Administrer StorageGRID

StorageGRID software

NetApp
July 23, 2026

Sommaire

Administrer StorageGRID

Administrer StorageGRID

Utilisez ces instructions pour configurer et administrer un système StorageGRID.

À propos de ces instructions

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

- Utilisez le Gestionnaire de grille pour configurer les groupes et les utilisateurs
- Créez des comptes locataires pour permettre aux applications clientes S3 de stocker et de récupérer des objets
- Configurer et gérer les réseaux StorageGRID
- Configurez AutoSupport
- Gérer les paramètres du nœud

Avant de commencer

- Vous avez une compréhension générale du système StorageGRID.
- Vous possédez des connaissances assez détaillées des interpréteurs de commandes Linux, des réseaux et de la configuration matérielle des serveurs.

Commencez à utiliser Grid Manager

Configuration requise du navigateur Web pour StorageGRID

Vous devez utiliser un navigateur Web compatible.

Navigateur Web	Version minimale prise en charge
Google Chrome	138
Microsoft Edge	138
Mozilla Firefox	140

Définissez la fenêtre du navigateur sur une largeur recommandée.

Largeur du navigateur	Pixels
Minimum	1024
Optimum	1280

Connectez-vous au gestionnaire de grille StorageGRID

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

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

Se connecter au groupe HA

Si des nœuds d'administration sont inclus dans un groupe à haute disponibilité (HA), vous vous connectez à l'aide de l'adresse IP virtuelle du groupe HA ou d'un domaine complet qui pointe vers cette 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 via le nœud d'administration principal, sauf si celui-ci n'est pas disponible. Voir "Gérer les groupes à haute disponibilité".

Utilisez l'authentification unique (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 qui possède au moins une autorisation.
- Vous disposez de l'URL du Grid Manager :

  `https://FQDN_or_Admin_Node_IP/`

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

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

  `https://FQDN_or_Admin_Node_IP:port/`

  > L'authentification unique (SSO) n'est pas disponible sur le port restreint de Grid Manager. Vous devez utiliser le port 443.

Étapes

1. Lancez un navigateur web compatible.
2. Dans la barre d'adresse du navigateur, saisissez l'URL du Grid Manager.
3. Si vous recevez une alerte de sécurité, installez le certificat à l'aide de l'assistant d'installation de votre navigateur. Voir "Gérer les certificats de sécurité".

4. Connectez-vous au Grid Manager.

   L'écran de connexion qui apparaît dépend de la configuration de l'authentification unique (SSO) pour StorageGRID.

   Ne pas utiliser l'authentification unique (SSO)

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

   b. Sélectionnez **Se connecter**.

   Utilisation de l'authentification unique (SSO)

   - Si StorageGRID utilise l'authentification unique (SSO) et que c'est la première fois que vous accédez à l'URL sur ce navigateur :

     i. Sélectionnez **Se connecter**. Vous pouvez laisser le 0 dans le champ Compte.

     ii. Saisissez vos identifiants SSO standard sur la page de connexion SSO de votre organisation.

     Par exemple, si StorageGRID utilise l'authentification unique (SSO) et que vous avez déjà accédé à Grid Manager ou à un compte locataire :

     A. Saisissez **0** (l'identifiant du compte pour le Grid Manager) ou sélectionnez **Grid Manager** s'il apparaît dans la liste des comptes récents.

     B. Sélectionnez **Se connecter**.

     C. Connectez-vous avec vos identifiants SSO habituels sur la page de connexion SSO de votre organisation.

Une fois connecté, la page d'accueil du Grid Manager s'affiche et contient le tableau de bord. Pour savoir quelles informations sont fournies, consultez "Afficher et gérer le tableau de bord".

Connectez-vous à un autre nœud d'administration

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

Ne pas utiliser l'authentification unique (SSO)

Étapes

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

Utilisation de l'authentification unique (SSO)

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

Étapes

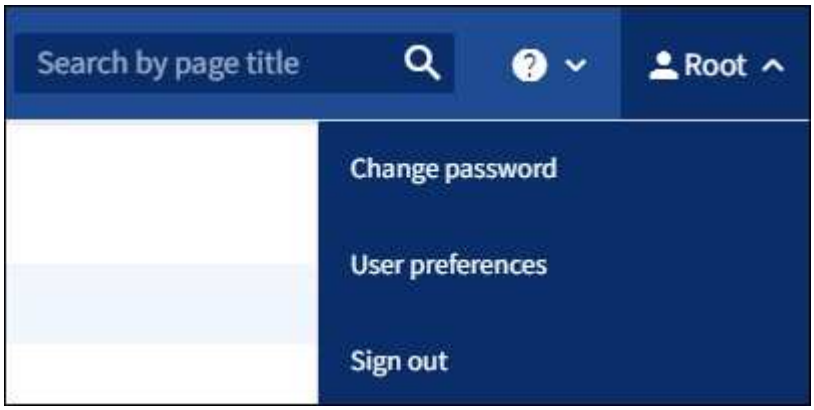
1. Saisissez le nom de domaine complet ou l'adresse IP de l'autre nœud d'administration dans la barre d'adresse du navigateur.
2. Si votre session SSO a expiré, veuillez saisir à nouveau vos identifiants.

Déconnectez-vous du StorageGRID Grid Manager

Une fois votre session d'utilisation de Grid Manager terminée, vous devez vous déconnecter afin d'empêcher tout accès non autorisé au système StorageGRID. La fermeture de votre navigateur ne vous déconnectera pas nécessairement du système, selon les paramètres des cookies de votre navigateur.

Étapes

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



2. Sélectionnez **Se déconnecter**.

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 indiqué par défaut dans le menu déroulant **Recent Accounts**, et le champ **Account ID** affiche 0. **Remarque :** Si l'authentification unique (SSO) est activée et que vous êtes également connecté au Tenant Manager, vous devez également "déconnectez-vous du compte locataire" à "Déconnexion de SSO".

Modifiez votre mot de passe StorageGRID Grid Manager

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".

À propos de cette tâche

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

Étapes

1. Dans l'en-tête du Grid Manager, sélectionnez ***your name*** > **Change password**.
2. Saisissez votre mot de passe actuel.
3. Saisissez un nouveau mot de passe.

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

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

Consultez les informations de licence StorageGRID

Vous pouvez consulter les informations de licence de votre système StorageGRID, telles que la capacité de stockage maximale de votre grille, à tout moment.

Avant de commencer

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

À propos de cette tâche

En cas de problème de licence logicielle pour ce système StorageGRID, la carte « État de santé » du tableau de bord affiche une icône d'état de licence et un lien **Licence**. Le nombre indique le nombre de problèmes liés à la licence.

Étapes

1. Accédez à la page de licence en procédant de l'une des manières suivantes :
   - Sélectionnez **Maintenance** > **Système** > **Licence**.
   - Depuis la carte d'état de santé du tableau de bord, sélectionnez l'icône d'état de la licence ou le lien **License**.

     Ce lien n'apparaît que s'il y a un problème avec la licence.
2. Consultez 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 **Perpetual** ou **Subscription**
   - Capacité de stockage autorisée du grid
   - Capacité de stockage prise en charge
   - Date de fin de licence. **N/A** apparaît pour une licence perpétuelle.
   - Date de fin de support

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

Mettre à jour les informations de licence StorageGRID

Vous devez mettre à jour les informations de licence de votre système StorageGRID chaque fois que les conditions de votre licence changent. Par exemple, vous devez

mettre à jour les informations de licence si vous achetez une capacité de stockage supplémentaire pour votre grid.

Avant de commencer

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

Étapes

1. Sélectionnez **Maintenance** > **Système** > **Licence**.
2. Dans la section Mise à jour de 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 de provisionnement.
5. Sélectionnez **Enregistrer**.

Utilisez la ligne de commandes (API)

Utilisez l'API de gestion de grille StorageGRID

Vous pouvez effectuer des tâches de gestion système à l'aide de l'API REST de Grid Management plutôt qu'en utilisant l'interface utilisateur de Grid Manager. Par exemple, vous pourriez vouloir utiliser l'API pour automatiser des opérations ou pour créer plusieurs entités, telles que des utilisateurs, plus rapidement.

Ressources de haut niveau

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

- `/grid` : L'accès est réservé aux utilisateurs de Grid Manager et dépend des autorisations de groupe configurées.
- `/org` : L'accès est limité aux utilisateurs appartenant à un groupe LDAP local ou fédéré pour un compte locataire. Pour plus de détails, consultez "Utilisez un compte locataire".
- `/private` : L'accès est réservé aux utilisateurs de Grid Manager et dépend des autorisations de groupe configurées. Les API privées sont susceptibles d'être modifiées sans préavis. Les points de terminaison privés de StorageGRID ignorent également la version de l'API de la requête.

Émettre des requêtes API

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

L'interface utilisateur Swagger fournit des informations et une documentation complètes pour chaque opération API.

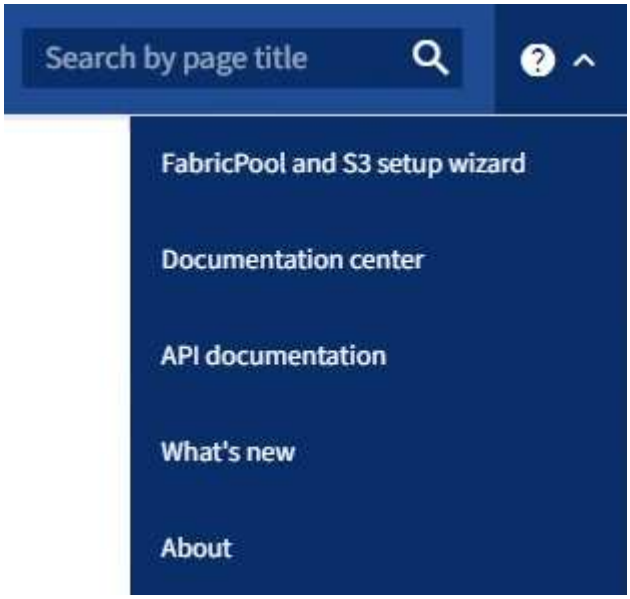
Avant de commencer

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

> Toute opération API effectuée via la page de documentation API est une opération en direct. Veillez à ne pas créer, modifier ou supprimer par erreur des données de configuration ou autres.

