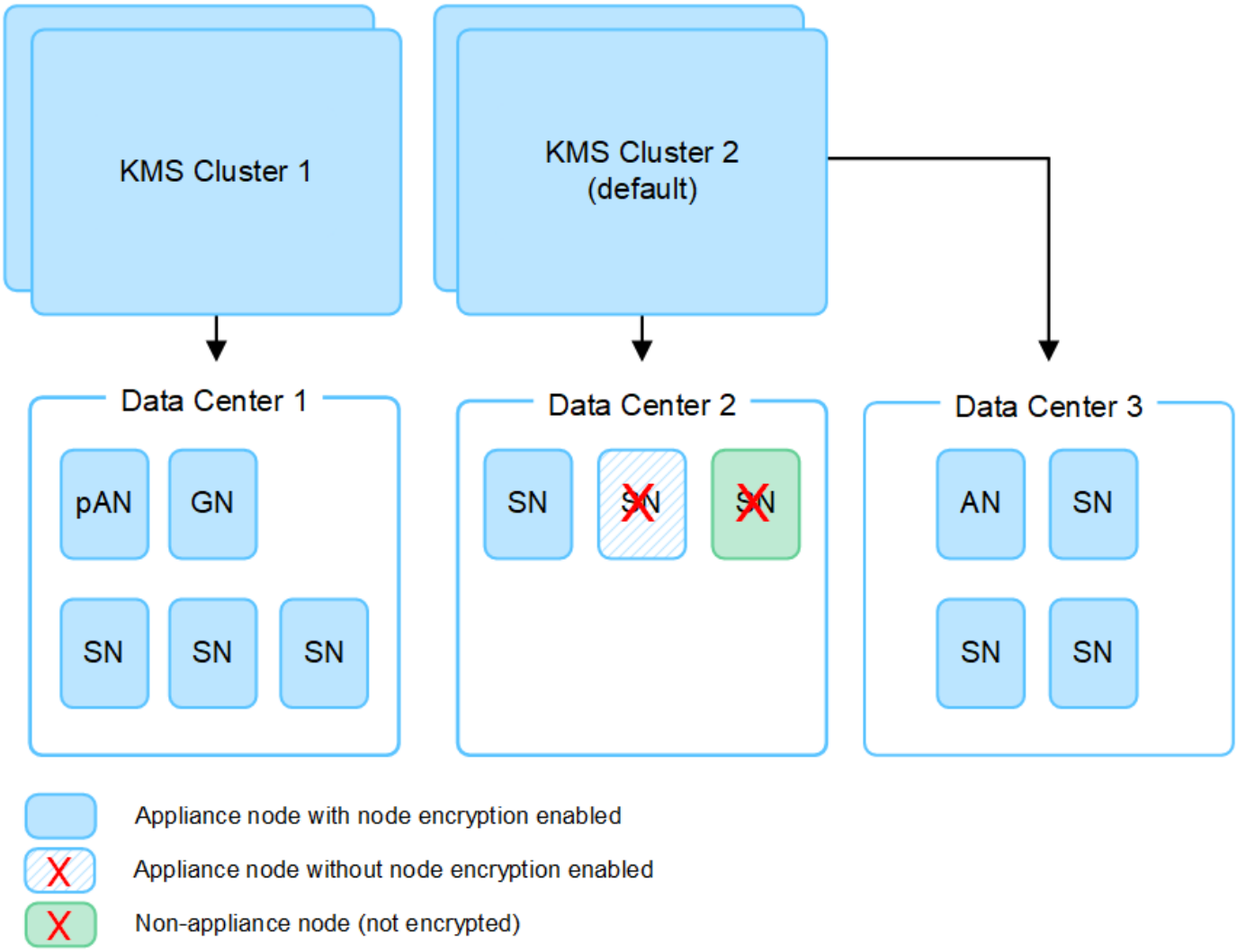
Vous pouvez configurer un ou plusieurs serveurs de gestion externe des clés de chiffrement pour les nœuds d'appliance de votre système StorageGRID. Chaque KMS fournit une clé de chiffrement unique aux nœuds d'appliance StorageGRID sur un seul site ou dans un groupe de sites.

StorageGRID prend en charge l'utilisation des clusters KMS. Chaque cluster KMS contient plusieurs serveurs de gestion des 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 il améliore les fonctionnalités de

basculement d'une configuration haute disponibilité.

Supposons par exemple que votre système StorageGRID possède trois sites de data Center. Vous pouvez configurer un cluster KMS pour que tous les nœuds d'appliance soient essentiels dans le Data Center 1 et un second cluster KMS pour que ces derniers soient essentiels pour que tous les nœuds d'appliance soient disponibles sur les autres sites. Lorsque vous ajoutez le second cluster KMS, vous pouvez configurer un KMS par défaut pour Data Center 2 et Data Center 3.

Notez que vous ne pouvez pas utiliser de KMS pour les nœuds non liés à l'appliance ou pour les nœuds d'appliance sur lesquels le paramètre **Node Encryption** n'a pas été activé lors de l'installation.



Que se passe-t-il lorsqu'une clé est tournée ?

En tant que pratique exemplaire en matière de sécurité, vous devez régulièrement "faites pivoter la clé de cryptage" utiliser chaque KMS configuré.

Lorsque la nouvelle version de clé est disponible :

- Elle est automatiquement distribuée aux nœuds d'appliance chiffrés sur le site ou les sites associés au KMS. La distribution doit se produire dans une heure après la rotation de la clé.
- Si le nœud d'appliance chiffré est hors ligne lorsque la nouvelle version de clé est distribuée, le nœud reçoit la nouvelle clé dès le 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 **Echec 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 afin de résoudre cette alerte.

Puis-je réutiliser un nœud d'appliance après chiffrement ?

Si vous devez installer une appliance chiffrée dans un autre système StorageGRID, vous devez d'abord désactiver le nœud de grille pour déplacer les données d'objet vers un autre nœud. Vous pouvez ensuite utiliser le programme d'installation de l'appliance StorageGRID pour "Effacez la configuration KMS". L'effacement de la configuration KMS désactive le paramètre **Node Encryption** et supprime l'association entre le nœud de l'appliance et la configuration KMS pour le site StorageGRID.

> Étant donnée l'accès à la clé de chiffrement KMS, toutes les données conservées sur l'appliance ne sont plus accessibles et sont verrouillées en permanence.

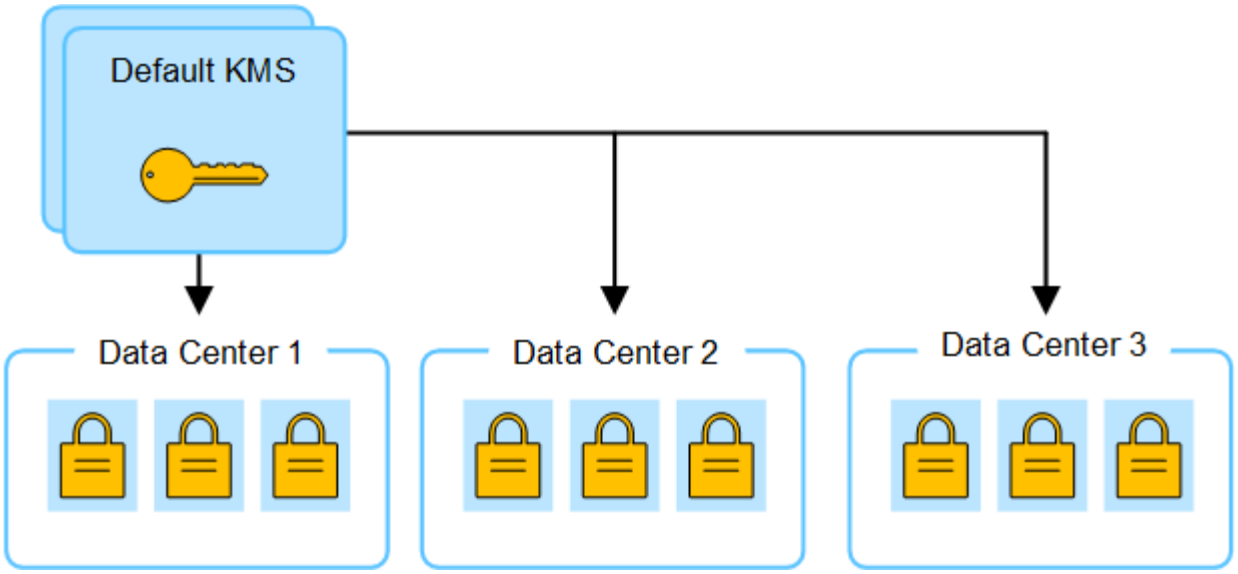
Considérations relatives à la modification du KMS pour un site

Chaque cluster de serveur de gestion des clés (KMS) ou KMS fournit une clé de chiffrement à tous les nœuds d'appliance sur un site unique ou dans 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 vers un autre.

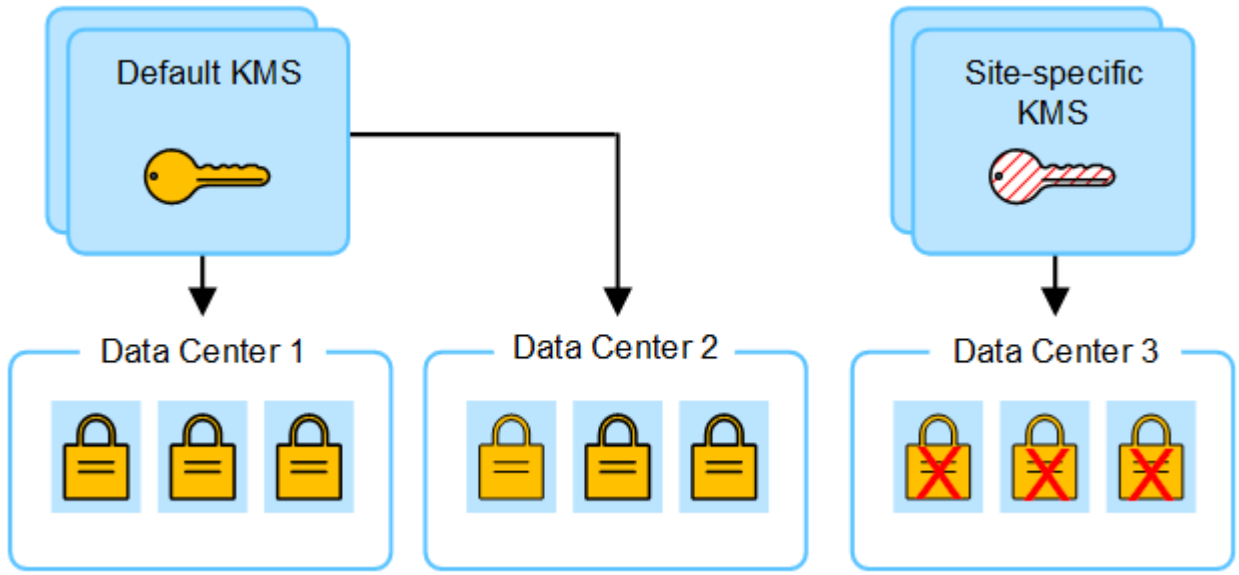
Si vous modifiez le KMS utilisé pour un site, vous devez vous assurer que les nœuds d'appliance précédemment cryptés de ce site peuvent être déchiffrés à l'aide de la clé stockée sur le nouveau KMS. Dans certains cas, vous devrez peut-être copier la version actuelle de la clé de chiffrement à partir du KMS d'origine vers le nouveau KMS. Vous devez vous assurer que le KMS dispose de la clé correcte pour décrypter les nœuds de l'appliance chiffrée sur le site.

Par exemple :

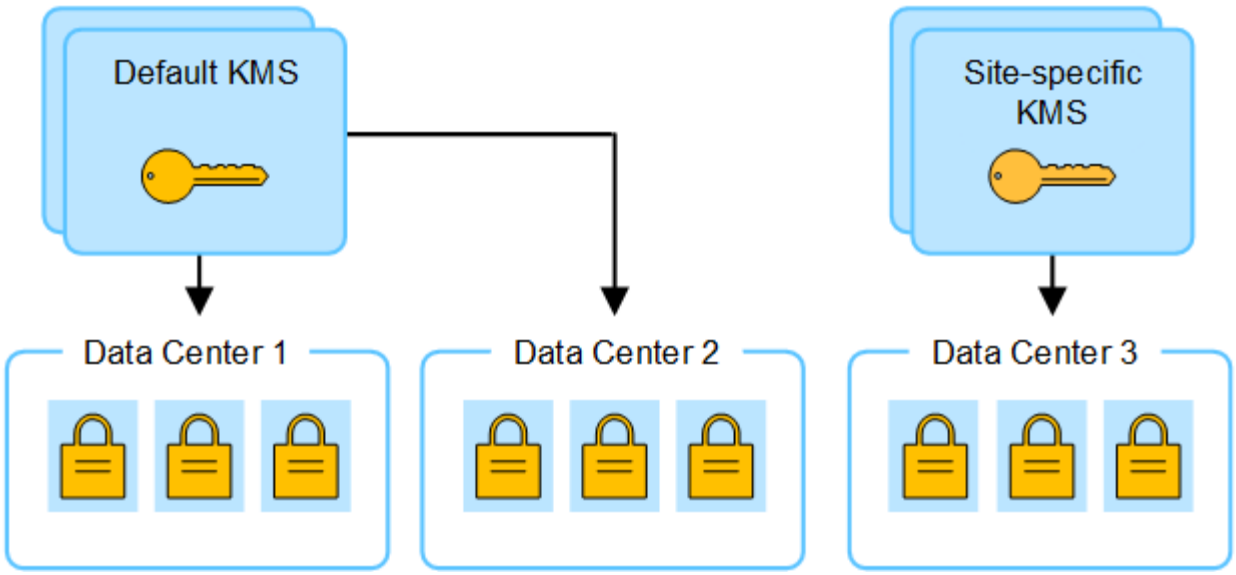
1. Vous configurez initialement un KMS par défaut qui s'applique à tous les sites qui ne disposent pas d'un KMS dédié.
2. Lorsque le KMS est enregistré, tous les nœuds de l'appliance dont le paramètre **Node Encryption** est activé se connectent au KMS et demandent la clé de chiffrement. Cette clé est utilisée pour chiffrer les nœuds de l'appliance sur tous les sites. Cette même clé doit également être utilisée pour décrypter ces dispositifs.



3. Vous décidez d'ajouter un KMS spécifique au site pour un site (Data Center 3 dans la figure). Toutefois, les nœuds d'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 décrypter les nœuds de ce site.



4. Pour résoudre ce problème, vous copiez la version actuelle de la clé de chiffrement à partir du KMS par défaut vers le nouveau KMS. (Techniquement, vous copiez la clé d'origine dans 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 appropriée pour décrypter les nœuds de l'appliance sur le data Center 3, afin que ces nœuds puissent être enregistrés dans StorageGRID.



Cas d'utilisation pour changer quel KMS est utilisé pour un site

Le tableau résume les étapes requises pour les cas les plus courants de modification du KMS pour un site.

Cas d'utilisation lors de la modification du KMS d'un site	Étapes requises
Vous avez une ou plusieurs entrées KMS spécifiques au site, et vous souhaitez utiliser l'une d'entre elles comme étant le KMS par défaut.	Modifiez le KMS spécifique au site. Dans le champ **gère clés pour**, sélectionnez **sites non gérés par un autre KMS (KMS par défaut)**. Le KMS spécifique au site sera maintenant utilisé comme KMS par défaut. Il s'appliquera à tous les sites qui n'ont pas de KMS dédié. "Modification d'un serveur de gestion des clés (KMS)"
Vous avez 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 d'appliance du 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 à partir du KMS par défaut vers un nouveau KMS. 2. À l'aide de Grid Manager, ajoutez le nouveau KMS et sélectionnez le site. "Ajout d'un serveur de gestion des clés (KMS)"
Vous souhaitez que le KMS pour un site utilise un serveur différent.	1. Si les nœuds d'appliance du site ont déjà été chiffrés par le KMS existant, utilisez le logiciel KMS pour copier la version actuelle de la clé de chiffrement à partir du KMS existant vers le nouveau KMS. 2. À l'aide de Grid Manager, modifiez la configuration KMS existante et entrez le nouveau nom d'hôte ou l'adresse IP. "Ajout d'un serveur de gestion des clés (KMS)"

Configurer StorageGRID en tant que client dans le KMS

Vous devez configurer StorageGRID en tant que client pour chaque serveur de gestion

externe des clés ou cluster KMS avant de pouvoir ajouter le KMS à StorageGRID.

> Ces instructions s'appliquent à Thales CipherTrust Manager et à Hashicorp Vault. Pour obtenir la liste des produits et versions pris en charge, utilisez le "Matrice d'interopérabilité NetApp (IMT)".

Étapes

1. À partir du logiciel KMS, créez un client StorageGRID pour chaque cluster KMS ou KMS que vous souhaitez utiliser.

   Chaque KMS gère une clé de chiffrement unique pour les nœuds d'appliances StorageGRID dans un seul site ou dans un groupe de sites.

2. Créez une clé à l'aide de 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 cluster KMS ou 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 lorsque vous testez et enregistrez après "téléchargement de certificats client".
3. Notez les informations suivantes pour chaque cluster KMS ou 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 cryptage dans le KMS.
4. Pour chaque cluster KMS ou KMS, procurez-vous un certificat de serveur signé par une autorité de certification (CA) ou un bundle de certificats contenant chacun des fichiers de certificat d'autorité de certification codés au 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 encodé au format PEM (Privacy Enhanced Mail) Base-64.
   - Le champ Subject alternative Name (SAN) de chaque certificat de serveur doit inclure le nom de domaine complet (FQDN) ou l'adresse IP à laquelle StorageGRID se connectera.

     > Lorsque vous configurez le KMS dans StorageGRID, vous devez entrer les mêmes FQDN ou adresses IP dans le champ **Hostname**.

   - Le certificat du serveur doit correspondre au certificat utilisé par l'interface KMIP du KMS, qui utilise généralement le port 5696.
5. Obtenir le certificat du client public délivré à StorageGRID par le KMS externe et la clé privée du certificat du client.

   Le certificat client permet à StorageGRID de s'authentifier auprès du KMS.

Ajout d'un serveur de gestion des clés (KMS)

L'assistant de serveur de gestion des clés StorageGRID vous permet d'ajouter chaque cluster KMS ou KMS.

Avant de commencer

- Vous avez examiné le "considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés".
- Vous avez "Configuration de StorageGRID en tant que client dans le KMS"et vous avez les informations requises pour chaque cluster KMS ou KMS.
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine".

Description de la 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, toutes les appliances chiffrées par nœud dans le grid seront chiffrées 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 à partir du KMS par défaut vers le nouveau KMS. Voir "Considérations relatives à la modification du KMS pour un site" pour plus de détails.

Étape 1 : détails KM

À l'étape 1 (détails KMS) de l'assistant Add a Key Management Server (Ajouter un serveur de gestion des clés), vous fournissez des informations sur le cluster KMS ou KMS.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **serveur de gestion des clés**.

   La page serveur de gestion des clés s'affiche avec l'onglet Détails de la configuration sélectionné.

2. Sélectionnez **Créer**.

   L'étape 1 (détails KMS) de l'assistant Add a Key Management Server (Ajouter un serveur de gestion des clés) s'affiche.

3. Entrez 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	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 des 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 gère 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 n'ont pas de KMS dédié et à tous les sites que vous ajoutez dans les extensions suivantes. **Remarque :** Une erreur de validation se produit lorsque vous enregistrez la configuration KMS si vous sélectionnez un site qui a été précédemment crypté par le KMS par défaut, mais que vous n'avez pas fourni la version actuelle de la clé de cryptage d'origine au nouveau KMS.
Port	Le port utilisé par le serveur KMS pour les communications KMIP (Key Management Interoperability Protocol). 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 Subject alternative Name (SAN) du certificat de serveur doit inclure le nom de domaine complet ou l'adresse IP que vous entrez 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 de serveur) de l'assistant Ajouter un serveur de gestion des clés, vous téléchargez le certificat de serveur (ou le paquet de certificats) pour le KMS. Le certificat du serveur permet au KMS externe de s'authentifier auprès de StorageGRID.

Étapes

1. A partir de **Etape 2 (Télécharger le certificat de serveur)**, accédez à l'emplacement du certificat de serveur ou du paquet de certificats enregistré.
2. Téléchargez le fichier de certificat.

   Les métadonnées du certificat de serveur s'affichent.

   Si vous avez téléchargé un ensemble de certificats, les métadonnées de chaque certificat s'affichent sur son propre onglet.

3. Sélectionnez **Continuer**.

étape 3 : téléchargement des certificats client

À l'étape 3 (Téléchargement de certificats client) de l'assistant Ajouter un serveur de gestion des 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. A partir de **Etape 3 (Téléchargement de certificats client)**, naviguez jusqu'à l'emplacement du certificat client.
2. Téléchargez le fichier de certificat client.

   Les métadonnées du certificat client s'affichent.

3. Accédez à l'emplacement de la clé privée pour le certificat client.
4. Téléchargez le fichier de clé privée.
5. Sélectionnez **Tester et enregistrer**.

   Si aucune clé n'existe, vous êtes invité à en créer une par StorageGRID.

   Les connexions entre le serveur de gestion des clés et les nœuds de dispositif sont testées. Si toutes les connexions sont valides et que la clé correcte est trouvée sur le KMS, le nouveau serveur de gestion des clés est ajouté à la table de la page serveur de gestion des clés.

   > Immédiatement après l'ajout d'un KMS, l'état du certificat sur la page Key Management Server apparaît comme inconnu. Le statut réel de chaque certificat peut prendre jusqu'à 30 minutes pour StorageGRID. Vous devez actualiser votre navigateur Web pour voir l'état actuel.

6. Si un message d'erreur s'affiche lorsque vous sélectionnez **Test and save**, vérifiez les détails du message, puis sélectionnez **OK**.

   Par exemple, vous pourriez recevoir une erreur 422 : entité impossible à traiter 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 elle ne teste pas la connexion externe de chaque appliance à ce KMS. En cas de problème avec la configuration, vous ne pouvez pas redémarrer les nœuds d'appliance pour lesquels le chiffrement de nœud est activé sur le site affecté. L'accès à vos données risque d'être perdu jusqu'à la résolution des problèmes.

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 des 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 Gestionnaire de grille 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 des clés (KMS) de votre système StorageGRID, y compris les détails des clés et l'état actuel des certificats du serveur et du client.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **serveur de gestion des clés**.

   La page serveur de gestion des clés s'affiche et affiche les informations suivantes :

   - L'onglet Détails de la configuration répertorie tous les serveurs de gestion des clés configurés.
   - L'onglet nœuds cryptés répertorie tous les nœuds sur 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	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 des clés, le nom de domaine complet ou l'adresse IP des deux serveurs sont répertoriés. S'il y a plus de deux serveurs de gestion des 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 des 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'hôte d'une grappe, sélectionnez un KMS et sélectionnez **Modifier** ou **actions** > **Modifier**.

3. Sélectionnez un onglet sur la page de détails KMS pour afficher les informations suivantes :

Onglet	Champ	Description
Détails clés	Nom de la clé	Alias de clé pour le client StorageGRID dans le KMS.
UID de clé	Identifiant unique de la dernière version de la clé.	Dernière modification
Date et heure de la dernière version de la clé.	Certificat de serveur	Les métadonnées
Métadonnées du certificat, telles que le numéro de série, la date et l'heure d'expiration et le PEM du certificat.	Certificat PEM	Contenu du fichier PEM (Privacy Enhanced mail) du certificat.
Certificat client	Les métadonnées	Métadonnées du certificat, telles que le numéro de série, la date et l'heure d'expiration et le PEM du certificat.

4. [[clé de rotation]]aussi souvent que requis par les pratiques de sécurité de votre organisation, sélectionnez **clé de rotation**, ou utilisez le logiciel KMS, pour créer une nouvelle version de la clé.

   Lorsque la rotation de la clé a réussi, 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 complètement différente.

   Ne tentez jamais de faire pivoter une clé en modifiant le nom de clé (alias) du KMS. StorageGRID nécessite que toutes les versions de clés déjà utilisées (ainsi que toutes les versions à venir) soient accessibles depuis le KMS avec le même alias de clé. Si vous modifiez l'alias de clé pour un KMS configuré, StorageGRID risque de ne pas être en mesure de décrypter vos données.

Gérer les certificats

Répondez rapidement à tous les problèmes de certificat de serveur ou de client. Si possible, remplacez les certificats avant qu'ils n'expirent.

Vous devez corriger 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, examinez 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 qu'il est sur le point d'expirer, sélectionnez KMS pour accéder à la page de détails 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 du certificat serveur.
5. Lorsque les alertes **KMS CA Certificate expiration**, **KMS client Certificate expiration** et **KMS Server Certificate expiration** sont déclenchées, notez la description de chaque alerte et effectuez les actions recommandées.

   StorageGRID peut prendre 30 minutes pour obtenir les mises à jour de l'expiration du certificat. Actualisez votre navigateur Web pour afficher les valeurs actuelles.

> Si vous obtenez un état de **l'état du certificat du serveur est inconnu**, assurez-vous que votre KMS permet d'obtenir un certificat du serveur sans exiger 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 **Node Encryption** est activé.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **serveur de gestion des clés**.

   La page Key Management Server s'affiche. L'onglet Détails de la configuration affiche tous les serveurs de gestion des clés qui ont été configurés.

2. En haut de la page, sélectionnez l'onglet **encrypted nodes**.

   L'onglet noeuds cryptés répertorie les noeuds de l'appliance de votre système StorageGRID sur lesquels le paramètre **chiffrement de noeud** est activé.

3. Vérifiez les informations du tableau pour chaque nœud d'appliance.

Colonne	Description
Nom du nœud	Nom du nœud d'appliance.
Type de nœud	Le type de nœud : stockage, Administrateur ou passerelle.
Le site	Nom du site StorageGRID sur lequel le nœud est installé.
Nom du KMS	Nom descriptif du KMS utilisé pour le nœud. Si aucun KMS n'est répertorié, sélectionnez l'onglet Détails de la configuration pour ajouter un KMS. "Ajout d'un serveur de gestion des clés (KMS)"

Colonne	Description
UID de clé	ID unique de la clé de cryptage utilisée pour crypter et décrypter les données sur le nœud de l'appliance. Pour afficher un UID de clé entier, sélectionnez le texte. Un tiret (--) indique que l'UID de clé est inconnu, peut-être en raison d'un problème de connexion entre le nœud de l'appliance et le KMS.
État	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 connexion peut prendre plusieurs minutes après la modification de la configuration KMS. **Remarque :** Rafraîchir votre navigateur Web pour voir les nouvelles valeurs.

4. Si la colonne État indique un problème KMS, répondez immédiatement au problème.

   Pendant les opérations KMS normales, l'état sera **connecté à KMS**. Si un nœud est déconnecté de la grille, l'état de connexion du nœud est affiché (administrativement arrêté ou inconnu).

   Les autres messages d'état correspondent aux alertes StorageGRID portant le même nom :

   - Echec du chargement de la configuration DES KMS
   - Erreur de connectivité KMS
   - Nom de la clé de cryptage KMS introuvable
   - Echec de la rotation de la clé de chiffrement KMS
   - La clé KMS n'a pas réussi à décrypter un volume d'appliance
   - LES KMS ne sont pas configurés

   Effectuez les actions recommandées pour ces alertes.

> Vous devez immédiatement résoudre tout problème pour assurer la protection intégrale de vos données.

Modifier un KMS

Vous devrez peut-être modifier la configuration d'un serveur de gestion des clés, par exemple si un certificat est sur le point d'expirer.

Avant de commencer

- Si vous prévoyez de mettre à jour le site sélectionné pour un KMS, vous avez examiné le "Considérations relatives à la modification du KMS pour un site".
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine".

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **serveur de gestion des clés**.

La page serveur de gestion des clés s'affiche et affiche tous les serveurs de gestion des clés qui ont été configurés.

2. Sélectionnez le KMS à modifier, puis sélectionnez **actions** > **Modifier**.

   Vous pouvez également modifier un KMS en sélectionnant le nom KMS dans la table et en sélectionnant **Modifier** sur la page de détails KMS.

3. Vous pouvez également mettre à jour les détails dans **Etape 1 (détails KMS)** de l'assistant Modifier un serveur de gestion des 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	Alias de clé exact pour le client StorageGRID dans le KMS. Doit comporter entre 1 et 255 caractères. Il vous suffit de modifier le nom de la clé 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 KMIP (Key Management Interoperability Protocol). 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 Subject alternative Name (SAN) du certificat de serveur doit inclure le nom de domaine complet ou l'adresse IP que vous entrez 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 de serveur) de l'assistant Modifier un serveur de gestion des clés s'affiche.

6. Si vous devez remplacer le certificat de serveur, sélectionnez **Parcourir** et téléchargez le nouveau fichier.
7. Sélectionnez **Continuer**.

   L'étape 3 (Téléchargement de certificats client) de l'assistant Modifier un serveur de gestion des 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'appliance chiffrés sur les sites affectés sont testées. Si toutes les connexions de nœud sont valides et que la clé correcte est trouvée sur le KMS, le serveur de gestion des clés est ajouté à la table de la page Key Management Server.

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 impossible à traiter 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 elle ne teste pas la connexion externe de chaque appliance à ce KMS. En cas de problème avec la configuration, vous ne pouvez pas redémarrer les nœuds d'appliance pour lesquels le chiffrement de nœud est activé sur le site affecté. L'accès à vos données risque d'être perdu jusqu'à la résolution des problèmes.

    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.

Suppression d'un serveur de gestion des clés (KMS)

Dans certains cas, vous pouvez supprimer un serveur de gestion des clés. Par exemple, vous pouvez vouloir supprimer un KMS spécifique au site si vous avez désactivé le site.

Avant de commencer

- Vous avez examiné le "considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés".
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine".

Description de la tâche

Vous pouvez supprimer un KMS dans les cas suivants :

- Vous pouvez supprimer un KMS spécifique au site si le site a été désactivé ou si le site ne contient aucun nœud d'appliance lorsque le chiffrement de nœud est activé.

- Vous pouvez supprimer le KMS par défaut si un KMS spécifique au site existe déjà pour chaque site sur lequel des nœuds d'appliance sont activés pour que le chiffrement des nœuds soit activé.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **serveur de gestion des clés**.

   La page serveur de gestion des clés s'affiche et affiche tous les serveurs de gestion des clés qui ont été configurés.

2. Sélectionnez le KMS à supprimer, puis sélectionnez **actions** > **Supprimer**.

   Vous pouvez également supprimer un KMS en sélectionnant le nom KMS dans la table et en sélectionnant **Supprimer** dans la page de détails KMS.

3. Vérifiez que ce qui suit est vrai :
   - Vous supprimez un KMS spécifique au site pour un site qui n'a aucun nœud d'appliance pour lequel le chiffrement des nœuds est activé.
   - Vous supprimez le KMS par défaut, mais un KMS spécifique au site existe déjà pour chaque site avec chiffrement des nœuds.
4. Sélectionnez **Oui**.

   La configuration KMS est supprimée.

Gérer les paramètres 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 terminaux S3 externes. Par exemple, vous aurez peut-être besoin d'un proxy non transparent pour permettre l'envoi de messages de services de plate-forme vers des noeuds finaux externes, tels qu'un noeud final sur Internet.

> Les paramètres configurés du proxy de stockage ne s'appliquent pas aux terminaux des services de la plateforme Kafka.

Avant de commencer

- Vous avez "autorisations d'accès spécifiques".
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".

Description de la 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 du proxy de stockage.
4. Entrez le nom d'hôte ou l'adresse IP du serveur proxy.

5. Vous pouvez également saisir le port utilisé pour vous connecter au serveur proxy.

   Laissez ce champ vide pour utiliser le port par défaut du protocole : 80 pour HTTP ou 1080 pour SOCKS5.

6. Sélectionnez **Enregistrer**.

   Une fois le proxy de stockage enregistré, il est possible de configurer et de tester de nouveaux terminaux pour les services de plateforme ou les pools de stockage cloud.

   > Les modifications de proxy peuvent prendre jusqu'à 10 minutes.

7. Vérifiez les paramètres de votre serveur proxy pour vous assurer que les messages relatifs au service de la plate-forme 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 "Configurez AutoSupport".

Avant de commencer

- Vous avez "autorisations d'accès spécifiques".
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".

Description de la tâche

Vous pouvez configurer les paramètres d'un proxy d'administration unique.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **Paramètres proxy**.

   La page Paramètres proxy s'affiche. Par défaut, l'option stockage est sélectionnée dans le menu de l'onglet.

2. Sélectionnez l'onglet **Admin**.
3. Cochez la case **Activer le proxy Admin**.
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 requiert 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 d'administration, sélectionnez **vérifier le certificat proxy**. Téléchargez un paquet CA pour vérifier l'authenticité des certificats SSL présentés par le serveur proxy d'administration.

AutoSupport On Demand, E-Series AutoSupport via StorageGRID et la détermination du chemin de mise à jour sur la page mise à niveau StorageGRID ne fonctionneront pas si un certificat proxy est vérifié.

Une fois le paquet 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.

9. Si vous devez désactiver le proxy admin, décochez la case **Activer le proxy Admin**, puis sélectionnez **Enregistrer**.

Contrôle des pare-feu

Contrôler l'accès au niveau du 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 des nœuds d'administration StorageGRID en ouvrant ou en fermant des ports spécifiques au pare-feu externe. Par exemple, vous pouvez empêcher les locataires de se connecter à 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, reportez-vous à la section "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 d'API de gestion peuvent accéder à Grid Manager, à l'API de gestion du grid, au gestionnaire des locataires et à l'API de gestion des locataires. **Remarque :** le port 443 est également utilisé pour un trafic interne.
8443	Port restreint de Grid Manager sur les nœuds d'administration	• Les navigateurs Web et les clients d'API de gestion peuvent accéder à Grid Manager et à l'API de gestion Grid via HTTPS. • Les navigateurs Web et les clients de l'API de gestion ne peuvent pas accéder au gestionnaire de locataires ou à l'API de gestion des locataires. • Les demandes de contenu interne seront rejetées.

Port	Description	Si le port est ouvert…
9443	Port de gestionnaire de locataires restreint sur les nœuds d'administration	• Les navigateurs Web et les clients d'API de gestion peuvent accéder au Gestionnaire de locataires et à l'API de gestion des locataires via HTTPS. • Les navigateurs Web et les clients API de gestion ne peuvent pas accéder à Grid Manager ou à l'API Grid Management. • Les demandes de contenu interne seront rejetées.

L'authentification unique (SSO) n'est pas disponible sur les ports du gestionnaire de grille restreinte ou du gestionnaire de locataires. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec une connexion unique.

Informations associées

- "Connectez-vous au Grid Manager"
- "Créer un compte de locataire"
- "Communications externes"

Gérer les contrôles de pare-feu internes

StorageGRID comprend 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 effectuées 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 indiquer 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 accepte uniquement les connexions sur les ports de point final de l'équilibreur de charge configurés sur ce nœud (points finaux globaux, liés à l'interface de nœud et au type de nœud).
  - Les ports de point final 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.
  - Une fois approuvés, tous les ports ouverts sous l'onglet gérer l'accès externe sont accessibles, ainsi

que tous les noeuds finaux d'équilibrage de charge ouverts sur le réseau client.

> Les paramètres que vous effectuez sur un onglet peuvent affecter les modifications d'accès que vous effectuez sur un autre onglet. Vérifiez les paramètres de tous les onglets pour vous assurer que votre réseau se comporte comme vous le souhaitez.

Pour configurer les contrôles de pare-feu internes, reportez-vous à la section "Configurer les contrôles de pare-feu".

Pour plus d'informations sur les pare-feu externes et la sécurité réseau, reportez-vous à la section "Contrôler l'accès au niveau du 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 qui ont accès aux ports de la grille fermés. 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-grid). Ces deux onglets peuvent souvent être utilisés ensemble pour personnaliser l'accès réseau exact dont vous avez besoin pour votre grille.

> Par défaut, les adresses IP privilégiées n'ont pas d'accès au port de la grille interne.

Exemple 1 : utilisez un hôte de secours pour les tâches de maintenance

Supposons que vous souhaitiez utiliser un hôte de secours (un hôte renforcé par la sécurité) pour l'administration du réseau. Vous pouvez utiliser les étapes générales suivantes :

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 à moins que leur adresse IP n'ait 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 secours pour effectuer des tâches de maintenance sur votre grille de manière plus sécurisée.

Exemple 2 : verrouiller les ports sensibles

Supposons que vous souhaitez 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 aux ports affectés à Grid Manager et au gestionnaire de locataires (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 à moins que leur adresse IP n'ait 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'origine de 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 pouvez utiliser la 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 protéger StorageGRID des attaques hostiles en acceptant le trafic client entrant uniquement sur les noeuds finaux configurés explicitement.

Par défaut, le réseau client sur chaque nœud de la grille est *Trusted*. C'est-à-dire, par défaut, StorageGRID approuve les connexions entrantes à chaque nœud de grille sur tous "ports externes disponibles".

Vous pouvez réduire la menace d'attaques hostiles sur votre système StorageGRID en spécifiant que le réseau client sur chaque nœud est *non fiable*. Si le réseau client d'un nœud n'est pas fiable, le nœud accepte uniquement les connexions entrantes sur les ports explicitement configurés en tant que points finaux d'équilibreur de charge. Voir "Configurer les terminaux de l'équilibreur de charge" et "Configurer les contrôles de pare-feu".

Exemple 1 : le nœud de passerelle n'accepte que les requêtes HTTPS S3

Supposons que vous souhaitiez qu'un nœud de passerelle refuse tout trafic entrant sur le réseau client, à l'exception des requêtes HTTPS S3. Vous devez effectuer les étapes générales suivantes :

1. À partir de la "Terminaux d'équilibrage de charge" page, configurez un terminal d'équilibreur de charge pour S3 sur HTTPS sur le port 443.
2. Sur la page de contrôle du pare-feu, sélectionnez non approuvé pour indiquer que le réseau client sur le nœud passerelle n'est pas fiable.

Après avoir enregistré votre configuration, tout le trafic entrant sur le réseau client du nœud passerelle est supprimé, sauf pour les requêtes HTTPS S3 sur le port 443 et les requêtes ICMP Echo (ping).

Exemple 2 : le nœud de stockage envoie des demandes de services de 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 à ce nœud de stockage sur le réseau client. Vous devez effectuer cette étape générale :

- Dans l'onglet réseaux de clients non approuvés de la page de contrôle du pare-feu, indiquez que le réseau client sur le nœud de stockage n'est pas fiable.

Une fois la configuration enregistrée, le nœud de stockage n'accepte plus le trafic entrant sur le réseau client, mais continue à autoriser les requêtes sortantes vers les destinations de 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 à Grid Manager uniquement sur un sous-réseau spécifique. Procédez comme suit :

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 fiable.
3. Lorsque vous créez un noeud final d'équilibreur de charge dans l'interface de gestion, entrez le port et sélectionnez l'interface de gestion à laquelle le port accérera.
4. Sélectionnez **Oui** pour réseau client non sécurisé.
5. Utilisez l'onglet gérer l'accès externe pour bloquer tous les ports externes (avec ou sans adresses IP privilégiées définies pour les hôtes situés en dehors de ce sous-réseau).

Après avoir enregistré votre configuration, seuls les hôtes du sous-réseau que vous avez spécifié peuvent accéder à Grid Manager. 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 Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez "autorisations d'accès spécifiques".
- Vous avez examiné les informations dans "Gérer les contrôles de pare-feu" et "Instructions de mise en réseau".
- Si vous souhaitez qu'un nœud d'administration ou un nœud de passerelle accepte le trafic entrant uniquement sur des noeuds finaux configurés explicitement, vous avez défini les noeuds finaux de l'équilibreur de charge.

> ⓘ Lors de la modification de la configuration du réseau client, les connexions client existantes peuvent échouer si les noeuds finaux de l'équilibreur de charge n'ont pas été configurés.

Description de la tâche

StorageGRID comprend un pare-feu interne sur chaque nœud qui vous permet d'ouvrir ou de fermer certains ports sur les nœuds de votre grille. Vous pouvez utiliser les onglets de contrôle du pare-feu pour ouvrir ou fermer des ports ouverts par défaut sur le réseau Grid, le réseau Admin et le réseau client. Vous pouvez également créer une liste d'adresses IP privilégiées pouvant accéder aux ports de la grille fermés. Si vous utilisez un réseau client, vous pouvez spécifier si un nœud approuve le trafic entrant à partir du réseau client et configurer l'accès à des ports spécifiques sur le réseau client.

Limiter le nombre de ports ouverts aux adresses IP en dehors de votre grille à ceux qui sont absolument nécessaires améliore la sécurité de votre grille. 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, notamment des exemples, reportez-vous à la section "Gérer les contrôles de pare-feu".

Pour plus d'informations sur les pare-feu externes et la sécurité réseau, reportez-vous à la section "Contrôler l'accès au niveau du pare-feu externe".

Accès aux contrôles de pare-feu

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **contrôle du pare-feu**.

   Les trois onglets de cette page sont décrits dans "Gérer les contrôles de 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 effectuées 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 des paramètres de l'onglet gérer l'accès externe.

Par défaut, les adresses IP privilégiées et les sous-réseaux ne disposent pas d'un accès au grid interne. En outre, les noeuds finaux d'équilibrage de charge et les ports supplémentaires ouverts dans l'onglet liste d'adresses privilégiées sont accessibles même si 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 que vous souhaitez accorder à l'accès aux ports fermés.
2. Si vous le souhaitez, sélectionnez **Ajouter une autre adresse IP ou un autre sous-réseau en notation CIDR** pour ajouter des clients privilégiés supplémentaires.

   > Ajoutez autant d'adresses que possible à la liste privilégiée.

3. Vous pouvez également sélectionner **Autoriser les adresses IP privilégiées à accéder aux ports internes StorageGRID**. Voir "Ports internes StorageGRID".

   > Cette option supprime certaines protections pour les services internes. Laissez-le désactivé si possible.

4. Sélectionnez **Enregistrer**.

Gérer l'accès externe

Lorsqu'un port est fermé dans l'onglet gérer l'accès externe, il est impossible d'accéder au port par une adresse IP non grille à moins que vous n'ajoutiez 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 contenant tous les ports externes (ports accessibles par défaut par les nœuds non GRID) pour les nœuds de votre grille.
2. Configurez les ports que vous souhaitez ouvrir et fermer à l'aide des options suivantes :
   - Utilisez la bascule située en regard 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 Grid Manager 443 ou 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.

   Utilisez la barre de défilement située à droite du tableau pour vous assurer que vous avez affiché tous les ports disponibles. Utilisez le champ de recherche pour trouver les paramètres de n'importe quel port externe en entrant un numéro de port. Vous pouvez entrer un numéro de port partiel. Par exemple, si vous entrez un **2**, tous les ports dont le nom contient la chaîne "2" s'affichent.
3. Sélectionnez **Enregistrer**

Réseau client non fiable

Si le réseau client d'un nœud n'est pas approuvé, le nœud accepte uniquement le trafic entrant sur les ports configurés comme points finaux de l'équilibreur 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 pour les 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 effectuées 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 les nouveaux nœuds par défaut, spécifiez le paramètre par défaut lorsque de nouveaux nœuds sont ajoutés à la grille dans une procédure d'extension.
   - **Approuvé** (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 du système StorageGRID.
3. Utilisez les options suivantes pour sélectionner les nœuds qui doivent autoriser les connexions client uniquement sur les terminaux d'équilibrage de charge configurés explicitement ou sur les ports sélectionnés supplémentaires :

- Sélectionnez **ne pas faire confiance aux nœuds affichés** pour ajouter tous les nœuds affichés dans le tableau à la liste réseau client non approuvé.
- Sélectionnez **confiance sur les nœuds affichés** pour supprimer tous les nœuds affichés dans le tableau de la liste réseau client non approuvé.
- Utilisez la bascule en regard de chaque nœud pour définir le réseau client comme approuvé ou non fiable pour le nœud sélectionné.

  Par exemple, vous pouvez sélectionner **ne plus faire confiance aux nœuds affichés** pour ajouter tous les nœuds à la liste réseau client non approuvé, puis utiliser la bascule à côté d'un nœud individuel pour ajouter ce nœud à la liste réseau client approuvé.

> Utilisez la barre de défilement située à droite du tableau pour vous assurer que vous avez affiché tous les nœuds disponibles. Utilisez le champ de recherche pour rechercher les paramètres d'un nœud en saisissant son nom. Vous pouvez entrer un nom partiel. Par exemple, si vous entrez un **GW**, tous les nœuds qui ont la chaîne "GW" comme partie de leur nom sont affichés.

4. Sélectionnez **Enregistrer**.

   Les nouveaux paramètres de pare-feu sont immédiatement appliqués et appliqués. Les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.

Gérer les locataires

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

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

> Les détails SWIFT ont été supprimés de cette version du site doc. Voir "StorageGRID 11.8 : gestion des locataires".

En tant qu'administrateur du grid, vous créez et gérez les comptes de locataire utilisés par les clients S3 pour stocker et récupérer des objets.

Chaque compte de locataire comprend des groupes, utilisateurs, compartiments S3 et objets fédérés ou locaux.

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

- **Cas d'utilisation entreprise :** si vous gérez un système StorageGRID dans une application d'entreprise, vous pourriez vouloir isoler le stockage objet de la grille par les différents départements de votre organisation. Dans ce cas, vous pouvez créer des comptes de tenant pour le département Marketing, le service Customer support, le service des ressources humaines, etc.

> Si vous utilisez le protocole client S3, vous pouvez utiliser des compartiments S3 et des règles de compartiments pour isoler les objets entre les services d'une entreprise. Vous n'avez pas besoin d'utiliser de comptes de locataire. Voir les instructions d'implémentation "Compartiments S3 et règles de compartiments" pour plus d'informations.

- **Cas d'utilisation de fournisseur de services :** si vous gérez un système StorageGRID en tant que fournisseur de services, vous pouvez isoler le stockage objet de la grille par les différentes entités qui loueront le stockage sur votre grille. Dans ce cas, vous créeriez des comptes de tenant pour la société A, la société B, la société C, etc.

Pour plus d'informations, voir "Utilisez un compte de locataire".

Comment créer un compte de locataire ?

Utilisez le gestionnaire de grille pour créer un compte de locataire. Lorsque vous créez un compte de locataire, vous spécifiez les informations suivantes :

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

En outre, vous pouvez activer le paramètre de verrouillage des objets S3 pour le système StorageGRID si les comptes de locataires S3 doivent se conformer aux exigences réglementaires. Lorsque le verrouillage des objets S3 est activé, tous les comptes de locataires S3 peuvent créer et gérer des compartiments conformes.

À quoi sert le gestionnaire de locataires ?

Une fois le compte de tenant créé, les utilisateurs de tenant peuvent se connecter au gestionnaire de tenant pour effectuer les tâches suivantes :

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

Les locataires S3 peuvent créer et gérer des clés d'accès S3 et des compartiments avec le gestionnaire de locataires. Ils doivent utiliser une application client S3 pour ingérer et gérer les objets. Voir "UTILISEZ L'API REST S3" pour plus de détails.

Créez un compte de locataire

Vous devez créer au moins un compte de locataire pour contrôler l'accès au stockage dans votre système StorageGRID.

Les étapes de création d'un compte de locataire varient selon que "fédération des identités" et sont configurés et "authentification unique"si le compte Grid Manager que vous utilisez pour créer le compte de locataire

appartient à un groupe d'administration avec l'autorisation d'accès racine.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine ou de comptes de locataires".
- Si le compte de tenant utilise le référentiel d'identité qui a été configuré pour Grid Manager et que vous souhaitez accorder l'autorisation d'accès racine au compte de tenant à un groupe fédéré, vous avez importé ce groupe fédéré dans Grid Manager. Vous n'avez pas besoin d'affecter d'autorisations Grid Manager à ce groupe d'administration. Voir "Gérez les groupes d'administration".
- Si vous souhaitez autoriser un locataire S3 à cloner les données de compte et à répliquer les objets de compartiment vers une autre grille à l'aide d'une connexion de fédération de grille :
  - Vous avez "configurez la connexion de fédération de grille - effectué".
  - L'état de la connexion est **connecté**.
  - Vous disposez de l'autorisation d'accès racine.
  - Vous avez examiné les considérations relatives à "gestion des locataires autorisés pour la fédération dans le grid".
  - Si le compte de tenant utilise le référentiel d'identité configuré pour Grid Manager, vous avez importé le même groupe fédéré dans Grid Manager sur les deux grilles.

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

> Si ce groupe d'administration n'existe pas sur les deux grilles avant la création du tenant, celui-ci n'est pas répliqué vers la destination.

Accéder à l'assistant

Étapes

1. Sélectionnez **LOCATAIRES**.
2. Sélectionnez **Créer**.

Entrez les détails

Étapes

1. Entrez les détails du locataire.

Champ	Description
Nom	Nom du compte de locataire. Les noms de locataires n'ont pas besoin d'être uniques. Lorsque le compte de locataire est créé, il reçoit un ID de compte unique à 20 chiffres.

Champ	Description
Description (facultatif)	Une description pour aider à identifier le locataire. Si vous créez un locataire qui utilisera une connexion de fédération de grille, vous pouvez utiliser ce champ pour identifier le locataire source et le locataire de destination. Par exemple, cette description pour un locataire créé sur la grille 1 s'affiche également pour le locataire répliqué dans 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** soit **Swift**. **Remarque** : la prise en charge des applications clientes Swift a été obsolète et sera supprimée dans une version ultérieure.
Quota de stockage (facultatif)	Si vous souhaitez que ce locataire ait un quota de stockage, une valeur numérique pour le quota et les unités.

2. Sélectionnez **Continuer**.

sélectionnez les autorisations

Étapes

1. Si vous le souhaitez, sélectionnez les autorisations de base dont ce locataire doit disposer.

> Certaines de ces autorisations ont des exigences supplémentaires. Pour plus de détails, sélectionnez l'icône d'aide pour chaque autorisation.

Autorisations	Si cette option est sélectionnée…
Autoriser les services de plate-forme	Le locataire peut utiliser des services de plateforme S3 tels que CloudMirror. Voir "Gestion des services de plateforme pour les comptes de locataires S3".
Utiliser son propre référentiel d'identité	Le locataire peut configurer et gérer son propre référentiel d'identité pour les groupes et utilisateurs fédérés. Cette option est désactivée si vous disposez de "SSO configuré" pour votre système StorageGRID.
Autoriser la sélection S3	Le locataire peut émettre des requêtes d'API S3 SelectObjectContent pour filtrer et récupérer des données d'objet. Voir "Gérez S3 Select pour les comptes de locataires". **Important** : les requêtes 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. Si vous le souhaitez, sélectionnez les autorisations avancées dont ce locataire doit disposer.

Autorisations	Si cette option est sélectionnée…
Connexion de fédération de grille	Le locataire peut utiliser une connexion de fédération de grille qui : • Provoque le clonage de ce locataire et de tous les groupes de locataires et utilisateurs ajoutés au compte à partir 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 entre les compartiments correspondants sur chaque grille. Voir "Gérer les locataires autorisés pour la fédération dans le grid".
Verrouillage d'objet S3	Autoriser le locataire à utiliser des fonctionnalités spécifiques de S3 Object Lock : • **Set maximum Retention Period** définit la durée pendant laquelle les nouveaux objets ajoutés à ce compartiment doivent être conservés, à partir du moment où ils sont ingérés. • **Autoriser le mode de conformité** empêche les utilisateurs d'écraser ou de supprimer les versions d'objets protégés pendant la période de rétention.

3. Sélectionnez **Continuer**.

Définissez l'accès racine et créez un locataire

Étapes

1. Définissez l'accès racine pour le compte de locataire, selon que votre système StorageGRID utilise ou non la fédération des identités, l'authentification unique (SSO), ou les deux.

Option	Faites ça
Si la fédération des identités n'est pas activée	Spécifiez le mot de passe à utiliser lors de la connexion au tenant en tant qu'utilisateur root local.
Si la fédération des identités est activée	a. Sélectionnez un groupe fédéré existant pour obtenir l'autorisation d'accès racine pour le tenant. b. Vous pouvez également spécifier le mot de passe à utiliser lors de la connexion au tenant en tant qu'utilisateur root local.
Si la fédération des identités et l'authentification unique (SSO) sont toutes deux activées	Sélectionnez un groupe fédéré existant pour obtenir l'autorisation d'accès racine pour le tenant. Aucun utilisateur local ne peut se connecter.

2. Sélectionnez **Créer locataire**.

   Un message de réussite s'affiche et le nouveau locataire apparaît sur la page locataires. Pour savoir comment afficher les détails des locataires et surveiller l'activité des locataires, reportez-vous à la section "Surveillez l'activité des locataires".

L'application des paramètres de locataire sur l'ensemble du grid 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 de fédération de grille** pour le locataire :
   a. Confirmez qu'un locataire identique a été répliqué sur l'autre grille de la connexion. Les locataires des deux grilles auront les mêmes ID de compte, nom, description, quota et autorisations à 20 chiffres.

      Si le message d'erreur « tenant created without a clone » s'affiche, reportez-vous aux instructions de la section "Dépanner 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, "modifiez le mot de passe de l'utilisateur root local" pour le tenant répliqué.

      Un utilisateur root local ne peut pas se connecter au gestionnaire de locataires sur la grille de destination tant que le mot de passe n'est pas modifié.

Se connecter au locataire (facultatif)

Si nécessaire, vous pouvez vous connecter au nouveau locataire maintenant pour terminer la configuration ou vous pouvez vous connecter ultérieurement au locataire. Les étapes de connexion dépendent si vous êtes connecté à Grid Manager à l'aide du port par défaut (443) ou d'un port restreint. Voir "Contrôler l'accès au niveau du pare-feu externe".

Connectez-vous dès maintenant

Si vous utilisez…	Procédez comme ça…
Le port 443 et vous définissez un mot de passe pour l'utilisateur root local	1. Sélectionnez **se connecter en tant que root**. Lorsque vous vous connectez, des liens s'affichent pour la configuration des compartiments, de la fédération des identités, des groupes et des utilisateurs. 2. Sélectionnez les liens pour configurer le compte de tenant. Chaque lien ouvre la page correspondante dans le Gestionnaire de locataires. Pour compléter la page, reportez-vous à la "instructions d'utilisation des comptes de tenant".
Le port 443 et vous n'avez pas défini de mot de passe pour l'utilisateur root local	Sélectionnez **se connecter** et entrez les informations d'identification d'un utilisateur dans le groupe fédéré d'accès racine.

Si vous utilisez…	Procédez comme ça…
Un port restreint	1. Sélectionnez **Terminer** 2. Sélectionnez **Restricted** dans la table tenant pour en savoir plus sur l'accès à ce compte de tenant. L'URL du Gestionnaire de locataires a le format suivant : `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'ID de compte unique du locataire

Connectez-vous plus tard

Si vous utilisez…	Effectuez l'une d'entre elles…
Orifice 443	• Dans Grid Manager, sélectionnez **TENANTS**, puis **connexion** à droite du nom du locataire. • Entrez 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'ID de compte unique du locataire
Un port restreint	• Dans le Gestionnaire de grille, sélectionnez **TENANTS** et sélectionnez **restreint**. • Entrez 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 réservé aux locataires ◦ *20-digit-account-id* Est l'ID de compte unique du locataire

Configurez le tenant

Suivez les instructions de la section "Utilisez un compte de locataire" pour gérer les groupes de locataires et les utilisateurs, les clés d'accès S3, les compartiments, les services de plateforme et le clone de compte et la

réplication inter-grid.

Modifiez le compte de tenant

Vous pouvez modifier un compte de locataire pour modifier le nom d'affichage, le quota de stockage ou les autorisations de locataire.

Si un locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, vous pouvez modifier les détails du locataire à partir de l'une des grilles de la connexion. Toutefois, toute modification apportée à une grille dans la connexion ne sera pas copiée dans l'autre grille. Si vous souhaitez que les détails du locataire soient synchronisés exactement entre les grilles, effectuez les mêmes modifications sur les deux grilles. Voir "Gérez les locataires autorisés pour la connexion de fédération de grille".

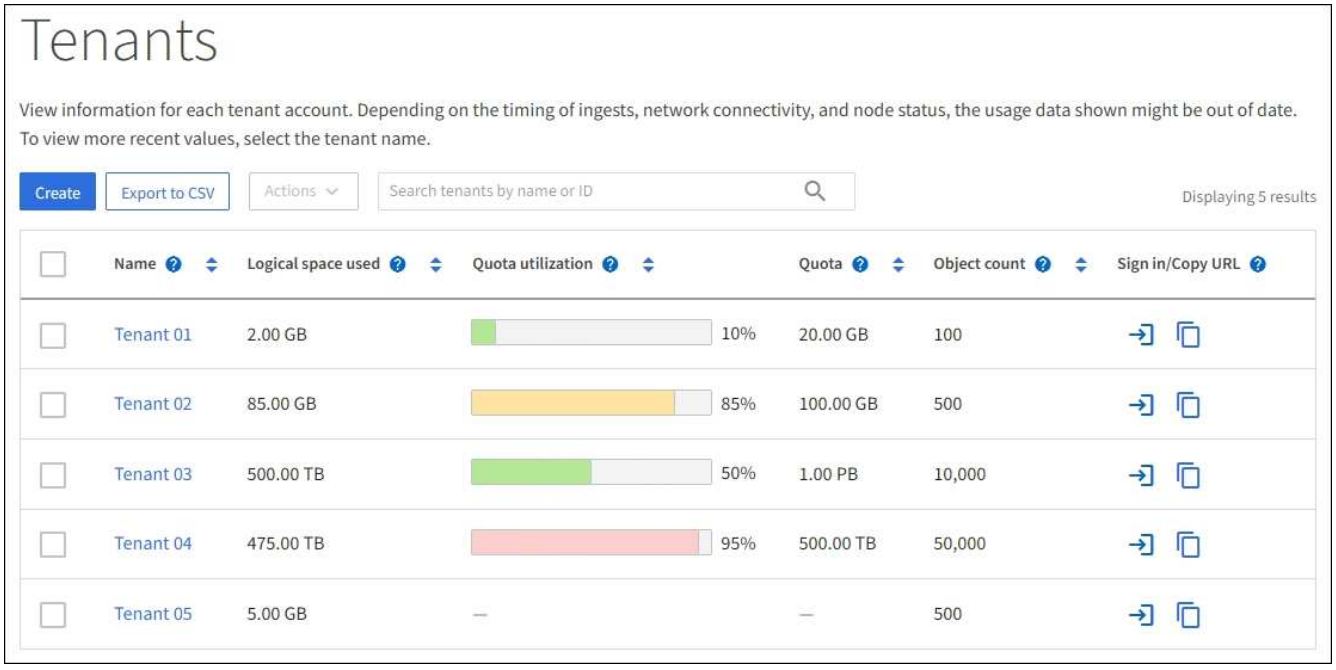
Avant de commencer

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

L'application des paramètres de locataire sur l'ensemble du grid 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. Recherchez le compte de locataire à modifier.

   Utilisez la zone de recherche pour rechercher un locataire par nom ou ID locataire.

3. Sélectionnez le locataire. Vous pouvez effectuer l'une des opérations suivantes :
   - Cochez la case du locataire, puis sélectionnez **actions** > **Modifier**.
   - Sélectionnez le nom du locataire pour afficher la page des détails, puis sélectionnez **Modifier**.

4. Si vous le souhaitez, modifiez les valeurs de ces champs :
   - **Nom**
   - **Description**
   - **Quota de stockage**
5. Sélectionnez **Continuer**.
6. Sélectionnez ou désélectionnez les autorisations pour le compte de tenant.
   - Si vous désactivez **Platform Services** pour un locataire qui les utilise déjà, les services qu'ils ont configurés pour leurs compartiments S3 cessent de fonctionner. Aucun message d'erreur n'est envoyé au locataire. Par exemple, si le locataire a configuré la réplication CloudMirror pour un compartiment S3, il peut toujours stocker les objets dans le compartiment, mais les copies de ces objets ne sont plus effectuées dans le compartiment S3 externe qu'ils ont configuré en tant que terminal. Voir "Gestion des services de plateforme pour les comptes de locataires S3".
   - Modifiez le paramètre de **Use own Identity source** pour déterminer si le compte de tenant utilisera son propre référentiel d'identité ou le référentiel d'identité configuré pour le gestionnaire de grille.

     Si **utiliser le propre référentiel d'identité** est :

     - Désactivé et sélectionné, le locataire a déjà activé son propre référentiel d'identité. Un locataire doit désactiver son référentiel d'identité avant de pouvoir utiliser le référentiel d'identité configuré pour Grid Manager.
     - Désactivé et non sélectionné, SSO est activé pour le système StorageGRID. Le locataire doit utiliser le référentiel d'identité qui a été configuré pour Grid Manager.
   - Sélectionnez ou désélectionnez l'autorisation **Autoriser S3 Select** selon les besoins. Voir "Gérez S3 Select pour les comptes de locataires".
   - Pour supprimer l'autorisation **utiliser la connexion de fédération de grille** :
     i. Sélectionnez l'onglet **Grid federation**.
     ii. Sélectionnez **Supprimer l'autorisation**.
   - Pour ajouter l'autorisation **utiliser la connexion de fédération de grille** :
     i. Sélectionnez l'onglet **Grid federation**.
     ii. Cochez la case **utiliser la connexion de fédération de grille**.
     iii. Si vous le souhaitez, sélectionnez **Cloner les utilisateurs et groupes locaux existants** pour les cloner dans 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 dernière opération de clonage.
   - Pour définir une période de rétention maximale ou autoriser le mode de conformité :

     > ⓘ Le verrouillage d'objet S3 doit être activé sur la grille pour que vous puissiez utiliser ces paramètres.

     i. Sélectionnez l'onglet **S3 Object Lock**.
     ii. Pour **définir la période de rétention maximale**, entrez une valeur et sélectionnez la période dans le menu déroulant.
     iii. Pour **Autoriser le mode de conformité**, cochez la case.

Modifiez le mot de passe de l'utilisateur racine local du locataire

Vous devrez peut-être modifier le mot de passe de l'utilisateur root local d'un locataire si celui-ci est verrouillé hors du compte.

Avant de commencer

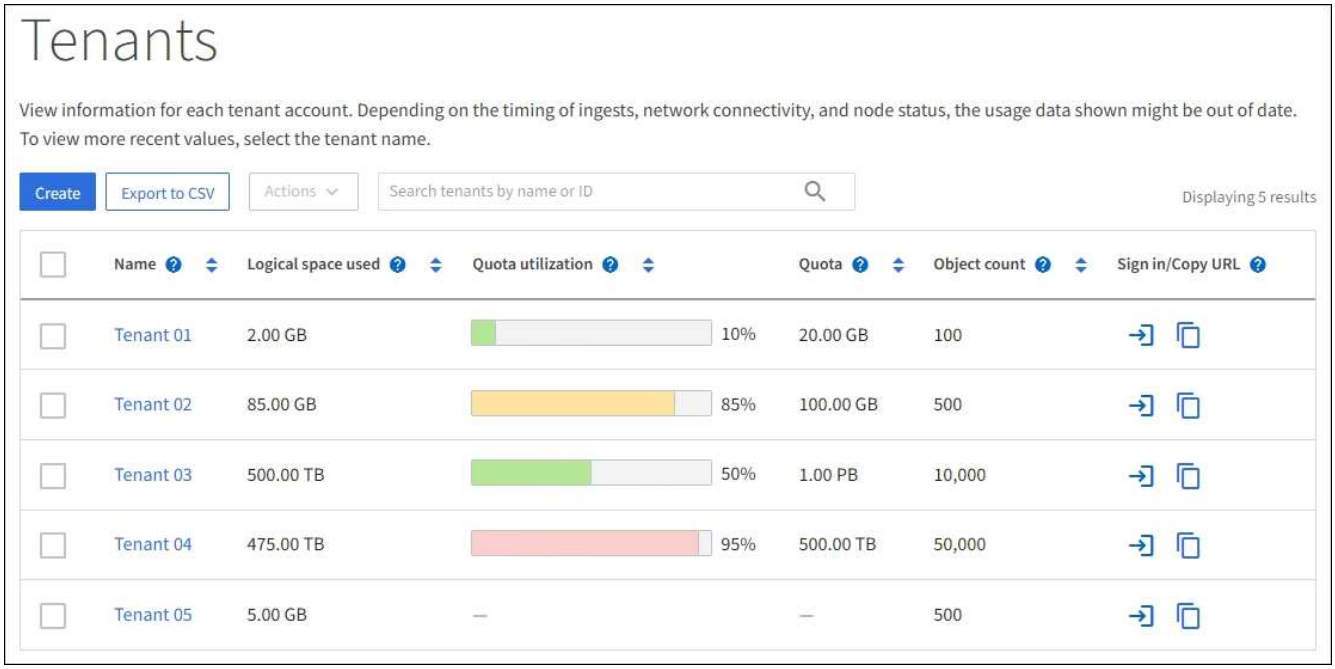
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez "autorisations d'accès spécifiques".

Description de la tâche

Si l'authentification unique (SSO) est activée pour votre système StorageGRID, l'utilisateur root local ne peut pas se connecter au compte de locataire. Pour effectuer des tâches utilisateur racine, les utilisateurs doivent appartenir à un groupe fédéré disposant de l'autorisation d'accès racine pour le locataire.

Étapes

1. Sélectionnez **LOCATAIRES**.



2. Sélectionnez le compte locataire. Vous pouvez effectuer l'une des opérations suivantes :
   - Cochez la case du 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 de tenant.
4. Sélectionnez **Enregistrer**.

Supprimer le compte de locataire

Vous pouvez supprimer un compte de tenant si vous souhaitez supprimer définitivement l'accès du tenant au système.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez "autorisations d'accès spécifiques".
- Vous avez supprimé tous les compartiments S3 et tous les objets associés au compte de locataire.
- Si le locataire est autorisé à utiliser une connexion de fédération de grille, vous avez examiné les considérations relatives à "Suppression d'un locataire avec l'autorisation utiliser la connexion de fédération de grille".

Étapes

1. Sélectionnez **LOCATAIRES**.
2. Recherchez le ou les comptes de tenant que vous souhaitez supprimer.

   Utilisez la zone de recherche pour rechercher un locataire par nom ou ID 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 et sélectionnez **actions** > **Supprimer**.
   - Sélectionnez le nom du locataire pour afficher la page des détails, puis sélectionnez **actions** > **Supprimer**.
5. Sélectionnez **Oui**.

Gestion des services de plateforme

Qu'est-ce que les services de plateforme ?

Les services de plateforme incluent la réplication CloudMirror, les notifications d'événement et le service d'intégration de la recherche.

Si vous activez des services de plateforme pour les comptes de locataires S3, vous devez configurer votre grid de manière à ce que les locataires puissent accéder aux ressources externes nécessaires à l'utilisation de ces services.

Réplication CloudMirror

Le service de réplication StorageGRID CloudMirror est utilisé pour mettre en miroir des objets spécifiques d'un compartiment StorageGRID vers une destination externe spécifiée.

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

> La réplication CloudMirror présente des similarités et des différences importantes avec la fonction de réplication multigrille. Pour en savoir plus, voir "Comparez la réplication entre les grilles et la réplication CloudMirror".

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

Notifications

Les notifications d'événements par compartiment permettent d'envoyer des notifications sur des actions

spécifiques réalisées sur des objets à un cluster Kafka externe spécifié ou à Amazon simple notification Service.

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

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

Service d'intégration de la recherche

Le service d'intégration de la recherche permet d'envoyer des métadonnées d'objet S3 à un index Elasticsearch spécifié pour une recherche ou une analyse des métadonnées à l'aide du service externe.

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

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

Les services de plateforme permettent aux locataires 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 ne fait généralement pas partie de votre déploiement StorageGRID, vous devez décider si vous souhaitez autoriser les locataires à utiliser ces services. Dans ce cas, vous devez activer l'utilisation des services de plateforme lorsque vous créez ou modifiez des comptes de tenant. Vous devez également configurer votre réseau de sorte que les messages de services de plate-forme générés par les locataires puissent atteindre leurs destinations.

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

Avant d'utiliser les services de plate-forme, tenez compte des recommandations suivantes :

- Si le contrôle de versions et la réplication CloudMirror sont activés pour un compartiment S3 dans le système StorageGRID, vous devez également activer la gestion des versions du compartiment S3 pour le terminal de destination. Cela permet à la réplication CloudMirror de générer des versions d'objet similaires sur le noeud final.
- Vous ne devez pas utiliser plus de 100 locataires actifs avec les demandes S3 nécessitant la réplication CloudMirror, les notifications et l'intégration de la recherche. Avec plus de 100 locataires actifs, les performances des clients S3 sont plus lentes.
- Les demandes adressées à un point final qui ne peut pas être terminé seront mises en file d'attente pour un maximum de 500,000 demandes. Cette limite est également partagée 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 pénalisés injustement.

Informations associées

- "Gestion des services de plateforme"

- "Configurez les paramètres du proxy de stockage"
- "Surveillez StorageGRID"

Réseau et ports pour les services de plate-forme

Si vous autorisez un locataire S3 à utiliser des services de plateforme, vous devez configurer la mise en réseau pour le grid de manière à ce que les messages des services de plateforme puissent être envoyés vers leur destination.

Lorsque vous créez ou mettez à jour le compte de locataire, vous pouvez activer des services de plateforme pour un compte de locataire S3. Si les services de plateforme sont activés, le locataire peut créer des terminaux qui servent de destination à la réplication CloudMirror, à la notification d'événement ou aux 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 terminaux de destination.

Par exemple, les locataires peuvent configurer les types de terminaux de destination suivants :

- Un cluster Elasticsearch hébergé localement
- Application locale qui prend en charge la réception des messages Amazon simple notification Service
- Cluster Kafka hébergé localement
- Un compartiment S3 hébergé localement sur la même instance d'StorageGRID ou sur une autre instance
- Un terminal externe, tel qu'un terminal sur Amazon Web Services.

Pour vous assurer que les messages des services de plate-forme peuvent être envoyés, vous devez configurer le réseau 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 plate-forme aux noeuds finaux de destination.

Par défaut, les messages des services de plate-forme sont envoyés sur les ports suivants :

- **80** : pour les URI de noeud final commençant par http (la plupart des noeuds finaux)
- **443** : pour les URI de noeud final commençant par https (la plupart des noeuds finaux)
- **9092** : pour les URI de noeud final commençant par http ou https (noeuds finaux Kafka uniquement)

Les locataires peuvent spécifier un port différent lorsqu'ils créent ou modifient un noeud final.

> Si un déploiement StorageGRID est utilisé comme destination pour la réplication CloudMirror, des messages de réplication peuvent être reçus sur un port autre que 80 ou 443. Vérifiez que le port utilisé pour S3 par le déploiement StorageGRID de destination est spécifié dans le terminal.

Si vous utilisez un serveur proxy non transparent, vous devez également "configurez les paramètres du proxy de stockage"autoriser l'envoi de messages à des points finaux externes, tels qu'un point de terminaison sur Internet.

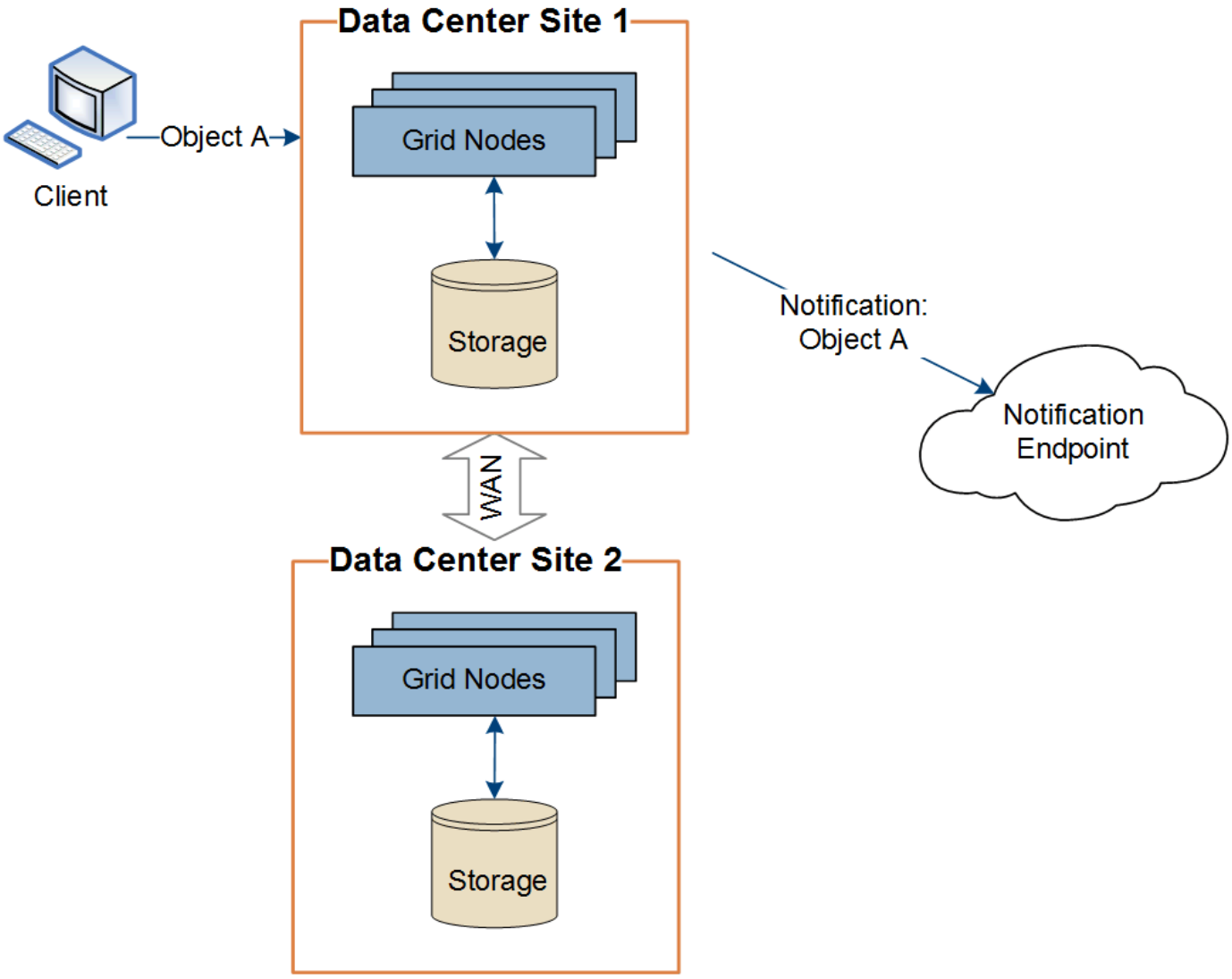
Informations associées

"Utilisez un compte de locataire"

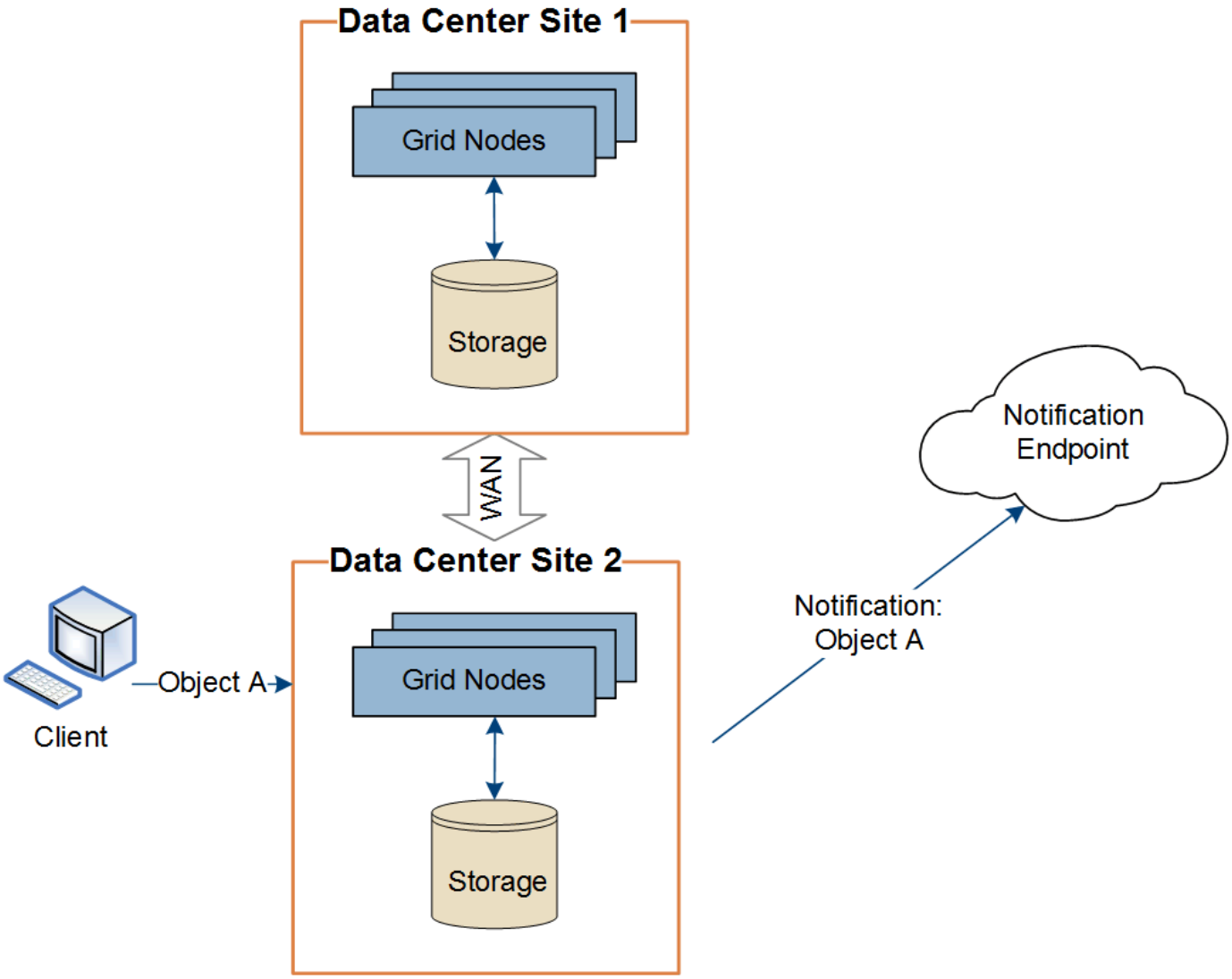
Livraison par site de messages de services de plate-forme

Toutes les opérations de services de plateforme sont réalisées sur une base par site.