Étapes

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



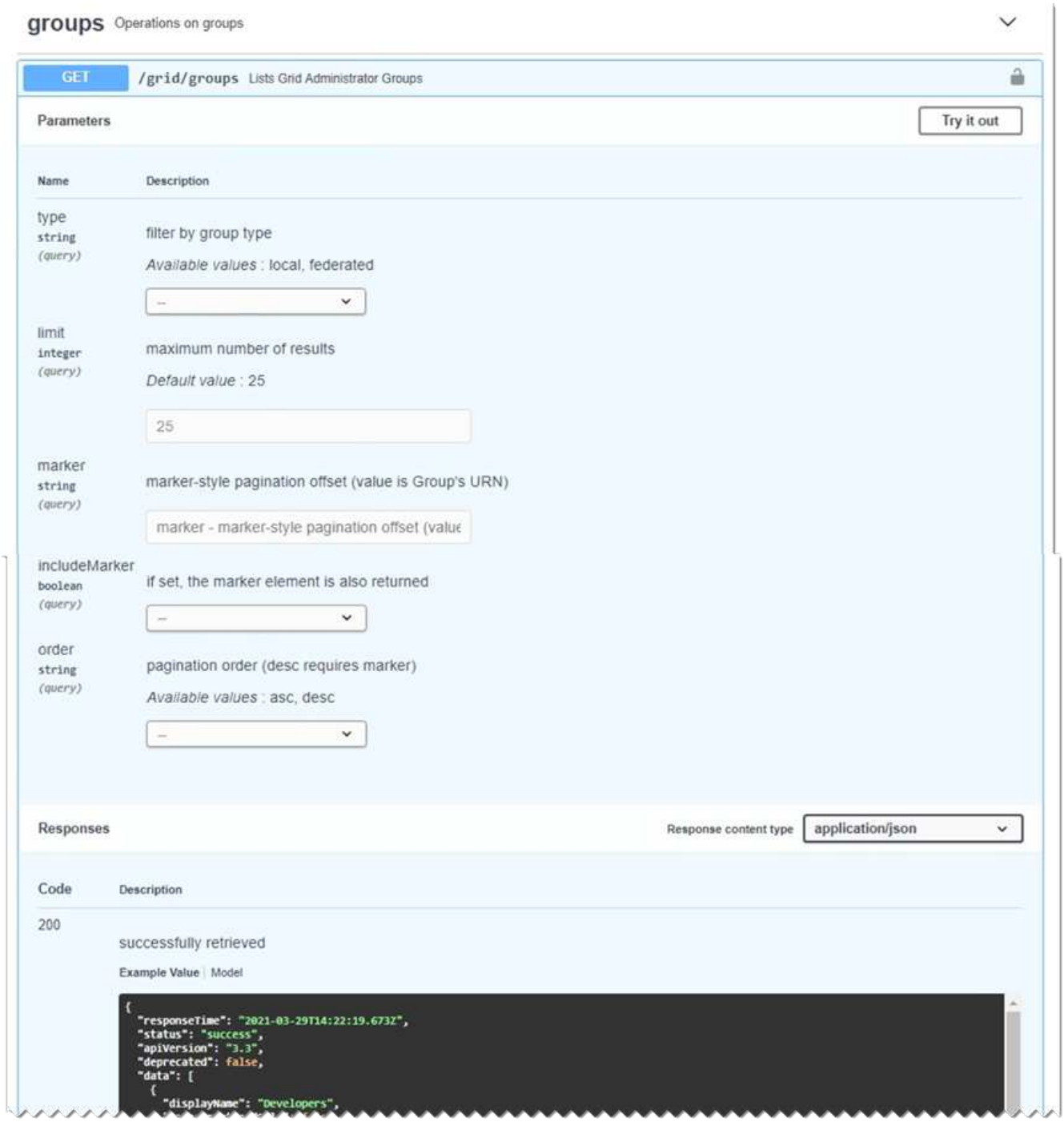
2. Pour effectuer une opération avec l'API privée, sélectionnez **Accéder à la documentation de l'API privée** sur la page de l'API de gestion StorageGRID.

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

3. Sélectionnez l'opération souhaitée.

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

4. Sélectionnez une action HTTP pour afficher les détails de la requête, notamment l'URL du point de terminaison, la liste des paramètres obligatoires ou facultatifs, un exemple du corps de la requête (le cas échéant) et les réponses possibles.



5. Déterminez si la requête nécessite des paramètres supplémentaires, tels qu'un identifiant de groupe ou d'utilisateur. Ensuite, obtenez ces valeurs. Vous devrez peut-être d'abord effectuer une autre requête API pour obtenir les informations dont vous avez besoin.
6. Déterminez si vous devez modifier le corps de la requête d'exemple. Le cas échéant, vous pouvez sélectionner **Modèle** pour connaître les exigences relatives à chaque champ.
7. Sélectionnez **Try it out**.
8. Fournissez les paramètres requis ou modifiez le corps de la requête selon les besoins.
9. Sélectionnez **Exécuter**.
10. Examinez le code de réponse pour déterminer si la requête a réussi.

Opérations de l'API de gestion de la grille dans StorageGRID

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

Cette liste ne comprend que les opérations disponibles dans l'API publique.

- **comptes** : Opérations permettant de gérer les comptes locataires de stockage, y compris la création de nouveaux comptes et la récupération de l'utilisation du stockage pour un compte donné.
- **historique des alertes** : opérations sur les alertes résolues.
- **récepteurs d'alertes** : Opérations sur les récepteurs de notifications d'alerte (courriel).
- **règles d'alerte** : Opérations sur les règles d'alerte.
- **silences d'alerte** : opérations sur les silences d'alerte.
- **Alertes** : Opérations sur les alertes.
- **audit** : Opérations permettant de lister et de mettre à jour la configuration d'audit.
- **auth** : Opérations permettant d'authentifier la session utilisateur.

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

  Si l'authentification unique est activée pour le système StorageGRID, vous devez suivre une procédure différente. Consultez la section « Authentification à l'API si l'authentification unique est activée ».

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

- **client-certificates** : Opérations permettant de configurer les certificats clients afin que StorageGRID puisse être accessible en toute sécurité à l'aide d'outils de surveillance externes.
- **config** : Opérations relatives à la version du produit et aux versions de l'API de gestion de grille. Vous pouvez afficher la version de la publication du produit et les versions majeures de l'API de gestion de grille prises en charge par cette publication, et vous pouvez désactiver les versions obsolètes de l'API.
- **Fonctionnalités désactivées** : Opérations permettant d'afficher les fonctionnalités qui pourraient avoir été désactivées.
- **serveurs DNS** : Opérations permettant de lister et de modifier les serveurs DNS externes configurés.
- **drive-details** : Opérations sur les disques pour des modèles spécifiques d'appliances de stockage.
- **endpoint-domain-names** : Opérations permettant de lister et de modifier les noms de domaine des endpoints S3.
- **codage d'effacement** : opérations sur les profils de codage d'effacement.
- **expansion** : opérations sur l'expansion (niveau procédure).
- **expansion-nodes** : Opérations sur l'expansion (niveau du nœud).
- **sites d'expansion** : Opérations sur l'expansion (au niveau du site).
- **grid-networks** : Opérations permettant de lister et de modifier la liste du Grid Network.

- **grid-passwords** : 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 une source d'identité externe et de synchroniser manuellement les informations de groupe et d'utilisateur fédérés.
- **ilm** : Opérations sur la gestion du cycle de vie de l'information (ILM).
- **in-progress-procedures** : Récupère les procédures de maintenance en cours.
- **licence** : Opérations permettant de récupérer et de mettre à jour la licence StorageGRID.
- **journaux** : Opérations de collecte et de téléchargement des fichiers journaux.v
- **Métriques** : Opérations sur les métriques StorageGRID, notamment les requêtes de métriques instantanées à un instant précis et les requêtes de métriques sur une plage de temps. L'API de gestion du réseau utilise l'outil de surveillance système Prometheus comme source de données principale. Pour plus d'informations sur la construction de requêtes Prometheus, consultez le site web de Prometheus.

> Les indicateurs dont le nom contient *`private`* sont destinés à un usage interne uniquement. Ces indicateurs sont susceptibles d'être modifiés entre les versions de StorageGRID sans préavis.

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

Gestion des versions de l'API Grid Management dans StorageGRID

L'API de gestion de grille utilise le versionnage pour permettre des mises à niveau sans interruption de service.

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

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

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

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

Type de modification de l'API	Ancienne version	Nouvelle version
Compatible avec les versions antérieures	2,1	2,2
Non compatible avec les versions antérieures	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 avoir accès à l'ancienne version de l'API pendant au moins une version de StorageGRID.

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

Les requêtes obsolètes sont marquées comme dépréciées de la manière suivante :

- L'en-tête de réponse est « Deprecated: true »
- Le corps de la réponse JSON inclut "deprecated": true
- Un avertissement de dépréciation est ajouté au fichier nms.log. Par exemple :

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

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

Utilisez la `GET /versions` requête API pour obtenir une liste des versions majeures de l'API prises en charge. Cette requête 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 d'API pour une requête

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

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

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

Protégez-vous contre les attaques Cross-Site Request Forgery (CSRF) dans StorageGRID

Vous pouvez contribuer à protéger StorageGRID contre les attaques de type Cross-Site Request Forgery (CSRF) en utilisant des jetons CSRF pour renforcer l'authentification qui utilise des cookies. Le Grid Manager et le Tenant Manager activent automatiquement cette fonctionnalité de sécurité ; les autres clients API peuvent choisir de l'activer ou non lors de leur connexion.

Un attaquant capable de déclencher une requête vers un autre site (par exemple avec un formulaire HTTP POST) peut faire en sorte que certaines requêtes soient effectuées en utilisant les cookies de l'utilisateur connecté.

StorageGRID contribue à la protection contre les attaques CSRF grâce à l'utilisation de jetons CSRF. Lorsqu'elle est activée, le contenu d'un cookie spécifique doit correspondre à celui d'un en-tête spécifique ou d'un paramètre spécifique du corps de la requête POST.

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

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

Lorsque cette option est activée, un `GridCsrfToken` cookie est défini avec une valeur aléatoire pour les connexions au Grid Manager, et le `AccountCsrfToken` cookie est défini avec une valeur aléatoire pour les connexions au Tenant Manager.

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

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

Consultez la documentation API en ligne pour obtenir des exemples et des détails supplémentaires.

> Les requêtes comportant un cookie de jeton CSRF défini appliqueront également l'en-tête "Content-Type: application/json" à toute requête attendant un corps de requête JSON, comme protection supplémentaire contre les attaques CSRF.

Utilisez l'API si l'authentification unique est activée

Utilisez l'API StorageGRID 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 la 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 qui appartient à un groupe d'utilisateurs StorageGRID.
- Pour accéder à l'API de gestion des locataires, vous devez connaître l'identifiant du compte locataire.

À propos de cette tâche

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

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

- Un exemple de workflow de requêtes curl.

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

  > Le flux de travail curl présenté en exemple ne protège pas le mot de passe contre la consultation par d'autres utilisateurs.

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

Étapes

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

   Lorsque vous y êtes invité, saisissez les valeurs des arguments suivants :
   - La méthode SSO. Saisissez ADFS ou adfs.
   - Nom d'utilisateur SSO
   - Le domaine sur lequel StorageGRID est installé
   - L'adresse de StorageGRID
   - L'identifiant du compte locataire, si vous souhaitez accéder à l'API de gestion des locataires.

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

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

   Le jeton d'autorisation StorageGRID est fourni dans le résultat. Vous pouvez désormais utiliser le jeton pour d'autres requêtes, comme vous le feriez avec l'API si l'authentification unique n'était pas utilisée.
3. Si vous souhaitez utiliser des requêtes curl, suivez la procédure suivante.
   a. Déclarez les variables nécessaires à la connexion.

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

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

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

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

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

La réponse pour cet exemple inclut une URL signée et encodée en URL, mais elle n'inclut pas la couche d'encodage JSON supplémentaire.

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

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

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

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

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

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

La réponse inclut l'identifiant de la requête du client :

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

e. Enregistrez l'identifiant de la requête client à partir de la réponse.

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

f. Envoyez vos identifiants à l'action du formulaire de la réponse précédente.

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

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

> Si l'authentification multifactorielle (MFA) est activée pour votre système SSO, le formulaire envoyé 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 issu de la réponse.

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

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

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

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

```
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. Enregistrez le `SAMLResponse` du champ caché :

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

j. À l'aide des données enregistrées `SAMLResponse`, effectuez une demande StorageGRID`/api/saml-response` pour générer un jeton d'authentification StorageGRID.

Pour `RelayState`, utilisez l'ID du compte locataire ou 0 si vous souhaitez vous connecter à l'API de gestion de la 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 en tant que `MYTOKEN`.

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

Vous pouvez désormais utiliser `MYTOKEN` pour d'autres requêtes, de la même manière que vous utiliseriez l'API si l'authentification unique n'était pas utilisée.

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

Si l'authentification unique (SSO) est activée, vous devez effectuer une série de requêtes API pour vous déconnecter de l'API de gestion de la grille ou de l'API de gestion des locataires. Ces instructions s'appliquent si vous utilisez Active Directory comme fournisseur d'identité SSO.

À propos de cette tâche

Si nécessaire, vous pouvez vous déconnecter de l'API StorageGRID depuis la page de déconnexion unique de votre organisation. Ou, vous pouvez déclencher une déconnexion unique (SLO) depuis StorageGRID, ce qui requiert un jeton d'authentification StorageGRID valide.

Étapes

1. Pour générer une requête de déconnexion signée, transmettez le `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 requête à l'URL de déconnexion pour déclencher le SLO et pour être redirigé vers StorageGRID.

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

La réponse 302 est renvoyée. L'emplacement de redirection n'est pas applicable à la déconnexion via l'API uniquement.

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

4. Supprimez le jeton porteur StorageGRID.

La suppression du jeton d'accès StorageGRID fonctionne de la même manière qu'en l'absence d'authentification unique (SSO). Si le cookie « sso=true » n'est pas fourni, l'utilisateur est déconnecté de StorageGRID sans affecter l'état de l'authentification unique.