C'est-à-dire que 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 de Data Center 1, la notification concernant cette action est déclenchée et envoyée depuis le site de Data Center 1.



Si le client exécute ensuite une opération de suppression d'API S3 sur ce même objet à partir du site du centre de données 2, la notification concernant l'action de suppression est déclenchée et envoyée depuis le site du centre de données 2.



Assurez-vous que le réseau de chaque site est configuré de manière à ce que les messages des services de plate-forme puissent être transmis à leurs destinations.

Résoudre les problèmes liés aux services de plateforme

Les terminaux utilisés dans les services de plateforme sont créés et gérés par les utilisateurs locataires dans le Gestionnaire de locataires. Toutefois, si un locataire a des problèmes de configuration ou d'utilisation des services de plateforme, vous pouvez utiliser le Gestionnaire de grille pour résoudre le problème.

Problèmes liés aux nouveaux terminaux

Avant qu'un locataire ne puisse utiliser les services de plateforme, il doit créer un ou plusieurs terminaux à l'aide du Gestionnaire des locataires. Chaque terminal représente une destination externe pour un service de plateforme, par exemple un compartiment StorageGRID S3, un compartiment Amazon Web Services, une rubrique Amazon simple notification Service, une rubrique Kafka ou un cluster Elasticsearch hébergé localement ou sur AWS. Chaque noeud final comprend 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 noeud final, le système StorageGRID valide que ce dernier existe et qu'il peut être atteint à l'aide des identifiants spécifiés. La connexion au noeud final est validée à partir d'un nœud sur chaque

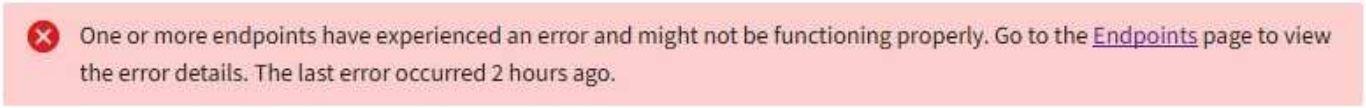
site.

Si la validation du noeud final échoue, un message d'erreur explique pourquoi la validation du noeud final a échoué. L'utilisateur locataire doit résoudre le problème, puis essayer de créer à nouveau le noeud final.

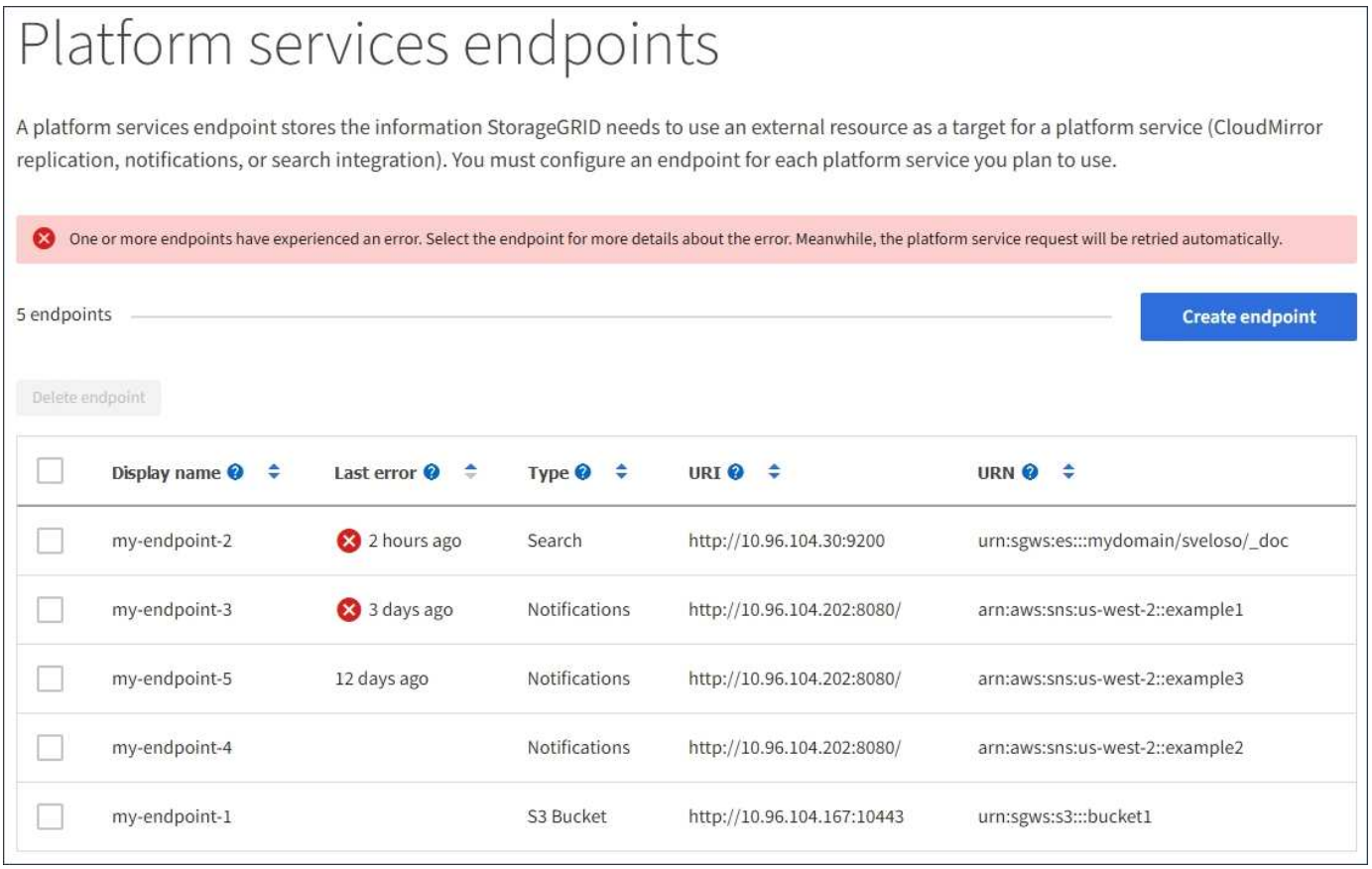
La création du terminal échoue si les services de plateforme ne sont pas activés pour le compte de locataire.

Problèmes avec les terminaux existants

Si une erreur se produit lorsque StorageGRID tente d'atteindre un noeud final existant, un message s'affiche sur le tableau de bord dans le Gestionnaire de locataires.



Les utilisateurs locataires peuvent accéder à la page noeuds finaux pour consulter le message d'erreur le plus récent pour chaque noeud final et déterminer la durée de l'erreur. La colonne **dernière erreur** affiche le message d'erreur le plus récent pour chaque noeud final et indique la durée de l'erreur. Des erreurs incluant l'icône se sont produites 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 le support technique peut utiliser cet ID pour trouver des informations plus détaillées sur l'erreur dans bycast.log.

Problèmes liés aux serveurs proxy

Si vous avez configuré un "proxy de stockage" entre les noeuds de stockage et les noeuds finaux du service de plate-forme, des erreurs peuvent se produire si votre service proxy n'autorise pas les messages de StorageGRID. Pour résoudre ces problèmes, vérifiez les paramètres de votre serveur proxy pour vous assurer que les messages liés au service de plate-forme ne sont pas bloqués.

Déterminez si une erreur s'est produite

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

Échec des opérations client

Certains problèmes de service de plateforme peuvent entraîner l'échec des opérations client dans le compartiment S3. Par exemple, les opérations client S3 échouent si le service RSM (Replicated State machine) interne s'arrête ou s'il y a trop de messages de services de plate-forme en file d'attente pour la livraison.

Pour vérifier l'état des services :

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez ***site*** > ***Storage Node*** > **SSM** > **Services**.

Erreurs récupérables et récupérables du point final

Une fois les noeuds finaux créés, des erreurs de demande de service de plate-forme peuvent se produire pour diverses raisons. Certaines erreurs peuvent être récupérées 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 compartiment de destination n'existe pas.
- La notification ne peut pas être remise.

Si StorageGRID rencontre une erreur récupérable, la demande de service de plate-forme sera relancée jusqu'à ce qu'elle réussisse.

D'autres erreurs sont irrécupérables. Par exemple, une erreur irrécupérable se produit si le noeud final est supprimé.

Si StorageGRID rencontre une erreur de point final irrécupérable :

- Dans Grid Manager, accédez à **support** > **Tools** > **Metrics** > **Grafana** > **Platform Services Overview** pour afficher les détails de l'erreur.
- Dans le Gestionnaire de locataires, accédez à **STORAGE (S3)** > **Platform Services Endpoints** pour afficher les détails de l'erreur.
- Vérifier si le `/var/local/log/bycast-err.log` présente des erreurs. Les nœuds de stockage disposant du service ADC contiennent ce fichier journal.

Les messages des services de plateforme ne peuvent pas être transmis

Si la destination rencontre un problème qui l'empêche d'accepter des messages de services de plate-forme,

l'opération client sur le compartiment réussit, mais le message des services de plate-forme n'est pas livré. Par exemple, cette erreur peut se produire si les informations d'identification sont mises à jour sur la destination de sorte que StorageGRID ne puisse plus s'authentifier auprès du service de destination.

Recherchez les alertes associées.

Des performances plus lentes pour les demandes de services de plateforme

Le logiciel StorageGRID peut canaliser les demandes S3 entrantes pour un compartiment si le taux d'envoi des demandes dépasse le taux à partir duquel le terminal de destination peut recevoir les demandes. La restriction ne se produit que lorsqu'il existe un arriéré de demandes en attente d'envoi vers le noeud final de destination.

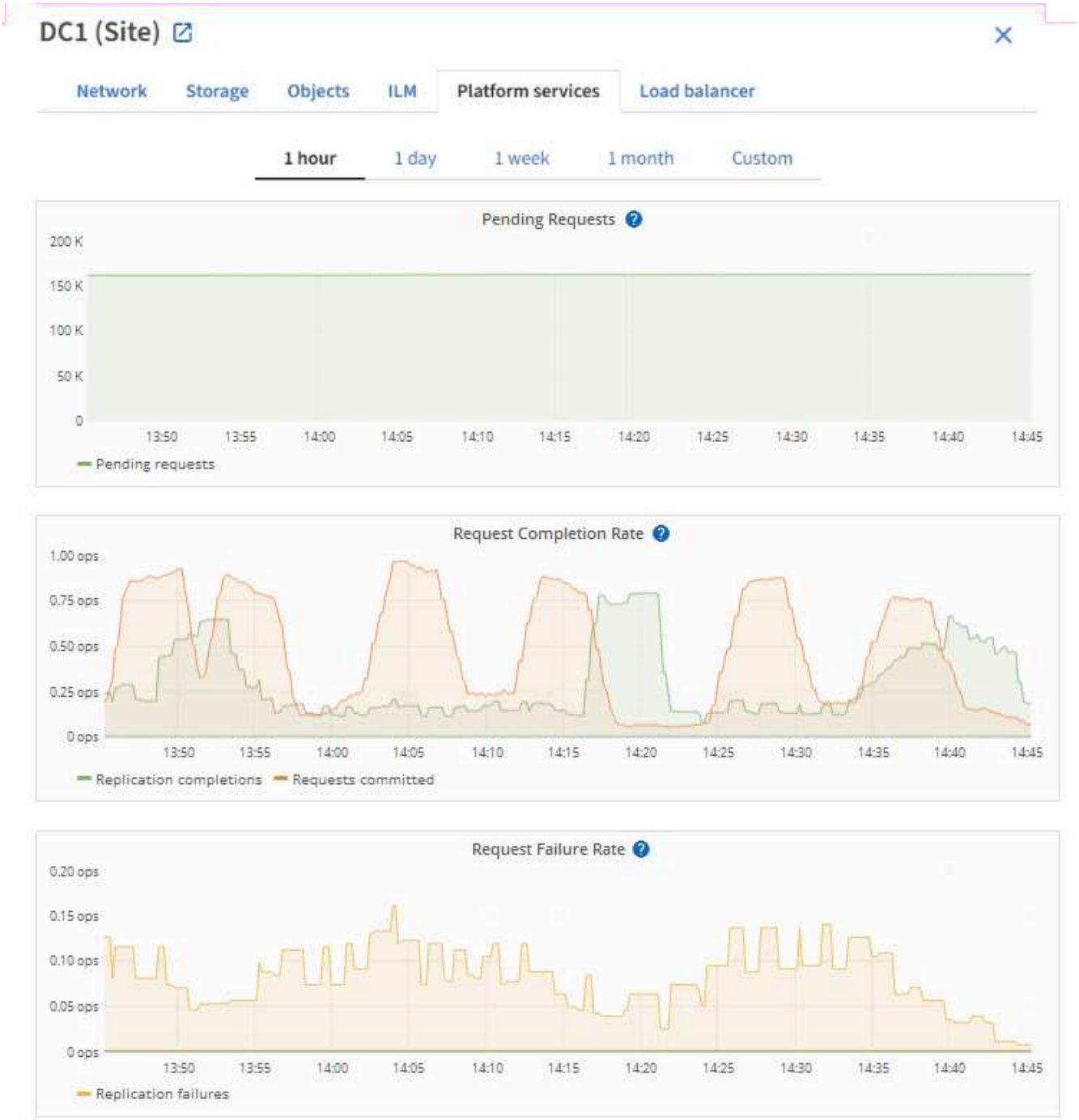
Le seul effet visible est que les requêtes S3 entrantes prennent plus de temps à s'exécuter. Si vous commencez à détecter les performances beaucoup plus lentes, vous devez réduire le taux d'entrée ou utiliser un terminal avec une capacité plus élevée. Si l'carnet de commandes des requêtes continue d'augmenter, les opérations S3 des clients (par EXEMPLE, LES requêtes PUT) finiront par échouer.

Les demandes CloudMirror sont plus susceptibles d'être affectées par les performances du terminal de destination, car ces demandes impliquent généralement plus de transfert de données que les demandes d'intégration de recherche ou de notification d'événements.

Les demandes de service de la plateforme échouent

Pour afficher le taux d'échec de la demande pour les services de plate-forme :

1. Sélectionnez **NOEUDS**.
2. Sélectionnez ***site*** > **Platform Services**.
3. Afficher le tableau des taux d'erreur de demande.



Alerte de services de plate-forme non disponibles

L'alerte **Platform services unavailable** indique qu'aucune opération de service de plate-forme ne peut être effectuée sur un site car trop 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 plate-forme 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 toute demande de service de plateforme en attente pour ce site.

Conseils de dépannage supplémentaires pour les terminaux des services de plateforme

Pour plus d'informations, voir "Utiliser un compte locataire ; dépanner les terminaux des services de plateforme".

Informations associées

"Dépanner le système StorageGRID"

Gérez S3 Select pour les comptes de locataires

Vous pouvez autoriser certains locataires S3 à utiliser S3 Select pour émettre des demandes SelectObjectContent sur des objets individuels.

S3 Select constitue un moyen efficace d'effectuer des recherches dans de vastes volumes de données sans avoir à déployer une base de données et les ressources associées pour activer les recherches. Il réduit également le coût et la latence liés à la 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 partir d'un objet. L'implémentation d'StorageGRID de S3 Select inclut un sous-ensemble de commandes et de fonctionnalités S3 Select.

Considérations et configuration requise pour l'utilisation de S3 Select

Exigences d'administration du grid

L'administrateur du grid doit autoriser les locataires S3 Select. Sélectionnez **Autoriser la sélection S3** lorsque "création d'un locataire" ou "modification d'un locataire".

Exigences de format d'objet

L'objet que vous souhaitez interroger doit être dans l'un des formats suivants :

- **CSV**. Peut être utilisé tel qu'il est ou compressé dans des archives GZIP ou BZIP2.
- **Parquet**. Exigences supplémentaires pour les objets parquet :
  - S3 Select prend uniquement en charge la compression par colonne à l'aide de GZIP ou de 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 compressées est de 512 Mo.
  - Vous devez utiliser les types de données spécifiés dans le schéma de l'objet.
  - Vous ne pouvez pas utiliser de types logiques D'INTERVALLE, de JSON, DE LISTE, DE TEMPS ou d'UUID.

Exigences relatives aux terminaux

La demande SelectObjectContent doit être envoyée à un "Terminal d'équilibrage de charge StorageGRID".

Les nœuds d'administration et de passerelle utilisés par le noeud final doivent être l'un des suivants :

- Nœud d'appliance de services
- Nœud logiciel basé sur VMware
- Nœud bare Metal exécutant un noyau avec cgroup v2 activé

Considérations générales

Les requêtes ne peuvent pas être envoyées directement aux nœuds de stockage.

> SelectObjectContent les demandes peuvent réduire les performances d'équilibrage 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 la "Instructions d'utilisation de S3 Select".

Pour afficher "Graphiques Grafana" les opérations S3 Select dans le temps, sélectionnez **SUPPORT** > **Outils** > **Metrics** dans le Gestionnaire de grille.

Configurer les connexions client

Configurer les connexions client S3

En tant qu'administrateur du grid, vous gérez les options de configuration qui contrôlent la façon dont les applications client S3 se connectent à votre système StorageGRID pour stocker et récupérer les données.

> Les détails SWIFT ont été supprimés de cette version du site doc. Voir "StorageGRID 11.8 : configurez les connexions client S3 et Swift".

Tâches de configuration

1. Effectuez les tâches requises dans StorageGRID, en fonction de la façon dont l'application client se connecte à StorageGRID.

Tâches requises

Vous devez obtenir :

- Adresses IP
- Noms de domaine
- Certificat SSL

Tâches facultatives

Éventuellement, configurer :

- fédération des identités
- SSO

1. Utilisez StorageGRID pour obtenir les valeurs dont l'application a besoin pour se connecter à la grille. Vous pouvez utiliser l'assistant d'installation S3 ou configurer chaque entité StorageGRID manuellement.

Utilisation de l'assistant d'installation S3

Suivez les étapes de l'assistant d'installation de S3.

Configurer manuellement

1. Créer un groupe haute disponibilité
2. Créer un noeud final d'équilibreur de charge
3. Créer un compte de locataire
4. Créez un compartiment et des clés d'accès
5. Configuration de la règle et de la règle 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 supplémentaire de l'application.

2. Effectuez des tâches continues dans l'application et dans StorageGRID afin de gérer et de surveiller le stockage objet au fil du temps.

Informations nécessaires pour joindre StorageGRID à une application client

Avant de connecter StorageGRID à une application client S3, vous devez effectuer les étapes de configuration dans StorageGRID et obtenir une certaine valeur.

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)	Groupe StorageGRID > HA	Entrée DNS
Port	StorageGRID > terminal de l'équilibreur de charge	Application client
Certificat SSL	StorageGRID > terminal de l'équilibreur de charge	Application client
Nom du serveur (FQDN)	StorageGRID > terminal de l'équilibreur de charge	• Application client • Entrée DNS
ID de clé d'accès S3 et clé d'accès secrète	StorageGRID > locataire et compartiment	Application client
Nom du compartiment/conteneur	StorageGRID > locataire et compartiment	Application client

Comment obtenir ces valeurs ?

Selon vos besoins, vous pouvez effectuer l'une des opérations suivantes pour obtenir les informations dont vous avez besoin :

- **Utilisez le "Assistant d'installation S3"**. L'assistant d'installation S3 vous aide à configurer rapidement les valeurs requises dans StorageGRID et génère un ou deux fichiers que vous pouvez utiliser pour configurer l'application S3. L'assistant vous guide tout au long des étapes requises et vous aide à vous assurer que vos paramètres sont conformes aux bonnes pratiques de StorageGRID.

  Si vous configurez une application S3, il est recommandé d'utiliser l'assistant d'installation S3, sauf si vous savez que vous disposez d'exigences spéciales, faute de quoi votre implémentation nécessitera une personnalisation importante.

- **Utilisez le "Assistant d'installation FabricPool"**. À l'instar de l'assistant d'installation de S3, l'assistant d'installation de FabricPool vous aide à configurer rapidement les valeurs requises et génère un fichier que vous pouvez utiliser pour configurer un Tier cloud FabricPool dans ONTAP.

  Si vous prévoyez d'utiliser StorageGRID en tant que système de stockage objet pour un niveau cloud FabricPool, il est recommandé d'utiliser l'assistant d'installation FabricPool, sauf si vous disposez d'une configuration spécifique ou si votre implémentation nécessite une personnalisation importante.

- **Configurer les éléments manuellement**. Si vous vous connectez à une application S3 et que vous préférez ne pas utiliser l'assistant d'installation S3, vous pouvez obtenir les valeurs requises en effectuant la configuration manuellement. Voici la procédure à suivre :

  a. Configurez le groupe haute disponibilité (HA) que vous souhaitez utiliser pour l'application S3. Voir "Configurez les groupes haute disponibilité".

  b. Créez le terminal d'équilibrage de charge que l'application S3 utilisera. Voir "Configurer les terminaux de l'équilibreur de charge".

c. Créez le compte locataire que l'application S3 utilisera. Voir "Créez un compte de locataire".

d. Pour un locataire S3, connectez-vous au compte du locataire et générez un ID de clé d'accès et une clé d'accès secrète pour chaque utilisateur qui accérera à l'application. Voir "Créez vos propres clés d'accès".

e. Créez un ou plusieurs compartiments S3 dans le compte de locataire. Pour S3, voir "Créer un compartiment S3".

f. Pour ajouter des instructions de placement spécifiques pour les objets appartenant au nouveau locataire ou compartiment/conteneur, créez une règle ILM et activez une nouvelle règle ILM pour utiliser cette règle. Voir "Création d'une règle ILM" et "Création de la règle ILM".

Sécurité pour les clients S3

Les comptes de locataires StorageGRID utilisent les applications client S3 pour enregistrer les données d'objet dans StorageGRID. Vous devez examiner les mesures de sécurité mises en œuvre pour les applications client.

Récapitulatif

La liste ci-dessous résume la mise en œuvre de la sécurité pour l'API REST S3 :

Sécurité de la connexion
TLS

Authentification du serveur
Certificat de serveur X.509 signé par l'autorité de certification du système ou certificat de serveur personnalisé fourni par l'administrateur

Authentification client
ID de clé d'accès de compte S3 et clé d'accès secrète

Autorisation du client
Propriété des compartiments et toutes les règles de contrôle d'accès applicables

Comment StorageGRID assure la sécurité des applications client

Les applications client S3 peuvent se connecter au service Load Balancer sur des nœuds de passerelle ou des nœuds d'administration ou directement sur les nœuds de stockage.

- Les clients qui se connectent au service Load Balancer peuvent utiliser HTTPS ou HTTP, en fonction de la façon dont vous "configurez le noeud final de l'équilibreur de charge".

  Le protocole HTTPS fournit une communication sécurisée et cryptée TLS. Il est recommandé de le faire. Vous devez associer un certificat de sécurité au noeud final.

  HTTP fournit une communication non chiffrée moins sécurisée 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 non chiffrée moins sécurisée, mais peut être facultatif "activé" pour les

grilles de non-production ou de test.

- Les communications entre StorageGRID et le client sont chiffrées à l'aide de TLS.
- Les communications entre le service Load Balancer et les nœuds de stockage dans la grille sont cryptées que le terminal de l'équilibreur de charge soit configuré pour accepter les connexions HTTP ou HTTPS.
- Les clients doivent fournir "En-têtes d'authentification HTTP" à StorageGRID pour effectuer les opérations de l'API REST.

Certificats de sécurité et applications client

Dans tous les cas, les applications client peuvent établir des connexions TLS à l'aide d'un certificat de serveur personnalisé chargé par l'administrateur de la grille ou d'un certificat généré par le système StorageGRID :

- Lorsque les applications client se connectent au service Load Balancer, elles utilisent le certificat configuré pour le noeud final de l'équilibreur de charge. Chaque noeud final de l'équilibreur de charge possède son propre certificat—soit un certificat de serveur personnalisé téléchargé par l'administrateur de la grille, soit un certificat généré par l'administrateur de la grille dans StorageGRID lors de la configuration du noeud final.

  Voir "Considérations relatives à l'équilibrage de charge".

- Lorsque les applications client se connectent directement à un nœud de stockage, elles utilisent les certificats de serveur générés par le système qui ont été générés pour les nœuds de stockage lors de l'installation du système StorageGRID (qui sont signés par l'autorité de certification du système), ou un seul certificat de serveur personnalisé fourni pour la grille par un administrateur de grille. Voir "Ajoutez un certificat d'API S3 personnalisé".

Les clients doivent être configurés pour approuver l'autorité de certification qui a signé le certificat qu'ils utilisent pour établir des connexions TLS.

Algorithmes de hachage et de cryptage 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 **règles TLS et SSH**.

Versions supportées de TLS

StorageGRID supporte TLS 1.2 et TLS 1.3.

SSLv3 et TLS 1.1 (ou versions antérieures) ne sont plus pris en charge.

Utilisation de l'assistant d'installation S3

Assistant d'installation S3 : considérations et configuration requise

À l'aide de l'assistant d'installation S3, vous pouvez configurer StorageGRID en tant que système de stockage objet d'une application S3.

Utilisation de l'assistant d'installation S3

L'assistant d'installation S3 vous guide à chaque étape de la configuration d'StorageGRID pour une utilisation avec une application S3. Dans le cadre 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 pour vous assurer que vos paramètres sont conformes aux meilleures pratiques de StorageGRID.

Si vous disposez du "Autorisation d'accès racine", vous pouvez compléter l'assistant d'installation S3 lorsque vous commencez à utiliser le Gestionnaire de grille StorageGRID, ou vous pouvez accéder à l'assistant et l'exécuter ultérieurement. Selon vos besoins, vous pouvez également configurer une partie ou la totalité des éléments requis manuellement, 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 terminé ces conditions préalables.

Obtenir des adresses IP et configurer des interfaces VLAN

Si vous configurez un groupe haute disponibilité, vous savez à quels nœuds l'application S3 se connectera et à quel réseau StorageGRID sera utilisé. Vous savez également quelles valeurs entrer pour le CIDR de sous-réseau, l'adresse IP de la passerelle et les adresses IP virtuelles (VIP).

Si vous prévoyez d'utiliser un réseau local virtuel pour isoler le trafic de l'application S3, vous avez déjà configuré l'interface VLAN. Voir "Configurez les interfaces VLAN".

Configurer la fédération des identités et SSO

Si vous prévoyez d'utiliser la fédération des identités ou l'authentification unique (SSO) pour votre système StorageGRID, vous avez activé ces fonctionnalités. Vous savez également quel groupe fédéré doit disposer d'un accès racine pour le compte locataire utilisé par l'application S3. Voir "Utiliser la fédération des identités" 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 de serveur de noms de domaine (DNS) mapperont ce FQDN aux adresses IP virtuelles (VIP) du groupe haute disponibilité que vous créez à l'aide de l'assistant.

Si vous prévoyez d'utiliser des requêtes de type hébergement virtuel S3, vous devriez avoir "Noms de domaine de terminaux S3 configurés". Il est recommandé d'utiliser des demandes de type hébergement virtuel.

Examinez les exigences en matière d'équilibreur de charge et de certificat de sécurité

Si vous envisagez d'utiliser l'équilibreur de charge StorageGRID, vous avez examiné les considérations générales relatives à l'équilibrage de la 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 noeud final externe (tiers) d'équilibreur de charge, vous disposez du nom de domaine complet (FQDN), du port et du certificat pour cet équilibreur de charge.

Configurez toutes les connexions de fédération de grille

Si vous souhaitez permettre au locataire S3 de cloner les données de compte et de répliquer les objets de compartiment vers une autre grille à l'aide d'une connexion de fédération de grille, vérifiez les points suivants avant de démarrer l'assistant :

- Vous avez "configurez la connexion de fédération de grille - effectué".
- L'état de la connexion est **connecté**.
- Vous disposez de l'autorisation d'accès racine.

Assistant d’installation de S3 et opérations à effectuer

L’assistant d’installation de S3 vous permet de configurer StorageGRID pour une utilisation avec une application S3. L’assistant d’installation fournit les valeurs dont l’application a besoin pour accéder à un compartiment StorageGRID et pour enregistrer des objets.

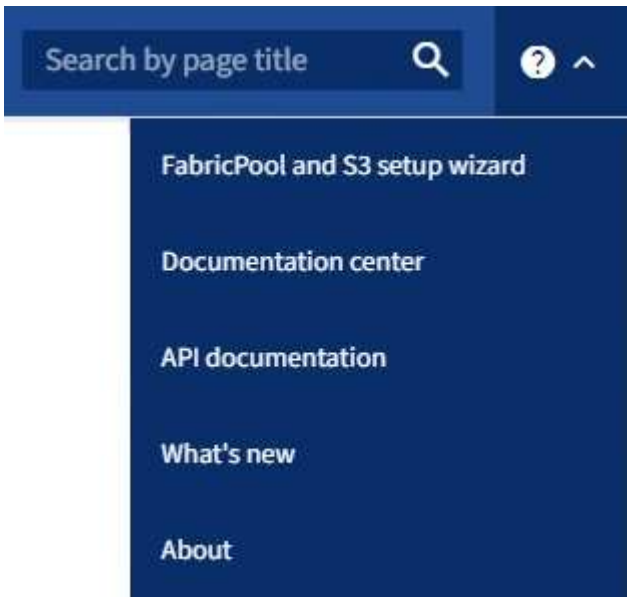
Avant de commencer

- Vous avez le "Autorisation d’accès racine".
- Vous avez examiné le "considérations et exigences" pour à l’aide de l’assistant.

Accéder à l’assistant

Étapes

1. Connectez-vous au Gestionnaire de grille à l’aide d’un "navigateur web pris en charge".
2. Si la bannière **FabricPool and S3 setup Wizard** apparaît sur le tableau de bord, sélectionnez le lien dans la bannière. Si la bannière ne s’affiche plus, sélectionnez l’icône d’aide dans la barre d’en-tête du Gestionnaire de grille et sélectionnez **Assistant d’installation FabricPool et S3**.



3. Dans la section application S3 de la page de l’assistant d’installation FabricPool et S3, sélectionnez **configurer maintenant**.

Étape 1 sur 6 : configuration du groupe haute disponibilité

Un groupe haute disponibilité est un ensemble de nœuds qui contiennent chacun le service StorageGRID Load Balancer. Un groupe haute disponibilité peut contenir des nœuds de passerelle, des nœuds d’administration, ou les deux.

Vous pouvez utiliser un groupe haute disponibilité pour maintenir les connexions de données S3 disponibles. En cas de défaillance de l’interface active du groupe haute disponibilité, 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, reportez-vous "Gérez les groupes haute disponibilité"à la section .

Étapes

1. Si vous prévoyez d'utiliser un équilibreur de charge externe, il n'est pas nécessaire de créer un groupe haute disponibilité. Sélectionnez **Ignorer cette étape** et passez à Étape 2 sur 6 : configuration du terminal de l'équilibreur de charge.
2. Pour utiliser l'équilibreur de charge StorageGRID, vous pouvez créer un nouveau groupe haute disponibilité ou utiliser un groupe haute disponibilité existant.

Création du groupe haute disponibilité

a. Pour créer un nouveau groupe HA, sélectionnez **Create HA group**.

b. Pour l'étape **entrer les détails**, remplissez les champs suivants.

Champ	Description
Nom du groupe HAUTE DISPONIBILITÉ	Un nom d'affichage unique pour ce groupe haute disponibilité.
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 haute disponibilité.

Utilisez les en-têtes de colonne pour trier les lignes ou entrez 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 **hiérarchiser les interfaces**, déterminez l'interface principale et les interfaces de sauvegarde pour ce groupe haute disponibilité.

Faites glisser des lignes pour modifier les valeurs de 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 défaillance.

Si le groupe haute disponibilité comprend plusieurs interfaces et que l'interface active est défaillante, les adresses IP virtuelles (VIP) sont déplacées vers la première interface de sauvegarde, dans l'ordre de priorité. Si cette interface échoue, les adresses VIP passent à l'interface de sauvegarde suivante, etc. Lorsque les pannes sont résolues, les adresses VIP reviennent à l'interface de priorité la plus élevée disponible.

e. Pour l'étape **entrer les adresses IP**, renseignez les champs suivants.

Champ	Description
Sous-réseau CIDR	Adresse du sous-réseau VIP en notation CIDR &#8212 ; adresse IPv4 suivie d'une barre oblique et de la longueur de sous-réseau (0-32). Aucun bit d'hôte ne doit être défini pour l'adresse réseau. Par exemple `192.16.0.0/22`,.
Adresse IP de la passerelle (facultative)	Si les adresses IP S3 utilisées pour accéder à StorageGRID ne se trouvent pas sur le même sous-réseau que les adresses VIP StorageGRID, entrez 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	Entrez au moins une et dix adresses VIP pour l'interface active du groupe HA. Toutes les adresses VIP doivent se trouver dans le sous-réseau VIP. Au moins une adresse doit être IPv4. Vous pouvez éventuellement spécifier des adresses IPv4 et IPv6 supplémentaires.

f. Sélectionnez **Create HA group**, puis **Finish** pour revenir à l'assistant d'installation S3.

g. Sélectionnez **Continuer** pour passer à l'étape d'équilibrage de charge.

Utilisez un groupe haute disponibilité existant

a. Pour utiliser un groupe HA existant, sélectionnez le nom du groupe HA dans le **Sélectionner un groupe HA**.

b. Sélectionnez **Continuer** pour passer à l'étape d'équilibrage de charge.

Étape 2 sur 6 : configuration du terminal de l'équilibreur de charge

StorageGRID utilise un équilibreur de charge pour gérer la charge de travail à partir des applications client. L'équilibrage de la charge optimise la vitesse et la capacité de connexion sur plusieurs nœuds de stockage.

Vous pouvez utiliser le service StorageGRID Load Balancer, qui existe sur tous les nœuds de passerelle et d'administration, ou vous pouvez 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, reportez-vous "Considérations relatives à l'équilibrage de charge"à la section .

Pour utiliser le service StorageGRID Load Balancer, sélectionnez l'onglet **StorageGRID load balancer**, puis créez ou sélectionnez le noeud final 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 final

Étapes

1. Pour créer un noeud final d'équilibrage de charge, sélectionnez **Créer un noeud final**.
2. Pour l'étape **entrer les détails du noeud final**, renseignez les champs suivants.

Champ	Description
Nom	Nom descriptif du noeud final.
Port	Port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est défini par défaut sur 10433 pour le premier noeud final que vous créez, mais vous pouvez entrer n'importe quel port externe inutilisé. Si vous entrez 80 ou 443, le noeud final est configuré uniquement sur les noeuds de passerelle, car ces ports sont réservés sur les noeuds d'administration. **Remarque :** les ports utilisés par d'autres services de grille ne sont pas autorisés. Voir la "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 elle n'est pas recommandée.

3. Pour l'étape **Sélectionner le mode de liaison**, spécifiez le mode de liaison. Le mode de liaison contrôle la façon dont le noeud final est accessible à l'aide d'une 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 final en utilisant l'adresse IP de n'importe quel nœud de passerelle ou nœud d'administration, l'adresse IP virtuelle (VIP) de n'importe quel groupe haute disponibilité sur n'importe quel réseau, ou un FQDN correspondant. Utilisez le paramètre **Global** (valeur par défaut) sauf si vous devez restreindre l'accessibilité de ce point final.
Adresses IP virtuelles de groupes haute disponibilité	Les clients doivent utiliser une adresse IP virtuelle (ou le nom de domaine complet correspondant) d'un groupe haute disponibilité pour accéder à ce point final. Les terminaux associés à ce mode de liaison peuvent tous utiliser le même numéro de port, tant que les groupes haute disponibilité que vous sélectionnez pour les terminaux ne se chevauchent pas.

Mode	Description
Interfaces de nœuds	Les clients doivent utiliser les adresses IP (ou les FQDN correspondants) des interfaces de nœud sélectionnées pour accéder à ce noeud final.
Type de nœud	En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud d'administration ou l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud de passerelle pour accéder à ce point final.

4. Pour l'étape d'accès locataire, sélectionnez l'une des options suivantes :

Champ	Description
Autoriser tous les locataires (par défaut)	Tous les comptes de locataires peuvent utiliser ce terminal pour accéder à leurs compartiments.
Autoriser les locataires sélectionnés	Seuls les comptes de locataire sélectionnés peuvent utiliser ce terminal pour accéder à leurs compartiments.
Bloquez les locataires sélectionnés	Les comptes de locataire sélectionnés ne peuvent pas utiliser ce terminal pour accéder à leurs compartiments. Tous les autres locataires peuvent utiliser ce noeud final.

5. Pour l'étape **joindre un 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.
Générez un certificat	Utilisez cette option pour générer un certificat auto-signé. Voir "Configurer les terminaux de l'équilibreur de charge" pour plus de détails sur ce que vous devez 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 d'API S3" pour plus de détails.

6. Sélectionnez **Terminer** pour revenir à l'assistant d'installation S3.
7. Sélectionnez **Continuer** pour accéder à l'étape tenant et bucket.

Les modifications apportées à un certificat de point final peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

Utilisez le terminal d'équilibrage de charge existant

Étapes

1. Pour utiliser un noeud final existant, sélectionnez son nom dans le **sélectionnez un noeud final d'équilibrage de charge**.
2. Sélectionnez **Continuer** pour accéder à l'étape tenant et bucket.

Utiliser un équilibreur de charge externe

Étapes

1. Pour utiliser un équilibreur de charge externe, renseignez les champs suivants.

Champ	Description
FQDN	Nom de domaine complet (FQDN) de l'équilibreur de charge externe.
Port	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 tenant et bucket.

Étape 3 sur 6 : création d'un locataire et d'un compartiment

Un locataire est une entité qui peut utiliser les applications S3 pour stocker et récupérer des objets dans StorageGRID. Chaque locataire dispose de ses propres utilisateurs, clés d'accès, compartiments, objets et un ensemble spécifique de fonctionnalités.

Un compartiment est un conteneur utilisé pour stocker les objets d'un locataire et ses métadonnées d'objet. Même si les locataires peuvent disposer de plusieurs compartiments, l'assistant vous aide à créer un locataire et un compartiment de la manière la plus rapide et la plus simple. Si vous avez besoin d'ajouter des compartiments ou de définir des options ultérieurement, vous pouvez utiliser le Gestionnaire de locataires.

Pour plus d'informations sur cette tâche, reportez-vous aux sections "Créer un compte de locataire" et "Créer un compartiment S3".

Étapes

1. Entrez un nom pour le compte de locataire.

   Les noms de locataires n'ont pas besoin d'être uniques. Lors de la création du compte locataire, il reçoit un ID de compte numérique unique.

2. Définissez l'accès racine du compte de tenant, selon que votre système StorageGRID utilise "fédération des identités" "Authentification unique (SSO)"ou les deux.

Option	Faites ça
Si la fédération des identités n'est pas activée	Spécifiez le mot de passe à utiliser lors de la connexion au tenant en tant qu'utilisateur root local.

Option	Faites ça
Si la fédération des identités est activée	a. Sélectionnez un groupe fédéré existant "Autorisation d'accès racine"pour le tenant. b. Vous pouvez également spécifier le mot de passe à utiliser lors de la connexion au tenant en tant qu'utilisateur root local.
Si la fédération des identités et l'authentification unique (SSO) sont toutes deux activées	Sélectionnez un groupe fédéré existant "Autorisation d'accès racine"pour le tenant. 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 tenant sera l'utilisateur root. Si d'autres utilisateurs utilisent ce locataire, "Utilisez le gestionnaire de locataires" pour configurer les clés et les autorisations.

4. Si vous voulez créer un compartiment pour ce tenant maintenant, sélectionnez **Créer un compartiment pour ce tenant**.

   Si le verrouillage d'objet S3 est activé pour la grille, le verrouillage d'objet S3 n'est pas activé pour le compartiment créé à cette étape. Si vous avez besoin d'utiliser un compartiment S3 Object Lock pour cette application S3, ne créez pas de compartiment maintenant. Utilisez plutôt le gestionnaire de locataires "créer le godet"plus tard.

   a. Entrez le nom du compartiment que l'application S3 utilisera. Par exemple `s3-bucket`, .

      Vous ne pouvez pas modifier le nom du compartiment après la création du compartiment.

   b. Sélectionnez la **région** pour ce compartiment.

      Utilisez la région par défaut (`us-east-1`) à moins d'utiliser ILM à l'avenir pour filtrer des objets en fonction de la région du compartiment.

5. Sélectionnez **Créer et continuer**.

étape 4 sur 6 : télécharger les données

Dans 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 la clé d'accès S3 de l'utilisateur root automatiquement**, 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 noeud final de l'équilibreur de charge, du locataire, du compartiment et de l'utilisateur root.

3. Enregistrez ces informations dans un emplacement sécurisé.

> Ne fermez pas cette page tant que vous n'avez pas copié les deux clés d'accès. Les touches ne seront pas disponibles après la fermeture de cette page. Veillez à enregistrer ces informations dans un emplacement sécurisé 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 la règle ILM et à l'étape de stratégie.

Étape 5 sur 6 : examen de la règle ILM et de la règle 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 règle ILM incluse à StorageGRID effectue deux copies répliquées de tous les objets. Cette stratégie est en vigueur jusqu'à ce que vous activiez au moins une nouvelle police.

Étapes

1. Passez en revue les informations fournies sur la page.
2. Si vous souhaitez ajouter des instructions spécifiques pour les objets appartenant au nouveau locataire ou compartiment, créez une règle et une nouvelle règle. Voir "Création d'une règle ILM" et "Règles ILM".
3. Sélectionnez **J'ai passé en revue 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 à **Résumé**.

Étape 6 sur 6 : passez en revue le résumé

Étapes

1. Passez en revue le résumé.
2. Notez les détails des étapes suivantes, qui décrivent la configuration supplémentaire qui peut être nécessaire avant de vous connecter au client S3. Par exemple, la sélection de **se connecter en tant que root** vous amène au gestionnaire de locataires, où vous pouvez ajouter des utilisateurs de tenant, créer des compartiments supplémentaires et mettre à jour les paramètres de compartiment.
3. Sélectionnez **Terminer**.
4. Configurez l'application à l'aide du fichier téléchargé à partir de StorageGRID ou des valeurs obtenues manuellement.

Gérer les groupes de haute disponibilité

Que sont les groupes à haute disponibilité ?

Les groupes haute disponibilité proposent des connexions de données extrêmement disponibles pour les clients S3 et des connexions extrêmement disponibles pour Grid Manager et tenant Manager.

Vous pouvez regrouper les interfaces réseau de plusieurs nœuds d'administration et de passerelle dans un groupe haute disponibilité. En cas de défaillance de l'interface active dans le groupe haute disponibilité, une interface de sauvegarde peut gérer la charge de travail.

Chaque groupe HA permet d'accéder aux services partagés sur les nœuds sélectionnés.

- Les groupes HAUTE DISPONIBILITÉ, tels que les nœuds de passerelle et/ou les nœuds d'administration, assurent des connexions de données extrêmement disponibles pour les clients S3.
- Les groupes HAUTE DISPONIBILITÉ comprenant uniquement des nœuds d'administration fournissent des connexions hautement disponibles au Grid Manager et au tenant Manager.
- Un groupe haute disponibilité qui ne comprend que des appliances de services et des nœuds logiciels VMware peut fournir des connexions hautement disponibles pour "Locataires S3 avec S3 Select". Les groupes HAUTE DISPONIBILITÉ sont recommandés lors de l'utilisation de S3 Select, mais pas requis.

Comment créer un groupe haute disponibilité ?

1. Vous sélectionnez une interface réseau pour un ou plusieurs nœuds d'administration ou de passerelle. Vous pouvez utiliser une interface Grid Network (eth0), une interface réseau client (eth2), une interface VLAN ou une interface d'accès que vous avez ajoutée au nœud.

   > Vous ne pouvez pas ajouter d'interface à un groupe haute disponibilité si son adresse IP est attribuée par DHCP.

2. Vous spécifiez une interface à utiliser comme interface principale. L'interface principale est l'interface active, sauf en cas de défaillance.
3. Vous déterminez l'ordre de priorité des interfaces de sauvegarde.
4. Vous affectez une à 10 adresses IP virtuelles (VIP) au groupe. Les applications clients peuvent utiliser l'une de ces adresses VIP pour se connecter à StorageGRID.

Pour obtenir des instructions, reportez-vous à la section "Configurez les groupes haute disponibilité".

Qu'est-ce que l'interface active ?

En fonctionnement normal, toutes les adresses VIP du groupe haute disponibilité sont ajoutées à l'interface principale, qui est la première interface dans l'ordre prioritaire. Tant que l'interface principale reste disponible, elle est utilisée lorsque les clients se connectent à n'importe quelle adresse VIP pour le groupe. C'est-à-dire, pendant le fonctionnement normal, l'interface principale est l'interface « active » du groupe.

De même, pendant le fonctionnement normal, toute interface de priorité inférieure du groupe haute disponibilité fait office d'interfaces de « sauvegarde ». Ces interfaces de sauvegarde ne sont utilisées que si l'interface principale (actuellement active) est indisponible.

Afficher l'état actuel du groupe haute disponibilité d'un nœud

Pour vérifier si un nœud est affecté à un groupe HA et déterminer son état actuel, sélectionnez **NOEUDS** > ***node***.

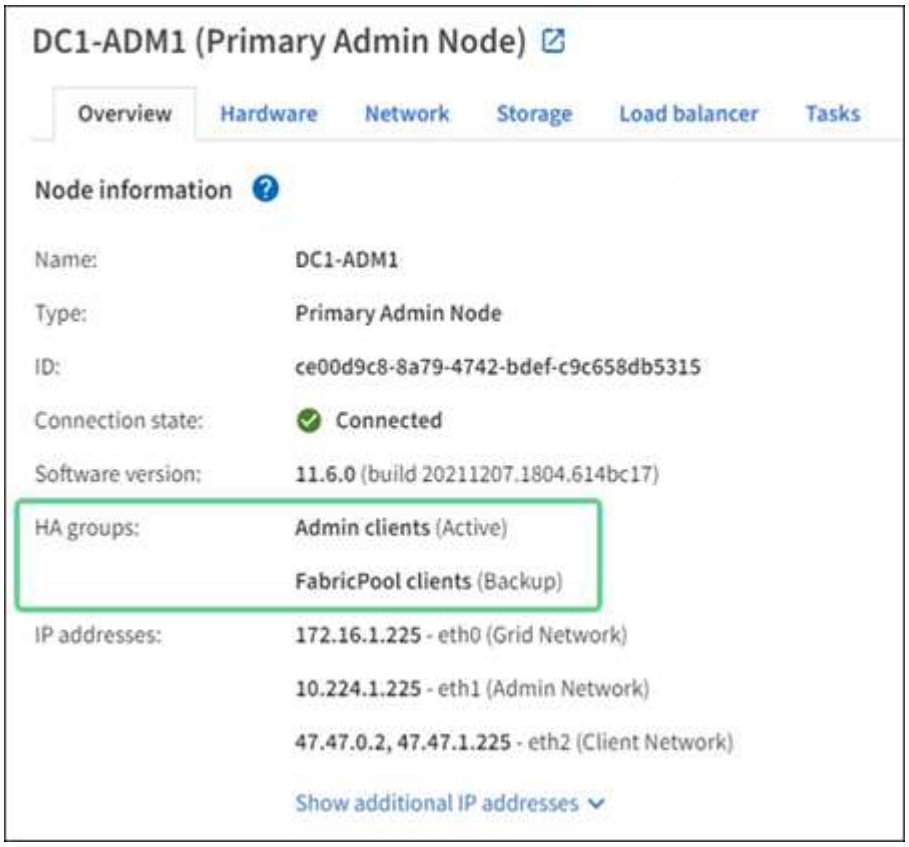
Si l'onglet **Présentation** inclut une entrée pour **groupes HA**, le nœud est affecté aux groupes HA répertoriés. La valeur après le nom du groupe est l'état actuel du nœud du groupe HA :

- **Actif** : le groupe HA est actuellement hébergé sur ce nœud.
- **Backup** : le groupe HA n'utilise pas ce noeud, c'est une interface de sauvegarde.
- **Arrêté** : le groupe HA ne peut pas être hébergé sur ce nœud car le service haute disponibilité (keepalived) a été arrêté manuellement.
- **Fault** : le groupe HA ne peut pas être hébergé sur ce nœud en raison d'un ou plusieurs des éléments

suivants :

- Le service Load Balancer (ninx-gw) n'est pas exécuté sur le nœud.
- L'interface eth0 ou VIP du nœud est en panne.
- Le nœud ne fonctionne pas.

Dans cet exemple, le nœud d'administration principal a été ajouté à deux groupes HA. Ce nœud est actuellement l'interface active du groupe clients Admin et une interface de sauvegarde pour le groupe clients FabricPool.



Que se passe-t-il lorsque l'interface active tombe en panne ?

L'interface qui héberge actuellement les adresses VIP est l'interface active. Si le groupe haute disponibilité inclut plusieurs interfaces et que l'interface active tombe en panne, les adresses VIP sont transférées vers la première interface de sauvegarde disponible dans l'ordre de priorité. Si cette interface échoue, les adresses VIP passent à la prochaine interface de sauvegarde disponible, etc.

Le basculement peut être déclenché pour l'une des raisons suivantes :

- Le nœud sur lequel l'interface est configurée s'éteint.
- Le nœud sur lequel l'interface est configurée perd la connectivité sur tous les autres nœuds pendant au moins 2 minutes.
- L'interface active tombe en panne.
- Le service Load Balancer s'arrête.
- Le service haute disponibilité s'arrête.

Le basculement peut ne pas être déclenché par des pannes réseau externes au nœud qui héberge l'interface active. De même, le basculement n'est pas déclenché par les services pour le Grid Manager ou le tenant Manager.

Le processus de basculement ne prend généralement que quelques secondes et est suffisamment rapide pour que les applications clientes aient peu d'impact et peuvent compter sur des comportements de tentatives normales pour poursuivre le fonctionnement.

Lorsqu'une panne est résolue et qu'une interface de priorité supérieure est à nouveau disponible, les adresses VIP sont automatiquement transférées vers l'interface de priorité la plus élevée disponible.

Comment sont utilisés les groupes haute disponibilité ?

Vous pouvez utiliser des groupes haute disponibilité pour fournir des connexions extrêmement disponibles à StorageGRID pour les données d'objet et pour les tâches d'administration.

- Un groupe haute disponibilité peut fournir des connexions administratives hautement disponibles vers le Grid Manager ou le tenant Manager.
- Un groupe haute disponibilité peut fournir des connexions de données extrêmement disponibles pour les clients S3.
- Un groupe haute disponibilité ne contenant qu'une interface vous permet de fournir de nombreuses adresses VIP et de définir explicitement des adresses IPv6.

Un groupe haute disponibilité peut assurer la haute disponibilité uniquement si tous les nœuds du groupe fournissent les mêmes services. Lorsque vous créez un groupe haute disponibilité, ajoutez des interfaces à partir des types de nœuds qui fournissent les services requis.

- **Nœuds d'administration** : incluez le service Load Balancer et activez l'accès au Grid Manager ou au Gestionnaire de locataires.
- **Nœuds de passerelle** : inclure le service Load Balancer.

Objectif du groupe haute disponibilité	Ajout de nœuds de ce type au groupe haute disponibilité
Accès à Grid Manager	• Nœud d'administration principal (**primaire**) • Nœuds d'administration non primaires **Remarque :** le noeud d'administration principal doit être l'interface principale. Certaines procédures de maintenance peuvent uniquement être effectuées depuis le nœud d'administration principal.
Accès au Gestionnaire de locataires uniquement	• Nœuds d'administration primaires ou non primaires
Accès client S3 — Service d'équilibrage de la charge	• Nœuds d'administration • Nœuds de passerelle

Objectif du groupe haute disponibilité	Ajout de nœuds de ce type au groupe haute disponibilité
Accès client S3 pour "S3 Select"	• Appliances de services • Nœuds logiciels VMware **Remarque** : les groupes HA sont recommandés lors de l'utilisation de S3 Select, mais pas requis.

Restrictions liées à l'utilisation de groupes haute disponibilité avec Grid Manager ou tenant Manager

En cas de défaillance d'un service Grid Manager ou tenant Manager, le basculement du groupe haute disponibilité n'est pas déclenché.

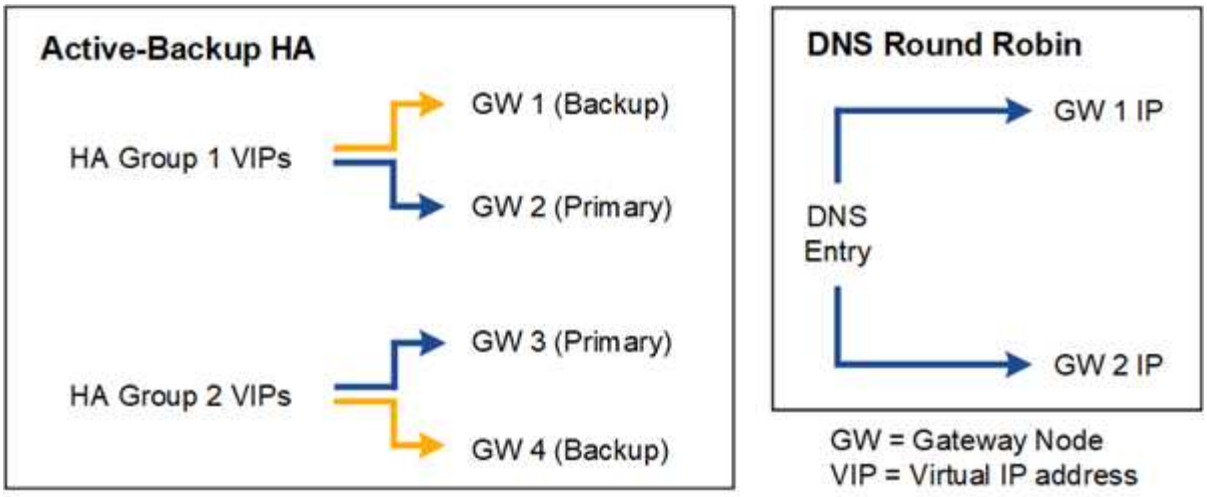
Si vous êtes connecté au Grid Manager ou au tenant Manager lors du basculement, vous êtes déconnecté et vous devez vous reconnecter pour reprendre votre tâche.

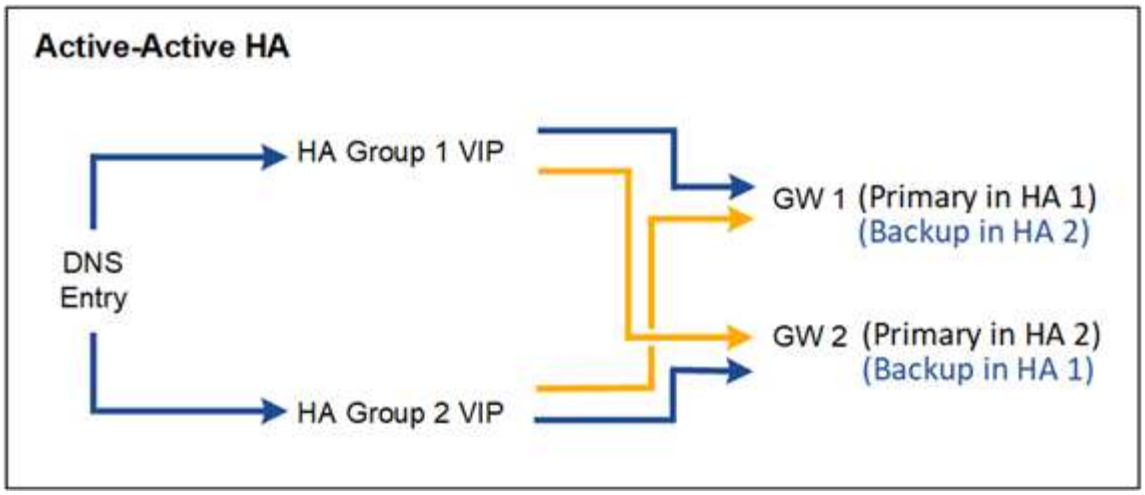
Certaines procédures de maintenance ne peuvent pas être effectuées lorsque le nœud d'administration principal n'est pas disponible. Pendant le basculement, vous pouvez utiliser le Gestionnaire de grille pour surveiller votre système StorageGRID.

Options de configuration pour les groupes haute disponibilité

Les schémas ci-dessous fournissent des exemples de différentes façons de configurer les groupes haute disponibilité. Chaque option présente des avantages et des inconvénients.

Dans les schémas, le bleu indique l'interface principale du groupe haute disponibilité et la jaune indique l'interface de sauvegarde du groupe haute disponibilité.





Le tableau récapitule les avantages de chaque configuration de haute disponibilité illustrée sur le schéma.

Configuration	Avantages	Inconvénients
Active-Backup HA	• Gérées par StorageGRID sans dépendances externes • Basculement rapide	• Un seul nœud d'un groupe haute disponibilité est actif. Au moins un nœud par groupe haute disponibilité sera inactif.
DNS Round Robin	• Un débit global supérieur. • Aucun hôte inactif.	• Basculement lent, qui peut dépendre du comportement des clients. • Nécessite une configuration matérielle en dehors du StorageGRID. • Nécessite une vérification de l'état implémentée par le client.

Configuration	Avantages	Inconvénients
Haute disponibilité actif-actif	• Le trafic est réparti entre plusieurs groupes haute disponibilité. • Débit global élevé qui évolue en même temps que le nombre de groupes HA. • Basculement rapide	• Configuration plus complexe. • Nécessite une configuration matérielle en dehors du StorageGRID. • Nécessite une vérification de l'état implémentée par le client.

Configurez les groupes haute disponibilité

Vous pouvez configurer des groupes haute disponibilité pour fournir un accès haute disponibilité aux services sur des nœuds d'administration ou de passerelle.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine".
- Si vous prévoyez d'utiliser une interface VLAN dans un groupe haute disponibilité, vous avez créé cette interface. Voir "Configurez les interfaces VLAN".
- Si vous prévoyez d'utiliser une interface d'accès pour un nœud d'un groupe haute disponibilité, vous avez créé l'interface :
  - **Red Hat Enterprise Linux (avant d'installer le nœud)** : "Créez des fichiers de configuration de nœud"
  - **Ubuntu ou Debian (avant d'installer le nœud)** : "Créez des fichiers de configuration de nœud"
  - **Linux (après l'installation du nœud)** : "Linux : ajoutez une jonction ou des interfaces d'accès à un nœud"
  - **VMware (après l'installation du nœud)** : "VMware : ajoutez du jonction ou des interfaces d'accès à un nœud"

Créez un groupe haute disponibilité

Lorsque vous créez un groupe haute disponibilité, vous sélectionnez une ou plusieurs interfaces et organisez-les par ordre de priorité. Vous affectez ensuite une ou plusieurs adresses VIP au groupe.

Pour qu'un nœud de passerelle ou un nœud d'administration soit inclus dans un groupe haute disponibilité, une interface doit être configurée pour inclure un nœud de passerelle. Un groupe haute disponibilité ne peut utiliser qu'une interface pour un nœud donné. Toutefois, les autres interfaces du même nœud peuvent être utilisées dans d'autres groupes haute disponibilité.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **groupes haute disponibilité**.
2. Sélectionnez **Créer**.

Entrez les détails du groupe haute disponibilité

Étapes

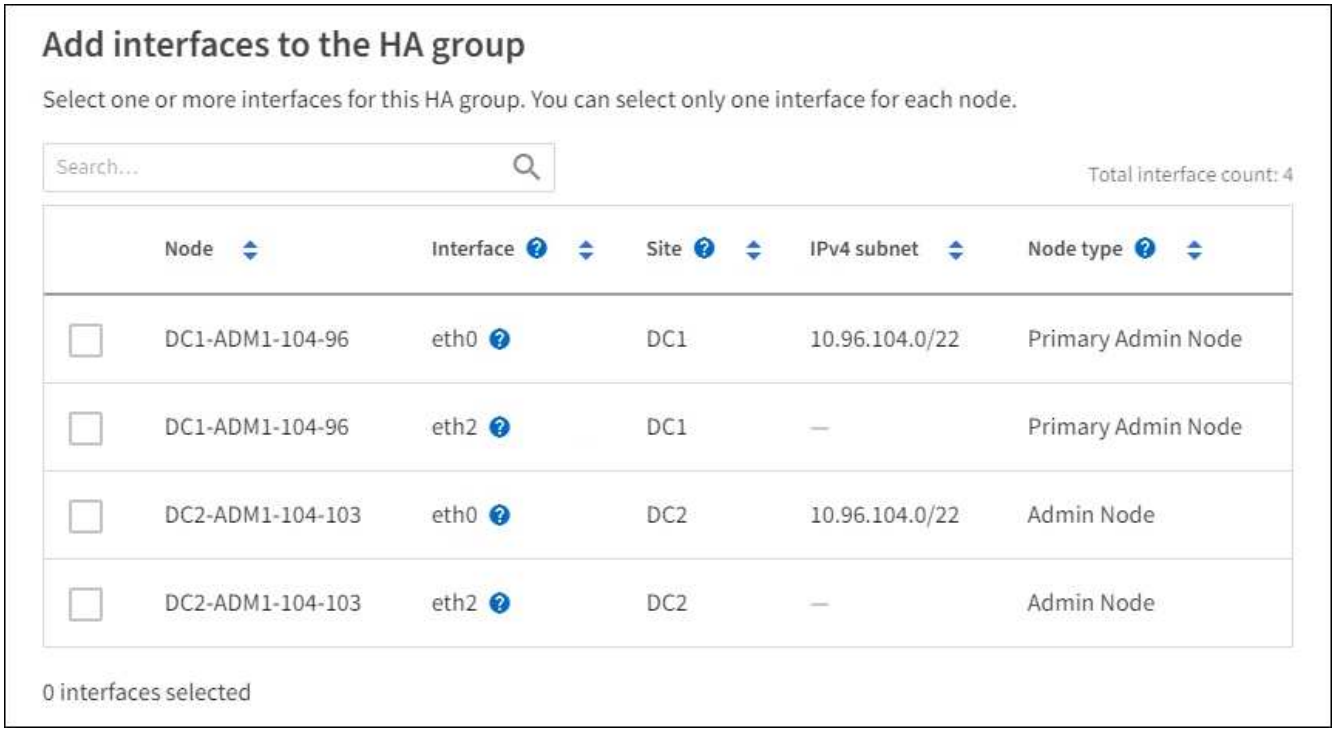
1. Indiquez un nom unique pour le groupe HA.
2. Si vous le souhaitez, entrez une description pour le groupe HA.
3. Sélectionnez **Continuer**.

Ajouter des interfaces au groupe haute disponibilité

Étapes

1. Sélectionnez une ou plusieurs interfaces à ajouter à ce groupe haute disponibilité.

   Utilisez les en-têtes de colonne pour trier les lignes ou entrez un terme de recherche pour localiser les interfaces plus rapidement.

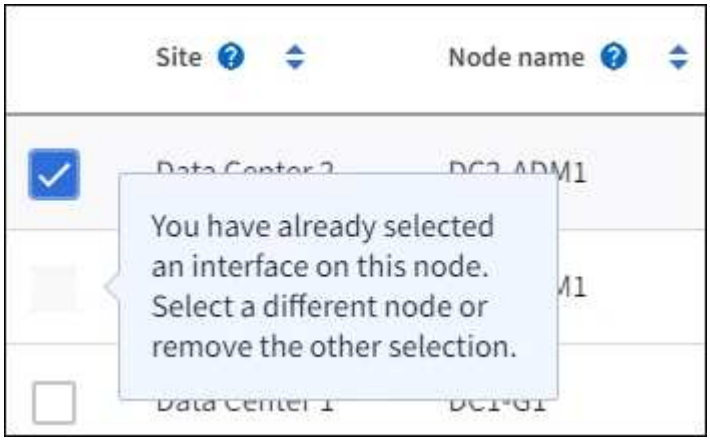


> Après avoir créé une interface VLAN, attendez jusqu'à 5 minutes que la nouvelle interface apparaisse dans le tableau.

Consignes de sélection des interfaces

- Vous devez sélectionner au moins une interface.
- Vous ne pouvez sélectionner qu'une interface pour un nœud.
- Si le groupe HA est destiné à la protection haute disponibilité des services des nœuds d'administration, qui incluent le Grid Manager et le tenant Manager, sélectionnez les interfaces sur les nœuds d'administration uniquement.
- Si le groupe haute disponibilité est dédié à la protection HA du trafic client S3, sélectionnez interfaces sur les nœuds d'administration, 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 que en cas de basculement, les services fournis par le nœud actif précédemment risquent de ne pas être disponibles sur le nouveau nœud actif. Par exemple, un nœud de passerelle de sauvegarde ne peut pas assurer la protection haute disponibilité des services du nœud d'administration. De même, un nœud d'administration des sauvegardes 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 d'interface si sa valeur de sous-réseau ou sa passerelle entre 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**.

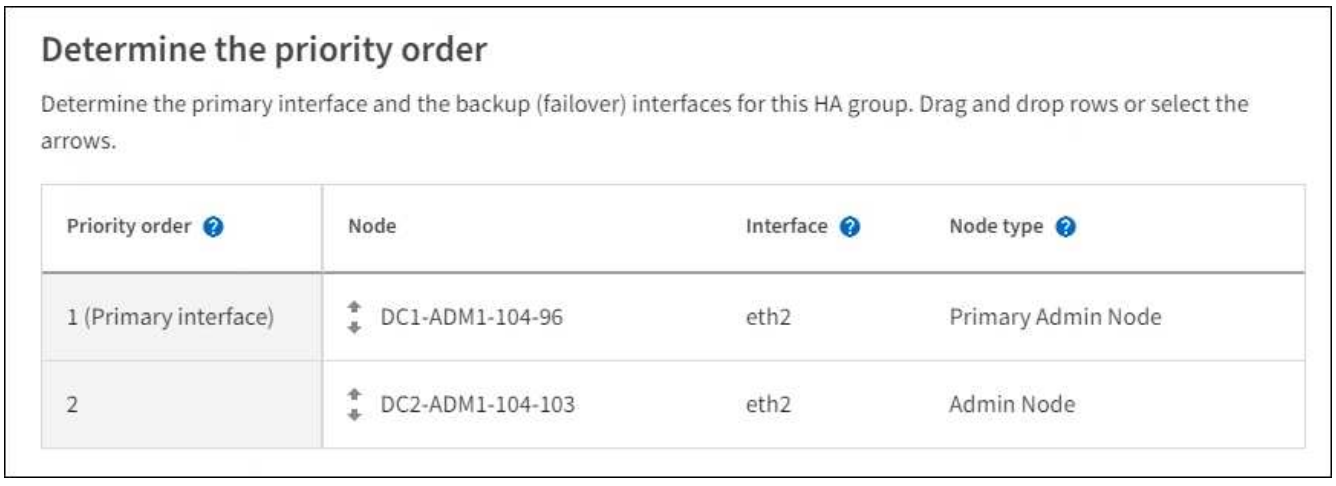
Déterminez l'ordre de priorité

Si le groupe haute disponibilité comprend plusieurs interfaces, vous pouvez déterminer qui est l'interface principale et quelles sont les interfaces de sauvegarde (basculement). Si l'interface principale échoue, les adresses VIP passent à l'interface de priorité la plus élevée disponible. En cas d'échec de cette interface, les adresses VIP passent à l'interface de priorité supérieure suivante disponible, etc.

Étapes

1. Faites glisser des lignes dans la colonne **ordre de priorité** pour déterminer l'interface principale et 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 défaillance.



Si le groupe HA donne accès à Grid Manager, vous devez sélectionner une interface sur le nœud d'administration principal pour qu'il soit l'interface principale. Certaines procédures de maintenance peuvent uniquement être effectuées depuis le nœud d'administration principal.

2. Sélectionnez **Continuer**.

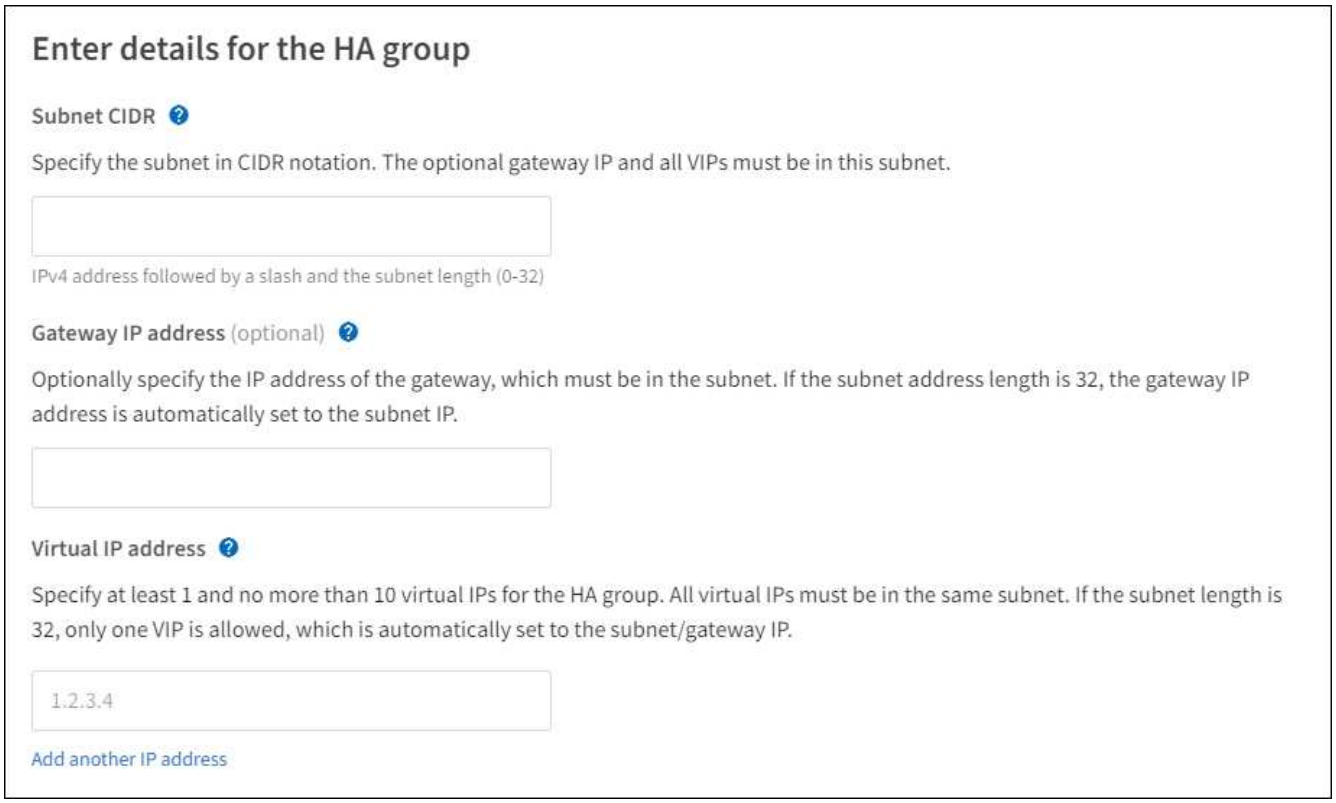
Saisissez les adresses IP

Étapes

1. Dans le champ **Subnet 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).

   Aucun bit d'hôte ne doit être défini pour l'adresse réseau. 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. Si vous le souhaitez, si des clients d'administration ou de locataire S3 accèdent à ces adresses VIP à partir d'un sous-réseau différent, entrez l'adresse IP **Gateway**. L'adresse de la passerelle doit se trouver dans le sous-réseau VIP.

   Les utilisateurs client et admin utiliseront cette passerelle pour accéder aux adresses IP virtuelles.

3. Entrez au moins une et dix adresses VIP pour l'interface active du 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. Vous pouvez éventuellement spécifier des adresses IPv4 et IPv6 supplémentaires.

4. Sélectionnez **Créer groupe HA** et **Terminer**.

   Le groupe haute disponibilité est créé et vous pouvez maintenant utiliser les adresses IP virtuelles configurées.

Étapes suivantes

Si vous utilisez ce groupe haute disponibilité pour équilibrer la charge, créez un terminal d'équilibreur de charge afin de déterminer le port et le protocole réseau, et de connecter tous les certificats requis. Voir "Configurer les terminaux de l'équilibreur de charge".

Modifiez un groupe haute disponibilité

Vous pouvez modifier un groupe haute disponibilité (HA) pour modifier 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 haute disponibilité si vous souhaitez supprimer le nœud associé à une interface sélectionnée dans la procédure de mise hors service d'un site ou d'un nœud.

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **groupes haute disponibilité**.

   La page groupes haute disponibilité affiche tous les groupes haute disponibilité existants.

2. Cochez la case du groupe haute disponibilité à 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 du groupe haute disponibilité.
   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 donne accès à Grid Manager, vous devez sélectionner une interface sur le nœud d'administration principal pour qu'il soit l'interface principale. Certaines procédures de maintenance peuvent uniquement être effectuées depuis le nœud d'administration principal

   c. Vous pouvez également faire glisser des lignes pour modifier l'ordre de priorité de l'interface principale et des interfaces de sauvegarde de ce groupe haute disponibilité.
   d. Si vous le souhaitez, mettez à jour les adresses IP virtuelles.
   e. Sélectionnez **Enregistrer**, puis **Terminer**.

Supprimer un groupe haute disponibilité

Vous pouvez supprimer un ou plusieurs groupes haute disponibilité (HA) à la fois.

> Vous ne pouvez pas supprimer un groupe haute disponibilité s'il est lié à un terminal d'équilibrage de charge. Pour supprimer un groupe haute disponibilité, vous devez le supprimer de tous les terminaux d'équilibrage de charge qui l'utilisent.

Pour éviter toute interruption de service, mettez à jour toutes les applications client S3 affectées avant de supprimer un groupe haute disponibilité. Mettre à jour chaque client pour se connecter à l'aide d'une autre adresse IP, par exemple l'adresse IP virtuelle d'un autre groupe haute disponibilité ou l'adresse IP configurée pour une interface lors de l'installation.

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **groupes haute disponibilité**.
2. Consultez la colonne **Load Balancer Endpoints** pour chaque groupe HA que vous souhaitez supprimer. Si des terminaux d'équilibrage de charge sont répertoriés :
   a. Accédez à **CONFIGURATION** > **réseau** > **noeuds finaux de l'équilibreur de charge**.
   b. Cochez la case du point final.
   c. Sélectionnez **actions** > **Modifier le mode de liaison du point final**.
   d. Mettez à jour le mode de liaison pour supprimer le groupe HA.
   e. Sélectionnez **Enregistrer les modifications**.
3. Si aucun point final de l'équilibreur de charge n'est répertorié, cochez la case de chaque groupe haute disponibilité à supprimer.
4. Sélectionnez **actions** > **Supprimer groupe HA**.
5. Vérifiez le message et sélectionnez **Supprimer le groupe HA** pour confirmer votre sélection.

   Tous les groupes HA sélectionnés sont supprimés. Une bannière de réussite verte apparaît sur la page groupes de haute disponibilité.

Gérer l'équilibrage des charges

Considérations relatives à l'équilibrage de charge

L'équilibrage des charges vous permet de gérer les workloads d'ingestion et de récupération à partir des clients S3.

Qu'est-ce que l'équilibrage de la charge ?

Lorsqu'une application client enregistre ou récupère les données d'un système StorageGRID, StorageGRID utilise un équilibreur de charge pour gérer la charge de travail d'ingestion et de récupération. L'équilibrage de la charge optimise 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 sur tous les nœuds de passerelle. Il assure l'équilibrage de la charge de couche 7. Il effectue la résiliation du protocole TLS (transport Layer Security) des requêtes du client, inspecte les requêtes et établit de nouvelles connexions sécurisées vers les nœuds de stockage.

Le service Load Balancer de chaque nœud fonctionne indépendamment lors du transfert du trafic client vers les nœuds de stockage. Par le biais d'un processus de pondération, le service Load Balancer achemine davantage de requêtes vers des nœuds de stockage avec une disponibilité de processeur supérieure.

> Bien que le service StorageGRID Load Balancer soit le mécanisme d'équilibrage de la charge recommandé, vous pouvez à la place intégrer un équilibreur de charge tiers. Pour plus d'informations, contactez votre représentant de compte NetApp ou reportez-vous à la "Tr-4626 : équilibreurs de charge mondiaux et tiers StorageGRID".

De combien de nœuds d'équilibrage de charge ai-je besoin ?

Dans le cadre des meilleures pratiques générales, chaque site de votre système StorageGRID doit inclure au moins deux nœuds 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.

Qu'est-ce qu'un terminal d'équilibrage de charge ?

Un noeud final d'équilibrage de charge définit le port et le protocole réseau (HTTPS ou HTTP) utilisés par les demandes d'applications clientes entrantes et sortantes pour accéder aux noeuds qui contiennent le service d'équilibrage de charge. Le noeud final définit également le type de client (S3), le mode de liaison et éventuellement une liste de locataires autorisés ou bloqués.

Pour créer un noeud final d'équilibrage de charge, sélectionnez **CONFIGURATION** > **réseau** > **noeuds finaux d'équilibrage de charge** ou exécutez l'assistant d'installation FabricPool et S3. Pour obtenir des instructions :

- "Configurer les terminaux de l'équilibreur de charge"
- "Utilisez l'assistant d'installation S3"
- "Utilisez l'assistant de configuration FabricPool"

Considérations relatives au port

Par défaut, le port d'un noeud final d'équilibrage de charge est 10433 pour le premier noeud final que vous créez, mais vous pouvez spécifier tout port externe inutilisé compris entre 1 et 65535. Si vous utilisez le port 80 ou 443, le noeud final utilisera le service Load Balancer sur les noeuds passerelle uniquement. Ces ports sont réservés sur des nœuds d'administration. Si vous utilisez le même port pour plusieurs noeuds finaux, vous devez spécifier un mode de liaison différent pour chaque noeud final.

Les ports utilisés par d'autres services de grille ne sont pas autorisés. Voir la "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 chiffrement TLS (transport Layer Security). La connexion à StorageGRID sans chiffrement TLS est prise en charge, mais elle n'est pas recommandée, en particulier dans les environnements de production. Lorsque vous sélectionnez le protocole réseau pour le noeud final de l'équilibreur de charge StorageGRID, vous devez sélectionner **HTTPS**.