```
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
```

Utilisez l'API StorageGRID si l'authentification unique est activée (Entra ID)

Si vous avez "authentification unique (SSO) configurée et activée" et que vous utilisez Entra ID comme fournisseur SSO, vous pouvez utiliser deux exemples de scripts 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 Entra ID est activée

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

Avant de commencer

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

À propos de cette tâche

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

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

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

Pour créer votre propre intégration API avec Entra ID, consultez le script `storagegrid-ssoauth-azure.py`. Le script Python effectue deux requêtes directement à StorageGRID (la première pour obtenir la SAMLRequest, et la seconde pour obtenir le jeton d'autorisation), et appelle également le script Node.js pour interagir avec Entra ID afin d'effectuer les opérations SSO.

Les opérations d'authentification unique (SSO) peuvent être exécutées via une série de requêtes API, mais leur mise en œuvre n'est pas simple. Le module Puppeteer Node.js est utilisé pour extraire les données de l'interface SSO Entra ID.

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

Étapes

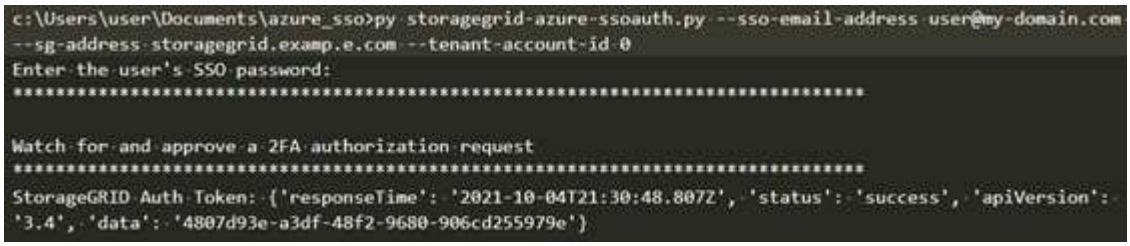
1. Installez les dépendances requises, comme suit :
   a. Installez Node.js (voir "https://nodejs.org/en/download/").
   b. Installez les modules Node.js requis (puppeteer et jsdom) :

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

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

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

3. Lorsque vous y êtes invité, saisissez les valeurs des arguments suivants (ou transmettez-les en tant que paramètres) :
   - L'adresse e-mail SSO utilisée pour vous connecter à Entra ID
   - L'adresse de StorageGRID
   - L'identifiant du compte locataire, si vous souhaitez accéder à l'API de gestion des locataires
4. Lorsque vous y serez invité, saisissez votre mot de passe et soyez prêt à fournir une autorisation MFA à Entra ID si cela vous est demandé.



> Ce script suppose que l'authentification multifacteur (MFA) est effectuée via Microsoft Authenticator. Il se peut que vous deviez modifier le script pour prendre en charge d'autres formes de MFA (comme la saisie d'un code reçu par message texte).

Le jeton d'autorisation StorageGRID est fourni dans le résultat. Vous pouvez désormais utiliser le jeton pour d'autres requêtes, comme vous le feriez avec l'API si l'authentification unique n'était pas utilisée.

Utilisez l'API StorageGRID 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 la 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 PingFederate comme fournisseur d'identité SSO

Avant de commencer

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

À propos de cette tâche

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

- Le `storagegrid-ssoauth.py` script Python, qui se trouve dans le répertoire des fichiers d'installation de StorageGRID (`./rpms` pour RHEL, `./debs` pour Ubuntu ou Debian, et `./vsphere` pour VMware).
- Un exemple de workflow de requêtes curl.

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

  > Le flux de travail curl présenté en exemple ne protège pas le mot de passe contre la consultation par d'autres utilisateurs.

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

Étapes

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

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

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

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

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

   Le jeton d'autorisation StorageGRID est fourni dans le résultat. Vous pouvez désormais utiliser le jeton pour d'autres requêtes, comme vous le feriez avec l'API si l'authentification unique n'était pas utilisée.

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

   a. Déclarez les variables nécessaires à la connexion.

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

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

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

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

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

   La réponse pour cet exemple inclut une URL signée et encodée en URL, mais elle n'inclut pas la couche d'encodage JSON supplémentaire.

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

   c. Enregistrez le `SAMLRequest` 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, puis affichez la réponse :

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

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

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

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

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

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

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

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

g. Exportez la valeur « action » :

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

h. Envoyez les cookies avec les identifiants :

```
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. Enregistrez le `SAMLResponse` du champ caché :

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

j. À l'aide des données enregistrées `SAMLResponse`, effectuez une demande StorageGRID`/api/saml-response` pour générer un jeton d'authentification StorageGRID.

   Pour `RelayState`, utilisez l'ID du compte locataire ou 0 si vous souhaitez vous connecter à l'API de gestion de la 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 en tant que `MYTOKEN`.

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

Vous pouvez désormais utiliser `MYTOKEN` pour d'autres requêtes, de la même manière que vous utiliseriez l'API si l'authentification unique n'était pas utilisée.

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

Si l'authentification unique (SSO) est activée, vous devez effectuer une série de requêtes API pour vous déconnecter de l'API de gestion de la grille ou de l'API de gestion des locataires. Ces instructions s'appliquent si vous utilisez PingFederate comme fournisseur d'identité SSO

À propos de cette tâche

Si nécessaire, vous pouvez vous déconnecter de l'API StorageGRID depuis la page de déconnexion unique de votre organisation. Ou, vous pouvez déclencher une déconnexion unique (SLO) depuis StorageGRID, ce qui requiert un jeton d'authentification StorageGRID valide.

Étapes

1. Pour générer une requête de déconnexion signée, transmettez le `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 requête à l'URL de déconnexion pour déclencher le SLO et pour être redirigé vers StorageGRID.

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

La réponse 302 est renvoyée. L'emplacement de redirection n'est pas applicable à la déconnexion via l'API uniquement.