Considérations relatives aux certificats de terminaux d'équilibrage de charge

Si vous sélectionnez **HTTPS** comme protocole réseau pour le noeud final de l'équilibreur de charge, vous devez fournir un certificat de sécurité. Lorsque vous créez le terminal de l'équilibreur de charge, vous pouvez

utiliser l'une de ces trois options :

- **Télécharger un certificat signé (recommandé)**. Ce certificat peut être signé par une autorité de certification publique ou privée. Il est recommandé d'utiliser un certificat de serveur d'autorité de certification de confiance publique pour sécuriser la connexion. Contrairement aux certificats générés, les certificats signés par une autorité de certification peuvent être permutés sans interruption, ce qui permet d'éviter les problèmes d'expiration.

  Vous devez obtenir les fichiers suivants avant de créer le noeud final de l'équilibreur de charge :

  - Le fichier de certificat de serveur personnalisé.
  - Le fichier de clé privée du certificat de serveur personnalisé.
  - Éventuellement, un paquet CA des certificats de chaque autorité de certification intermédiaire émettrice.
- **Générer un certificat auto-signé**.
- **Utilisez le certificat StorageGRID S3 global**. Vous devez télécharger ou générer une version personnalisée de ce certificat avant de pouvoir le sélectionner pour le noeud final de l'équilibreur de charge. Voir "Configurer les certificats d'API S3".

Quelles valeurs ai-je besoin ?

Pour créer le certificat, vous devez connaître tous les noms de domaine et adresses IP utilisés par les applications client S3 pour accéder au terminal.

L'entrée **Subject DN** (Distinguished Name) du certificat doit inclure le nom de domaine complet que l'application client 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 Load Balancer. 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 hébergement virtuel S3, le certificat doit également inclure une entrée **alternative Name** pour chaque "Nom du domaine du terminal S3" que vous avez configuré, y compris 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 "Consignes de renforcement des certificats de serveur".

Vous devez également définir une entrée DNS pour chaque nom du certificat de sécurité.

Comment gérer les certificats arrivant à expiration ?

> Si le certificat utilisé pour sécuriser la connexion entre l'application S3 et StorageGRID expire, l'application risque de perdre temporairement l'accès à StorageGRID.

Pour éviter les problèmes d'expiration des certificats, suivez les bonnes pratiques suivantes :

- Surveillez attentivement toutes les alertes signalant l'approche des dates d'expiration des certificats, telles que le **expiration du certificat de noeud final de l'équilibreur de charge** et le **expiration du certificat de serveur global pour les alertes de l'API S3**.
- Synchronisez toujours les versions du certificat des applications StorageGRID et S3. Si vous remplacez ou renouvelez le certificat utilisé pour un terminal d'équilibrage de charge, vous devez remplacer ou renouveler le certificat équivalent utilisé par l'application S3.
- Utiliser un certificat d'autorité de certification signé publiquement. Si vous utilisez un certificat signé par une autorité de certification, vous pouvez remplacer les certificats bientôt expirés sans interruption.
- Si vous avez généré un certificat StorageGRID auto-signé et que ce certificat est sur le point d'expirer, vous devez le remplacer manuellement dans StorageGRID et dans l'application S3 avant que le certificat existant n'expire.

Considérations relatives au mode de liaison

Le mode de liaison vous permet de contrôler les adresses IP qui peuvent être utilisées pour accéder à un noeud final de l'équilibreur de charge. Si un noeud final utilise un mode de liaison, les applications clientes peuvent uniquement accéder au noeud final 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 autre nom de domaine complet ne peuvent pas accéder au point final.

Vous pouvez spécifier l'un des modes de reliure suivants :

- **Global** (par défaut) : les applications clientes peuvent accéder au noeud final en utilisant l'adresse IP de n'importe quel noeud de passerelle ou noeud d'administration, l'adresse IP virtuelle (VIP) de n'importe quel groupe HA sur n'importe quel réseau, ou un FQDN correspondant. Utilisez ce paramètre, sauf si vous avez besoin de restreindre l'accessibilité d'un noeud final.
- **Adresses IP virtuelles des groupes HA**. Les applications client doivent utiliser une adresse IP virtuelle (ou le nom de domaine complet correspondant) d'un groupe haute disponibilité.
- **Interfaces de nœud**. Les clients doivent utiliser les adresses IP (ou les FQDN correspondants) des interfaces de nœud sélectionnées.
- **Type de noeud**. En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud d'administration ou l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud de passerelle.

Considérations relatives à l'accès des locataires

L'accès aux locataires est une fonction de sécurité facultative qui vous permet de contrôler quels comptes de locataires StorageGRID peuvent utiliser un terminal d'équilibrage des charges pour accéder à leurs compartiments. Vous pouvez autoriser tous les locataires à accéder à un noeud final (par défaut), ou vous pouvez spécifier une liste des locataires autorisés ou bloqués pour chaque noeud final.

Vous pouvez utiliser cette fonction pour améliorer l'isolation de sécurité entre les locataires et leurs terminaux. Par exemple, vous pouvez utiliser cette fonction pour vous assurer que les matériaux les plus secrets ou les matériaux hautement classés appartenant à un locataire restent complètement 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 (par exemple avec un accès anonyme), le propriétaire du compartiment est utilisé pour déterminer le locataire.

Exemple d'accès aux locataires

Pour comprendre le fonctionnement de cette fonction de sécurité, prenez l'exemple suivant :

1. Vous avez créé deux terminaux d'équilibrage de charge, comme suit :
   - **Noeud final public** : utilise le port 10443 et permet l'accès à tous les locataires.
   - **Point final Top secret** : utilise le port 10444 et permet l'accès au locataire **Top secret** uniquement. Tous les autres locataires ne peuvent pas accéder à ce noeud final.
2. Le `top-secret.pdf` est dans un seau appartenant au locataire **Top secret**.

Pour accéder au `top-secret.pdf`, un utilisateur du locataire **Top secret** peut émettre une demande GET à `https://w.x.y.z:10444/top-secret.pdf`. Comme ce locataire est autorisé à utiliser le noeud final 10444, l'utilisateur peut accéder à l'objet. Cependant, si un utilisateur appartenant à un autre locataire envoie la même requête à la même URL, il reçoit un message accès refusé immédiat. L'accès est refusé même si les informations d'identification et la signature sont valides.

Disponibilité du processeur

Le service Load Balancer sur chaque nœud d'administration et de passerelle fonctionne de manière indépendante lors du transfert du trafic S3 vers les nœuds de stockage. Par le biais d'un processus de pondération, le service Load Balancer achemine davantage de requêtes vers des nœuds de stockage avec une disponibilité de processeur supérieure. Les informations de charge de l'UC du nœud sont mises à jour toutes les quelques minutes, mais la pondération peut être mise à jour plus fréquemment. Tous les nœuds de stockage se voient attribuer une valeur de poids de base minimale, même si un nœud indique une utilisation de 100 % ou ne parvient pas à signaler son utilisation.

Dans certains cas, les informations relatives à la disponibilité du processeur sont limitées au site où se trouve le service Load Balancer.

Configurer les terminaux de l'équilibreur de charge

Les terminaux d'équilibrage de la 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 noeuds finaux pour accéder au Gestionnaire de grille, au Gestionnaire de locataires, ou aux deux.

Les détails SWIFT ont été supprimés de cette version du site doc. Voir "Configurez les connexions des clients S3 et Swift".

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine".
- Vous avez examiné le "considérations relatives à l'équilibrage de charge".

- Si vous avez précédemment remappé un port que vous prévoyez d'utiliser pour le noeud final de l'équilibreur de charge, vous avez "retirez le schéma de câblage des ports - effectué".
- Vous avez créé tous les groupes à haute disponibilité (HA) que vous prévoyez d'utiliser. Les groupes HAUTE DISPONIBILITÉ sont recommandés, mais pas obligatoires. Voir "Gérez les groupes haute disponibilité".
- Si le noeud final de l'équilibreur de charge sera utilisé par "Locataires S3 pour S3 Select", il ne doit pas utiliser les adresses IP ou les FQDN des nœuds sans système d'exploitation. Seules les appliances de services et les nœuds logiciels basés sur VMware sont autorisés pour les terminaux d'équilibrage de charge utilisés pour S3 Select.
- Vous avez configuré toutes les interfaces VLAN que vous prévoyez d'utiliser. Voir "Configurez les interfaces VLAN".
- Si vous créez un noeud final HTTPS (recommandé), vous disposez des informations relatives au certificat de serveur.

> Les modifications apportées à un certificat de point final peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

  - Pour télécharger un certificat, vous avez besoin du certificat de serveur, de la clé privée de certificat et, éventuellement, d'un bundle CA.
  - Pour générer un certificat, vous devez disposer de tous les noms de domaine et adresses IP que les clients S3 utiliseront pour accéder au terminal. Vous devez également connaître le sujet (Nom unique).
  - Si vous souhaitez utiliser le certificat d'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 d'API S3".

Créer un noeud final d'équilibreur de charge

Chaque terminal de l'équilibreur de charge client S3 spécifie un port, un type de client (S3) et un protocole réseau (HTTP ou HTTPS). Les noeuds finaux de l'équilibreur de charge de l'interface de gestion indiquent un port, un type d'interface et un réseau client non fiable.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **noeuds finaux de l'équilibreur de charge**.
2. Pour créer un noeud final pour un client S3 ou Swift, sélectionnez l'onglet **S3 ou Swift client**.
3. Pour créer un noeud final permettant d'accéder au Gestionnaire de grille, au Gestionnaire de locataires ou aux deux, sélectionnez l'onglet **interface de gestion**.
4. Sélectionnez **Créer**.

Saisissez les détails du point final

Étapes

1. Sélectionnez les instructions appropriées pour entrer les détails du type de point final que vous souhaitez créer.

Client S3 ou Swift

Champ	Description
Nom	Nom descriptif du noeud final, qui apparaîtra dans le tableau sur la page noeuds finaux de l'équilibreur de charge.
Port	Port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est défini par défaut sur 10433 pour le premier noeud final que vous créez, mais vous pouvez entrer n'importe quel port externe inutilisé de 1 à 65535. Si vous entrez **80** ou **8443**, le noeud final est configuré uniquement sur les noeuds passerelle, sauf si vous avez libéré le port 8443. Vous pouvez ensuite utiliser le port 8443 en tant que terminal S3 et le port sera configuré à la fois sur les nœuds de passerelle et d'administration.
Type de client	Type d'application client qui utilisera ce noeud final, **S3** ou **Swift**.
Protocole réseau	Protocole réseau utilisé par les clients lors de la connexion à ce noeud final. • Sélectionnez **HTTPS** pour la communication sécurisée et cryptée TLS (recommandé). Vous devez joindre un certificat de sécurité avant de pouvoir enregistrer le noeud final. • Sélectionnez **HTTP** pour une communication moins sécurisée et non chiffrée. Utilisez HTTP uniquement pour une grille autre que la production.

Interface de gestion

Champ	Description
Nom	Nom descriptif du noeud final, qui apparaîtra dans le tableau sur la page noeuds finaux de l'équilibreur de charge.
Port	Port StorageGRID que vous souhaitez utiliser pour accéder au Gestionnaire de grille, au Gestionnaire de locataires ou aux deux. • Gestionnaire de grille : **8443** • Gestionnaire de locataires : **9443** • Gestionnaire de grille et gestionnaire de locataire : **443** **Remarque** : vous pouvez utiliser ces ports prédéfinis ou d'autres ports disponibles.
Type d'interface	Sélectionnez le bouton radio de l'interface StorageGRID à laquelle vous allez accéder à l'aide de ce noeud final.

Champ	Description
Réseau client non fiable	Sélectionnez **Oui** si ce noeud final 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 qu'un port pour qu'il soit ouvert ou fermé aux réseaux clients non approuvés lorsque vous créez le noeud final de l'équilibreur de charge.

1. Sélectionnez **Continuer**.

Sélectionnez un mode de reliure

Étapes

1. Sélectionnez un mode de liaison pour le noeud final afin de contrôler la façon dont le noeud final 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 noeuds finaux clients ou les noeuds finaux de l'interface de gestion. Tous les modes pour les deux types de point final sont répertoriés ici.

Mode	Description
Global (par défaut pour les noeuds finaux clients)	Les clients peuvent accéder au point final en utilisant l'adresse IP de n'importe quel nœud de passerelle ou nœud d'administration, l'adresse IP virtuelle (VIP) de n'importe quel groupe haute disponibilité sur n'importe quel réseau, ou un FQDN correspondant. Utilisez le paramètre **Global** sauf si vous devez restreindre l'accessibilité de ce noeud final.
Adresses IP virtuelles de groupes haute disponibilité	Les clients doivent utiliser une adresse IP virtuelle (ou le nom de domaine complet correspondant) d'un groupe haute disponibilité pour accéder à ce point final. Les terminaux associés à ce mode de liaison peuvent tous utiliser le même numéro de port, tant que les groupes haute disponibilité que vous sélectionnez pour les terminaux ne se chevauchent pas.
Interfaces de nœuds	Les clients doivent utiliser les adresses IP (ou les FQDN correspondants) des interfaces de nœud sélectionnées pour accéder à ce noeud final.
Type de nœud (terminaux client uniquement)	En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud d'administration ou l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud de passerelle pour accéder à ce point final.

Mode	Description
Tous les nœuds d'administration (valeur par défaut pour les terminaux de l'interface de gestion)	Les clients doivent utiliser l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud d'administration pour accéder à ce point final.

Si plusieurs noeuds finaux utilisent le même port, StorageGRID utilise cet ordre de priorité pour décider quel noeud final utiliser : **adresses IP virtuelles des groupes HA** > **interfaces de noeud** > **Type de noeud** > **Global**.

Si vous créez des terminaux 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 terminaux d'interface de gestion, sélectionnez les VIP associés uniquement aux nœuds d'administration.

3. Si vous avez sélectionné **Node interfaces**, sélectionnez une ou plusieurs interfaces de nœud pour chaque noeud d'administration ou nœud de passerelle que vous souhaitez associer à ce noeud final.
4. Si vous avez sélectionné **Type de noeud**, sélectionnez soit noeuds Admin, qui comprend à la fois le noeud Admin principal et tous les noeuds Admin non primaires, soit noeuds Gateway.

Contrôle de l'accès des locataires

> Un noeud final de l'interface de gestion ne peut contrôler l'accès des locataires que lorsque le noeud final possède le Type d'interface du gestionnaire de locataires.

Étapes

1. Pour l'étape **tenant Access**, sélectionnez l'une des options suivantes :

Champ	Description
Autoriser tous les locataires (par défaut)	Tous les comptes de locataires peuvent utiliser ce terminal pour accéder à leurs compartiments. Vous devez sélectionner cette option si vous n'avez pas encore créé de compte de locataire. Après avoir ajouté des comptes de locataire, vous pouvez modifier le terminal de l'équilibreur de charge pour autoriser ou bloquer des comptes spécifiques.
Autoriser les locataires sélectionnés	Seuls les comptes de locataire sélectionnés peuvent utiliser ce terminal pour accéder à leurs compartiments.
Bloquez les locataires sélectionnés	Les comptes de locataire sélectionnés ne peuvent pas utiliser ce terminal pour accéder à leurs compartiments. Tous les autres locataires peuvent utiliser ce noeud final.

2. Si vous créez un noeud final **HTTP**, vous n'avez pas besoin de joindre un certificat. Sélectionnez **Créer** pour ajouter le nouveau noeud final de l'équilibreur de charge. Ensuite, passez à Une fois que vous avez

terminé. Sinon, sélectionnez **Continuer** pour joindre le certificat.

Joindre un certificat

Étapes

1. Si vous créez un noeud final **HTTPS**, sélectionnez le type de certificat de sécurité que vous souhaitez associer au noeud final.

   Le certificat sécurise les connexions entre les clients S3 et le service Load Balancer sur un nœud d'administration ou des 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 avez les valeurs nécessaires pour générer un certificat personnalisé.
   - **Utiliser le certificat StorageGRID S3**. Sélectionnez cette option si vous souhaitez utiliser le certificat d'API S3 global, qui peut également être utilisé pour les connexions directes aux nœuds de stockage.

     Vous ne pouvez sélectionner cette option que si vous avez remplacé le certificat d'API S3 par défaut, signé par l'autorité de certification de la grille, par un certificat personnalisé signé par une autorité de certification externe. Voir "Configurer les certificats d'API S3".

   - **Utiliser le certificat d'interface de gestion**. Sélectionnez cette option si vous souhaitez utiliser le certificat de l'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** : fichier de certificat de serveur personnalisé dans le codage PEM.
- **Clé privée de certificat** : fichier de clé privée de certificat de serveur personnalisé (`.key`).

> Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2048 bits ou plus.

- **Paquet CA** : un fichier facultatif unique contenant les certificats de chaque autorité de certification intermédiaire (AC). Le fichier doit contenir chacun des fichiers de certificat d'autorité de certification codés au PEM, concaténés dans l'ordre de la chaîne de certificats.

c. Développez **Détails du certificat** pour afficher 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 paquet CA** pour enregistrer le lot 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 **Copy certificate PEM** ou **Copy CA bundle PEM** pour copier le contenu du certificat pour le coller ailleurs.

d. Sélectionnez **Créer**. + le noeud final 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 terminal.

Générez un certificat

a. Sélectionnez **générer certificat**.

b. Spécifiez les informations de certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine complets à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.
IP	Une ou plusieurs adresses IP à inclure dans le certificat.
Objet (facultatif)	Objet 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 l'adresse IP comme nom commun de l'objet (CN).

Champ	Description
Jours valides	Nombre de jours après la création, pendant lesquels le certificat expire.
Ajouter des extensions d'utilisation de clé	Si cette option est sélectionnée (par défaut et recommandée), l'utilisation des clés et les extensions d'utilisation des clés étendues sont ajoutées au certificat généré. Ces extensions définissent l'objectif de la clé contenue dans le certificat. **Remarque** : ne cochez pas cette case si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **generate**.

d. Sélectionnez **Détails du certificat** pour afficher 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 pour le coller ailleurs.

e. Sélectionnez **Créer**.

Le noeud final 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 terminal.

Une fois que vous avez 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 de l'utilisation ou non d'un groupe HA de nœuds d'équilibrage de la charge :

   - Si vous avez configuré un groupe haute disponibilité, les clients se connectent aux adresses IP virtuelles de ce groupe haute disponibilité.
   - Si vous n'utilisez pas de groupe haute disponibilité, les clients se connectent 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 final requis, y compris les noms de caractères génériques.

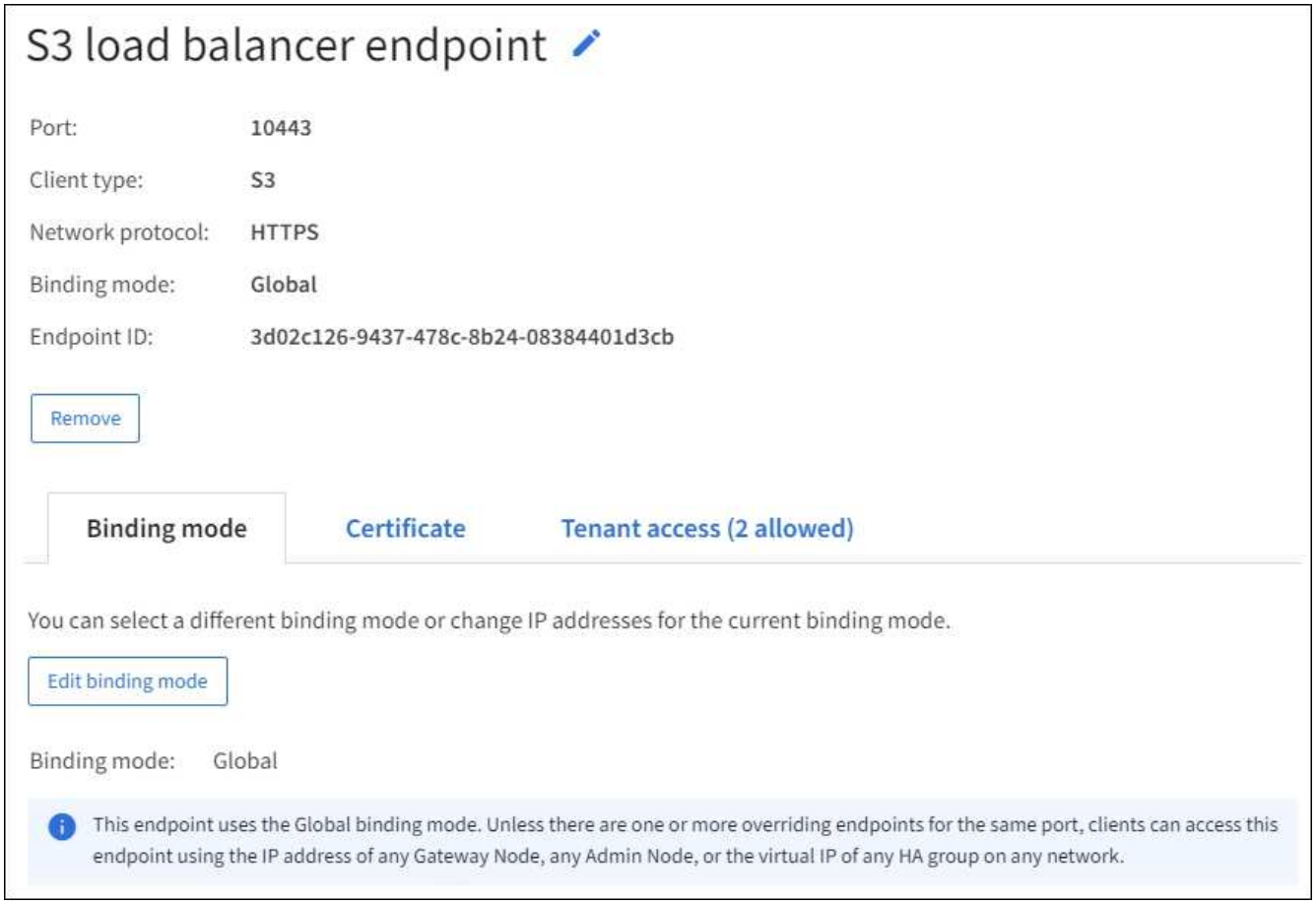
2. Fournir aux clients S3 les informations nécessaires pour se connecter au terminal :

- Numéro de port
- Nom de domaine ou adresse IP complet
- Tous les détails de certificat requis

Afficher et modifier les points finaux de l'équilibreur de charge

Vous pouvez afficher les détails des noeuds finaux existants de l'équilibreur de charge, y compris les métadonnées de certificat d'un noeud final sécurisé. Vous pouvez modifier certains paramètres pour un point final.

- Pour afficher les informations de base de tous les noeuds finaux de l'équilibreur de charge, consultez les tableaux de la page noeuds finaux de l'équilibreur de charge.
- Pour afficher tous les détails sur un noeud final spécifique, y compris les métadonnées du certificat, sélectionnez le nom du noeud final dans le tableau. Les informations affichées varient en fonction du type de noeud final et de sa configuration.



- Pour modifier un noeud final, utilisez le menu **actions** de la page noeuds finaux du répartiteur de charge.

Si vous perdez l'accès à Grid Manager lors de la modification du port d'un noeud final d'interface de gestion, mettez à jour l'URL et le port pour rétablir l'accès.

Après avoir modifié un noeud final, vous devrez peut-être attendre jusqu'à 15 minutes que vos modifications soient appliquées à tous les noeuds.

Tâche	Menu actions	Page de détails
Modifier le nom du point final	a. Cochez la case du point final. b. Sélectionnez **actions** > **Modifier le nom du point final**. c. Saisissez le nouveau nom. d. Sélectionnez **Enregistrer**.	a. Sélectionnez le nom du noeud final pour afficher les détails. b. Sélectionnez l'icône Modifier . c. Saisissez le nouveau nom. d. Sélectionnez **Enregistrer**.
Modifier le port du point final	a. Cochez la case du point final. b. Sélectionnez **actions** > **Modifier le port de point final** c. Entrez un numéro de port valide. d. Sélectionnez **Enregistrer**.	*n/a*
Modifier le mode de liaison du point final	a. Cochez la case du point final. b. Sélectionnez **actions** > **Modifier le mode de liaison du point final**. c. Mettez à jour le mode de liaison si nécessaire. d. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom du noeud final 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 de point final	a. Cochez la case du point final. b. Sélectionnez **actions** > **Modifier le certificat de point final**. c. Chargez ou générez un nouveau certificat personnalisé ou commencez à utiliser le certificat S3 global, si nécessaire. d. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom du noeud final pour afficher les détails. b. Sélectionnez l'onglet **certificat**. c. Sélectionnez **Modifier le certificat**. d. Chargez ou générez un nouveau certificat personnalisé ou commencez à utiliser le certificat S3 global, si nécessaire. e. Sélectionnez **Enregistrer les modifications**.

Tâche	Menu actions	Page de détails
Modifier l'accès du locataire	a. Cochez la case du point final. b. Sélectionnez **actions** > **Modifier l'accès locataire**. c. Choisissez une autre option d'accès, sélectionnez ou supprimez des locataires de la liste, ou effectuez les deux. d. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom du noeud final pour afficher les détails. b. Sélectionnez l'onglet **tenant Access**. c. Sélectionnez **Modifier l'accès locataire**. d. Choisissez une autre option d'accès, sélectionnez ou supprimez des locataires de la liste, ou effectuez les deux. e. Sélectionnez **Enregistrer les modifications**.

Supprimez les points finaux de l'équilibreur de charge

Vous pouvez supprimer un ou plusieurs noeuds finaux à l'aide du menu **actions**, ou vous pouvez supprimer un seul noeud final de la page de détails.

> Pour éviter toute interruption de service, mettez à jour toutes les applications client S3 affectées avant de supprimer un terminal d'équilibrage de la charge. Mettez à jour chaque client pour vous connecter à l'aide d'un port attribué à un autre noeud final de l'équilibreur de charge. Assurez-vous également de mettre à jour les informations de certificat requises.

> Si vous perdez l'accès à Grid Manager lors de la suppression d'un noeud final d'interface de gestion, mettez l'URL à jour.

- Pour supprimer un ou plusieurs noeuds finaux :
  a. Sur la page équilibreur de charge, cochez la case correspondant à chaque noeud final à supprimer.
  b. Sélectionnez **actions** > **Supprimer**.
  c. Sélectionnez **OK**.
- Pour supprimer un noeud final de la page de détails :
  a. Dans la page équilibreur de charge, sélectionnez le nom du noeud final.
  b. Sélectionnez **Supprimer** sur la page de détails.
  c. Sélectionnez **OK**.

Configuration des noms de domaine de terminaux S3

Pour prendre en charge les requêtes de type hébergement virtuel S3, vous devez utiliser le gestionnaire Grid pour configurer la liste des noms de domaine de terminaux S3 auxquels les clients S3 se connectent.

> L'utilisation d'une adresse IP pour un nom de domaine de noeud final n'est pas prise en charge. Les versions ultérieures empêcheront cette configuration.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez "autorisations d'accès spécifiques".
- Vous avez confirmé qu'une mise à niveau de la grille n'est pas en cours.

> N'apportez aucune modification à la configuration du nom de domaine lorsqu'une mise à niveau de grille est en cours.

Description de la tâche

Pour permettre aux clients d'utiliser les noms de domaine de terminaux S3, vous devez effectuer toutes les opérations suivantes :

- Utilisez le Gestionnaire de grille pour ajouter les noms de domaine de points de terminaison S3 au système StorageGRID.
- Assurez-vous que le "Certificat utilisé par le client pour les connexions HTTPS à StorageGRID" est signé pour tous les noms de domaine requis par le client.

  Par exemple, si le noeud final est `s3.company.com`, vous devez vous assurer que le certificat utilisé pour les connexions HTTPS inclut le `s3.company.com` noeud final et le caractère générique Subject alternative Name (SAN): `*.s3.company.com`.

- Configurez le serveur DNS utilisé par le client. Incluez les enregistrements DNS pour les adresses IP utilisées par les clients pour établir des connexions et assurez-vous que les enregistrements référencent tous les noms de domaine de point final S3 requis, y compris 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 haute disponibilité. Vous devez comprendre comment les applications client se connectent à la grille pour inclure les adresses IP correctes dans les enregistrements DNS.

Les clients qui utilisent des connexions HTTPS (recommandées) au grid peuvent utiliser l'un des certificats suivants :

- Les clients qui se connectent à un noeud final d'équilibreur de charge peuvent utiliser un certificat personnalisé pour ce noeud final. Chaque terminal d'équilibrage de la charge peut être configuré de manière à reconnaître différents noms de domaine de terminaux S3.
- Les clients qui se connectent à un terminal d'équilibrage de charge ou directement à un nœud de stockage peuvent personnaliser le certificat d'API S3 global pour inclure tous les noms de domaine de terminaux S3 requis.

> Si vous n'ajoutez pas de noms de domaine de terminaux S3 et que la liste est vide, la prise en charge des demandes de type hébergement virtuel S3 est désactivée.

Ajoutez un nom de domaine de terminal S3

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **noms de domaine de noeud final S3**.
2. Entrez 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 noeud final S3 requis.
   - Si les clients se connectent à un noeud final d'équilibreur de charge qui utilise son propre certificat, "mettez à jour le certificat associé au noeud final".
   - Si les clients se connectent à un terminal d'équilibrage de charge qui utilise le certificat d'API S3 global ou directement aux nœuds de stockage, "Mettez à jour le certificat d'API S3 global".
5. Ajoutez les enregistrements DNS requis pour vous assurer que les demandes de nom de domaine de point final peuvent être résolues.

Résultat

Maintenant, lorsque les clients utilisent le noeud final `bucket.s3.company.com`, le serveur DNS se résout sur le noeud final correct et le certificat authentifie le noeud final comme prévu.

Renommer un nom de domaine de terminal S3

Si vous modifiez un nom utilisé par les applications S3, les demandes de type hébergement virtuel échouent.

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **noms de domaine de noeud final S3**.
2. Sélectionnez le champ de nom de domaine que vous souhaitez modifier et apportez les modifications nécessaires.
3. Sélectionnez **Enregistrer**.
4. Sélectionnez **Oui** pour confirmer votre modification.

Supprimez un nom de domaine de terminal S3

Si vous supprimez un nom utilisé par les applications S3, les demandes de type hébergement virtuel échoueront.

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **noms de domaine de noeud final S3**.
2. Sélectionnez l'icône de suppression ✕ en regard du nom de domaine.
3. Sélectionnez **Oui** pour confirmer la suppression.

Informations associées

- "UTILISEZ L'API REST S3"
- "Afficher les adresses IP"
- "Configurez les groupes haute disponibilité"

Résumé : adresses IP et ports pour les connexions client

Pour stocker ou récupérer des objets, les applications client S3 se connectent au service Load Balancer, qui est inclus sur tous les nœuds d'administration et les nœuds de passerelle, ou au service LDR (local distribution Router), qui est inclus sur tous les nœuds de stockage.

Les applications client peuvent se connecter à StorageGRID en utilisant l'adresse IP d'un nœud grid et le numéro de port du service sur ce nœud. Vous pouvez également créer des groupes haute disponibilité de nœuds d'équilibrage de la charge pour fournir des connexions haute disponibilité utilisant 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 récapitule les différentes façons 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 terminaux d'équilibrage de charge et des groupes haute disponibilité (HA), reportez-vous à la section Où trouver les adresses IP pour localiser ces valeurs dans le Gestionnaire de grille.

Là où la connexion est établie	Service auquel le client se connecte	Adresse IP	Port
Groupe HAUTE DISPONIBILITÉ	Équilibreur de charge	Adresse IP virtuelle d'un groupe haute disponibilité	Port attribué au noeud final de l'équilibreur de charge
Nœud d'administration	Équilibreur de charge	Adresse IP du nœud d'administration	Port attribué au noeud final de l'équilibreur de charge
Nœud de passerelle	Équilibreur de charge	Adresse IP du nœud de passerelle	Port attribué au noeud final 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 client au point de terminaison Load Balancer d'un groupe haute disponibilité 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 haute disponibilité est 192.0.2.5 et que le numéro de port du terminal 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. Connectez-vous au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
2. Pour trouver l'adresse IP d'un nœud de grille :
   a. Sélectionnez **NOEUDS**.
   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 entre les applications client et n'importe quelle adresse IP de la liste :

- **Eth0:** réseau de grille
- **Eth1:** réseau d'administration (facultatif)
- **Eth2:** réseau client (facultatif)

> ⓘ Si vous affichez 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 haute disponibilité est affichée sur eth2.

3. Pour trouver l'adresse IP virtuelle d'un groupe haute disponibilité :
   a. Sélectionnez **CONFIGURATION** > **réseau** > **groupes haute disponibilité**.
   b. Dans le tableau, noter l'adresse IP virtuelle du groupe haute disponibilité.
4. Pour trouver le numéro de port d'un noeud final Load Balancer :
   a. Sélectionnez **CONFIGURATION** > **réseau** > **noeuds finaux de l'équilibreur de charge**.
   b. Notez le numéro de port du noeud final que vous souhaitez utiliser.

> ⓘ Si le numéro de port est 80 ou 443, le noeud final est configuré uniquement sur les noeuds de passerelle, car ces ports sont réservés sur les noeuds d'administration. Tous les autres ports sont configurés sur les nœuds de passerelle et sur les nœuds d'administration.

   c. Sélectionnez le nom du noeud final dans la table.
   d. Vérifiez que le **Type de client** (S3) correspond à l'application cliente qui utilisera le noeud final.

Gestion des réseaux et des connexions

Configurez les paramètres réseau

Vous pouvez configurer différents paramètres réseau à partir du Gestionnaire de grille pour affiner le fonctionnement de votre système StorageGRID.

Configurez les interfaces VLAN

Vous pouvez "Créez des interfaces VLAN (Virtual LAN)"isoler et partitionner le trafic pour assurer la sécurité, la flexibilité et les performances. Chaque interface VLAN est associée à une ou plusieurs interfaces parents sur les nœuds d'administration et les nœuds de passerelle. Vous pouvez utiliser des interfaces VLAN dans des groupes haute disponibilité et dans des terminaux d'équilibrage de charge pour isoler le trafic client ou administratif 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, notamment le trafic lié à des compartiments, des locataires, des sous-réseaux clients ou des terminaux d'équilibrage de charge spécifiques. Ces règles peuvent vous aider à limiter le trafic et à surveiller le trafic.

Instructions pour les réseaux StorageGRID

Vous pouvez utiliser le Gestionnaire de grille pour configurer et gérer les réseaux et les connexions StorageGRID.

Reportez-vous à la section "Configurer les connexions client S3" pour savoir comment connecter les clients S3.

Réseaux StorageGRID par défaut

Par défaut, StorageGRID prend en charge trois interfaces réseau par nœud grid, ce qui vous permet de configurer le réseau pour chaque nœud grid en fonction de vos besoins de sécurité et d'accès.

Pour plus d'informations sur la topologie réseau, reportez-vous à la section "Instructions de mise en réseau".

Réseau Grid

Obligatoire. Le réseau Grid est utilisé pour l'ensemble du trafic StorageGRID interne. Il assure la connectivité entre tous les nœuds de la grille, 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 Admin est généralement un réseau privé et n'a pas besoin d'être routable entre les sites.

Réseau client

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 tout sous-réseau accessible via la passerelle locale.

Directives

- Chaque nœud StorageGRID requiert une interface réseau, une adresse IP, un masque de sous-réseau et une passerelle dédiés pour chaque réseau auquel il est attribué.
- Un nœud de grille ne peut pas avoir plus d'une interface sur un réseau.
- Une passerelle unique, par réseau et par nœud grid est prise en charge et doit être 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.

Le réseau	Nom de l'interface
Grille	eth0

Le réseau	Nom de l'interface
Administrateur (en option)	eth1
Client (facultatif)	eth2

- Si le nœud est connecté à une appliance StorageGRID, des ports spécifiques sont utilisés pour chaque réseau. Pour plus de détails, reportez-vous aux instructions d'installation de votre appareil.
- La route par défaut est générée automatiquement, par nœud. Si eth2 est activé, 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 n'est opérationnel qu'après que le nœud de la grille ait rejoint la grille
- Le réseau Admin peut être configuré pendant le déploiement du nœud grid pour permettre l'accès à l'interface utilisateur d'installation avant que la grille soit entièrement installée.

Interfaces en option

Vous pouvez également ajouter des interfaces supplémentaires à un nœud. Par exemple, vous pouvez ajouter une interface de jonction à un noeud Admin ou Gateway, de sorte que vous pouvez utiliser "Interfaces VLAN" pour isoler le trafic appartenant à différentes applications ou locataires. Vous pouvez également ajouter une interface d'accès à utiliser dans un "Groupe haute disponibilité (HA)".

Pour ajouter une jonction ou des interfaces d'accès, consultez les éléments suivants :

- **VMware (après l'installation du nœud)** : "VMware : ajoutez du jonction ou des interfaces d'accès à un nœud"
  - **Red Hat Enterprise Linux (avant d'installer le nœud)** : "Créez des fichiers de configuration de nœud"
  - **Ubuntu ou Debian (avant d'installer le nœud)** : "Créez des fichiers de configuration de nœud"
  - **RHEL, Ubuntu ou Debian (après l'installation du nœud)** : "Linux : ajoutez une jonction ou des interfaces d'accès à un nœud"

Afficher les adresses IP

Vous pouvez afficher l'adresse IP de chaque nœud grid 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 Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".

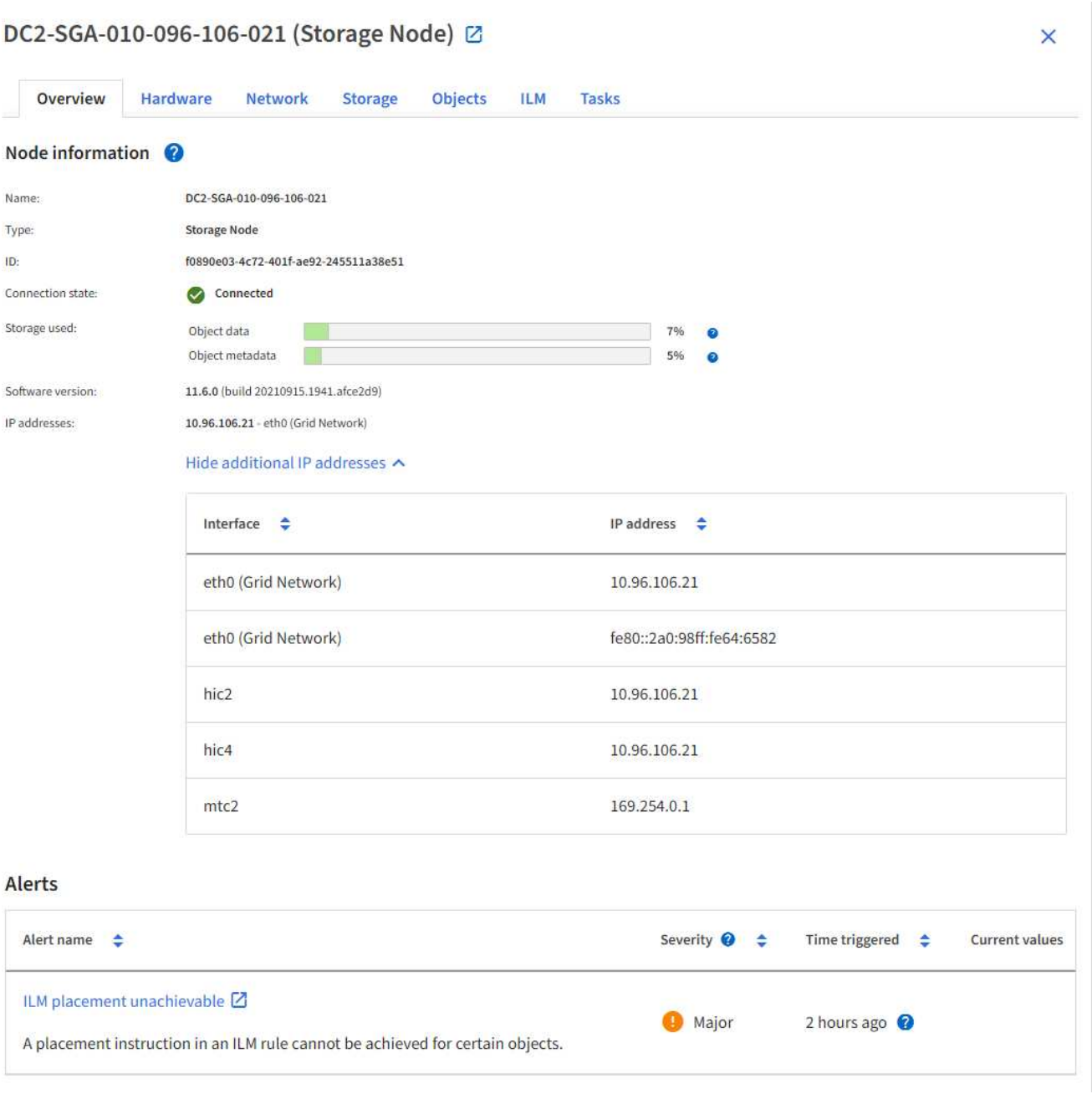
Description de la tâche

Pour plus d'informations sur la modification des adresses IP, reportez-vous à "Configurez les adresses IP"la section .

Étapes

1. Sélectionnez **NODES** > ***grid node*** > **Overview**.
2. Sélectionnez **Afficher plus** à droite du titre des adresses IP.

Les adresses IP de ce nœud de grille sont répertoriées dans un tableau.



Configurez les interfaces VLAN

Vous pouvez créer des interfaces VLAN sur des nœuds d'administration et de passerelle et les utiliser dans des groupes haute disponibilité et des terminaux d'équilibrage de la charge pour isoler et partitionner le trafic afin d'assurer la sécurité, la flexibilité et les performances.

Considérations relatives aux interfaces VLAN

- Vous créez une interface VLAN en entrant un ID VLAN et en choisissant une interface parent sur un ou plusieurs nœuds.

- Une interface parent doit être configurée comme une interface de ligne réseau au niveau du commutateur.
- Une interface parent peut être la Grid Network (eth0), le réseau client (eth2) ou une interface de ligne de jonction supplémentaire pour la VM ou l'hôte bare-Metal (par exemple, en256).
- 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 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 Grid Manager et au Gestionnaire de locataires, sélectionnez uniquement les interfaces sur les nœuds d'administration.
- Si l'interface VLAN est destinée au trafic client S3, sélectionnez les interfaces sur les nœuds d'administration ou les nœuds de passerelle.
- Si vous avez besoin d'ajouter des interfaces de jonction, consultez les informations suivantes :
  - **VMware (après l'installation du nœud)** : "VMware : ajoutez du jonction ou des interfaces d'accès à un nœud"
  - **RHEL (avant l'installation du nœud)** : "Créez des fichiers de configuration de nœud"
  - **Ubuntu ou Debian (avant d'installer le nœud)** : "Créez des fichiers de configuration de nœud"
  - **RHEL, Ubuntu ou Debian (après l'installation du nœud)** : "Linux : ajoutez une jonction ou des interfaces d'accès à un nœud"

Créez une interface VLAN

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine".
- Une interface de ligne réseau a été configurée sur le réseau et connectée au VM ou au nœud Linux. Vous connaissez le nom de l'interface de ligne réseau.
- Vous connaissez l'ID du VLAN que vous configurez.

Description de la tâche

Votre administrateur réseau a peut-être configuré une ou plusieurs interfaces de jonction et un ou plusieurs VLAN pour isoler 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 des interfaces parent (trunk) sur un ou plusieurs nœuds.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **interfaces VLAN**.
2. Sélectionnez **Créer**.

Entrez les détails des interfaces VLAN

Étapes

1. Spécifiez l'ID du VLAN de votre réseau. Vous pouvez entrer n'importe quelle valeur comprise 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 administratif 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 parent 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 déjà utilisé, un message s'affiche.

2. Vous pouvez également saisir une brève description de l'interface VLAN.
3. Sélectionnez **Continuer**.

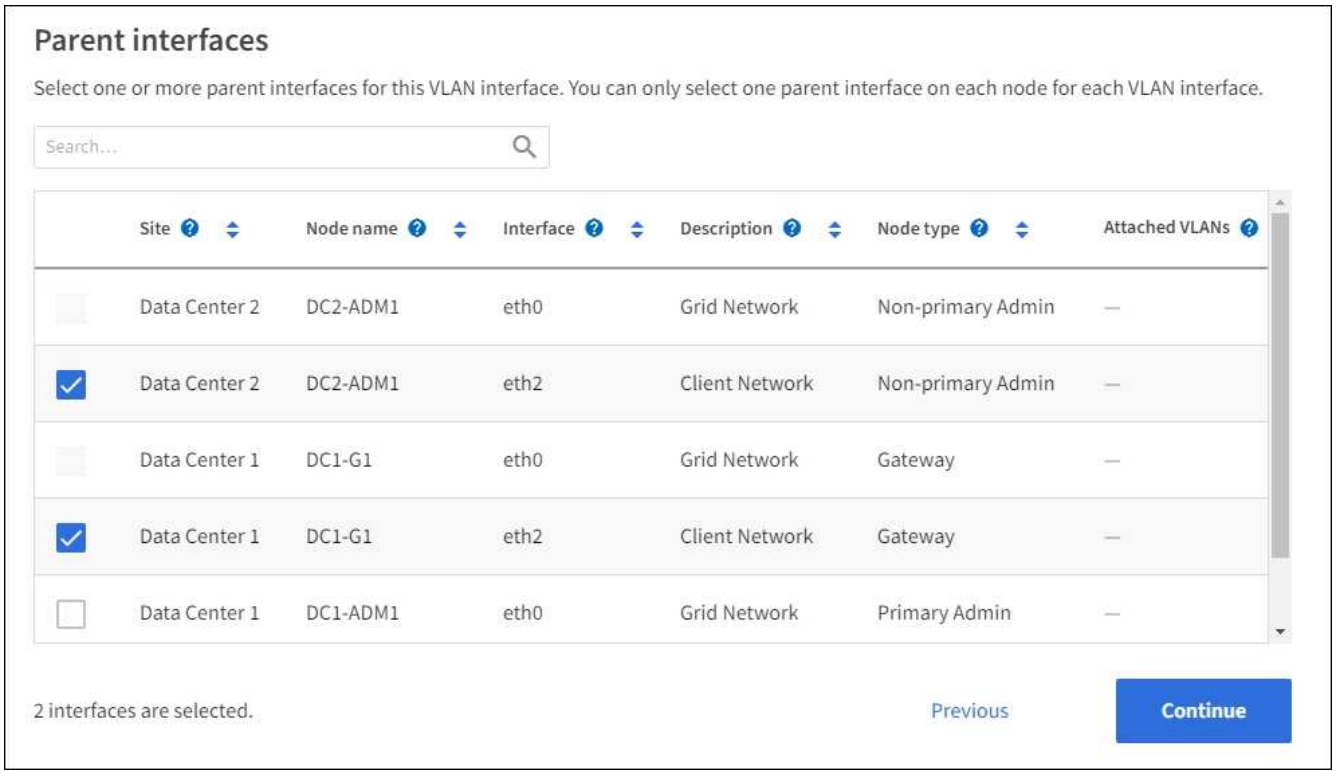
Choisissez les interfaces parents

Le tableau répertorie les interfaces disponibles pour tous les nœuds d'administration et de passerelle de chaque site de votre grille. Les interfaces Admin Network (eth1) ne peuvent pas être utilisées comme interfaces parents et ne sont pas affichées.

Étapes

1. Sélectionnez une ou plusieurs interfaces parent à laquelle relier ce VLAN.

   Par exemple, il peut être nécessaire de connecter un VLAN à l'interface eth2 (client Network) pour un nœud de passerelle et un nœud d'administration.



2. Sélectionnez **Continuer**.

Confirmez les paramètres

Étapes

1. Passez en revue 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 parent, sélectionnez **Choisissez les interfaces parent** 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 que la nouvelle interface apparaisse comme une sélection sur la page groupes haute disponibilité et qu'elle soit répertoriée dans la table **interfaces réseau** pour le nœud (**NOEUDS** > ***parent interface node*** > **Network**).

Modifiez 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 parent.

Par exemple, vous pouvez vouloir supprimer une interface parent d'une interface VLAN si vous envisagez de désaffecter le nœud associé.

Notez ce qui suit :

- Vous ne pouvez pas modifier un ID de VLAN si l'interface VLAN est utilisée dans un groupe haute disponibilité.
- Vous ne pouvez pas supprimer une interface parent si cette interface parent est utilisée dans un groupe haute disponibilité.

  Par exemple, supposons que le VLAN 200 est connecté aux interfaces parents sur les nœuds A et B. si un groupe haute disponibilité utilise l'interface VLAN 200 pour le nœud A et l'interface eth2 pour le nœud B, vous pouvez supprimer l'interface parent inutilisée pour le nœud B, mais vous ne pouvez pas supprimer l'interface parent utilisée pour le nœud A.

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **interfaces VLAN**.
2. Cochez la case correspondant à l'interface VLAN à modifier. Sélectionnez ensuite **actions** > **Modifier**.
3. Vous pouvez également mettre à jour l'ID VLAN ou la description. Sélectionnez ensuite **Continuer**.

   Vous ne pouvez pas mettre à jour un ID VLAN si ce dernier est utilisé dans un groupe haute disponibilité.

4. Si vous le souhaitez, cochez ou décochez les cases pour ajouter des interfaces parent ou supprimer des interfaces inutilisées. Sélectionnez ensuite **Continuer**.
5. Passez en revue la configuration et apportez les modifications nécessaires.
6. Sélectionnez **Enregistrer**.

Supprime 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 haute disponibilité. Vous devez supprimer l'interface VLAN du groupe haute disponibilité avant de pouvoir le supprimer.

Pour éviter toute perturbation du trafic client, envisagez d'effectuer l'une des opérations suivantes :

- Ajoutez une nouvelle interface VLAN au groupe haute disponibilité avant de supprimer cette interface VLAN.
- Créez un nouveau groupe haute disponibilité 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 au bas de la liste des priorités. Attendez que la communication soit établie sur la nouvelle interface principale, puis retirez l'ancienne interface du groupe haute disponibilité. Enfin, supprimez l'interface VLAN de ce nœud.

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **interfaces VLAN**.
2. Cochez la case correspondant à chaque interface VLAN à supprimer. Sélectionnez ensuite **actions** > **Supprimer**.
3. Sélectionnez **Oui** pour confirmer votre sélection.

   Toutes les interfaces VLAN sélectionnées sont supprimées. Une bannière de réussite verte apparaît sur la page interfaces VLAN.

Gérer les stratégies de classification du trafic

Que sont les politiques de classification du trafic ?

Les stratégies de classification du trafic vous permettent d'identifier et de surveiller différents types de trafic réseau. Ces règles contribuent au contrôle et à la limitation du trafic pour améliorer vos offres de qualité de services (QoS).

Les règles de classification du trafic sont appliquées aux terminaux du service StorageGRID Load Balancer pour les nœuds de passerelle et les nœuds d'administration. Pour créer des stratégies de classification de trafic, vous devez avoir déjà créé des points d'extrémité d'équilibreur de charge.

Règles de correspondance

Chaque règle de classification de trafic contient une ou plusieurs règles de correspondance permettant d'identifier le trafic réseau lié à une ou plusieurs des entités suivantes :

- Seaux
- Sous-réseau
- Locataire
- Terminaux d'équilibrage de charge

StorageGRID surveille le trafic qui correspond à n'importe quelle règle de la stratégie conformément aux objectifs de la règle. Tout trafic qui correspond à une règle d'une stratégie est géré par cette règle. Inversement, vous pouvez définir des règles qui correspondent à tout le trafic, à l'exception d'une entité spécifiée.

Limitation du trafic

Vous pouvez également ajouter les types de limite suivants à une règle :

- Bande passante de l'agrégat

- Bande passante par demande
- Requêtes simultanées
- Taux de demande

Les valeurs limites sont appliquées par équilibreur de charge. Si le trafic est réparti simultanément sur plusieurs équilibreurs de charge, les débits maximaux totaux sont un multiple des limites de débit que vous spécifiez.

> Vous pouvez créer des règles pour limiter la bande passante agrégée ou limiter la bande passante par requête. Cependant, StorageGRID ne peut pas limiter les deux types de bande passante en même temps. Les limites de bande passante globales peuvent imposer un impact mineur supplémentaire sur les performances du trafic non limité.

Pour les limites de bande passante globale ou par requête, les demandes sont envoyées vers l'intérieur ou vers l'extérieur au débit défini. StorageGRID ne peut appliquer qu'une seule vitesse. La correspondance des règles la plus spécifique, par type de contrôleur, est donc la plus appliquée. La bande passante consommée par la requête n'est pas prise en compte par rapport à d'autres stratégies de correspondance moins spécifiques contenant des règles de limite de bande passante de l'agrégat. Pour tous les autres types de limite, les demandes des clients sont retardées de 250 millisecondes et reçoivent une réponse lente de 503 pour les demandes dépassant toute limite de stratégie correspondante.

Dans Grid Manager, vous pouvez afficher les diagrammes de trafic et vérifier que les stratégies appliquent les limites de trafic que vous attendez.

Utilisez les stratégies de classification du trafic avec les contrats de niveau de service

Vous pouvez utiliser des règles de classification du trafic en association avec les limites de capacité et la protection des données pour appliquer des accords de niveau de service (SLA) qui fournissent des spécificités en matière de capacité, de protection des données et de performances.

L'exemple suivant montre trois niveaux d'un SLA. Vous pouvez créer des règles de classification du trafic pour atteindre les objectifs de performances de chaque niveau de contrat de niveau de service.

Niveau de service	Capacité	Protection des données	Performances maximales autorisées	Le coût
Or	1 po de stockage autorisé	Règle ILM 3 copies	25 000 demandes/s Bande passante de 5 Go/s (40 Gbit/s)	par mois
Argent	Stockage de 250 To autorisé	Règle ILM 2 copies	10 000 demandes/s Bande passante de 1.25 Go/s (10 Gbit/s)	$$ par mois
Bronze	Stockage de 100 To autorisé	Règle ILM 2 copies	5 000 demandes/s Bande passante de 1 Go/s (8 Gbit/s)	$ par mois

Créer des stratégies de classification du trafic

Vous pouvez créer des règles de classification du trafic si vous souhaitez contrôler et éventuellement limiter le trafic réseau par compartiment, Regex de compartiment, CIDR, terminal d'équilibrage de charge ou locataire. Vous pouvez également définir des limites pour une stratégie en fonction de la bande passante, du nombre de demandes simultanées ou du taux de demande.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine".
- Vous avez créé tous les noeuds finaux de l'équilibreur de charge que vous souhaitez associer.
- Vous avez créé les locataires que vous souhaitez associer.

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **classification du trafic**.
2. Sélectionnez **Créer**.
3. Entrez un nom et une description (facultatif) pour la stratégie et sélectionnez **Continuer**.

   Par exemple, décrivez à quoi s'applique cette politique de classification de trafic et à quoi elle limite.

4. Sélectionnez **Ajouter une règle** et spécifiez les détails suivants pour créer une ou plusieurs règles de correspondance pour la stratégie. Toute stratégie que vous créez doit comporter au moins une règle correspondante. Sélectionnez **Continuer**.

Champ	Description
Type	Sélectionnez les types de trafic auxquels s'applique la règle correspondante. Les types de trafic sont le compartiment, le Regex de compartiment, le CIDR, le terminal d'équilibrage de la charge et le locataire.

Champ	Description
Valeur de correspondance	Entrez la valeur correspondant au type sélectionné. • Compartiment : entrez un ou plusieurs noms de compartiment. • Regex de compartiment : saisissez une ou plusieurs expressions régulières utilisées pour correspondre à un ensemble de noms de compartiment. L'expression régulière n'est pas ancrée. Utilisez l'ancrage ^ pour faire correspondre au début du nom du compartiment et utilisez l'ancrage $ pour faire correspondre à la fin du nom. La correspondance d'expression régulière 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. • Noeud final de l'équilibreur de charge : sélectionnez un nom de noeud final. Il s'agit des noeuds finaux de l'équilibreur de charge que vous avez définis sur le "Configurer les terminaux de l'équilibreur de charge". • Tenant : le tenant Matching 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 compartiment auquel vous accédez est utilisée pour déterminer le locataire.
Comparaison inverse	Si vous voulez faire correspondre tout le trafic réseau *except* avec la valeur Type et correspondance que vous venez de définir, cochez la case **comparaison inverse**. Sinon, laissez la case à cocher désactivée. Par exemple, si vous souhaitez que cette stratégie s'applique à tous les noeuds finaux de l'équilibreur de charge sauf un, spécifiez le noeud final de l'équilibreur de charge à exclure et sélectionnez **comparaison inverse**. Dans le cas d'une règle contenant plusieurs matcheurs où au moins un est un matcher inverse, veillez à ne pas créer une règle qui correspond à toutes les demandes.

5. Si vous le souhaitez, sélectionnez **Ajouter une limite** et sélectionnez les détails suivants pour ajouter une ou plusieurs limites afin de contrôler le trafic réseau correspondant à une règle.

> StorageGRID collecte des mesures, même si vous n'ajoutez aucune limite, pour vous permettre de comprendre les tendances du trafic.

Champ	Description
Type	Type de limite que vous souhaitez appliquer au trafic réseau correspondant à la règle. Par exemple, vous pouvez limiter la bande passante ou le taux de demande. **Remarque** : vous pouvez créer des stratégies pour limiter la bande passante agrégée ou pour limiter la bande passante par demande. Cependant, StorageGRID ne peut pas limiter les deux types de bande passante en même temps. Lorsque la bande passante de l'agrégat est utilisée, la bande passante par demande n'est pas disponible. Inversement, lorsque la bande passante par demande est utilisée, la bande passante de l'agrégat n'est pas disponible. Les limites de bande passante globales peuvent imposer un impact mineur supplémentaire sur les performances du trafic non limité. Pour les limites de bande passante, StorageGRID applique la règle qui correspond le mieux au type de limite défini. Par exemple, si vous avez une stratégie qui limite le trafic dans une seule direction, alors le trafic dans la direction opposée sera illimité, même s'il y a un trafic qui correspond à des stratégies supplémentaires qui ont des limites de bande passante. StorageGRID met en œuvre les « meilleures » correspondances pour les limites de bande passante dans l'ordre suivant : • Adresse IP exacte (/32 masque) • Nom exact du compartiment • Seau regex • Locataire • Point final • Correspondances CIDR non exactes (pas /32) • Correspondances inverses
S'applique à	Indique si cette limite s'applique aux demandes de lecture client (GET ou HEAD) ou aux demandes d'écriture (PUT, POST ou DELETE).
Valeur	Valeur à laquelle le trafic réseau sera limité, en fonction de l'unité sélectionnée. Par exemple, entrez 10 et sélectionnez MIB/s pour empêcher le trafic réseau correspondant à cette règle de dépasser 10 Mio/s. **Remarque** : selon le réglage des unités, les unités disponibles seront soit binaires (par exemple, Gio), soit décimales (par exemple, GB). Pour modifier le paramètre unités, sélectionnez la liste déroulante utilisateur dans le coin supérieur droit du Gestionnaire de grille, puis sélectionnez **Préférences utilisateur**.
Unité	Unité qui décrit la valeur que vous avez saisie.

Par exemple, si vous souhaitez créer une limite de bande passante de 40 Gbit/s pour un niveau SLA, créez deux limites de bande passante agrégée : GET/HEAD à 40 Gbit/s et PUT/POST/DELETE à 40 Gbit/s.

6. Sélectionnez **Continuer**.
7. Lisez et passez en revue 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 stratégie, sélectionnez **Enregistrer et continuer**.

   Le trafic client S3 est désormais géré conformément à la règle de classification du trafic.

Une fois que vous avez terminé

"Afficher les données de trafic réseau" pour vérifier que les stratégies appliquent les limites de trafic que vous attendez.

Modifier la stratégie de classification du trafic

Vous pouvez modifier une stratégie de classification de trafic pour modifier son nom ou sa description, ou pour créer, modifier ou supprimer des règles ou des limites de la stratégie.

Avant de commencer

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

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **classification du trafic**.

   La page règles de classification du trafic s'affiche et les stratégies existantes sont répertoriées dans un tableau.

2. Modifiez la stratégie à l'aide du menu actions ou de la page de détails. Reportez-vous à la section "créez des stratégies de classification du trafic" pour savoir ce que vous devez saisir.

   Menu actions

   a. Cochez la case correspondant à la règle.

   b. Sélectionnez **actions** > **Modifier**.

   Page de détails

   a. Sélectionnez le nom de la stratégie.

   b. Sélectionnez le bouton **Modifier** en regard du nom de la stratégie.

3. Pour l'étape entrer le nom de la stratégie, modifiez éventuellement le nom ou la description de la stratégie et sélectionnez **Continuer**.
4. Pour l'étape Ajouter des règles de correspondance, ajoutez éventuellement une règle ou modifiez **Type** et **valeur de correspondance** de la règle existante, puis sélectionnez **Continuer**.
5. Pour l'étape définir les limites, ajoutez, modifiez ou supprimez une limite, et sélectionnez **Continuer**.
6. Consultez la stratégie mise à jour et sélectionnez **Enregistrer et continuer**.

   Les modifications apportées à la stratégie sont enregistrées et le trafic réseau est désormais géré conformément aux règles de classification du trafic. Vous pouvez afficher les diagrammes de trafic et

vérifier que les stratégies appliquent les limites de trafic auxquelles vous vous attendez.

Supprimer une règle de classification du trafic

Vous pouvez supprimer une stratégie de classification du trafic si vous n'en avez plus besoin. Assurez-vous de supprimer la stratégie appropriée car une stratégie ne peut pas être récupérée lorsqu'elle est supprimée.

Avant de commencer

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

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 stratégie à l'aide du menu actions ou de la page de détails.

   Menu actions

   a. Cochez la case correspondant à la règle.

   b. Sélectionnez **actions** > **Supprimer**.

   Page de détails de la police

   a. Sélectionnez le nom de la stratégie.

   b. Sélectionnez le bouton **Supprimer** en regard du nom de la stratégie.

3. Sélectionnez **Oui** pour confirmer que vous souhaitez supprimer la stratégie.

   La stratégie est supprimée.

Afficher les données de trafic réseau

Vous pouvez surveiller le trafic réseau en affichant les graphiques disponibles à partir de la page stratégies de classification du trafic.

Avant de commencer

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

Description de la tâche

Pour toute règle de classification de trafic existante, vous pouvez afficher les mesures du service d'équilibrage de charge pour déterminer si la règle limite avec succès le trafic sur le réseau. Les données des graphiques peuvent vous aider à déterminer si vous devez ajuster la règle.

Même si aucune limite n'est définie pour une stratégie de classification du trafic, des mesures sont recueillies et les graphiques fournissent des informations utiles pour comprendre les tendances du trafic.

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **classification du trafic**.

   La page règles de classification du trafic s'affiche et les stratégies existantes sont répertoriées dans le tableau.

2. Sélectionnez le nom de la stratégie de classification de trafic pour laquelle vous souhaitez afficher les mesures.
3. Sélectionnez l'onglet **Metrics**.

   Les graphiques de stratégie de classification du trafic s'affichent. Les graphiques affichent des mesures uniquement pour le trafic correspondant à la stratégie sélectionnée.

   Les graphiques suivants sont inclus sur la page.

   - Taux de demande : ce graphique indique la quantité de bande passante correspondant à cette règle 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 de corps pour les réponses qui ont des données de corps. Envoyé inclut les en-têtes de réponse pour toutes les demandes et la taille des données du corps de réponse pour les demandes qui incluent des données du corps dans la réponse.

     > Lorsque les demandes sont terminées, ce graphique indique uniquement l'utilisation de la bande passante. Pour les demandes d'objets lents ou volumineux, la bande passante instantanée réelle peut différer des valeurs indiquées dans ce graphique.

   - Taux de réponse aux erreurs : ce graphique fournit une fréquence approximative à laquelle les demandes correspondant à cette stratégie renvoient des erreurs (code d'état HTTP >= 400) aux clients.
   - Durée moyenne des demandes (sans erreur) : ce graphique fournit une durée moyenne des demandes réussies correspondant à cette stratégie.
   - Utilisation de la bande passante de la règle : ce graphique indique la quantité de bande passante correspondant à cette règle 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 de corps pour les réponses qui ont des données de corps. Envoyé inclut les en-têtes de réponse pour toutes les demandes et la taille des données du corps de réponse pour les demandes qui incluent des données du corps dans la réponse.

4. Placez le curseur sur un graphique linéaire pour afficher une fenêtre contextuelle de valeurs sur une partie spécifique du graphique.
5. Sélectionnez **Grasana Dashboard** juste en dessous du titre Metrics pour afficher tous les graphiques d'une police. 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 pour les demandes PUT/POST/DELETE correspondant à cette règle. Le positionnement sur une cellule individuelle affiche des débits par seconde. Les taux affichés dans la vue de survol sont tronqués aux nombres entiers et peuvent indiquer 0 lorsqu'il y a des demandes non nulles dans le compartiment.
   - Taux de demande de lecture par taille d'objet : taux des demandes GET/HEAD correspondant à cette règle. Le positionnement sur une cellule individuelle affiche des débits par seconde. Les taux affichés dans la vue de survol sont tronqués aux nombres entiers et peuvent indiquer 0 lorsqu'il y a des demandes non nulles dans le compartiment.

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 stratégie dans le menu en haut à gauche de la page.

d. Placez le curseur sur un graphique pour afficher une fenêtre contextuelle indiquant la date et l'heure de l'échantillon, les tailles d'objet agrégées dans le nombre et le nombre de demandes par seconde pendant cette période.

   Les politiques de classification du trafic sont identifiées par leur ID. Les ID de stratégie sont répertoriés sur la page règles de classification de trafic.

7. Analysez les graphiques pour déterminer à quelle fréquence la stratégie limite le trafic et si vous devez ajuster la stratégie.

Chiffrement 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) avec les systèmes externes utilisés pour la fédération des identités et les pools de stockage cloud.

Versions supportées de TLS

StorageGRID prend en charge TLS 1.2 et TLS 1.3 pour les connexions aux systèmes externes utilisés pour la fédération des identités et les pools de stockage cloud.

Les chiffrements TLS qui sont pris en charge pour une utilisation avec des systèmes externes ont été sélectionnés pour assurer la compatibilité avec une gamme de systèmes externes. La liste est plus grande que la liste des chiffrements pris en charge pour une utilisation avec les applications client S3. Pour configurer les chiffrements, accédez à **CONFIGURATION** > **sécurité** > **Paramètres de sécurité** et sélectionnez **règles 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 ingénieur commercial NetApp pour toute demande spécifique concernant ces paramètres.

Avantages des connexions HTTP actives, inactives et simultanées

La configuration des connexions HTTP peut avoir un impact sur les performances du système StorageGRID. Les configurations varient selon que la connexion HTTP est active ou inactive ou si vous avez simultanément plusieurs connexions.

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 maintenir les connexions HTTP inactives ouvertes

Vous devez maintenir les connexions HTTP ouvertes même lorsque les applications client sont inactives pour permettre aux applications client d'effectuer les transactions suivantes sur la connexion ouverte. En fonction des mesures du système et de l'expérience d'intégration, vous devez garder une connexion HTTP inactive ouverte pendant 10 minutes maximum. StorageGRID peut fermer automatiquement une connexion HTTP qui reste ouverte et inactive pendant plus de 10 minutes.

Les connexions HTTP ouvertes et inactives offrent les avantages suivants :

- Réduction de la latence 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 réduction de la latence constitue l'avantage principal, notamment pour la durée nécessaire à l'établissement des connexions TCP/IP et TLS.

- Augmentation de la vitesse de transfert des données en amorçant l'algorithme TCP/IP à démarrage lent avec des transferts effectués précédemment
- Notification instantanée de plusieurs classes de conditions de défaillance qui interrompent la connectivité entre l'application cliente et le système StorageGRID

Déterminer la durée d'ouverture d'une connexion inactive est un compromis entre les avantages du démarrage lent associés à la connexion existante et l'affectation idéale de la connexion aux ressources système internes.

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 des transactions en continu.

La détermination de la durée maximale pendant laquelle une connexion doit être maintenue ouverte est un compromis entre les avantages de la persistance de connexion et l'allocation idéale de la connexion aux ressources système internes.

Pour les connexions client aux nœuds de stockage, la limitation des connexions HTTP actives offre les avantages suivants :

- Équilibrage optimal de la charge sur l'ensemble du système StorageGRID.

  Avec le temps, une connexion HTTP pourrait ne plus être optimale au fur et à mesure que les besoins en équilibrage de la charge évoluent. Le système réalise son meilleur équilibrage de charge lorsque les applications client établissent une connexion HTTP distincte pour chaque transaction, mais cela annule les gains les plus importants associés aux connexions persistantes.

- Permet aux applications clientes de diriger des transactions HTTP vers des services LDR qui ont de l'espace disponible.
- Permet de démarrer les procédures de maintenance.

  Certaines procédures de maintenance ne démarrent qu'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 le démarrage rapide de certaines procédures de maintenance. Si la durée des connexions client n'est pas limitée, l'arrêt automatique des connexions actives peut prendre plusieurs minutes.

Avantages des connexions HTTP simultanées

Vous devez maintenir plusieurs connexions TCP/IP ouvertes au système StorageGRID 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 commencer immédiatement au lieu d'attendre que d'autres transactions soient effectuées.

- Rendement accru

  Le système StorageGRID peut effectuer des transactions parallèles et augmenter le débit des transactions globales.

Les applications client doivent établir plusieurs connexions HTTP. Lorsqu'une application client doit effectuer une transaction, elle peut sélectionner et utiliser immédiatement toute connexion établie qui ne traite pas actuellement une transaction.

Le débit maximal de chaque topologie de chaque système StorageGRID est différent pour les transactions et les connexions simultanées, avant que les performances ne commencent à se dégrader. Le pic de débit dépend de facteurs tels que les ressources informatiques, les ressources réseau, les ressources de stockage et les liaisons WAN. Des facteurs sont également pris en charge par le nombre de serveurs et de services, ainsi que par le nombre d'applications prises en charge par le système StorageGRID.

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 client. Si l'application client se compose de plusieurs entités logicielles qui établissent chacune des connexions avec le système StorageGRID, vous devez ajouter toutes les connexions entre les entités. Vous devrez peut-être régler 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 pris en charge par le système.
- Les applications client qui interagissent avec le système StorageGRID sur un réseau avec une bande passante limitée peuvent être contraintes de réduire le niveau de simultanéité pour s'assurer que les transactions individuelles sont effectuées dans un délai raisonnable.
- Lorsque de nombreuses applications client partagent le système StorageGRID, il peut être nécessaire de réduire le degré de simultanéité pour ne pas dépasser les limites du système.

Séparation des pools de connexions HTTP pour les opérations de lecture et d'écriture

Vous pouvez utiliser des pools séparés de connexions HTTP pour les opérations en lecture et écriture, et contrôler la proportion que vous souhaitez utiliser pour chacun d'eux. Le recours à des pools séparés de connexions HTTP vous permet de contrôler les transactions et d'équilibrer la charge plus efficacement.

Les applications client peuvent créer des chargements qui sont dominants par la récupération (lecture) ou dominants par le stockage (écriture). Grâce à des pools séparés de connexions HTTP pour les transactions en lecture et écriture, vous pouvez ajuster la quantité de chaque pool à dédier pour les transactions en lecture ou en écriture.

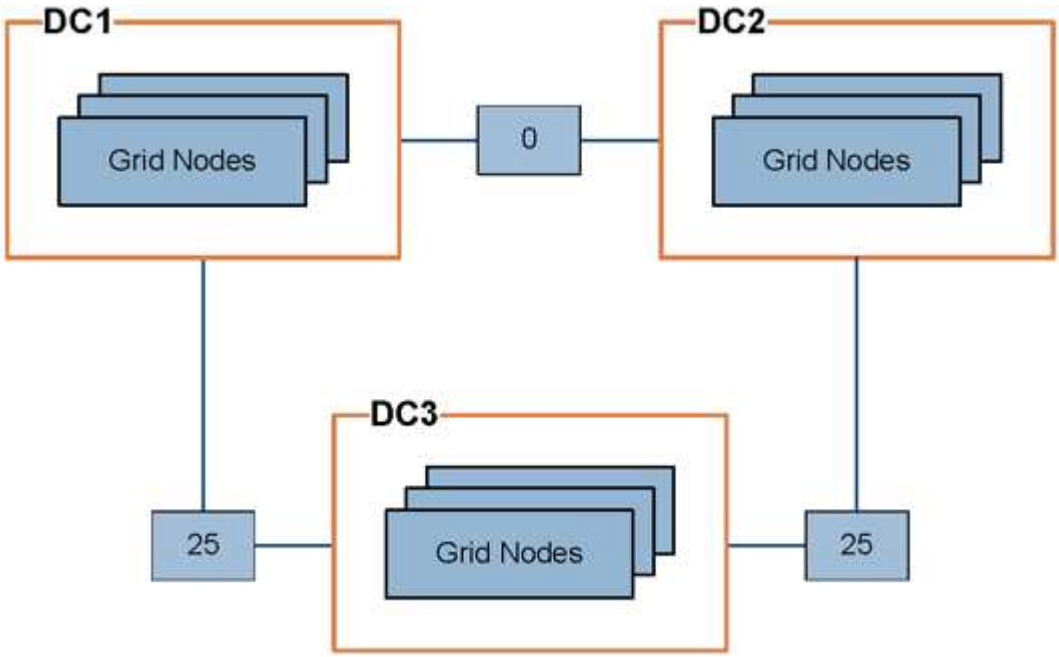
Gérer les coûts de liaison

Les coûts de liaison vous permettent de définir la priorité du site de data Center qui fournit un service demandé lorsqu'au moins deux sites de data Center existent. Vous pouvez ajuster les coûts de liaison pour refléter la latence entre les sites.

Quels sont les coûts de liaison ?

- Les coûts des liens permettent de classer par ordre de priorité la copie d'objet utilisée pour les récupérations d'objets.
- Les coûts des liaisons sont utilisés par l'API de gestion du grid et l'API de gestion des locataires pour déterminer quels services StorageGRID internes 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 schéma présente une grille de trois sites avec des coûts de liaison configurés entre les sites :



- Le service Load Balancer sur les nœuds d'administration et les nœuds de passerelle répartit uniformément les connexions client vers tous les nœuds de stockage sur le même site de data Center et vers tous les sites de data Center, avec un coût de liaison de 0.

  Dans l'exemple, un nœud passerelle du site de data Center 1 (DC1) distribue également les connexions client aux nœuds de stockage du DC1 et aux nœuds de stockage du DC2. Un nœud de passerelle du DC3 envoie des connexions client uniquement aux nœuds de stockage du DC3.

- Lors de la récupération d'un objet existant sous forme de plusieurs copies répliquées, StorageGRID récupère la copie au niveau du data Center présentant le coût de liaison le plus faible.

  Dans cet exemple, si une application client sur DC2 récupère un objet stocké à la fois sur DC1 et DC3, l'objet est récupéré de DC1, car le coût de la liaison de DC1 à DC2 est 0, ce qui est inférieur au coût de la 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 indique les coûts de liaison couramment utilisés.

Lien	Coût des liens	Remarques
Entre les sites de data centers physiques	25 (par défaut)	Data centers connectés par une liaison WAN.
Entre des sites de data centers logiques au même emplacement physique	0	Data centers logiques dans le même bâtiment physique ou campus connecté par un réseau LAN.

Mettre à jour les coûts des liens

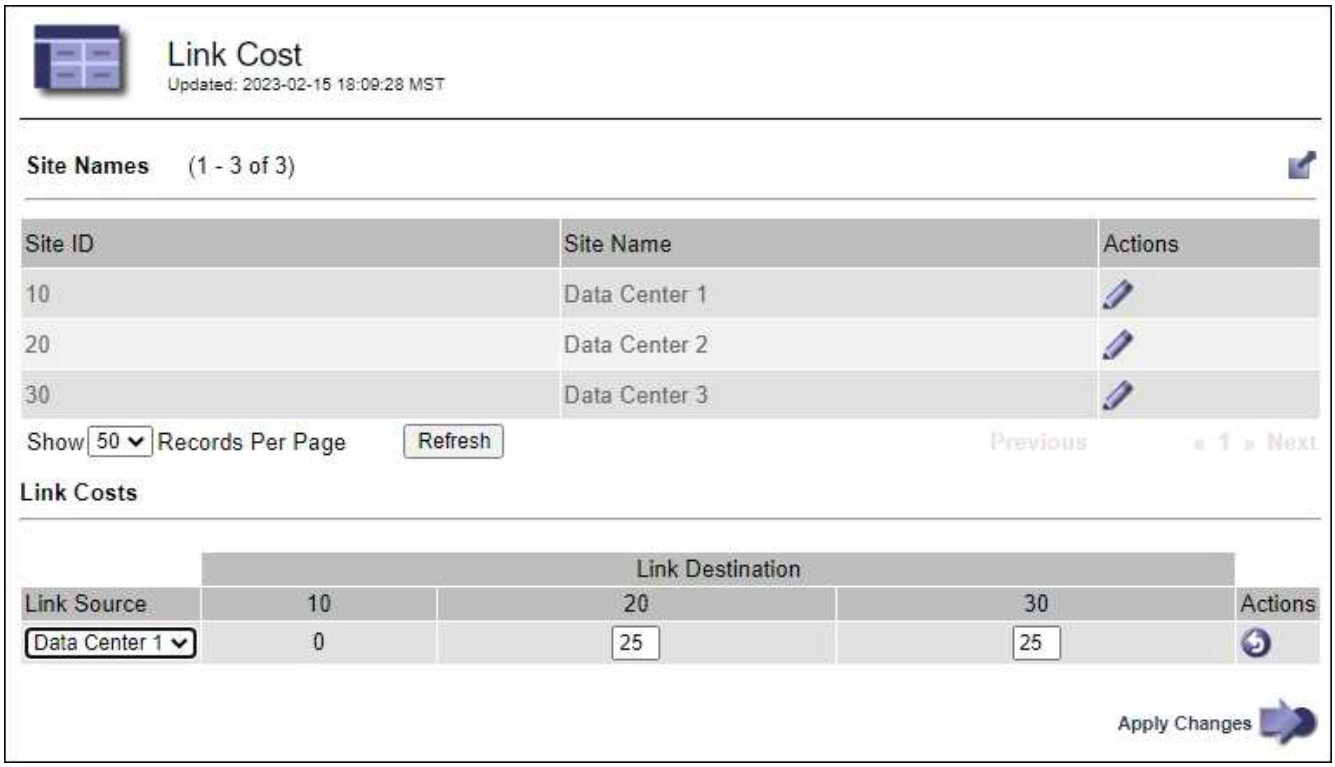
Vous pouvez mettre à jour les coûts de liaison entre les sites de data Center afin de refléter la latence entre les sites.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille 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 **Link Source** et entrez une valeur de coût comprise entre 0 et 100 sous **Link destination**.