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

4. Supprimez le jeton porteur StorageGRID.

La suppression du jeton d'accès StorageGRID fonctionne de la même manière qu'en l'absence d'authentification unique (SSO). Si le cookie « sso=true » n'est pas fourni, l'utilisateur est déconnecté de StorageGRID sans affecter l'état de l'authentification unique.

```
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 fonctionnalités de StorageGRID avec l'API

Vous pouvez utiliser l'API de gestion de la grille pour désactiver complètement certaines fonctionnalités dans le système StorageGRID. Lorsqu'une fonctionnalité est désactivée, personne ne peut se voir attribuer d'autorisations pour effectuer les tâches liées à cette fonctionnalité.

À propos de cette tâche

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

Pour comprendre en quoi cette fonctionnalité peut être utile, considérez le scénario suivant :

La société A est un fournisseur de services qui loue la capacité de stockage de son système StorageGRID en créant des comptes clients. Afin de protéger la sécurité des objets de ses locataires, la société A souhaite s'assurer que ses propres employés ne puissent jamais accéder à un compte client après son déploiement._

Company A peut atteindre cet objectif en utilisant le système Deactivate Features dans l'API Grid Management. En désactivant complètement la fonctionnalité **Change tenant root password** dans le Grid Manager (à la fois dans l'interface utilisateur et dans l'API), Company A s'assure que les utilisateurs Admin — y compris l'utilisateur root et les utilisateurs appartenant à des groupes disposant de l'autorisation **Root access** — ne peuvent pas modifier le mot de passe de l'utilisateur root de n'importe quel compte locataire._

Étapes

1. Accédez à la documentation Swagger de l'API de gestion de grille. Voir "Utilisez l'API de gestion de grille".
2. Localisez le point de terminaison Deactivate Features.
3. Pour désactiver une fonctionnalité, telle que Change tenant root password, envoyez un corps à l'API comme ceci :

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

   Lorsque la demande est terminée, la fonctionnalité Modifier le mot de passe root 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 requête API qui tente de modifier le mot de passe root d'un locataire échouera avec "403 Forbidden."

Réactiver les fonctionnalités désactivées

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

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

Étapes

1. Accédez à la documentation Swagger de l'API Grid Management.

2. Localisez le point de terminaison Deactivate Features.
3. Pour réactiver toutes les fonctionnalités, envoyez un corps de requête à l'API comme ceci :

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

Une fois cette requête terminée, toutes les fonctionnalités, y compris la fonctionnalité Changer le mot de passe racine du locataire, sont réactivées. L'autorisation de gestion **Changer le mot de passe racine du locataire** apparaît désormais dans l'interface utilisateur, et toute requête API visant à modifier le mot de passe racine d'un locataire aboutira, à condition que l'utilisateur dispose de l'autorisation de gestion **Accès racine** ou **Changer le mot de passe racine du locataire**.

L'exemple précédent réactive *toutes* les fonctionnalités désactivées. Si d'autres fonctionnalités ont été désactivées et doivent le rester, vous devez les spécifier explicitement dans la requête PUT. Par exemple, pour réactiver la fonctionnalité « Modifier le mot de passe racine du locataire » tout en continuant de désactiver l'autorisation de gestion storageAdmin, envoyez la requête PUT suivante :

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

Contrôlez l'accès à StorageGRID

Contrôlez l'accès à StorageGRID

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

Contrôler l'accès au Grid Manager

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

L'utilisation de "fédération d'identité" permet de configurer "groupes" et "utilisateurs" plus rapidement, et elle permet aux utilisateurs de se connecter à StorageGRID avec leurs identifiants habituels. Vous pouvez configurer la fédération d'identité si vous utilisez Active Directory, OpenLDAP ou Oracle Directory Server.

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

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

Vous pouvez éventuellement configurer un groupe en lecture seule. Les utilisateurs d'un groupe en lecture seule peuvent uniquement consulter les paramètres et les fonctionnalités. Ils ne peuvent effectuer aucune modification ni aucune opération dans Grid Manager ou Grid Management API.

Activer l'authentification unique

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

Modifier la phrase secrète de provisionnement

La phrase secrète de provisionnement est requise pour de nombreuses procédures d'installation et de maintenance, ainsi que pour télécharger le package de récupération StorageGRID. La phrase secrète est également requise pour télécharger les sauvegardes des informations de topologie du grid et les clés de chiffrement du système StorageGRID. Vous pouvez l'"modifier la phrase de passe"utiliser selon vos besoins.

Modifier les mots de passe de la console du nœud

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

Modifier la phrase secrète de provisionnement StorageGRID

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

Avant de commencer

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

À propos de cette tâche

La phrase de passe de configuration est requise pour de nombreuses procédures d'installation et de maintenance, et pour "téléchargement du package de récupération". La phrase de passe de configuration n'est pas indiquée dans le fichier `Passwords.txt`. Assurez-vous de documenter la phrase de passe de configuration et de la conserver en lieu sûr et sécurisé.

Étapes

1. Sélectionnez **Configuration** > **Contrôle d'accès** > **Mots de passe de la grille**.
2. Sous **Modifier la phrase secrète de provisionnement**, sélectionnez **Effectuer une modification**
3. Saisissez votre phrase secrète de provisionnement actuelle.
4. Saisissez la nouvelle phrase secrète. La phrase secrète doit contenir au moins 8 caractères et pas plus de 32 caractères. Les phrases secrètes sont sensibles à la casse.

Conservez la phrase secrète de configuration dans un endroit sûr. Elle est requise pour l'installation, l'extension et la maintenance.

5. Saisissez à nouveau la nouvelle phrase secrète, puis sélectionnez **Enregistrer**.

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

6. Sélectionnez **Recovery Package**.
7. Saisissez la nouvelle phrase secrète de provisionnement pour télécharger le nouveau package de récupération.

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

Modifier les mots de passe des consoles de nœud dans StorageGRID

Chaque nœud de votre grille possède un mot de passe de console, que vous utilisez pour vous connecter au nœud. Par défaut, chaque nœud possède un mot de passe unique. Vous pouvez modifier chaque mot de passe pour un nouveau mot de passe unique, ou vous pouvez modifier le mot de passe de chaque nœud afin d'utiliser un mot de passe global. Les mots de passe sont stockés dans le package de récupération.

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 à la maintenance ou à la racine".
- Vous disposez de la phrase secrète de provisionnement actuelle.

À propos de cette tâche

Vous utilisez un mot de passe de console de nœud pour vous connecter à un nœud en tant qu'« admin » via SSH, ou en tant qu'utilisateur root sur une connexion console VM/physique. Vous pouvez modifier les mots de passe de console de nœud à l'aide de l'une des options suivantes :

- Appliquer automatiquement des mots de passe aléatoires à chaque nœud
- Spécifiez et appliquez un mot de passe global à tous les nœuds
- Spécifiez et appliquez un mot de passe unique à un ou plusieurs nœuds

Les mots de passe sont stockés dans un fichier `Passwords.txt` mis à jour du package de récupération. Les mots de passe figurent dans la colonne « Mot de passe » de ce fichier.

Le "mots de passe d'accès SSH" des clés SSH utilisées pour la communication entre les nœuds est distinct des mots de passe de la console des nœuds. Cette procédure ne modifie pas les mots de passe d'accès SSH.

Accédez à l'assistant

Étapes

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

Télécharger le package de récupération actuel

Avant de modifier les mots de passe des consoles de nœuds, téléchargez le package de récupération actuel. Vous pouvez utiliser les mots de passe dans ce fichier si le processus de modification du mot de passe échoue pour un nœud.

Étapes

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

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

4. Sélectionnez **Continue**.

Fournissez de nouveaux mots de passe

1. Sélectionnez la méthode de changement de mot de passe que vous souhaitez utiliser.
   - **Automatique** : StorageGRID attribue automatiquement un nouveau mot de passe de console aléatoire à tous les nœuds.
   - **Personnalisé** : Vous fournissez les mots de passe de la console.

Automatique

1. Sélectionnez **Continue**.

Personnalisé

1. Sélectionnez l'une des options suivantes :
   - **Mot de passe global de la console** : appliquez le même mot de passe de console à tous les nœuds.
   - **Mots de passe uniques pour la console** : appliquez un mot de passe différent sur un ou plusieurs nœuds.
2. Si vous avez sélectionné **Global console password**, saisissez le mot de passe que vous souhaitez utiliser pour tous les nœuds.
3. Si vous avez sélectionné **Mots de passe de console uniques**, saisissez un mot de passe unique pour un ou plusieurs nœuds.
4. Sélectionnez **Continue**.

Finalisez la modification du mot de passe

1. Lorsque la boîte de dialogue de confirmation apparaît, sélectionnez **Oui** si vous êtes prêt à ce que StorageGRID commence à modifier les mots de passe de la console du nœud.

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

   StorageGRID génère un nouveau package de récupération contenant le nouveau mot de passe.

2. Lorsque le nouveau package de récupération est prêt, sélectionnez **Télécharger le nouveau package de récupération** et enregistrez le package de récupération.
3. Ouvrez le `.zip` fichier.
4. Confirmez que vous pouvez accéder au contenu, y compris au fichier `Passwords.txt` qui contient les nouveaux mots de passe de la console du nœud.
5. Copiez le nouveau fichier du package de récupération (`.zip` vers deux emplacements sûrs, sécurisés et distincts.

   Ne remplacez pas l'ancien package de récupération.

   Vous devez sécuriser le fichier de récupération, car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données du système StorageGRID.

6. Cochez la case pour indiquer que vous avez téléchargé le nouveau package de récupération et vérifié le contenu.
7. Sélectionnez **Continue**.

   StorageGRID met à jour le mot de passe de chaque nœud.

   En cas d'erreur lors du processus de mise à jour, la barre de progression indique le nombre de nœuds dont le mot de passe n'a pas pu être modifié. Le système réessaiera automatiquement le processus sur tout nœud dont le mot de passe n'a pas pu être modifié. Si le processus se termine avec certains nœuds dont le mot de passe n'a toujours pas été modifié, le bouton **Retry** apparaît.

8. Si la mise à jour du mot de passe a échoué pour un ou plusieurs nœuds :
   a. Veuillez consulter les messages d'erreur répertoriés dans le tableau.
   b. Résolvez les problèmes.
   c. Sélectionnez **Réessayer**.

   La nouvelle tentative ne modifie les mots de passe de la console des nœuds que sur les nœuds ayant échoué lors des précédentes tentatives de changement de mot de passe.

9. Lorsque la barre de progression indique qu'il ne reste plus de mises à jour, sélectionnez **Terminer**.
10. Une fois les mots de passe des consoles de nœuds modifiés pour tous les nœuds, supprimez le premier package de récupération que vous avez téléchargé.

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

La modification des mots de passe d'accès SSH des nœuds d'administration met

également à jour les ensembles uniques de clés SSH internes de chaque nœud du grid. 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 `admin` ou à l'utilisateur root sur une VM ou une connexion 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 "Autorisation d'accès à la maintenance ou à la racine".
- Vous disposez de la phrase secrète de provisionnement actuelle.

À propos de cette tâche

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

Les clés SSH utilisées pour la communication entre les nœuds possèdent des mots de passe d'accès SSH distincts. Cette procédure ne les modifie pas.

Accédez à l'assistant

Étapes

1. Sélectionnez **Configuration** > **Contrôle d'accès** > **Mots de passe de la grille**.
2. Sous **Changer les clés SSH**, sélectionnez **Apporter une modification**.

Télécharger le package de récupération actuel

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

Étapes

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

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

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

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

Modifier les clés d'accès SSH

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

Étapes

1. Veuillez patienter pendant la génération du nouveau package de récupération, ce qui peut prendre quelques minutes.
2. Lorsque le bouton Télécharger le nouveau package de récupération est activé, sélectionnez **Télécharger le nouveau package de récupération** et enregistrez le nouveau fichier de package de récupération (`.zip` dans deux emplacements sûrs, sécurisés et distincts.
3. Une fois le téléchargement terminé :

   a. Ouvrez le `.zip` fichier.

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

   c. Copiez le nouveau fichier du package de récupération (`.zip` vers deux emplacements sûrs, sécurisés et distincts.

   > ⚠ Ne remplacez pas l'ancien package de récupération.

   Le fichier du package de récupération doit être sécurisé, car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données 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 verte de succès apparaît.

   En cas d'erreur lors de la mise à jour, un message d'avertissement indique le nombre de nœuds dont la clé n'a pas pu être modifiée. Le système réessaiera automatiquement la procédure sur tout nœud dont la clé n'a pas pu être modifiée. Si la procédure se termine avec certains nœuds n'ayant toujours pas de clé modifiée, le bouton **Retry** s'affiche.

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

   a. Veuillez consulter les messages d'erreur répertoriés dans le tableau.

   b. Résolvez les problèmes.

   c. Sélectionnez **Réessayer**.

      La nouvelle tentative ne modifie que les clés d'accès SSH sur les nœuds qui ont échoué lors des précédentes tentatives 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. Vous pouvez également sélectionner **Maintenance** > **System** > **Recovery package** pour télécharger une copie supplémentaire du nouveau recovery package.

Utilisez la fédération d'identité dans StorageGRID

L'utilisation de la fédération d'identités accélère la configuration des groupes et des

utilisateurs et permet aux utilisateurs de se connecter à StorageGRID à l'aide d'identifiants familiers.

Configurer la fédération d'identités pour Grid Manager

Vous pouvez configurer la fédération d'identités dans Grid Manager si vous souhaitez que les groupes d'administrateurs et les utilisateurs soient gérés dans un autre système tel que Active Directory, Microsoft Entra ID, 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, Microsoft Entra ID, OpenLDAP ou Oracle Directory Server comme fournisseur d'identité.

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

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

À propos de cette tâche

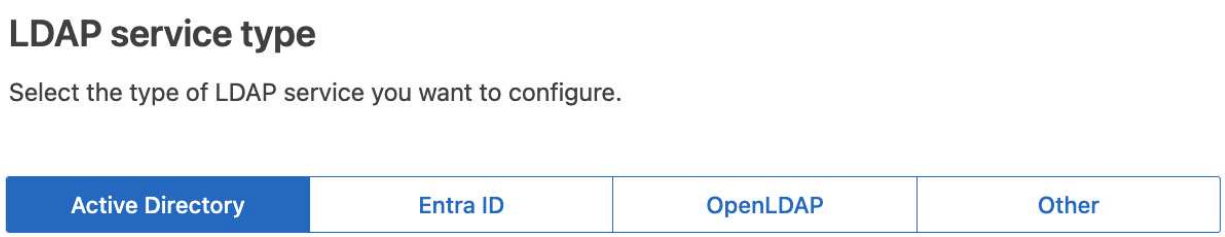
Vous pouvez configurer une source d'identité pour Grid Manager si vous souhaitez importer des groupes depuis un autre système tel qu'Active Directory, Microsoft Entra ID, OpenLDAP ou Oracle Directory Server. Vous pouvez importer les types de groupes suivants :

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

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

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

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

     Pour Active Directory, vous pouvez également spécifier le nom d'ouverture de session de niveau inférieur ou le User Principal Name.

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

     - `sAMAccountName` ou `uid`

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

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

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

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

> Les valeurs du **nom unique du groupe** doivent être uniques au sein du **DN de base du groupe** auquel elles appartiennent.

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

> Les valeurs du **nom unique de l'utilisateur** doivent être uniques au sein du **DN de base utilisateur** auquel elles appartiennent.

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

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

Saisissez l'un de ces modèles :

- **UserPrincipalName modèle (AD et Entra ID)**: `[USERNAME]@*example*.com`
- **Modèle de nom d'ouverture de session de niveau inférieur (AD et Entra ID)** : `*example*\[USERNAME]`
- **Modèle de nom unique** : `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

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

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

sécurisé. Cette option n'est pas prise en charge pour Microsoft Entra ID.

> L'option « Ne pas utiliser TLS » n'est pas prise en charge si votre serveur Active Directory impose la signature LDAP. Vous devez utiliser STARTTLS ou LDAPS.

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

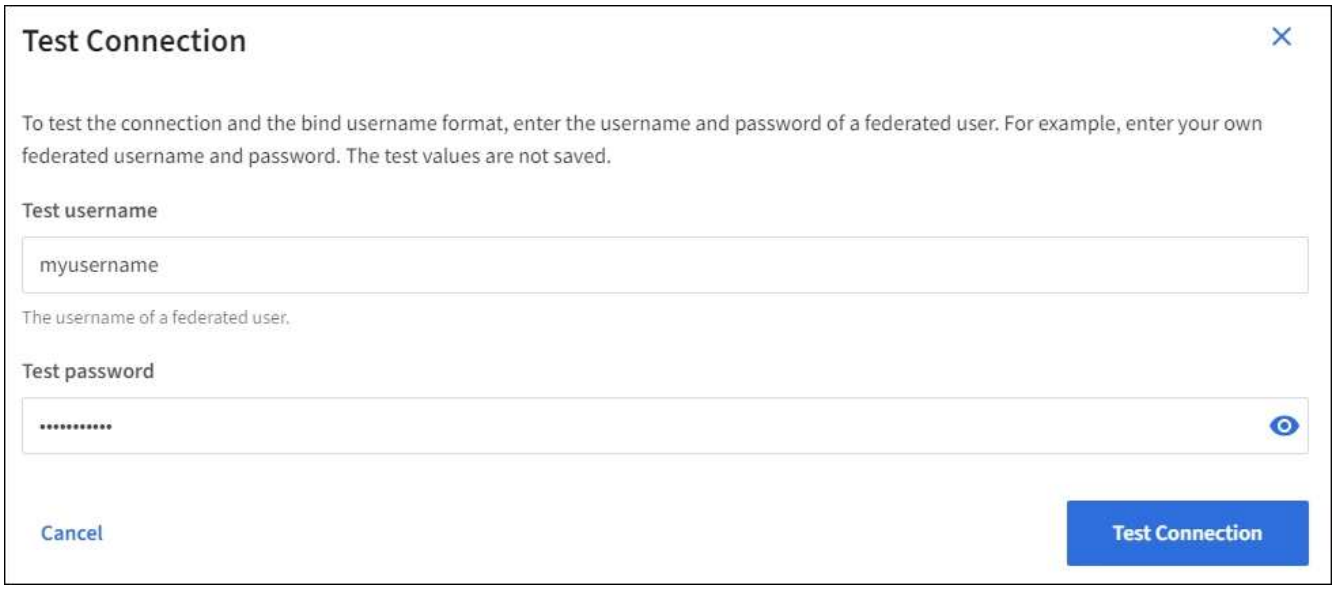
Testez la connexion et enregistrez la configuration

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

Étapes

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

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



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

Forcer la synchronisation avec la source d'identité

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

Étapes

1. Accédez à la page de fédération d'identités.
2. Sélectionnez **Sync server** en haut de la page.

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

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

Désactivez la fédération d'identités

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

À propos de cette tâche

Avant de désactiver la fédération d'identités, vous devez prendre en compte les points suivants :

- Les utilisateurs fédérés ne pourront pas se connecter.
- Les utilisateurs fédérés actuellement connectés conserveront l'accès au système StorageGRID jusqu'à l'expiration de leur session, mais ils ne pourront plus se connecter après l'expiration de celle-ci.
- La synchronisation entre le système StorageGRID et la source d'identité n'aura pas lieu et aucune alerte ne sera émise pour les comptes qui n'ont pas été synchronisés.
- La case à cocher **Activer la fédération d'identités** est désactivée si le statut de l'authentification unique (SSO) est **Activé** ou **Mode bac à sable**. Le statut SSO sur la page d'authentification unique doit être **Désactivé** avant que vous puissiez désactiver la fédération d'identités. Voir "Désactivez l'authentification unique".

Étapes

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

Directives pour la configuration d'un serveur OpenLDAP

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

Pour les sources d'identité autres qu'Active Directory ou Microsoft Entra ID, StorageGRID ne bloque pas automatiquement l'accès S3 aux utilisateurs désactivés en externe. Pour bloquer l'accès S3, supprimez les clés S3 de l'utilisateur ou retirez l'utilisateur de tous les groupes.

Overlays Memberof et refint

Les superpositions memberof et refint doivent être activées. Pour plus d'informations, consultez les instructions relatives à la gestion des appartenances aux groupes inversées dans le "Documentation OpenLDAP : Guide de l'administrateur version 2.4".

Indexage

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

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

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

Consultez les informations relatives à la gestion des appartenances aux groupes inversés dans le "Documentation OpenLDAP : Guide de l'administrateur version 2.4".

Gérer les groupes d'administrateurs dans StorageGRID

Vous pouvez créer des groupes d'administrateurs pour gérer les autorisations de sécurité d'un ou plusieurs utilisateurs administrateurs. Les utilisateurs doivent appartenir à un groupe pour obtenir l'accès 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 prévoyez d'importer un groupe fédéré, vous avez configuré la fédération d'identités et le groupe fédéré existe déjà dans la source d'identité configurée.

Créer un groupe d'administrateurs

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

Accédez à l'assistant

Étapes

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

Choisissez un type de groupe

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

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

Groupe local

Étapes

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

Groupe fédéré

Étapes

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

Gérer les autorisations de groupe

Étapes

1. Pour le **mode d'accès**, sélectionnez si les utilisateurs du groupe peuvent modifier les paramètres et effectuer des opérations dans Grid Manager et le Grid Management API, ou s'ils peuvent uniquement consulter les paramètres et les fonctionnalités.
   - **Lecture-écriture** (par défaut) : Les utilisateurs peuvent modifier les paramètres et effectuer les opérations autorisées par leurs permissions de gestion.
   - **Lecture seule** : Les utilisateurs peuvent uniquement consulter les paramètres et les fonctionnalités. Ils ne peuvent apporter aucune modification ni effectuer d'opérations dans Grid Manager ou Grid Management API. Les utilisateurs locaux en lecture seule peuvent changer leur propre mot de passe.

   > Si un utilisateur appartient à plusieurs groupes et que l'un de ces groupes est configuré en **Lecture seule**, l'utilisateur aura un accès en lecture seule à tous les paramètres et fonctionnalités sélectionnés.

2. Sélectionnez-en un ou plusieurs "autorisations du groupe d'administrateurs".

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

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

Ajouter des utilisateurs (groupes locaux uniquement)

Étapes

1. Facultativement, sélectionnez un ou plusieurs utilisateurs locaux pour ce groupe.

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

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

Afficher et modifier les groupes d'administrateurs

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

- Pour consulter les informations de base de tous les groupes, reportez-vous au 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 correspondant au 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 correspondant au groupe. b. Sélectionnez **Actions** > **Modifier le nom du groupe**. c. Saisissez le nouveau nom. d. Sélectionnez **Save changes**.	a. Sélectionnez le nom du groupe pour afficher les détails. b. Sélectionnez l'icône de modification . c. Saisissez le nouveau nom. d. Sélectionnez **Save changes**.
Modifier le mode d'accès ou les autorisations	a. Cochez la case correspondant au groupe. b. Sélectionnez **Actions** > **Afficher les détails du groupe**. c. Vous pouvez éventuellement modifier le mode d'accès du groupe. d. Vous pouvez sélectionner ou effacer "autorisations du groupe d'administrateurs". e. Sélectionnez **Save changes**.	a. Sélectionnez le nom du groupe pour afficher les détails. b. Vous pouvez éventuellement modifier le mode d'accès du groupe. c. Vous pouvez sélectionner ou effacer "autorisations du groupe d'administrateurs". d. Sélectionnez **Save changes**.

Dupliquer un groupe

Étapes

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

Supprimer un groupe

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

Étapes

1. Sur la page Groupes, sélectionnez la case à cocher pour chaque groupe que vous souhaitez supprimer.
2. Sélectionnez **Actions** > **Supprimer le groupe**.
3. Sélectionnez **Supprimer les groupes**.

Autorisations du groupe d'administrateurs dans StorageGRID

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

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

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
- Consultez les pages des nœuds
- Afficher les alertes en cours et résolues
- Modifier leur propre mot de passe (utilisateurs locaux uniquement)
- Consultez certaines informations fournies sur les pages de configuration et de maintenance

Interaction entre les autorisations et le mode d'accès

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

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

Accès root

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

Modifier le mot de passe root du locataire

Cette autorisation permet d'accéder à l'option **Modifier le mot de passe root** sur la page Locataires, ce qui vous permet de contrôler qui peut modifier le mot de passe de l'utilisateur root local du locataire. Cette autorisation est également utilisée pour la migration des 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 Tenants, qui contient l'option **Change root password**, attribuez également l'autorisation **Tenant accounts**.

ILM

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

- Règles
- Politiques
- Étiquettes de stratégie
- Pools de stockage
- Classes de stockage
- Régions
- Recherche de métadonnées d'objet

> Les utilisateurs doivent disposer de l'autorisation **Autre configuration de grille** pour gérer les niveaux de stockage.

Maintenance

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

- **Configuration** > **Contrôle d'accès** :
  - Mots de passe de la grille
- **Configuration** > **Réseau** :
  - Noms de domaine des points de terminaison S3
- **Maintenance** > **Tâches** :
  - Mise hors service
  - Extension
  - Vérification de l'existence de l'objet
  - Récupération
- **Maintenance** > **Système** :
  - Package de récupération

    - Mise à jour logicielle
- **Assistance** > **Outils** :
    - Journaux

Les utilisateurs ne disposant pas de l'autorisation de maintenance peuvent consulter ces pages, mais pas les modifier :

- **Maintenance** > **Réseau** :
    - Serveurs DNS
    - Réseau Grid
    - Serveurs NTP
- **Maintenance** > **Système** :
    - Licence
- **Configuration** > **Réseau** :
    - Noms de domaine des points de terminaison S3
- **Configuration** > **Sécurité** :
    - Certificats
- **Configuration** > **Surveillance** :
    - Serveur d'audit et de journalisation système

Gérer les alertes

Cette autorisation permet d'accéder aux options de gestion des alertes. Les utilisateurs doivent disposer de cette autorisation pour gérer les mises en sourdine, les notifications d'alerte et les règles d'alerte.

Requête de métriques

Cette autorisation donne accès à :

- **Support** > **Outils** > **Métriques** page
- Requêtes personnalisées sur les métriques Prometheus à l'aide de la section **Metrics** de l'API Grid Management
- Cartes du tableau de bord Grid Manager contenant des indicateurs

Recherche de métadonnées d'objet

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

Autre configuration de grille

Cette autorisation donne accès aux options de configuration de grille supplémentaires suivantes :

- **ILM**:
    - Classes de stockage
- **Configuration** > **Système** :
- **Assistance** > **Autre** :

- Coût de liaison

Administrateur d'appliance de stockage

Cette autorisation permet :

- Accès au SANtricity System Manager de la série E sur les appliances de stockage via le Grid Manager.
- La possibilité d'effectuer des tâches de dépannage et de maintenance sur l'onglet Manage drives pour les appliances qui prennent en charge ces opérations.

Comptes de locataire

Cette autorisation permet de :

- Accédez à la page Locataires, où vous pouvez créer, modifier et supprimer des comptes locataires
- Consultez les politiques de classification du trafic existantes
- Consultez les cartes du tableau de bord Grid Manager qui contiennent les détails du locataire

Gérer les utilisateurs dans StorageGRID

Vous pouvez consulter les utilisateurs locaux et fédérés. Vous pouvez également créer des utilisateurs locaux et les affecter à des groupes d'administrateurs locaux afin de déterminer les fonctionnalités 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".

Créer un utilisateur local

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

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

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

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

Accédez à l'assistant

Étapes

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

Saisissez les identifiants 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 Grid Management API.
3. Sélectionnez **Continue**.

Attribuer aux groupes

Étapes

1. Vous pouvez, si vous le souhaitez, affecter l'utilisateur à un ou plusieurs groupes afin de déterminer les autorisations de l'utilisateur.

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

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

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

Afficher et modifier les utilisateurs locaux

Vous pouvez consulter les informations des utilisateurs locaux et fédérés existants. Vous pouvez modifier un utilisateur local pour changer 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 pouvez uniquement modifier les utilisateurs locaux. Utilisez la source d'identité externe pour gérer les utilisateurs fédérés.