   Vous ne pouvez pas modifier le coût du lien si la source est identique à la destination.

Pour annuler les modifications, sélectionnez **Revert**.

3. Sélectionnez **appliquer les modifications**.

Utiliser AutoSupport

Qu’est-ce que AutoSupport ?

La fonctionnalité AutoSupport permet à StorageGRID d’envoyer des packages d’état et d’intégrité au support technique NetApp.

L’utilisation de AutoSupport permet d’accélérer considérablement la détermination et la résolution des problèmes. Le support technique peut également surveiller les besoins en stockage de votre système et vous aider à déterminer si vous devez ajouter de nouveaux nœuds ou sites. Vous pouvez également configurer l’envoi des packages AutoSupport vers une destination supplémentaire.

StorageGRID propose deux types de AutoSupport :

- **StorageGRID AutoSupport** signale des problèmes de logiciel StorageGRID. Activé par défaut lors de la première installation de StorageGRID. Vous pouvez le "Modifier la configuration AutoSupport par défaut"faire si nécessaire.

> Si StorageGRID AutoSupport n’est pas activé, un message s’affiche sur le tableau de bord du Gestionnaire de grille. Le message inclut un lien vers la page de configuration de AutoSupport. Si vous fermez le message, il n’apparaîtra plus tant que le cache de votre navigateur n’aura pas été effacé, même si AutoSupport reste désactivé.

- **Le matériel de l’appareil AutoSupport** signale les problèmes de l’appareil StorageGRID. Vous devez "Configurez le matériel AutoSupport sur chaque appliance".

Qu’est-ce que Active IQ ?

Active IQ est un conseiller digital basé dans le cloud qui exploite l’analytique prédictive et les connaissances de la communauté issues de la base installée de NetApp. Les évaluations continues des risques, les alertes prédictives, les conseils normatifs et les actions automatisées vous aident à anticiper les problèmes, ce qui permet d’améliorer l’état et la disponibilité du système.

Si vous souhaitez utiliser les tableaux de bord et les fonctionnalités de Active IQ sur le site de support NetApp, vous devez activer AutoSupport.

"Documentation Active IQ sur le conseiller digital"

Informations incluses dans le package AutoSupport

Un package AutoSupport contient les fichiers et détails suivants.

Nom du fichier	Champs	Description
AUTOSUPPORT-HISTORY.XML	Numéro de séquence AutoSupport + destination pour ce AutoSupport + État de livraison + tentatives de livraison + objet AutoSupport + URI de livraison + dernière erreur + Nom de fichier AutoSupport PUT + heure de génération + taille compressée AutoSupport + taille décompressée AutoSupport + durée totale de collecte (ms)	Fichier d'historique AutoSupport.
AUTOSUPPORT.XML	Nœud + Protocole pour contacter le support + URL de support pour HTTP/HTTPS + adresse de support + Etat 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 le AutoSupport à la demande si activé ou désactivé.
BUCKETS.XML	ID de compartiment + ID de compte + version de build + Configuration de contrainte d'emplacement + conformité activée + Configuration de conformité + verrouillage d'objet S3 activé + Configuration de verrouillage d'objet S3 + Configuration de cohérence + CORS activée + Configuration de l'identification de compartiment activée + heure du dernier accès activée + Configuration de la stratégie + Notifications activées + Configuration de miroir cloud activée + Configuration de la recherche activée + Configuration de l'étiquetage de compartiment activée + Configuration de l'étiquetage de compartiment activée	Fournit des informations de configuration et des statistiques au niveau du compartiment. Les services de plateforme, la conformité et la cohérence des compartiments sont des exemples de configuration de compartiment.

Nom du fichier	Champs	Description
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 grid, l'espace réservé aux métadonnées, les paramètres de configuration de l'ensemble de la grille (conformité, verrouillage objet S3, compression d'objet, alertes, syslog et configuration ILM), les détails du profil de code d'effacement, le nom DNS et "Nom du NMS".
GRID-SPEC.XML	Spécifications de grille, XML brut	Permet de configurer et de déployer StorageGRID. Contient les spécifications du grid, l'adresse IP du serveur NTP, l'adresse IP du serveur DNS, la topologie 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 grille (procédures de maintenance). Fournit des détails sur les tâches actives, terminées, terminées, ayant échoué et en attente de la grille.
GRID.JSON	Grid + révision + version du logiciel + Description + Licence + mots de passe + DNS + NTP + sites + nœuds	Informations de grille.
ILM-CONFIGURATION.XML	ID d'attribut + Nom d'attribut + valeur + Index + ID de table + Nom de table	Liste des attributs des configurations ILM.
ILM-STATUS.XML	Nœud + chemin de service + ID d'attribut + Nom d'attribut + valeur + Index + ID de table + Nom de table	Fichier d'informations de metrics ILM. Les taux d'évaluation ILM pour chaque nœud et les metrics de la grille sont indiqués.
ILM.XML	XML brut ILM	Fichier de règles actif ILM. Contient des informations détaillées sur les règles ILM actives, telles que l'ID de 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.

Nom du fichier	Champs	Description
MANIFEST.XML	Ordre de collecte + nom de 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 des métadonnées AutoSupport et une brève description de tous les fichiers AutoSupport.
NMS-ENTITÉS.XML	Index des attributs + OID de l'entité + ID du nœud + ID du modèle du périphérique + version du modèle du périphérique + Nom de l'entité	Groupe et entités de service dans "Arborescence NMS". Fournit des détails sur la topologie de la grille. Le nœud peut être déterminé en fonction des services exécutés sur le nœud.
OBJECTS-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 d'analyse en arrière-plan, le transfert actif, le taux de transfert, le total des transferts, le taux de suppression, les fragments corrompus, les objets perdus, les objets manquants, la tentative de réparation, la vitesse 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 les détails suivants pour chaque nœud : type de plateforme, système d'exploitation, mémoire installée, mémoire disponible, connectivité du stockage, numéro de série du châssis de l'appliance 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 mesures Reaper de la base de données, la durée de réparation des segments, la durée des travaux de réparation, les redémarrages automatiques des travaux et la fin automatique des travaux.

Nom du fichier	Champs	Description
STORAGE-GRADES.XML	ID du niveau de stockage + Nom du niveau de stockage + ID du nœud de stockage + chemin du nœud de stockage	Fichier de définitions des niveaux de stockage pour chaque nœud de stockage.
SUMMARY-ATTRIBUTES.XML	OID groupe + chemin groupe + ID attribut résumé + Nom attribut résumé + valeur + Index + ID table + Nom table	Données générales sur l'état du système qui récapitule les informations d'utilisation de StorageGRID. Fournit des informations telles que le nom de la grille, le nom des sites, le nombre de nœuds de stockage par grid et par site, le type de licence, la capacité et l'utilisation de la licence, les conditions du support logiciel et des détails des opérations S3.
SYSTEM-ALERTS.XML	Nom + gravité + Nom du nœud + Statut de l'alerte + Nom du site + heure de déclenchement de l'alerte + heure de résolution de l'alerte + ID de la 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 POST (ms) + OPTIONS temps moyen (ms)	Statistiques basées sur les agents utilisateur 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.
DONNÉES-EN-TÊTE-X.	X-NetApp-asup-generated-on + X-NetApp-asup-hostname + X-NetApp-asup-os-version + X-NetApp-asup-num-série + X-NetApp-asup-subject + X-NetApp-asup-ID-système + X-NetApp-asup-nom-modèle	Données d'en-tête AutoSupport.

Configurez AutoSupport

Par défaut, la fonction StorageGRID AutoSupport est activée lors de la première installation de StorageGRID. Cependant, vous devez configurer le AutoSupport matériel sur chaque appliance. Si nécessaire, vous pouvez modifier la configuration de AutoSupport.

Si vous souhaitez modifier la configuration de StorageGRID AutoSupport, effectuez vos modifications uniquement sur le nœud d'administration principal. Vous devez Configurer le matériel AutoSupport sur chaque appareil.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine".
- Si vous utilisez HTTPS pour envoyer des packages AutoSupport, vous avez fourni un accès Internet sortant au nœud d'administration principal, soit directement, soit "utilisation d'un serveur proxy"(les connexions entrantes ne sont pas requises).
- Si HTTP est sélectionné sur la page StorageGRID AutoSupport, vous devez "configurez un serveur proxy"transférer les modules 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.

Description de la tâche

Vous pouvez utiliser n'importe quelle combinaison des options suivantes pour envoyer des packages AutoSupport au support technique :

- **Hebdomadaire**: Envoyer automatiquement des paquets AutoSupport une fois par semaine. Paramètre par défaut : activé.
- **Déclenché par un événement** : envoie automatiquement des paquets AutoSupport toutes les heures ou lorsque des événements système importants se produisent. Paramètre par défaut : activé.
- **À la demande** : permet au support technique de demander à votre système StorageGRID d'envoyer automatiquement des paquets AutoSupport, ce qui est utile lorsqu'ils travaillent activement à un problème (nécessite le protocole de transmission AutoSupport HTTPS). Paramètre par défaut : Désactivé.
- **Déclenché par l'utilisateur** : envoyez manuellement des paquets AutoSupport à tout moment.

Indiquez le protocole des 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 vous le souhaitez Activez la fonction AutoSupport On Demand, vous devez utiliser HTTPS.
- **HTTP** : si vous sélectionnez HTTP, vous devez configurer un serveur proxy pour transférer les paquets 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 voulez que les paquets 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**, choisissez d'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 paquets AutoSupport est sécurisée. Le certificat de support NetApp est déjà installé avec le logiciel StorageGRID.
   - **Ne pas vérifier le certificat** : sélectionnez cette option uniquement si vous avez une bonne raison de ne pas utiliser la validation de certificat, par exemple lorsqu'il y a un problème temporaire avec un certificat.
4. Sélectionnez **Enregistrer**. Tous les paquets hebdomadaires, déclenchés par l'utilisateur et déclenchés par des événements sont envoyés à l'aide du protocole sélectionné.

Désactivez 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 paquet AutoSupport hebdomadaire sera envoyé, allez à l'onglet **AutoSupport** > **Résultats**. Dans la section **AutoSupport hebdomadaire**, examinez la valeur de **prochaine heure planifiée**.

Vous pouvez désactiver à tout moment l'envoi automatique de packages AutoSupport hebdomadaires.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **AutoSupport** > **Paramètres**.
2. Décochez la case **Activer AutoSupport hebdomadaire**.
3. Sélectionnez **Enregistrer**.

Désactivez la fonction AutoSupport déclenchée par un événement

Par défaut, le système StorageGRID est configuré pour envoyer un package AutoSupport au support technique toutes les heures.

Vous pouvez désactiver les AutoSupport déclenchées par un événement à tout moment.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **AutoSupport** > **Paramètres**.
2. Décochez la case **Activer AutoSupport** déclenché par un événement.
3. Sélectionnez **Enregistrer**.

Activez AutoSupport on Demand

AutoSupport On Demand peut vous aider à résoudre les problèmes sur lesquels le support technique travaille activement.

AutoSupport On Demand est désactivé par défaut. L'activation de cette fonction permet au support technique de demander à votre système StorageGRID d'envoyer automatiquement des packages AutoSupport. Le support technique peut également définir l'intervalle d'interrogation pour les requêtes AutoSupport On

Demand.

Le support technique ne peut ni activer ni désactiver AutoSupport On Demand.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **AutoSupport** > **Paramètres**.
2. Sélectionnez le **HTTPS** pour le protocole.
3. Cochez la case **Activer AutoSupport hebdomadaire**.
4. Cochez la case **Activer AutoSupport On Demand**.
5. Sélectionnez **Enregistrer**.

   AutoSupport On Demand est activé et le support technique peut envoyer des demandes AutoSupport On Demand à StorageGRID.

Désactive 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 StorageGRID ou une nouvelle version est disponible, la nouvelle version s'affiche sur la page mise à niveau StorageGRID.

Si nécessaire, vous pouvez éventuellement désactiver la vérification des mises à jour logicielles. Par exemple, si votre système ne dispose pas d'un accès WAN, vous devez désactiver la vérification pour éviter les erreurs de téléchargement.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **AutoSupport** > **Paramètres**.
2. Décochez la case **Rechercher les mises à jour logicielles**.
3. Sélectionnez **Enregistrer**.

Ajouter une destination AutoSupport supplémentaire

Lorsque vous activez AutoSupport, les packages d'état et de santé 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 des packages AutoSupport, reportez-vous aux instructions à Spécifiez le protocole des 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. Spécifiez les éléments suivants :

   Nom d'hôte

   Nom d'hôte ou adresse IP du serveur d'un serveur de destination AutoSupport supplémentaire.

   > Vous ne pouvez entrer qu'une destination supplémentaire.

Port

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

Indique 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 si 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 de l'autorité de certification.
   b. Téléchargez le fichier de certificat de l'autorité de certification.

   Les métadonnées du certificat de l'autorité de certification s'affichent.
5. Sélectionnez **Enregistrer**.

Tous les packages AutoSupport hebdomadaires, déclenchés par des événements et déclenchés par l'utilisateur seront envoyés vers la destination supplémentaire.

configurez AutoSupport pour les appliances

AutoSupport for Appliances signale les problèmes liés au matériel StorageGRID. StorageGRID AutoSupport signale les problèmes liés au logiciel StorageGRID, à l'exception du SGF6112, StorageGRID AutoSupport signale les problèmes matériels et logiciels. Vous devez configurer AutoSupport sur chaque appliance, à l'exception du SGF6112, qui ne nécessite pas de configuration supplémentaire. AutoSupport est implémenté différemment pour les appliances de services et de stockage.

SANtricity vous permet d'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 appliances SG6000 et SG5700 "Configurez AutoSupport dans SANtricity System Manager"

Les packages AutoSupport des appliances E-Series peuvent être inclus dans StorageGRID AutoSupport si vous configurez la livraison AutoSupport par proxy dans "SANtricity System Manager".

StorageGRID AutoSupport ne signale pas de problèmes matériels, tels que des pannes de module DIMM ou de carte d'interface hôte (HIC). Cependant, certaines défaillances de composant peuvent "alertes matérielles"se déclencher . Pour les appliances StorageGRID dotées d'un contrôleur BMC (Baseboard Management Controller), vous pouvez configurer des interruptions SNMP et des e-mails pour signaler les défaillances matérielles :

- "Configurez les notifications par e-mail pour les alertes BMC"
- "Configurer les paramètres SNMP pour le contrôleur BMC"

Informations associées

"Support 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 pack AutoSupport.

Avant de commencer

- Vous devez être connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer de l'accès racine ou d'une autre autorisation de configuration de grille.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **AutoSupport**.
2. Dans l'onglet **actions**, sélectionnez **Envoyer AutoSupport déclenché par l'utilisateur**.

   StorageGRID tente d'envoyer un pack AutoSupport sur le site de support NetApp. Si la tentative réussit, les valeurs **résultat le plus récent** et **dernier temps** réussi 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 paquet AutoSupport.

   Après avoir envoyé un pack AutoSupport déclenché par l'utilisateur, actualisez la page AutoSupport de votre navigateur au bout d'une minute pour accéder aux résultats les plus récents.

Dépanner les packages AutoSupport

Si une tentative d'envoi d'un package AutoSupport échoue, le système StorageGRID prend différentes actions selon le type de package AutoSupport. Vous pouvez vérifier l'état des progiciels AutoSupport en sélectionnant **SUPPORT** > **Outils** > **AutoSupport** > **Résultats**.

Lorsque le paquet AutoSupport ne parvient pas à envoyer, "failed" apparaît sur l'onglet **Results** de la page **AutoSupport**.

Si vous avez configuré un serveur proxy pour transférer les paquets AutoSupport vers NetApp, vous devez "vérifiez que les paramètres de configuration du serveur proxy sont corrects".

Défaillance hebdomadaire du package AutoSupport

Si l'envoi d'un pack AutoSupport hebdomadaire échoue, le système StorageGRID prend les mesures suivantes :

1. Met à jour l'attribut de résultat le plus récent pour réessayer.
2. Tente de renvoyer le package AutoSupport 15 fois toutes les quatre minutes pendant une heure.
3. Après une heure d'échec d'envoi, met à jour l'attribut de résultat le plus récent sur échec.
4. Tente d'envoyer à nouveau un pack AutoSupport à la prochaine heure programmée.
5. Maintient le programme AutoSupport normal si le package échoue parce que le service NMS est indisponible et si un package est envoyé avant sept jours.
6. Lorsque le service NMS est de nouveau disponible, envoie un package AutoSupport immédiatement si un package n'a pas été envoyé pendant sept jours ou plus.

Défaillance du package AutoSupport déclenché par l'utilisateur ou l'événement

Si un package AutoSupport déclenché par l'utilisateur ou un événement ne parvient pas à être envoyé, le système StorageGRID prend les mesures suivantes :

1. Affiche un message d'erreur si l'erreur est connue. Par exemple, si un utilisateur sélectionne le protocole SMTP sans fournir de 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. Ne tente pas d'envoyer à nouveau le pack.
3. Consigne l'erreur dans `nms.log`.

En cas d'échec et si 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 (hérité)** > **Configuration du courrier électronique hérité**). Le message d'erreur suivant peut s'afficher 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".

Corrigez une défaillance du package AutoSupport

En cas d'échec et si 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 s'afficher sur la page AutoSupport : `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Envoyez des packages AutoSupport E-Series via StorageGRID

Vous pouvez envoyer des packages AutoSupport du Gestionnaire système SANtricity E-Series au support technique via un nœud d'administration StorageGRID plutôt que le port de gestion de l'appliance de stockage.

Pour plus d'informations sur l'utilisation de AutoSupport avec les appliances E-Series, reportez-vous à la section "Matériel E-Series AutoSupport".

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Administrateur de l'appliance de stockage ou autorisation d'accès racine".
- Vous avez configuré SANtricity AutoSupport :
  - Pour les appliances SG6000 et SG5700 "Configurez AutoSupport dans SANtricity System Manager"

> Vous devez disposer d'un firmware SANtricity 8.70 ou supérieur pour accéder à SANtricity System Manager à l'aide de Grid Manager.

Description de la tâche

Les packages AutoSupport E-Series contiennent des informations détaillées 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 le Gestionnaire système SANtricity pour

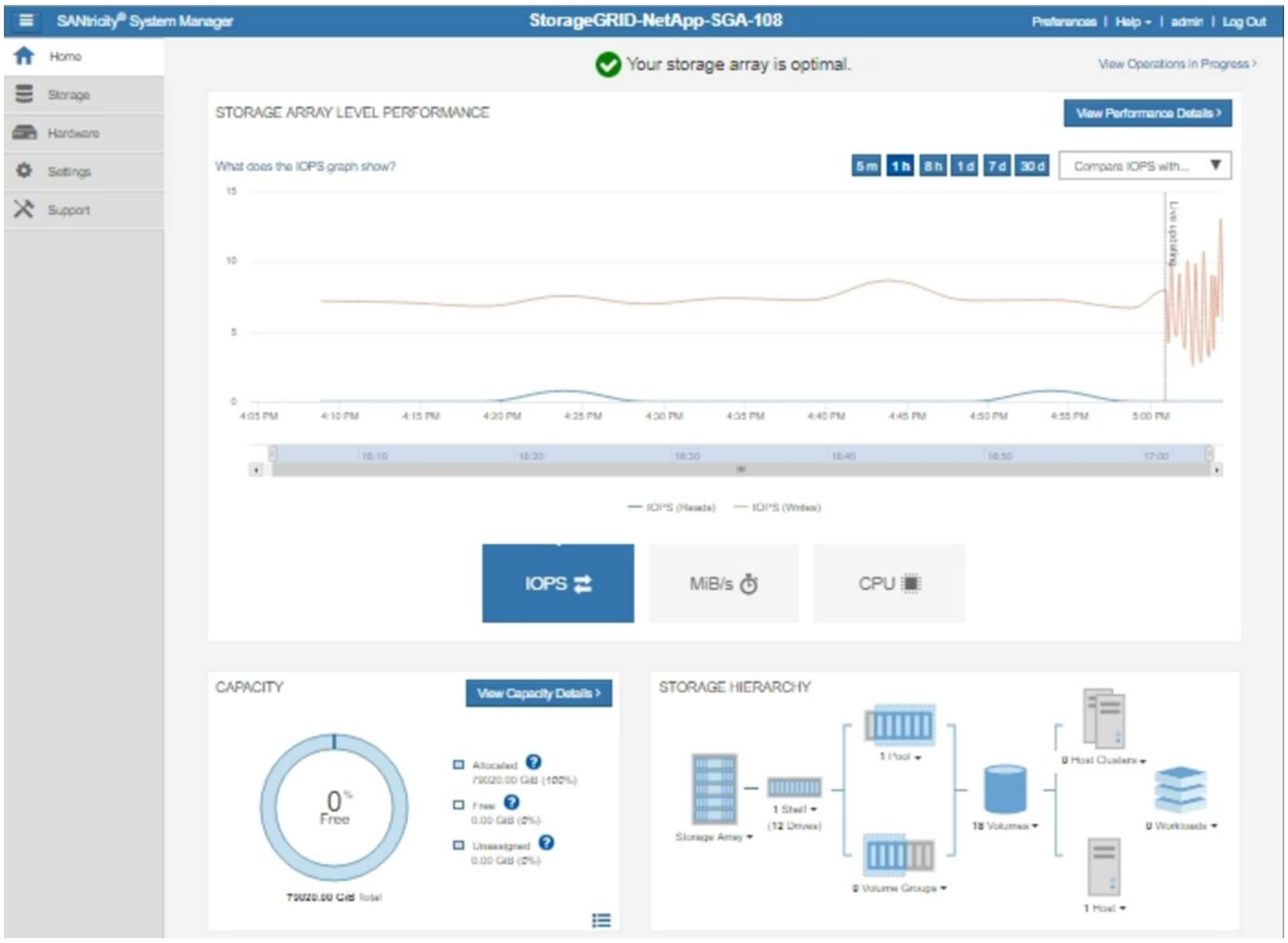
transmettre des packages AutoSupport via un nœud d'administration StorageGRID sans utiliser le port de gestion de l'appliance. Les paquets AutoSupport transmis de cette façon sont envoyés par le "Nœud d'administration de l'expéditeur préféré", et ils utilisent tous ceux "paramètres du proxy d'administration" qui ont été configurés dans le Gestionnaire de grille.

> Cette procédure concerne uniquement la configuration d'un serveur proxy StorageGRID pour les packages E-Series AutoSupport. Pour plus de détails sur la configuration E-Series AutoSupport, consultez le "Documentation NetApp E-Series et SANtricity".

Étapes

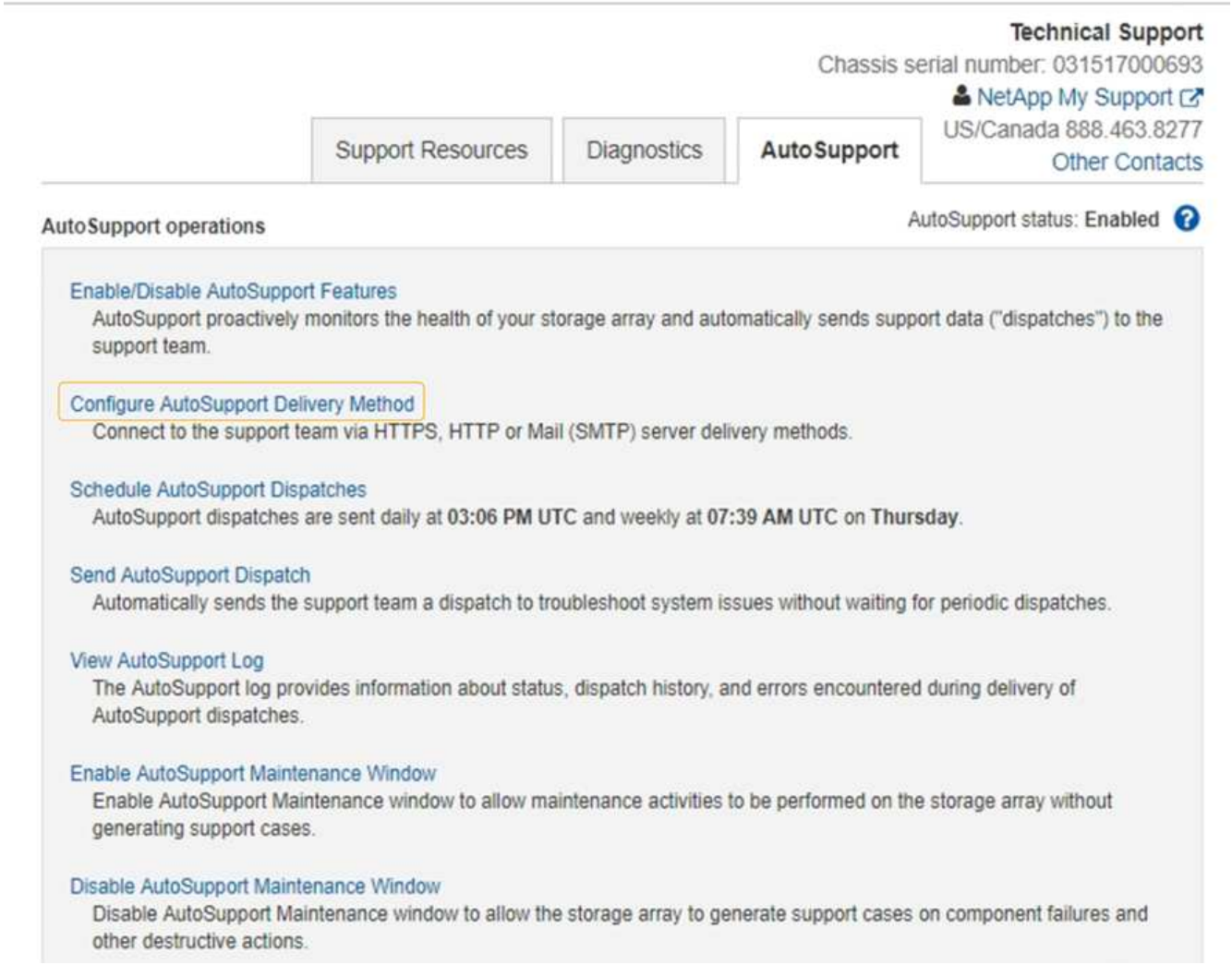
1. Dans le Gestionnaire de grille, sélectionnez **NOEUDS**.
2. Dans la liste des nœuds de gauche, sélectionnez le nœud d'appliance de stockage à configurer.
3. Sélectionnez **SANtricity System Manager**.

   La page d'accueil de SANtricity System Manager s'affiche.



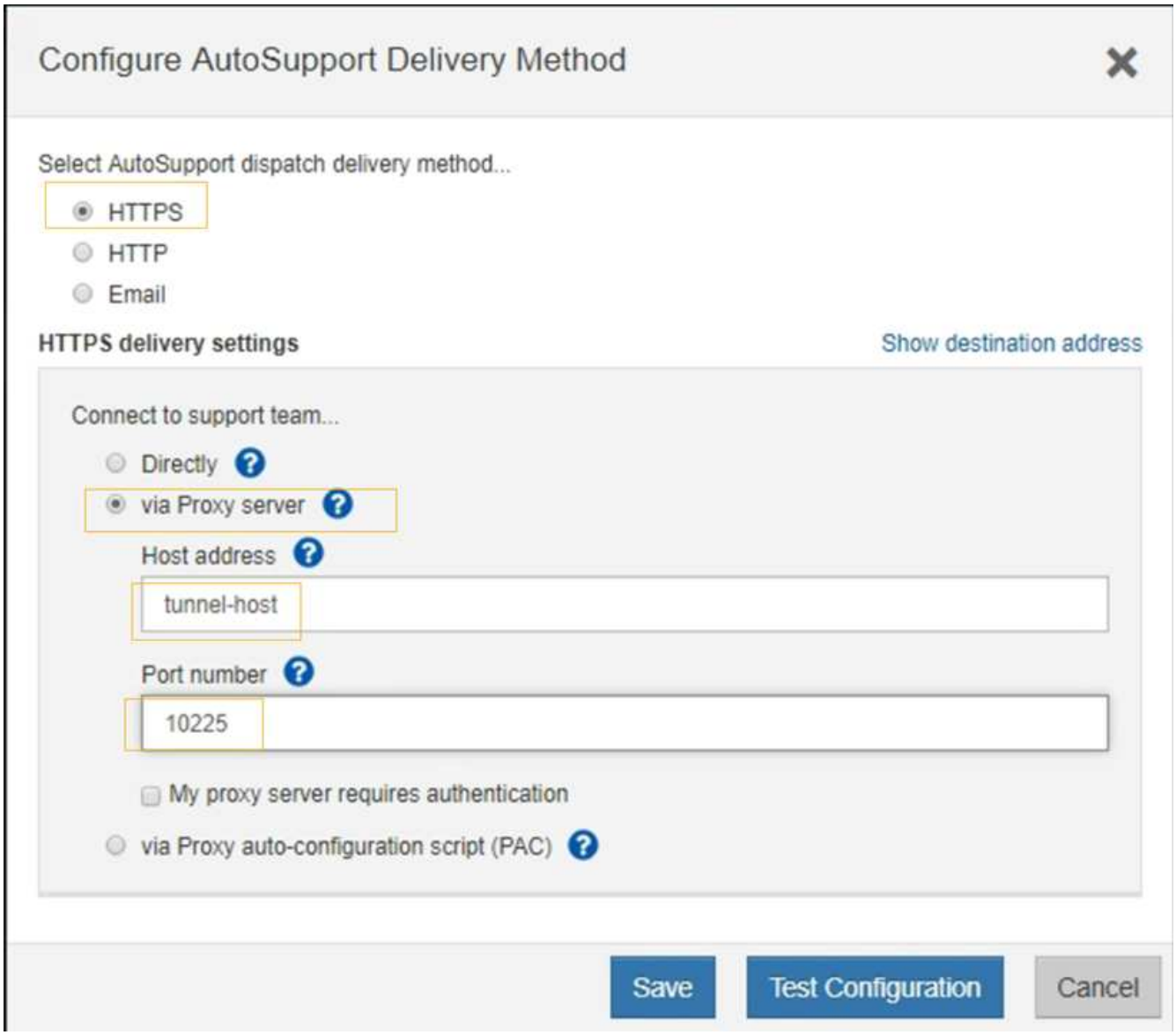
4. Sélectionnez **SUPPORT** > **support Center** > **AutoSupport**.

   La page 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** pour la méthode de livraison.

   Le certificat qui active HTTPS est préinstallé.

7. Sélectionnez **via le serveur proxy**.
8. Entrez `tunnel-host` l'adresse **hôte**.

   `tunnel-host` Est l'adresse spéciale permettant d'utiliser un nœud d'administration pour envoyer les packages AutoSupport E-Series.

9. Entrez `10225` 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 le cas, un message s'affiche dans une bannière verte : « votre configuration AutoSupport a été

vérifiée ».

Si le test échoue, un message d'erreur s'affiche dans une bannière rouge. Vérifiez vos paramètres DNS et la mise en réseau StorageGRID, assurez-vous que le système "Nœud d'administration de l'expéditeur préféré" peut se connecter au site de support NetApp, puis réessayez 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 des nœuds de stockage

Gérer des nœuds de stockage

Des nœuds de stockage fournissent de la capacité de stockage sur disque et des services. La gestion des nœuds de stockage implique les tâches suivantes :

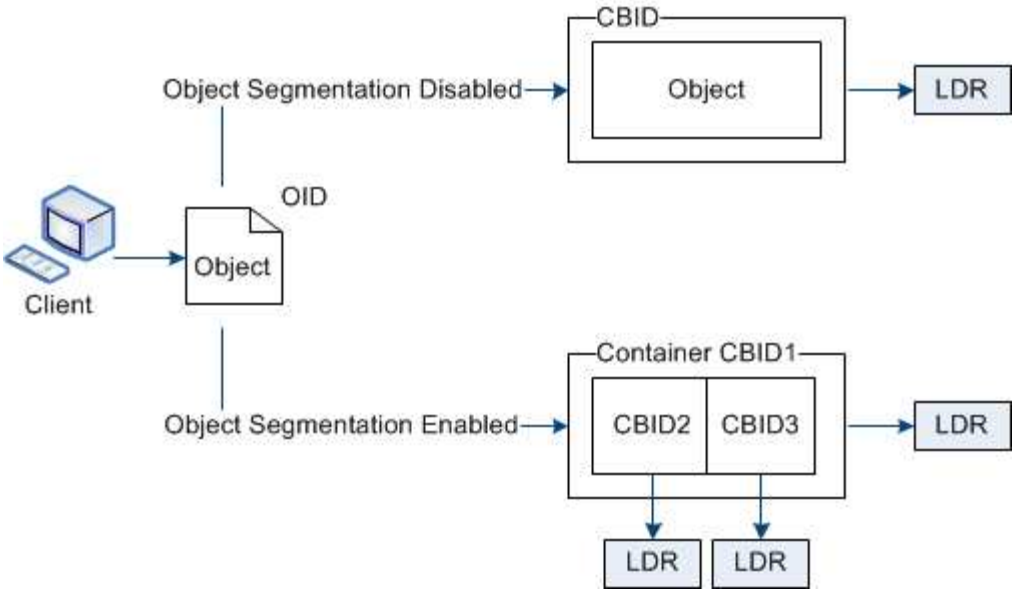
- Gestion des options de stockage
- Description des filigranes du volume de stockage et utilisation des filigranes pour contrôler le moment où les nœuds de stockage deviennent en lecture seule
- Contrôle et gestion de l'espace utilisé pour les métadonnées d'objet
- Configuration des paramètres globaux des objets stockés
- Application des paramètres de configuration du nœud de stockage
- Gestion des nœuds de stockage complets

Utilisez les options de stockage

Qu'est-ce que la segmentation d'objet ?

La segmentation d'objet consiste à diviser un objet en un ensemble d'objets de taille fixe plus petits afin d'optimiser l'utilisation du stockage et des ressources pour les objets de grande taille. Le téléchargement multi-pièces S3 crée également des objets segmentés, avec un objet représentant chaque pièce.

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 original à partir de ses segments et renvoie l'objet au client.

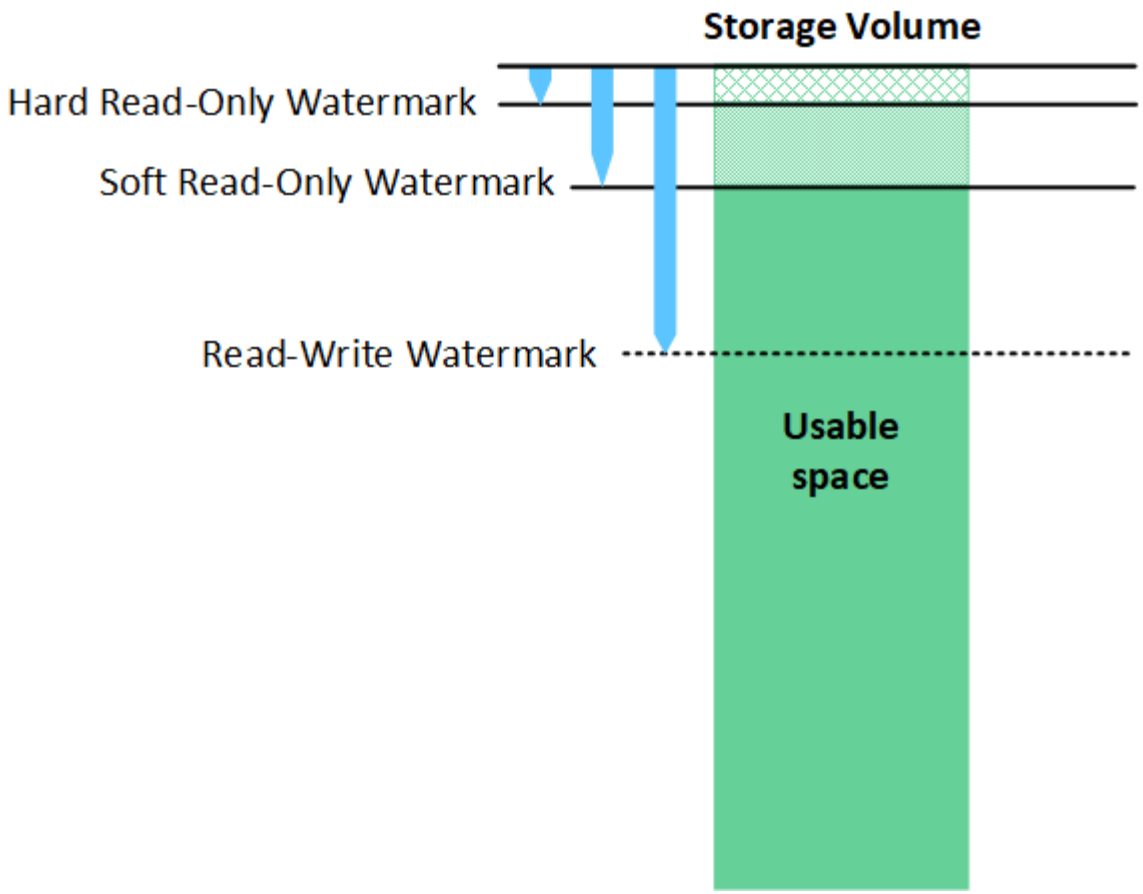
Le conteneur et les segments ne sont pas nécessairement stockés sur le même nœud de stockage. Les conteneurs et les segments peuvent être stockés sur n'importe quel nœud de stockage du pool de stockage spécifié dans la règle ILM.

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 après la fin de l'acquisition, comme suit :

```
segment container + segment 1 + segment 2 = three stored objects
```

Quelles sont les filigranes du volume de stockage ?

StorageGRID utilise trois filigranes de volume de stockage qui garantissent que les nœuds de stockage sont transférés en toute sécurité vers un état en lecture seule avant de s'exécuter avec un espace critique et que les nœuds de stockage ayant été transférés vers un état en lecture seule afin de devenir à nouveau en lecture/écriture.



Les filigranes du volume de stockage ne s'appliquent qu'à l'espace utilisé pour les données d'objets répliquées et codées par effacement. Pour en savoir plus sur l'espace réservé aux métadonnées d'objet sur le volume 0, rendez-vous "Gérer le stockage des métadonnées d'objet"sur .

Qu'est-ce que le filigrane logiciel en lecture seule ?

Le filigrane **soft read-only du volume de stockage** est le premier filigrane qui indique que l'espace utilisable d'un nœud de stockage pour les données d'objet est saturé.

Si chaque volume d'un nœud de stockage dispose d'un espace libre inférieur au 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 des services en lecture seule au reste du système StorageGRID, mais remplit toutes les demandes d'écriture en attente.

Supposons, par exemple, que chaque volume d'un nœud de stockage possède un filigrane en lecture seule de 10 Go. Dès que chaque volume dispose de moins de 10 Go d'espace libre, le nœud de stockage passe en mode veille souple en lecture seule.