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

  Les modifications sont appliquées lors de la prochaine déconnexion puis reconnexion de l'utilisateur au Grid Manager.

  > Les utilisateurs locaux peuvent modifier leur propre mot de passe en utilisant l'option **Changer le mot de passe** dans la bannière du Grid Manager.

Tâche	Menu Actions	Page de détails
Afficher les détails de l'utilisateur	a. Cochez la case pour l'utilisateur. b. Sélectionnez **Actions** > **Afficher les détails de l'utilisateur**.	Sélectionnez le nom de l'utilisateur dans le tableau.

Tâche	Menu Actions	Page de détails
Modifier le nom complet (utilisateurs locaux uniquement)	a. Cochez la case pour l'utilisateur. b. Sélectionnez **Actions** > **Modifier le nom complet**. c. Saisissez le nouveau nom. d. Sélectionnez **Save changes**.	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'icône de modification . c. Saisissez le nouveau nom. d. Sélectionnez **Save changes**.
Refuser ou autoriser l'accès à StorageGRID	a. Cochez la case pour 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 du Grid, ou sélectionnez **Non** pour autoriser l'utilisateur à se connecter. e. Sélectionnez **Save changes**.	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 du Grid, ou sélectionnez **Non** pour autoriser l'utilisateur à se connecter. d. Sélectionnez **Save changes**.
Changer le mot de passe (utilisateurs locaux uniquement)	a. Cochez la case pour 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 le 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 le mot de passe**.
Modifier les groupes (utilisateurs locaux uniquement)	a. Cochez la case pour l'utilisateur. b. Sélectionnez **Actions** > **Afficher les détails de l'utilisateur**. c. Sélectionnez l'onglet Groupes. d. Vous pouvez également sélectionner le lien situé après le nom d'un groupe pour afficher les détails de ce groupe dans un nouvel onglet de votre navigateur. e. Sélectionnez **Modifier les groupes** pour sélectionner différents groupes. f. Sélectionnez **Save changes**.	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'onglet Groupes. c. Vous pouvez également sélectionner le lien situé après le nom d'un groupe pour afficher les détails de ce groupe dans un nouvel onglet de votre navigateur. d. Sélectionnez **Modifier les groupes** pour sélectionner différents groupes. e. Sélectionnez **Save changes**.

Importer les utilisateurs fédérés

Vous pouvez importer un ou plusieurs utilisateurs fédérés, jusqu'à un maximum de 100 utilisateurs,

directement dans la page Utilisateurs.

Étapes

1. Sélectionnez **Configuration** > **Contrôle d'accès** > **Utilisateurs administrateurs**.
2. Sélectionnez **Importer les utilisateurs fédérés**.
3. Saisissez l'UUID ou le nom d'utilisateur d'un ou de plusieurs utilisateurs fédérés.

   Pour plusieurs entrées, ajoutez chaque UUID ou nom d'utilisateur sur une nouvelle ligne.

4. Sélectionnez **Importer**.

   Si l'importation dans le champ Utilisateurs échoue pour un ou plusieurs utilisateurs, procédez comme suit :

   a. Développez **Utilisateurs non importés** et sélectionnez **Copier les utilisateurs**.
   b. Réessayez l'importation en sélectionnant **Précédent** et en collant les utilisateurs copiés dans la boîte de dialogue **Import federated users**.

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

Dupliquer un utilisateur

Vous pouvez dupliquer un utilisateur existant pour créer un nouvel utilisateur disposant des mêmes autorisations.

Étapes

1. Cochez la case pour l'utilisateur.
2. Sélectionnez **Actions** > **Dupliquer l'utilisateur**.
3. Terminez l'assistant de duplication d'utilisateur.

Supprimer un utilisateur

Vous pouvez supprimer un utilisateur local pour le retirer définitivement du système.

Vous ne pouvez pas supprimer l'utilisateur root.

Étapes

1. Sur la page Utilisateurs, sélectionnez la case à cocher pour chaque utilisateur que vous souhaitez supprimer.
2. Sélectionnez **Actions** > **Supprimer l'utilisateur**.
3. Sélectionnez **Supprimer l'utilisateur**.

Utilisez l'authentification unique (SSO)

Découvrez l'authentification unique StorageGRID

Lorsque l'authentification unique (SSO) est activée, les utilisateurs peuvent accéder à Grid Manager, Tenant Manager, à l'API de gestion de Grid ou à l'API de gestion de locataires uniquement si leurs identifiants sont autorisés via le processus de connexion

SSO mis en place par votre organisation. Les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

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

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

Connectez-vous lorsque l'authentification unique est activée

Lorsque l'authentification unique (SSO) est activée et que vous vous connectez à StorageGRID, vous êtes redirigé vers la page SSO de votre organisation pour valider vos informations d'identification.

Étapes

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

   La page de connexion StorageGRID s'affiche.

   - Si c'est la première fois que vous accédez à l'URL sur ce navigateur, un identifiant de compte vous sera demandé.
   - Si vous avez déjà accédé au Grid Manager ou au Tenant Manager, vous êtes invité à sélectionner un compte récent ou à saisir un identifiant de compte.

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

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

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

4. Connectez-vous avec vos identifiants SSO.

   Si vos identifiants SSO sont corrects :

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

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

5. Vous pouvez également accéder à d'autres Admin Nodes, ou au Grid Manager ou au Tenant Manager, si vous disposez des autorisations nécessaires.

   Vous n'avez pas besoin de saisir à nouveau vos identifiants SSO.

Déconnectez-vous lorsque l'authentification unique est activée

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

Étapes

1. Repérez le lien **Se déconnecter** dans le coin supérieur droit de l'interface utilisateur.
2. Sélectionnez **Se déconnecter**.

   La page de connexion StorageGRID s'affiche. Le menu déroulant **Comptes récents** est mis 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.

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

Si vous êtes connecté à…	Et vous vous déconnectez de…	Vous êtes déconnecté(e) de…
Gestionnaire de grille sur un ou plusieurs nœuds d'administration	Gestionnaire de grille sur n'importe quel nœud d'administration	Gestionnaire de grille sur tous les nœuds d'administration **Remarque :** Si vous utilisez Entra ID pour l'authentification unique (SSO), il peut s'écouler quelques minutes avant que vous ne soyez déconnecté de tous les nœuds d'administration.
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	Uniquement le Grid Manager. Vous devez également vous déconnecter du Tenant Manager pour vous déconnecter de l'authentification unique (SSO).

Exigences et considérations relatives à l'authentification unique StorageGRID

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

Exigences du fournisseur d'identité

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

- Service de fédération Active Directory (AD FS)
- Microsoft Entra ID
- PingFederate

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

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

Exigences AD FS

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

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

> Windows Server 2016 doit utiliser la "Mise à jour KB3201845", ou une version supérieure.

Exigences supplémentaires

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

Considérations relatives à Entra ID

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

Exigences relatives aux certificats de serveur

Par défaut, StorageGRID utilise un certificat d'interface de gestion sur chaque nœud d'administration pour sécuriser l'accès au 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 parties de confiance (AD FS), des applications d'entreprise (Entra ID) ou des connexions de fournisseur de services (PingFederate) pour StorageGRID, vous utilisez le certificat du 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 serveur personnalisé, il est utilisé pour tous les nœuds d'administration, et vous pouvez l'utiliser dans toutes les approbations de parties de confiance StorageGRID, les applications d'entreprise ou les connexions SP.

> Il est déconseillé d'utiliser le certificat serveur par défaut d'un nœud d'administration dans une approbation de partie de confiance, une application d'entreprise ou une connexion SP. En cas de défaillance du nœud et de sa récupération, un nouveau certificat serveur par défaut est généré. Avant de pouvoir vous connecter au nœud récupéré, vous devez mettre à jour l'approbation de partie de confiance, l'application d'entreprise ou la connexion SP avec le nouveau certificat.

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

Exigences relatives aux ports

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

Confirmez que les utilisateurs fédérés peuvent se connecter à StorageGRID

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 tous les comptes locataires existants.

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 d'identité.

Étapes

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

> Lorsque vous activez l'authentification unique (SSO), la source d'identité configurée dans le Tenant Manager est remplacée par la source d'identité configurée dans le Grid Manager. Les utilisateurs appartenant à la source d'identité du locataire ne pourront plus se connecter à moins qu'ils ne disposent d'un compte auprès de la source d'identité du Grid Manager.

   a. Connectez-vous au Tenant Manager pour chaque compte locataire.

b. Sélectionnez **Gestion des accès** > **Fédération d'identités**.

c. Vérifiez que la case **Activer la fédération d'identités** n'est pas cochée.

d. Si c'est le cas, vérifiez que les groupes fédérés éventuellement utilisés pour ce compte locataire 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'administrateurs**.

b. Assurez-vous qu'au moins un groupe fédéré a été importé à partir de la source d'identité Active Directory et qu'il dispose de l'autorisation d'accès racine.

c. Déconnexion.

d. Vérifiez que vous pouvez vous reconnecter à Grid Manager en tant qu'utilisateur du groupe fédéré.

3. S'il existe des comptes locataires, vérifiez qu'un utilisateur fédéré disposant de l'autorisation d'accès Root peut se connecter :

a. Dans le Gestionnaire de grille, sélectionnez **Locataires**.

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

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

d. Si la case **Utiliser votre propre source d'identité** est cochée, décochez-la et sélectionnez **Enregistrer**.

La page du locataire s'affiche.

e. Sélectionnez le compte locataire, sélectionnez **Se connecter**, puis connectez-vous au compte locataire en tant qu'utilisateur racine local.

f. Dans le Gestionnaire de locataires, sélectionnez **Gestion des accès** > **Groupes**.

g. Assurez-vous qu'au moins un groupe fédéré du Grid Manager s'est vu attribuer l'autorisation d'accès racine pour ce locataire.

h. Déconnexion.

i. Vérifiez que vous pouvez vous reconnecter au locataire en tant qu'utilisateur du groupe fédéré.

Informations connexes

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

Configurer l'authentification unique (SSO) dans StorageGRID

Vous pouvez suivre l'assistant de configuration SSO et accéder au mode sandbox pour configurer et tester l'authentification unique (SSO) avant de l'activer pour tous les utilisateurs de StorageGRID. Une fois l'authentification unique (SSO) activée, vous pouvez revenir au mode sandbox si nécessaire pour 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 root".

- Vous avez configuré la fédération d'identités pour votre système StorageGRID.
- Pour le **type de service LDAP** de la fédération d'identités, vous avez sélectionné soit Active Directory, soit Entra ID, en fonction du fournisseur d'identités SSO que vous prévoyez d'utiliser.

Type de service LDAP configuré	Options pour le fournisseur d'identité SSO
Service de fédération Active Directory (AD FS)	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

À propos de cette tâche

Lorsque l'authentification unique (SSO) est activée et qu'un utilisateur tente de se connecter à un nœud d'administration, StorageGRID envoie une requête d'authentification au fournisseur d'identité SSO. À son tour, le fournisseur d'identité SSO renvoie une réponse d'authentification à StorageGRID, indiquant si la requête d'authentification a réussi. Pour les requêtes réussies :

- La réponse d'Active Directory ou PingFederate inclut un identifiant unique universel (UUID) pour l'utilisateur.
- La réponse d'Entra ID inclut un User Principal Name (UPN).

Pour permettre à StorageGRID (le fournisseur de services) et au fournisseur d'identité SSO de communiquer de manière sécurisée au sujet des demandes d'authentification des utilisateurs, vous devrez effectuer les tâches suivantes :

1. Configurez les paramètres dans StorageGRID.
2. Utilisez le logiciel du fournisseur d'identité SSO pour créer une approbation de partie de confiance (AD FS), une application d'entreprise (Entra ID) ou un fournisseur de services (PingFederate) pour chaque nœud d'administration.
3. Retournez à StorageGRID pour activer SSO.

Le mode bac à sable facilite les allers-retours de configuration et permet de tester tous vos paramètres avant d'activer l'authentification unique (SSO). Lorsque vous utilisez le mode bac à sable, les utilisateurs ne peuvent pas se connecter avec SSO.

Accédez à l'assistant

Étapes

1. Sélectionnez **Configuration** > **Contrôle d'accès** > **Authentification unique**. La page d'authentification unique s'affiche.

   > Si le bouton Configurer les paramètres SSO est désactivé, vérifiez que vous avez bien configuré le fournisseur d'identité comme source d'identité fédérée. Consultez "Exigences et considérations relatives à l'authentification unique".

2. Sélectionnez **Configurer les paramètres SSO**. La page « Fournir les détails du fournisseur d'identité » s'affiche.

Fournissez les détails du fournisseur d'identité

Étapes

1. Sélectionnez le **type d'authentification unique** dans la liste déroulante.
2. Si vous avez sélectionné Active Directory comme type SSO, saisissez le **nom du service de fédération** pour le fournisseur d'identité, exactement comme il apparaît dans Active Directory Federation Service (AD FS).

   Pour trouver le nom du service de fédération, ouvrez le Gestionnaire de serveur Windows. Sélectionnez **Outils** > **Gestion d'AD FS**. Dans le menu Action, sélectionnez **Modifier les propriétés du service de fédération**. Le nom du service de fédération s'affiche dans le deuxième champ.

3. 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.
   - **Utiliser le certificat CA du système d'exploitation** : Utilisez le certificat CA par défaut installé sur le système d'exploitation pour sécuriser la connexion.
   - **Utiliser un certificat CA personnalisé** : Utilisez un certificat CA personnalisé pour sécuriser la connexion.

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

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

     Si vous modifiez le certificat d'autorité de certification, "Redémarrez le service mgmt-api sur les nœuds d'administration" effectuez immédiatement cette opération et testez la réussite de l'authentification unique (SSO) dans Grid Manager.

4. Sélectionnez **Continuer**. La page « Fournir l'identifiant de la partie de confiance » s'affiche.

Fournissez l'identifiant de la partie de confiance

1. Remplissez les champs de la page « Fournir l'identifiant de la partie de confiance » en fonction du type d'authentification unique (SSO) que vous avez sélectionné.

Active Directory

a. Spécifiez l'**identificateur de la partie de confiance** pour StorageGRID. Cette valeur détermine le nom que vous utilisez pour chaque approbation de partie de confiance dans AD FS.

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

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

b. Sélectionnez **Enregistrer et passer en mode bac à sable**.

Entra ID

a. Dans la section Application d'entreprise, spécifiez le **nom de l'application d'entreprise** pour StorageGRID. Cette valeur détermine le nom que vous utilisez pour chaque application d'entreprise dans Entra ID.

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

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

b. Suivez les étapes décrites dans "Créez des applications d'entreprise dans Entra ID" pour créer une application d'entreprise pour chaque Admin Node répertorié dans le tableau.

c. À partir de Entra ID, copiez l'URL des métadonnées de fédération pour chaque application d'entreprise. Collez ensuite cette URL dans le champ **URL des métadonnées de fédération** correspondant dans StorageGRID.

d. Après avoir copié et collé une URL de métadonnées de fédération pour tous les Admin Nodes, sélectionnez **Enregistrer et entrer en mode sandbox**.

PingFederate

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

   - Par exemple, si votre grille ne comporte qu'un seul nœud d'administration et que vous ne prévoyez pas d'en ajouter d'autres à l'avenir, saisissez `SG` ou `StorageGRID`.

- Si votre grille comprend plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identifiant. Par exemple, `SG-[HOSTNAME]`. Inclure cette chaîne génère un tableau affichant l'ID de connexion SP pour chaque nœud d'administration de votre système, en fonction du nom d'hôte du nœud.

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

b. Spécifiez l'URL des métadonnées de fédération pour chaque nœud d'administration dans le champ **Federation metadata URL**.

Utilisez le format suivant :

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

c. Sélectionnez **Enregistrer et passer en mode bac à sable**.

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

Après avoir enregistré la configuration et activé le mode sandbox, vous pouvez finaliser et tester la configuration pour le type de SSO que vous avez sélectionné.

StorageGRID peut rester en mode sandbox aussi longtemps que nécessaire. Cependant, seuls les utilisateurs fédérés et les utilisateurs locaux peuvent se connecter.

Active Directory

Étapes

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

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

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

Entra ID

Étapes

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

PingFederate

Étapes

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

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

Tester la configuration

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

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

Active Directory

Étapes

1. Sur la page Configurer SSO, repérez le lien à l'étape Tester la configuration de l'assistant.

   L'URL est dérivée de la valeur que vous avez saisie dans le champ **Federation service name**.

2. Sélectionnez le lien, ou copiez et collez l'URL dans un navigateur, pour accéder à la page de connexion de votre fournisseur d'identité.
3. Pour confirmer que vous pouvez utiliser l'authentification unique (SSO) pour vous connecter à StorageGRID, sélectionnez **Se connecter à l'un des sites suivants**, sélectionnez l'identifiant de la partie de confiance pour votre nœud d'administration principal, puis sélectionnez **Se connecter**.
4. Saisissez votre nom d'utilisateur et votre mot de passe fédérés.
   - Si les opérations de connexion et de déconnexion SSO réussissent, un message de confirmation s'affiche.
   - En cas d'échec de l'authentification unique, un message d'erreur s'affiche. Résolvez le problème, effacez les cookies du navigateur et réessayez.
5. Répétez ces étapes pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

Entra ID

Étapes

1. Accédez à la page d'authentification unique dans le portail Azure.
2. Sélectionnez **Tester cette application**.
3. Saisissez les informations d'identification d'un utilisateur fédéré.
   - Si les opérations de connexion et de déconnexion SSO réussissent, un message de confirmation s'affiche.
   - En cas d'échec de l'authentification unique, un message d'erreur s'affiche. Résolvez le problème, effacez les cookies du navigateur et réessayez.
4. Répétez ces étapes pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

PingFederate

Étapes

1. Sur la page Configurer l'authentification unique (SSO), sélectionnez le premier lien du message relatif au mode Sandbox.

   Sélectionnez et testez un lien à la fois.

2. Saisissez les informations d'identification d'un utilisateur fédéré.
   - Si les opérations de connexion et de déconnexion SSO réussissent, un message de confirmation s'affiche.
   - En cas d'échec de l'authentification unique, un message d'erreur s'affiche. Résolvez le problème, effacez les cookies du navigateur et réessayez.
3. Sélectionnez le lien suivant pour vérifier la connexion SSO de chaque nœud d'administration de votre grille.

Si vous voyez un message « Page expirée », sélectionnez le bouton **Retour** de votre navigateur et soumettez à nouveau vos identifiants.

Activer l'authentification unique

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

Lorsque l'authentification unique (SSO) est activée, tous les utilisateurs doivent utiliser SSO pour accéder au Grid Manager, au Tenant Manager, à l'API de gestion de grille et à l'API de gestion de locataires. Les utilisateurs locaux ne peuvent plus accéder à StorageGRID.

Étapes

1. À l'étape de configuration de test de l'assistant de configuration SSO, sélectionnez **Activer SSO**.
2. Examinez le message d'avertissement et sélectionnez **Activer SSO**.

   L'authentification unique est désormais activée. La page d'authentification unique s'affiche et contient désormais les informations relatives à l'authentification unique que vous venez de configurer.

3. Pour modifier la configuration, sélectionnez **Modifier**.
4. Pour désactiver l'authentification unique, sélectionnez **Désactiver SSO**.

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

Créer des approbations de parties de confiance dans AD FS pour StorageGRID

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

Avant de commencer

- Vous avez configuré l'authentification unique pour StorageGRID et vous avez sélectionné **AD FS** comme type de SSO.
- Vous avez "mode bac à sable activé" dans Grid Manager.
- Vous connaissez le domaine complet (ou l'adresse IP) et l'identifiant de la partie de confiance pour chaque nœud d'administration de votre système. Vous pouvez trouver ces valeurs dans le tableau des détails des nœuds d'administration sur la page Configurer SSO de StorageGRID.

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

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

À propos de cette tâche

Ces instructions concernent Windows Server 2016 AD FS. Si vous utilisez une autre version d'AD FS, vous constaterez de légères différences dans la procédure. Consultez la documentation Microsoft AD FS si vous avez des questions.

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

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

Étapes

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

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

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

   L'outil de gestion AD FS apparaît.
4. Sélectionnez **AD FS** > **Approbations de parties de confiance**.

   La liste des relations d'approbation de parties approuvées apparaît.
5. Ajoutez une stratégie de contrôle d'accès à l'approbation de partie de confiance nouvellement créée :
   a. Localisez la relation d'approbation de partie utilisatrice que vous venez de créer.
   b. Cliquez avec le bouton droit sur l'approbation, puis sélectionnez **Modifier la stratégie de contrôle d'accès**.

c. Sélectionnez une politique de contrôle d'accès.

d. Sélectionnez **Appliquer**, puis **OK**

6. Ajoutez une politique d'émission de revendications à la nouvelle relation de confiance de partie utilisatrice :

a. Localisez la relation d'approbation de partie utilisatrice que vous venez de créer.

b. Cliquez avec le bouton droit sur la fiducie, puis sélectionnez **Modifier la politique d'émission des revendications**.

c. Sélectionnez **Ajouter une règle**.

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

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

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

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

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

h. Dans la colonne Outgoing Claim Type du tableau de mappage, sélectionnez **Name ID** dans la liste déroulante.

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

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

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

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

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

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

9. Une fois que vous avez terminé, retournez sur StorageGRID "tester toutes les relations d'approbation des parties dépendantes" pour confirmer qu'ils sont correctement configurés.

Créez une relation de confiance de partie utilisatrice en important les métadonnées de fédération

Vous pouvez importer les valeurs de chaque approbation de partie de confiance en accédant aux métadonnées SAML de chaque Admin Node.

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis sélectionnez **Gestion d'AD FS**.
2. Sous Actions, sélectionnez **Ajouter une fiducie de partie de confiance**.
3. Sur la page d'accueil, choisissez **Claims aware**, puis sélectionnez **Start**.
4. Sélectionnez **Importer les données relatives à la partie de confiance publiées en ligne ou sur un réseau local**.
5. Dans **Adresse des métadonnées de la fédération (nom de l'hôte ou URL)**, saisissez l'emplacement des métadonnées SAML pour cet Admin Node :

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

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

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

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

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

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

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

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

9. Répétez ces étapes pour configurer une relation de confiance de partie utilisatrice pour tous les nœuds d'administration de votre système StorageGRID.
10. Une fois que vous avez terminé, retournez sur StorageGRID et "tester toutes les relations d'approbation des parties dépendantes" pour confirmer qu'ils sont correctement configurés.

Créer manuellement une relation de confiance avec une partie utilisatrice

Si vous choisissez de ne pas importer les données pour les approbations de la partie dépendante, vous pouvez saisir les valeurs manuellement.

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis sélectionnez **Gestion d'AD FS**.
2. Sous Actions, sélectionnez **Ajouter une fiducie de partie de confiance**.
3. Sur la page d'accueil, choisissez **Claims aware**, puis sélectionnez **Start**.
4. Sélectionnez **Saisir manuellement les données relatives à la partie de confiance**, puis sélectionnez **Suivant**.
5. Terminez l'assistant de création de fiducie de partie de confiance :

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

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

   b. Ignorez l'étape de configuration d'un certificat de chiffrement de jeton facultatif.

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

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

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

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

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

      `Admin_Node_Identifier`

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

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

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

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

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

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

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

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

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

   d. Dans la colonne Attribut LDAP du tableau de mappage, saisissez **objectGUID** ou sélectionnez **User-**

Principal-Name.

e. Dans la colonne Outgoing Claim Type du tableau de mappage, sélectionnez **Name ID** dans la liste déroulante.

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

7. Cliquez avec le bouton droit sur l'entité de confiance pour ouvrir ses propriétés.
8. Dans l'onglet **Points de terminaison**, configurez le point de terminaison pour la déconnexion unique (SLO) :

a. Sélectionnez **Ajouter SAML**.

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

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

d. Dans le champ **URL de confiance**, saisissez l'URL utilisée pour la déconnexion unique (SLO) à partir de ce Admin Node :

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

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

a. Sélectionnez **OK**.

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

a. Ajouter le certificat personnalisé :

- Si vous avez téléchargé le certificat de gestion personnalisé sur StorageGRID, sélectionnez ce certificat.
- Si vous ne possédez pas le 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 lors de la restauration du nœud, et vous devrez mettre à jour la relation de confiance de la partie dépendante.

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

Les propriétés de la partie utilisatrice sont enregistrées et fermées.

10. Répétez ces étapes pour configurer une relation de confiance de partie utilisatrice pour tous les nœuds d'administration de votre système StorageGRID.
11. Une fois que vous avez terminé, retournez sur StorageGRID et "tester toutes les relations d'approbation des parties dépendantes" pour confirmer qu'ils sont correctement configurés.