Qu'est-ce que le filigrane en lecture seule ?

Le filigrane **en lecture seule du volume de stockage** est le filigrane suivant pour indiquer que l'espace utilisable d'un nœud pour les données d'objet est saturé.

Si l'espace disponible sur un volume est inférieur au filigrane en lecture seule, les écritures sur le volume échoueront. Cependant, les écritures sur d'autres volumes peuvent se poursuivre jusqu'à ce que l'espace libre sur ces volumes soit inférieur à leurs filigranes en lecture seule.

Supposons, par exemple, 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 de demandes d'écriture.

Le filigrane en lecture seule est toujours inférieur au filigrane en lecture seule.

Qu'est-ce que le filigrane de lecture-écriture ?

Le filigrane **lecture-écriture du volume de stockage** ne s'applique qu'aux nœuds de stockage qui sont passés en mode lecture seule. Il détermine quand le nœud peut redevenir 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.

Supposons par exemple que le nœud de stockage est passé en mode lecture seule. Supposons également que chaque volume possède un filigrane de lecture-écriture de 30 Go. Dès que l'espace libre d'un volume augmente jusqu'à 30 Go, le nœud redevient read-write.

Le filigrane en lecture-écriture est toujours plus grand que le filigrane en lecture seule et le filigrane en lecture seule.

Afficher les filigranes du volume de stockage

Vous pouvez afficher les paramètres actuels du filigrane ainsi que les valeurs optimisées par le système. Si les filigranes optimisés ne sont pas utilisés, vous pouvez déterminer si vous pouvez ou devez régler les paramètres.

Avant de commencer

- Vous avez terminé la mise à niveau vers StorageGRID 11.6 ou une version ultérieure.
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine".

Afficher les paramètres actuels du filigrane

Vous pouvez afficher les paramètres actuels du filigrane de stockage dans Grid Manager.

Étapes

1. Sélectionnez **SUPPORT** > **autre** > **filigranes de stockage**.
2. Sur la page filigranes de stockage, cochez la case utiliser les valeurs optimisées.
   - Si cette case est cochée, 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 pouvez Afficher des filigranes de stockage optimisés.

   - Si la case utiliser les valeurs optimisées n'est pas cochée, des filigranes personnalisés (non optimisés) sont utilisés. L'utilisation de paramètres de filigrane personnalisés n'est pas recommandée. Suivez les instructions de "Dépannage des alertes de remplacement du filigrane en lecture seule faible" pour déterminer si vous pouvez ou devez régler les paramètres.

     Lorsque vous spécifiez des paramètres de filigrane personnalisés, vous devez entrer des valeurs supérieures à 0.

Afficher les filigranes de stockage optimisés

StorageGRID utilise deux metrics Prometheus pour afficher les valeurs optimisées qu'il a calculées pour le seuil en lecture seule souple du volume de stockage. Vous pouvez afficher les valeurs minimale et maximale optimisées pour chaque nœud de stockage de la grille.

1. Sélectionnez **SUPPORT** > **Outils** > **métriques**.
2. Dans la section Prometheus, sélectionnez le lien permettant d'accéder à l'interface utilisateur Prometheus.
3. Pour afficher le filigrane minimum en lecture seule programmable recommandé, entrez la mesure Prometheus suivante et sélectionnez **Execute** :

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   La dernière colonne affiche la valeur minimale optimisée du filigrane en lecture seule pour tous les volumes de stockage de chaque nœud de stockage. Si cette valeur est supérieure au paramètre personnalisé du filigrane en lecture seule du volume de stockage, l'alerte **Low read-only filigrane override** est déclenchée pour le nœud de stockage.

4. Pour afficher le filigrane maximal en lecture seule programmable recommandé, entrez la mesure Prometheus suivante et sélectionnez **Execute** :

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   La dernière colonne affiche la valeur maximale optimisée du filigrane en lecture seule pour tous les volumes de stockage de chaque nœud de stockage.

Gérer le stockage des métadonnées d'objet

La capacité des métadonnées d'objet d'un système StorageGRID contrôle le nombre maximal d'objets qui peuvent être stockés sur le système en question. Pour s'assurer que votre système StorageGRID dispose d'un espace suffisant pour stocker les nouveaux objets, vous devez comprendre où et comment StorageGRID stocke les métadonnées d'objet.

Qu'est-ce que les métadonnées d'objet ?

Les métadonnées d'objet constituent toutes les informations qui décrivent un objet. StorageGRID utilise les métadonnées d'objet pour suivre l'emplacement de tous les objets de la grille, et pour gérer le cycle de vie de chaque objet au fil du temps.

Pour un objet dans StorageGRID, les métadonnées d'objet incluent les types d'information suivants :

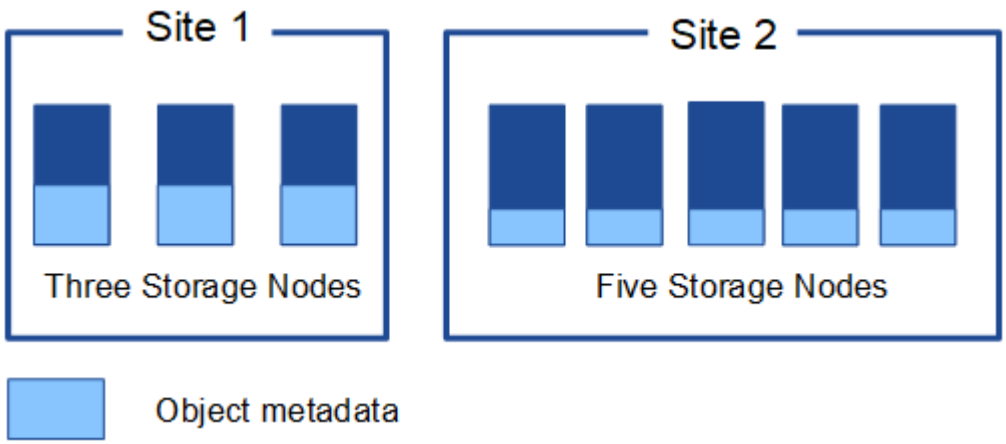
- Métadonnées du système, y compris un ID unique pour chaque objet (UUID), le nom de l'objet, le nom du compartiment S3, le nom ou l'ID du compte locataire, la taille logique de l'objet, la date et l'heure de création de l'objet, ainsi que la date et l'heure de la dernière modification de l'objet.
- Toutes les paires de clé-valeur de métadonnées utilisateur personnalisées associées à l'objet.
- Pour les objets S3, toutes les paires de clé-valeur de balise d'objet associées à l'objet.
- Pour les copies d'objet répliquées, emplacement de stockage actuel de chaque copie.
- Pour les copies d'objets avec code d'effacement, l'emplacement de stockage actuel de chaque fragment.

- Pour les copies d'objet dans Cloud Storage Pool, l'emplacement de l'objet, notamment le nom du compartiment externe et l'identifiant unique de l'objet.
- Pour les objets segmentés et les objets à plusieurs parties, les identificateurs de segment et la taille des données.

Comment les métadonnées d'objet sont-elles stockées ?

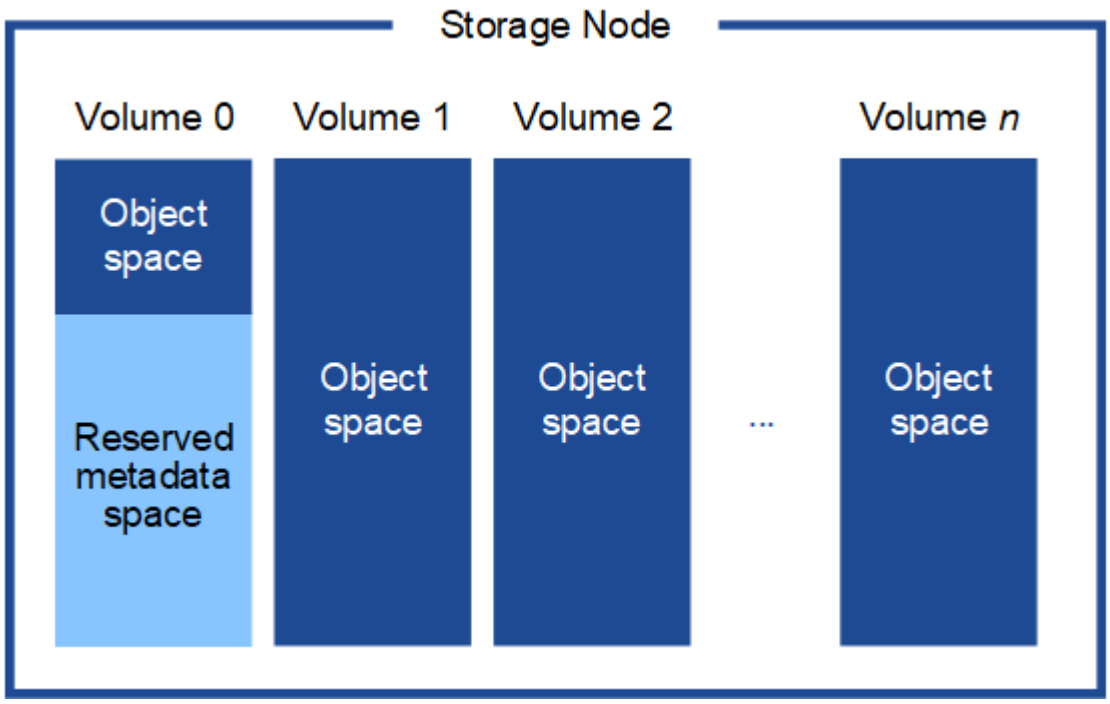
Les métadonnées d'objet sont conservées dans une base de données Cassandra, stockée indépendamment des données d'objet. StorageGRID Pour assurer la redondance et protéger les métadonnées d'objet contre la perte, StorageGRID stocke trois copies des métadonnées de tous les objets du système sur chaque site.

Cette figure représente les nœuds de stockage sur deux sites. Chaque site dispose du même volume de métadonnées objet, et les métadonnées de chaque site sont subdivisées en plusieurs nœuds de stockage sur ce site.



Où sont stockées les métadonnées d'objet ?

Cette figure représente les volumes de stockage d'un seul nœud de stockage.



Comme illustré dans la figure, StorageGRID réserve l'espace des métadonnées d'objet sur le volume de stockage 0 de chaque nœud de stockage. Il utilise l'espace réservé pour stocker les métadonnées d'objet et effectuer les opérations essentielles de la base de données. Tout espace restant sur le volume de stockage 0 et tous les autres volumes du nœud de stockage sont utilisés exclusivement pour les données d'objet (copies répliquées et fragments avec code d'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 de 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.
- 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 par défaut pour les métadonnées
11.5 à 11.9	Au moins 128 Go 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	4 TO (4,000 GO)
	Moins de 128 Go sur n'importe quel nœud de stockage de chaque site	3 TO (3,000 GO)
11.0 ou antérieure	Tout montant	2 TO (2,000 GO)

Afficher le paramètre d'espace réservé aux métadonnées

Procédez comme suit pour afficher le paramètre espace réservé aux métadonnées de 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 version ultérieure, 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 StorageGRID 11.6 ou supérieure dans laquelle chaque nœud de stockage dispose d'au moins 128 Go de RAM est de 8,000 Go (8 To).

Espace réservé réel pour les métadonnées

Contrairement au paramètre espace réservé pour les métadonnées à l'échelle du système, l'espace réservé *réel* pour les métadonnées de l'objet est déterminé pour chaque nœud de stockage. Pour un 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 pour les métadonnées à l'échelle du système.

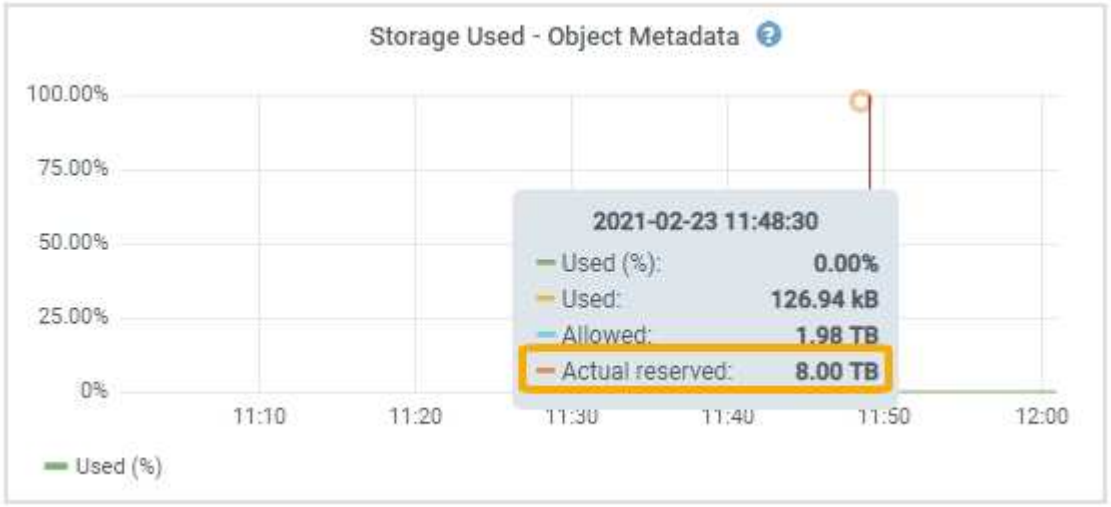
Taille du volume 0 pour le nœud	Espace réservé réel pour les métadonnées
Moins de 500 Go (utilisation hors production)	10 % du volume 0
500 Go ou plus + ou + nœuds de stockage des métadonnées uniquement	Plus ces valeurs sont faibles : • Volume 0 • Paramètre d'espace réservé de métadonnées **Remarque** : un seul rangedb est requis pour les nœuds de stockage de métadonnées uniquement.

Afficher l'espace réservé réel pour les métadonnées

La procédure suivante permet d'afficher l'espace réservé réel pour les métadonnées sur un nœud de stockage particulier.

Étapes

1. Dans Grid Manager, sélectionnez **NOEUDS** > ***Storage Node***.
2. Sélectionnez l'onglet **stockage**.
3. Placez votre curseur sur le graphique stockage utilisé - métadonnées de l'objet et localisez la valeur **réel réservé**.



Dans la capture d'écran, la valeur **réelle réservée** est de 8 To. Cette copie d'écran concerne un nœud de stockage grand format dans une nouvelle installation de StorageGRID 11.6. Comme l'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 espace réservé aux métadonnées.

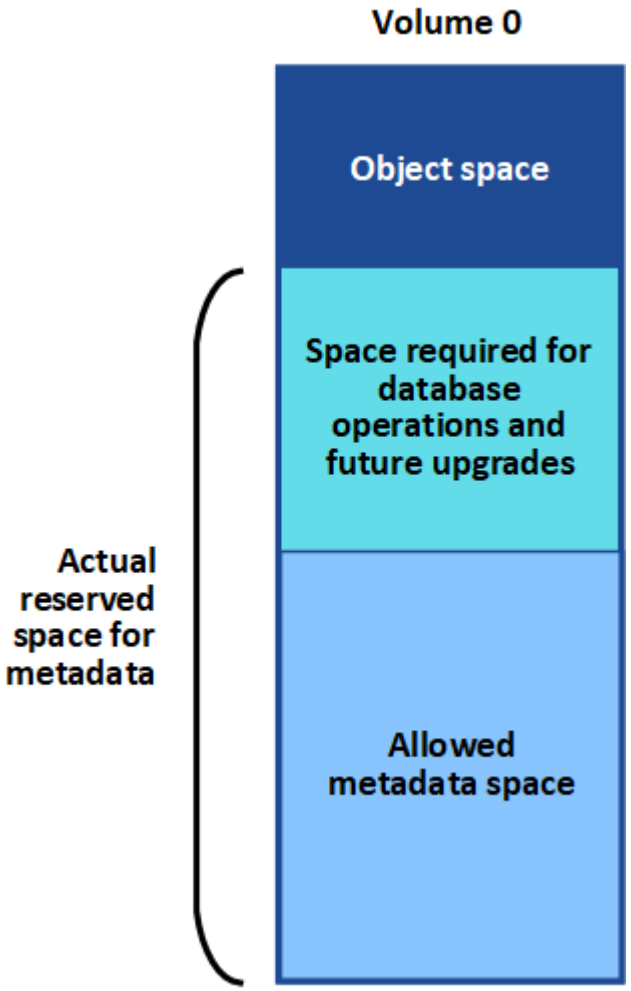
Exemple d’espace de métadonnées réservé réel

Supposons que vous installiez un nouveau système StorageGRID à l’aide de la version 11.7 ou ultérieure. Dans 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 **métadonnées** à l’échelle du système est défini sur 8 To. (Il s’agit de la valeur par défaut pour une nouvelle installation StorageGRID 11.6 ou supérieure si chaque nœud de stockage possède 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 inférieur au paramètre **Metadata reserved space**.)

Espace de métadonnées autorisé

L’espace réservé réel de chaque nœud de stockage pour les métadonnées est divisé en l’espace disponible pour les métadonnées d’objet (l’espace *autorisé metadata space*) et l’espace requis pour les opérations essentielles de bases de données (telles que la compaction et la réparation) et les mises à niveau matérielles et logicielles futures. L’espace de métadonnées autorisé régit la capacité globale des objets.



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.

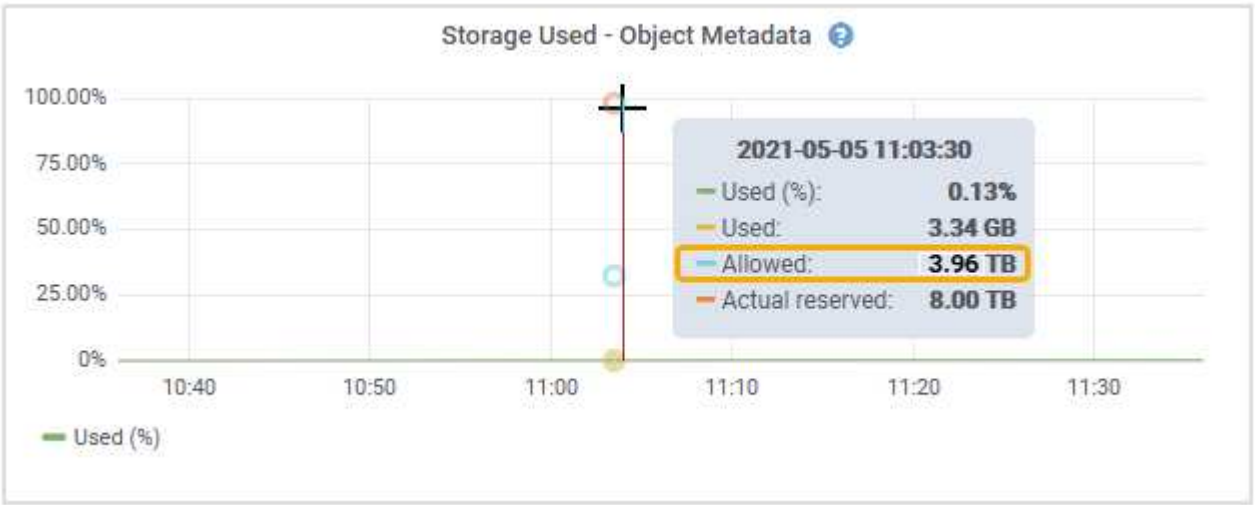
		Quantité de mémoire sur le noeud de stockage	
	&Lt ; 128 GB	&gt ;= 128 Go	**Espace réservé réel pour les métadonnées**
&Lt ;= 4 To	60 % de l'espace réservé réel pour les métadonnées, jusqu'à un maximum de 1.32 To	60 % de l'espace réservé réel pour les métadonnées, jusqu'à un maximum de 1.98 To	&gt ; 4 To

Afficher l'espace de métadonnées autorisé

La procédure suivante permet d'afficher l'espace de métadonnées autorisé pour un nœud de stockage.

Étapes

1. Dans Grid Manager, sélectionnez **NODES**.
2. Sélectionnez le nœud de stockage.
3. Sélectionnez l'onglet **stockage**.
4. Placez votre curseur sur le graphique de métadonnées de l'objet stockage utilisé - et localisez la valeur **autorisé**.



Dans la capture d'écran, la valeur **autorisé** est de 3.96 To, ce qui est la valeur maximale pour un noeud de stockage dont l'espace réservé réel pour les métadonnées est supérieur à 4 To.

La valeur **autorisé** correspond à cette métrique Prometheus :

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Exemple d'espace de métadonnées autorisé

Supposons que vous installez un système StorageGRID avec la version 11.6. Dans 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 **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 inférieur au paramètre **Metadata reserved space**.)
- L'espace autorisé pour les métadonnées sur SN1 est de 3 To, basé sur le calcul indiqué dans tableau pour l'espace autorisé pour les métadonnées: (espace réservé réel pour les métadonnées − 1 To) × 60 %, jusqu'à un maximum de 3.96 To.

La façon dont les nœuds de stockage de différentes tailles affectent la capacité des objets

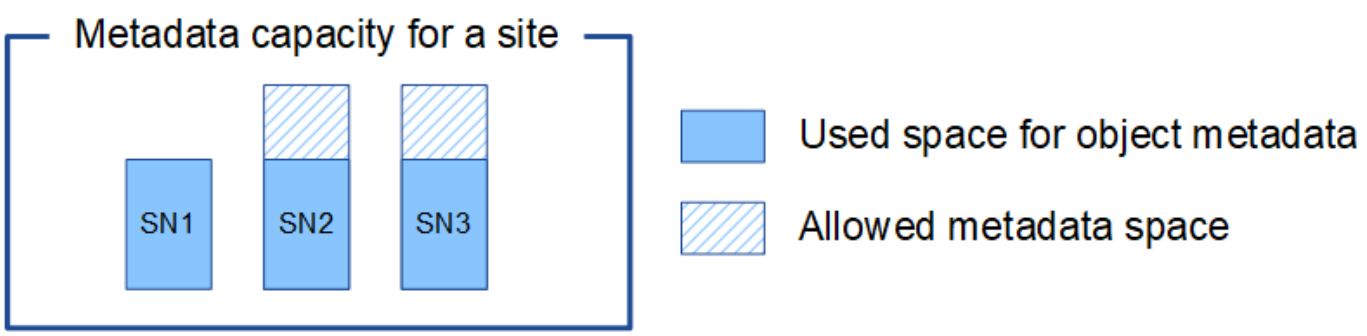
Comme décrit ci-dessus, StorageGRID distribue uniformément les métadonnées d'objet sur les nœuds de stockage sur chaque site. Par conséquent, si un site contient des nœuds de stockage de différentes tailles, le plus petit nœud du site détermine la capacité des métadonnées du site.

Prenons l'exemple suivant :

- Une grille sur un seul site contient 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 réservé réel des métadonnées et l'espace autorisé pour les métadonnées.

Nœud de stockage	Taille du volume 0	Espace réservé réel des métadonnées	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

Les métadonnées de l'objet sont réparties de manière uniforme sur les nœuds de stockage d'un site. En effet, chaque nœud de cet exemple ne peut contenir que 1.32 To de métadonnées. Les 0.66 To supplémentaires d'espace de métadonnées autorisé pour SN2 et SN3 ne peuvent pas être utilisés.



De même, puisque StorageGRID conserve toutes les métadonnées d'objet d'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.

Étant donné que la capacité des métadonnées contrôle le nombre maximal d'objets, lorsqu'un nœud vient à manquer de capacité de métadonnées, la grille est véritablement pleine.

Informations associées

- Pour savoir comment surveiller la capacité des métadonnées d'objet pour chaque nœud de stockage, reportez-vous aux instructions de la "Surveillance StorageGRID".
- Pour augmenter la capacité de métadonnées d'objet de votre système, "développez une grille"ajoutez de nouveaux nœuds de stockage.

Augmenter le paramètre espace réservé des métadonnées

Vous pouvez augmenter le paramètre système Metadata Reserved Space si vos nœuds de stockage répondent aux exigences spécifiques en matière de RAM et d'espace disponible.

Ce dont vous avez besoin

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Droits d'accès racine ou Configuration de la page topologie de la grille et autres autorisations de configuration de la grille".

> La page de topologie de la grille est obsolète et sera supprimée dans une version ultérieure.

Description de la tâche

Vous pouvez augmenter manuellement l'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 pour l'ensemble du système que si ces deux instructions sont vraies :

- Les nœuds de stockage de n'importe quel site de votre système disposent chacun d'au moins 128 Go de RAM.
- L'espace disponible des nœuds de stockage de n'importe quel site du système est suffisant pour le volume de stockage 0.

Notez que si vous augmentez ce paramètre, vous réduisez simultanément l'espace disponible pour le stockage objet sur le volume de stockage 0 de tous les nœuds de stockage. C'est pour cette raison que vous préférez définir l'espace réservé aux métadonnées sur une valeur inférieure à 8 To, en fonction des exigences de métadonnées de l'objet que vous prévoyez.

> En général, il est préférable d'utiliser une valeur plus élevée au lieu d'une valeur plus faible. Si le paramètre espace réservé aux métadonnées est trop grand, vous pouvez le réduire ultérieurement. Par opposition, si vous augmentez la valeur par la suite, le système peut avoir besoin de déplacer les données d'objet afin de libérer de l'espace.

Pour une explication détaillée de la façon dont le paramètre espace réservé des métadonnées affecte l'espace autorisé pour le stockage des métadonnées d'objet sur un nœud de stockage particulier, reportez-vous à la section "Gérer le stockage des métadonnées d'objet".

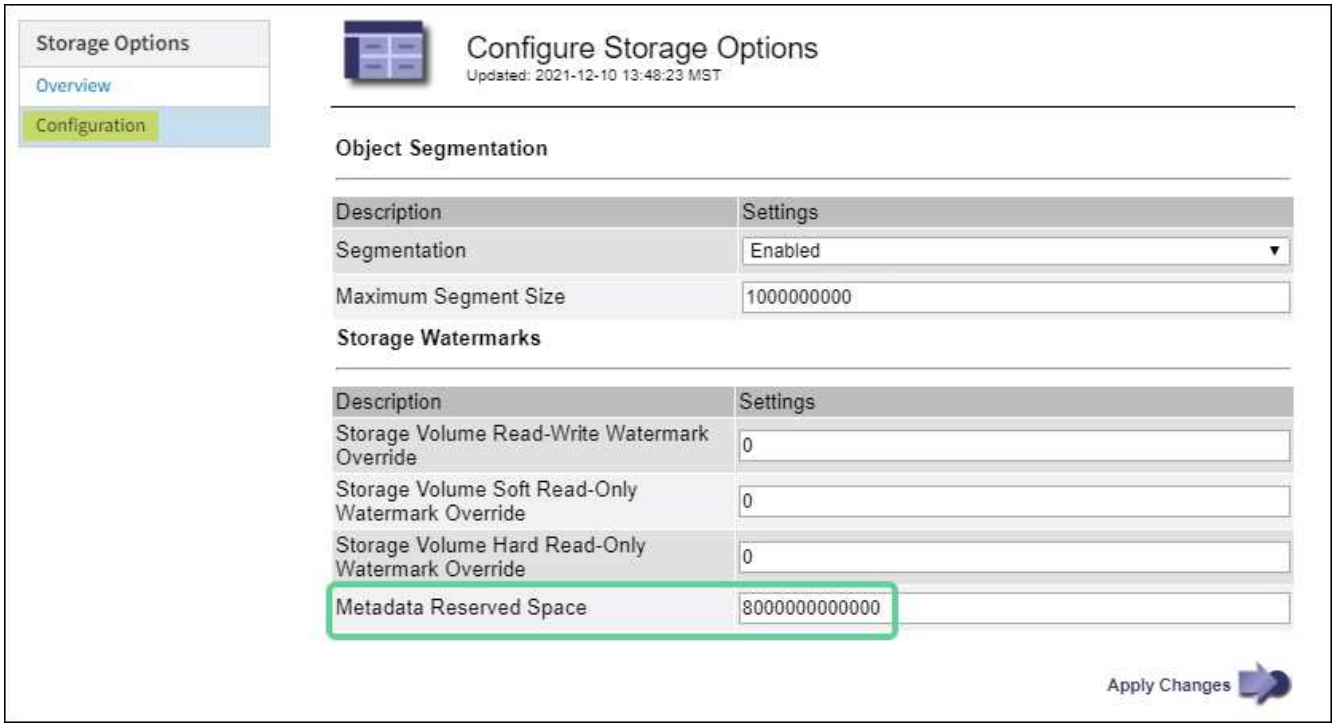
Étapes

1. Déterminez le paramètre actuel 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 d'avoir suffisamment d'espace disponible sur le volume de stockage 0 de chaque nœud de stockage pour augmenter cette valeur.
   a. Sélectionnez **NOEUDS**.
   b. Sélectionnez le premier nœud de stockage dans la grille.
   c. Cliquez sur l'onglet stockage.
   d. Dans la section volumes, recherchez l'entrée **/var/local/rangedb/0**.
   e. Vérifiez 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 cette procédure pour tous les nœuds de stockage.
      - Si un ou plusieurs nœuds de stockage ne disposent pas d'espace disponible suffisant, la valeur espace réservé aux métadonnées ne peut pas être augmentée. Ne pas poursuivre cette procédure.
      - Si chaque nœud de stockage dispose de suffisamment d'espace disponible sur le volume 0, passez à l'étape suivante.
3. Vérifiez que vous disposez d'au moins 128 Go de RAM sur chaque nœud de stockage.
   a. Sélectionnez **NOEUDS**.
   b. Sélectionnez le premier nœud de stockage dans la grille.
   c. Sélectionnez l'onglet **matériel**.
   d. Placez le curseur sur le graphique utilisation de la mémoire. Vérifiez que **mémoire totale** est d'au moins 128 Go.
   e. Répétez cette procédure 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 pas poursuivre cette procédure.
      - Si chaque nœud de stockage dispose d'au moins 128 Go de mémoire totale, passez à l'étape suivante.
4. Mettez à jour le paramètre Metadata Reserved Space.
   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, entrez **8000000000000** (8, suivi de 12 zéros).



a. Sélectionnez **appliquer les modifications**.

Compresser les objets stockés

Vous pouvez activer la compression des objets afin de réduire la taille des objets stockés dans StorageGRID, de sorte que les objets consomment moins d'espace de stockage.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez "autorisations d'accès spécifiques".

Description de la tâche

Par défaut, la compression des objets est désactivée. Si vous activez la compression, StorageGRID tente de compresser chaque objet lors de son enregistrement à l'aide de la compression sans perte.

> Si vous modifiez ce paramètre, il faudra environ une minute pour appliquer le nouveau paramètre. La valeur configurée est mise en cache pour les performances et l'évolutivité.

Avant d'activer la compression d'objets, tenez compte des points suivants :

- Vous ne devez pas sélectionner **Compresser les objets stockés**, sauf si vous savez 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 client a déjà compressé un objet avant de l'enregistrer dans StorageGRID, la sélection de cette option ne réduira pas davantage la taille d'un objet.
- Ne sélectionnez pas **Compresser les objets stockés** si vous utilisez NetApp FabricPool avec StorageGRID.
- Si **Compress Stored objects** est sélectionné, les applications client S3 doivent éviter d'effectuer des opérations GetObject qui spécifient une plage d'octets. 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 objet très volumineux 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 client peuvent être en attente.

> Si vous devez compresser des objets et que votre application client doit utiliser des lectures de plage, augmentez le délai de lecture de l'application.

Étapes

1. Sélectionnez **CONFIGURATION** > **système** > **Paramètres de stockage** > **compression objet**.
2. Cochez la case **Compresser les objets stockés**.
3. Sélectionnez **Enregistrer**.

Gérer des nœuds de stockage complets

Lorsque les nœuds de stockage atteignent leur capacité maximale, ils doivent étendre le système StorageGRID en ajoutant du nouveau stockage. Trois options sont disponibles : ajout de volumes de stockage, ajout de tiroirs d'extension de stockage et ajout de nœuds de stockage.

Ajout de volumes de stockage

Chaque nœud de stockage prend en charge un nombre maximal de volumes de stockage. Le maximum défini varie selon la plate-forme. Si un nœud de stockage contient moins de volumes de stockage que le nombre maximum, vous pouvez ajouter des volumes pour augmenter sa capacité. Voir les instructions pour "Extension d'un système StorageGRID".

Ajout de tiroirs d'extension de stockage

Certains nœuds de stockage d'appliance StorageGRID, tels que SG6060 ou SG6160, peuvent prendre en charge des tiroirs de stockage supplémentaires. Si vos appliances StorageGRID bénéficient de fonctionnalités d'extension qui n'ont pas encore été étendues à leur capacité maximale, vous pouvez ajouter des tiroirs de stockage pour augmenter la capacité. Voir les instructions pour "Extension d'un système StorageGRID".

Ajouter des nœuds de stockage

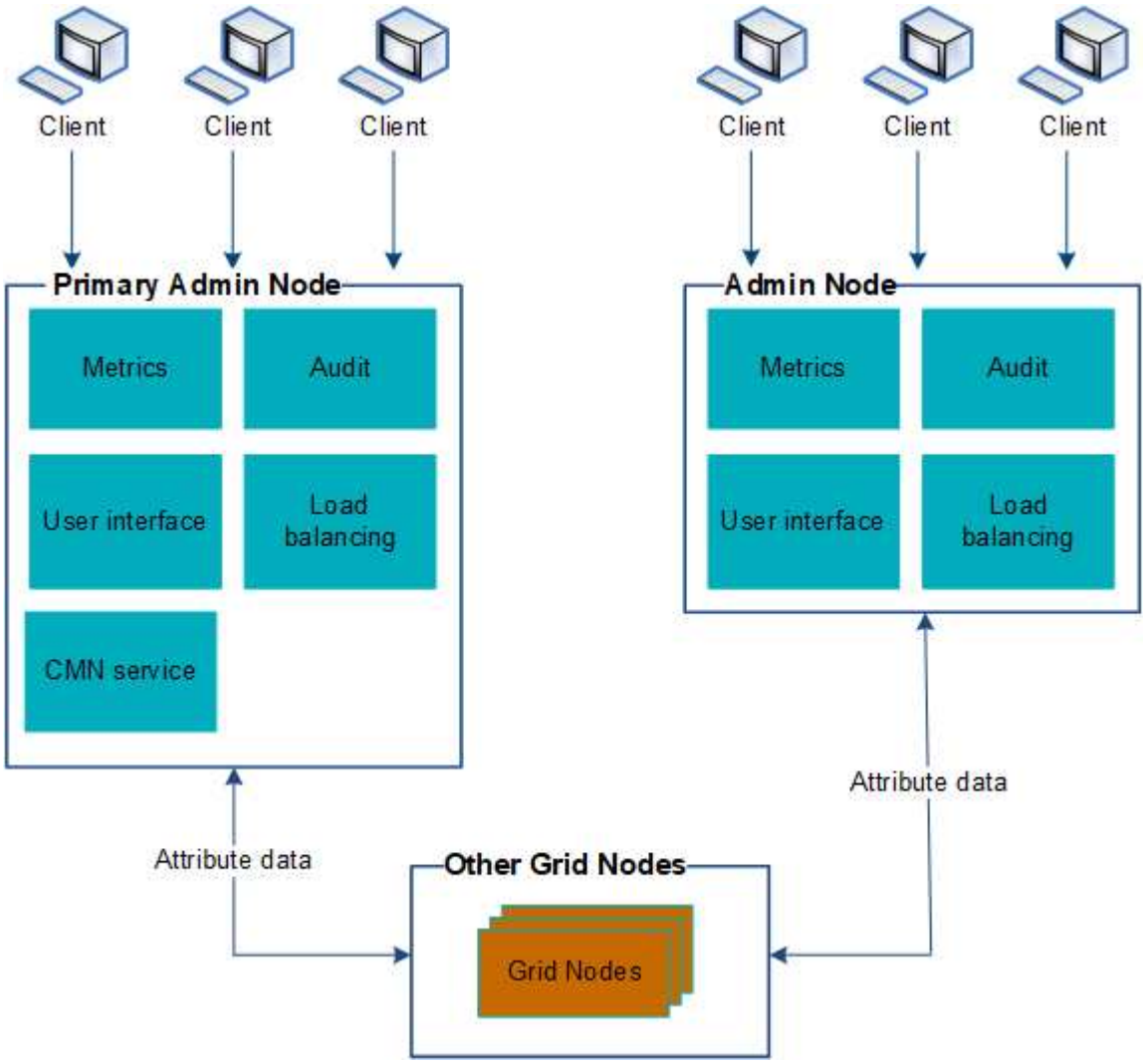
L'ajout de nœuds de stockage permet d'augmenter la capacité de stockage. L'ajout de stockage nécessite de prendre en compte les règles ILM et les exigences de capacité actuellement actives. Voir les instructions pour "Extension d'un système StorageGRID".

Gérer les nœuds d'administration

Utiliser plusieurs nœuds d'administration

Un système StorageGRID peut inclure plusieurs nœuds d'administration pour vous permettre de contrôler et de configurer en continu votre système StorageGRID, même en cas de panne d'un nœud d'administration.

Si un nœud d'administration n'est plus disponible, le traitement des attributs se poursuit, les alertes sont toujours déclenchées et les notifications par e-mail et les packs AutoSupport sont toujours envoyés. Toutefois, le fait d'avoir plusieurs nœuds d'administration n'offre pas de protection de basculement, à l'exception des notifications et des packages AutoSupport.



Deux options s'offrent à vous 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 tout autre nœud d'administration disponible.
- Si un administrateur système a configuré un groupe de nœuds d'administration haute disponibilité, les clients Web peuvent continuer à accéder à Grid Manager ou au Gestionnaire de locataires à l'aide de l'adresse IP virtuelle du groupe HA. Voir "Gérez les groupes haute disponibilité".

> En cas d'utilisation d'un groupe haute disponibilité, l'accès est interrompu en cas de panne du nœud d'administration actif. Les utilisateurs doivent se reconnecter une fois que l'adresse IP virtuelle du groupe HA bascule vers un autre noeud d'administration du groupe.

Certaines tâches de maintenance peuvent uniquement être effectuées à l'aide du nœud d'administration principal. En cas de panne du nœud d'administration principal, celui-ci doit être restauré avant que le système StorageGRID ne fonctionne à nouveau entièrement.

Identifiez le nœud d'administration principal

Le nœud d'administration principal offre davantage de fonctionnalités que les nœuds d'administration non primaires. 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, reportez-vous à la section "Qu'est-ce qu'un nœud d'administration".

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez "autorisations d'accès spécifiques".

Étapes

1. Sélectionnez **NOEUDS**.
2. Entrez **primary** dans la zone de recherche.

   Dans les résultats de la recherche, identifiez le nœud avec le « 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 Network Management System (NMS) sur les nœuds Admin envoie des notifications au serveur de messagerie. Vous pouvez afficher l'état actuel du service NMS ainsi que 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 de notifications par e-mail et sont envoyées au serveur de messagerie l'une après l'autre dans l'ordre dans lequel elles sont déclenchées. En cas de problème (par exemple, une erreur de connexion réseau) et si le serveur de messagerie n'est pas disponible lors de la tentative d'envoi de la notification, 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, elle est supprimée de la file d'attente de notifications et une tentative d'envoi de la notification suivante dans la file d'attente est effectuée.