Créez des applications d'entreprise dans Entra ID pour StorageGRID

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

Avant de commencer

- Vous avez commencé à configurer l'authentification unique pour StorageGRID et vous avez sélectionné **Entra ID** comme type de SSO.
- Vous avez "mode bac à sable activé" dans Grid Manager.
- Vous disposez du **nom de l'application d'entreprise** pour chaque nœud d'administration de votre système. Vous pouvez copier ces valeurs depuis le tableau des détails du nœud d'administration sur la page Configurer SSO.

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

- Vous avez de l'expérience dans la création d'applications d'entreprise dans Entra ID.
- Vous possédez un compte Entra ID avec un abonnement actif.
- Vous possédez l'un des rôles suivants dans le compte Entra ID : Global Administrator, Cloud Application Administrator, Application Administrator ou owner of the service principal.

Accéder à Entra ID

Étapes

1. Connectez-vous à l' "Portail Azure".
2. Accédez à "Entra ID".
3. Sélectionnez "Applications d'entreprise".

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

Pour enregistrer la configuration SSO d'Entra ID dans StorageGRID, vous devez utiliser Entra ID pour créer une application d'entreprise pour chaque Admin Node. Vous copierez les URL des métadonnées de fédération depuis Entra ID et les collerez dans les champs correspondants **Federation metadata URL** sur la page Configurer SSO.

Étapes

1. Répétez les étapes suivantes pour chaque nœud d'administration.
   a. Dans le volet Applications d'entreprise d'Entra ID, sélectionnez **Nouvelle application**.
   b. Sélectionnez **Créer votre propre application**.
   c. Pour le nom, saisissez le **nom de l'application d'entreprise** que vous avez copié du tableau des détails du nœud d'administration sur la page Configurer SSO.
   d. Laissez l'option **Intégrer toute autre application que vous ne trouvez pas dans la galerie (Hors galerie)** sélectionnée.
   e. Sélectionnez **Create**.
   f. Sélectionnez le lien **Get started** dans la **2. Set up single sign on** box, ou sélectionnez le lien **Single sign-on** dans la marge de gauche.
   g. Sélectionnez la case **SAML**.
   h. Copiez l'**App Federation Metadata Url**, que vous trouverez sous **Step 3 SAML Signing Certificate**.
   i. Accédez à la page Configurer SSO, puis collez l'URL dans le champ **Federation metadata URL** qui

correspond au **Enterprise application name** que vous avez utilisé.

2. Après avoir collé une URL de métadonnées de fédération pour chaque Admin Node et effectué toutes les autres modifications nécessaires à la configuration SSO, sélectionnez **Enregistrer** sur la page Configurer SSO.

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 depuis le nœud d'administration.
   b. Sélectionnez **Configuration** > **Contrôle d'accès** > **Authentification unique**.
   c. Sélectionnez le bouton pour télécharger les métadonnées SAML de ce nœud d'administration.
   d. Enregistrez le fichier, que vous téléchargerez ensuite dans Entra ID.

Téléversez les métadonnées SAML dans chaque application d'entreprise

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

Étapes

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

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

   a. Accédez à la page Propriétés de l'application d'entreprise.
   b. Définissez **Assignment required** sur **Non** (sauf si vous souhaitez configurer les affectations séparément).
   c. Accédez à la page d'authentification unique.
   d. Finalisez la configuration SAML.
   e. Sélectionnez le bouton **Téléverser un 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 êtes renvoyé à la page Configurer l'authentification unique avec SAML.
3. "Tester chaque application".

Créez des connexions de fournisseur de services dans PingFederate pour StorageGRID

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

Avant de commencer

- Vous avez configuré l'authentification unique pour StorageGRID et vous avez sélectionné **Ping Federate** comme type de SSO.
- Vous avez "mode bac à sable activé" dans Grid Manager.
- Vous disposez de l'**ID de connexion SP** pour chaque nœud d'administration de votre système. Vous pouvez trouver ces valeurs dans le tableau des détails des nœuds d'administration sur la page Configurer le SSO.
- Vous avez téléchargé les **métadonnées SAML** pour chaque nœud d'administration de votre système.
- Vous avez de l'expérience dans la création de connexions SP dans le serveur PingFederate.
- Vous disposez du "Guide de référence de l'administrateur" pour le serveur PingFederate. La documentation PingFederate fournit des instructions détaillées étape par étape et des explications.
- Vous disposez du "Autorisation d'administrateur" pour le serveur PingFederate.

À propos de cette tâche

Ces instructions résument comment configurer le serveur PingFederate 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. Consultez la documentation du serveur PingFederate pour obtenir des instructions détaillées concernant votre version.

Effectuez les prérequis 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 issues de ces prérequis lors de la configuration des connexions SP.

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 lors de "configuration de la fédération d'identités" dans StorageGRID.

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

Créer un validateur d'identifiants de mot de passe

Si ce n'est pas déjà fait, créez un validateur d'identifiants de mot de passe.

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

Créer une instance d'adaptateur IdP

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

Étapes

1. Accédez à **Authentification** > **Intégration** > **Adaptateurs IdP**.
2. Sélectionnez **Créer une nouvelle instance**.
3. Dans l'onglet Type, sélectionnez **HTML Form IdP Adapter**.
4. Dans l'onglet Adaptateur IdP, sélectionnez **Ajouter une nouvelle ligne à 'Credential Validators'**.
5. Sélectionnez validateur d'identifiants de mot de passe que vous avez créé.
6. Dans l'onglet Attributs de l'adaptateur, sélectionnez l'attribut **username** pour **Pseudonym**.
7. Sélectionnez **Enregistrer**.

Créer ou importer un certificat de signature

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

Étapes

1. Accédez à **Security** > **Signing & Decryption Keys & Certificates**.
2. Créez ou importez le certificat de signature.

Créer une connexion SP dans PingFederate

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

> Vous devez créer une connexion SP pour chaque nœud d'administration de votre système StorageGRID, afin que les utilisateurs puissent se connecter et se déconnecter en toute sécurité de n'importe quel nœud. Utilisez ces instructions pour créer la première connexion SP. Ensuite, allez 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** > **Integration** > **SP Connections**.
2. Sélectionnez **Créer une connexion**.
3. Sélectionnez **Ne pas utiliser de modèle pour cette connexion**.
4. Sélectionnez **Profils SSO du navigateur** et **SAML 2.0** comme protocole.

Importer les métadonnées SP

Étapes

1. Dans l'onglet Import Metadata, sélectionnez **File**.
2. Choisissez le fichier de métadonnées SAML que vous avez téléchargé depuis la page Configure SSO pour le nœud d'administration.
3. Consultez le résumé des métadonnées et les informations fournies dans l'onglet Informations générales.

   L'identifiant d'entité du partenaire et le nom de la connexion sont définis sur l'identifiant de connexion SP de 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 **Next**.

Configurer l'authentification unique (SSO) du navigateur IdP

Étapes

1. Dans l'onglet SSO du navigateur, sélectionnez **Configurer le SSO du navigateur**.
2. Dans l'onglet Profils SAML, sélectionnez les options **SSO initié par le SP**, **SLO initié par le SP**, **SSO initié par l'IdP** et **SLO initié par l'IdP**.
3. Sélectionnez **Next**.
4. Dans l'onglet Durée de vie de l'assertion, ne modifiez rien.
5. Dans l'onglet Création d'assertions, sélectionnez **Configurer la création d'assertions**.
   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 retirer la `urn:oid`, qui n'est pas utilisée.

Mapper l'instance d'adaptateur

Étapes

1. Dans l'onglet Mappage de la source d'authentification, sélectionnez **Mapper une nouvelle instance d'adaptateur**.
2. Dans l'onglet Instance d'adaptateur, sélectionnez instance d'adaptateur que vous avez créée.
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'attributs et recherche d'utilisateurs, sélectionnez **Ajouter une source d'attributs**.
5. Dans l'onglet « Stockage de données », saisissez une description et sélectionnez l'élément magasin de données que vous avez ajouté.
6. Dans l'onglet Recherche dans l'annuaire LDAP :
   - Saisissez le **DN de base**, qui doit correspondre exactement à la valeur que vous avez saisie dans StorageGRID pour le serveur LDAP.
   - Pour l'étendue de la recherche, sélectionnez **Sous-arbre**.
   - Pour la classe d'objet racine, recherchez et ajoutez l'un de ces attributs : **objectGUID** ou **userPrincipalName**.
7. Dans l'onglet Types d'encodage des attributs binaires LDAP, sélectionnez **Base64** pour l'attribut **objectGUID**.
8. Dans l'onglet Filtre LDAP, saisissez **sAMAccountName=${username}**.
9. Dans l'onglet Exécution du contrat d'attribut, sélectionnez **LDAP (attribut)** dans la liste déroulante Source et sélectionnez soit **objectGUID** ou **userPrincipalName** dans la liste déroulante Valeur.
10. Vérifiez puis enregistrez la source des attributs.
11. Dans l'onglet Source de l'attribut Failsave, sélectionnez **Annuler la transaction SSO**.
12. Vérifiez le récapitulatif et sélectionnez **Terminé**.
13. Sélectionnez **Terminé**.

Configurer les paramètres du protocole

Étapes

1. Dans l'onglet **SP Connection** > **Browser SSO** > **Protocol Settings**, sélectionnez **Configure Protocol Settings**.
2. Sur l'onglet URL du service de consommation d'assertion, acceptez les valeurs par défaut, qui ont été importées des métadonnées SAML de StorageGRID (**POST** pour la liaison et `/api/saml-response` pour l'URL du point de terminaison).
3. Dans l'onglet URL du service SLO, acceptez les valeurs par défaut, qui ont été importées des métadonnées SAML de StorageGRID (**REDIRECT** pour la liaison et `/api/saml-logout` pour l'URL du point de terminaison.
4. Dans l'onglet Liaisons SAML autorisées, décochez **ARTIFACT** et **SOAP**. Seuls **POST** et **REDIRECT** sont requis.
5. Dans l'onglet Signature Policy, laissez les cases à cocher **Require Authn Requests to be Signed** et **Always Sign Assertion** sélectionnées.
6. Dans l'onglet Encryption Policy, sélectionnez **None**.
7. Vérifiez le récapitulatif et sélectionnez **Terminé** pour enregistrer les paramètres du protocole.
8. Vérifiez le récapitulatif et sélectionnez **Terminé** pour enregistrer les paramètres Browser SSO.

Configurer les identifiants

Étapes

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

Créer des connexions SP supplémentaires

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

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

Étapes

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

b. Sélectionnez **Choisir un fichier** et téléchargez les métadonnées.

c. Sélectionnez **Next**.

d. Sélectionnez **Enregistrer**.

4. Résolvez l'erreur due à l'attribut inutilisé :

a. Sélectionnez la nouvelle connexion.

b. Sélectionnez **Configurer l'authentification unique du navigateur > Configurer la création d'assertions > Contrat d'attributs**.

c. Supprimez l'entrée pour **urn:oid**.

d. Sélectionnez **Enregistrer**.

Désactiver SSO dans StorageGRID

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

   La page d'authentification unique s'affiche.

2. Sélectionnez **Désactiver l'authentification unique**.
3. Sélectionnez **Oui**.

   Un message d'avertissement s'affiche, indiquant que les utilisateurs locaux pourront désormais se connecter.

La prochaine fois que vous vous connecterez à StorageGRID, la page de connexion StorageGRID s'affichera et vous devrez saisir le nom d'utilisateur et le mot de passe d'un utilisateur StorageGRID local ou fédéré.

Désactivez et réactivez temporairement l'authentification unique (SSO) pour un nœud d'administration StorageGRID

Il se peut que vous ne puissiez pas vous connecter à Grid Manager si le système d'authentification unique (SSO) est indisponible. Dans ce cas, vous pouvez désactiver puis réactiver temporairement le SSO pour un Admin Node. Pour désactiver puis réactiver le 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 root local.

À propos de cette tâche

Après avoir désactivé l'authentification unique (SSO) pour un nœud d'administration, vous pouvez vous connecter au Grid Manager en tant qu'utilisateur root local. Pour sécuriser votre système StorageGRID, vous devez utiliser le shell de commande du nœud pour réactiver l'authentification unique (SSO) sur le nœud d'administration dès que vous vous déconnectez.

> La désactivation de l'authentification unique (SSO) pour un nœud d'administration n'affecte pas les paramètres SSO des autres nœuds d'administration de la grille. La case à cocher **Enable SSO** sur la page Single Sign-on dans le Grid Manager reste sélectionnée, et tous les paramètres SSO existants sont conservés, sauf si vous les mettez à jour.

Étapes

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

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

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

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

3. Confirmez que vous souhaitez désactiver SSO.

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

4. Depuis un navigateur Web, accédez au Grid Manager sur le même nœud d'administration.

   La page de connexion de Grid Manager s'affiche désormais 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 temporairement l'authentification unique (SSO) parce que vous deviez corriger la configuration SSO :
   a. Sélectionnez **Configuration** > **Contrôle d'accès** > **Authentification unique**.
   b. Modifiez les paramètres SSO incorrects ou obsolètes.
   c. Sélectionnez **Enregistrer**.

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

7. Si vous avez désactivé temporairement l'authentification unique (SSO) parce que vous aviez besoin d'accéder au Grid Manager pour une autre raison :
   a. Effectuez la ou les tâches que vous devez accomplir.
   b. Sélectionnez **Se déconnecter**, puis fermez le Grid Manager.
   c. Réactivez l'authentification unique (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 l'authentification unique (SSO).

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

- Redémarrez le nœud de grille : `reboot`

8. Depuis un navigateur Web, accédez au Grid Manager depuis le même nœud d'administration.
9. Vérifiez que la page de connexion StorageGRID s'affiche et que vous devez saisir vos identifiants SSO pour accéder au Grid Manager.

${post_edited_translations.segment}

Découvrez la fédération de grilles StorageGRID

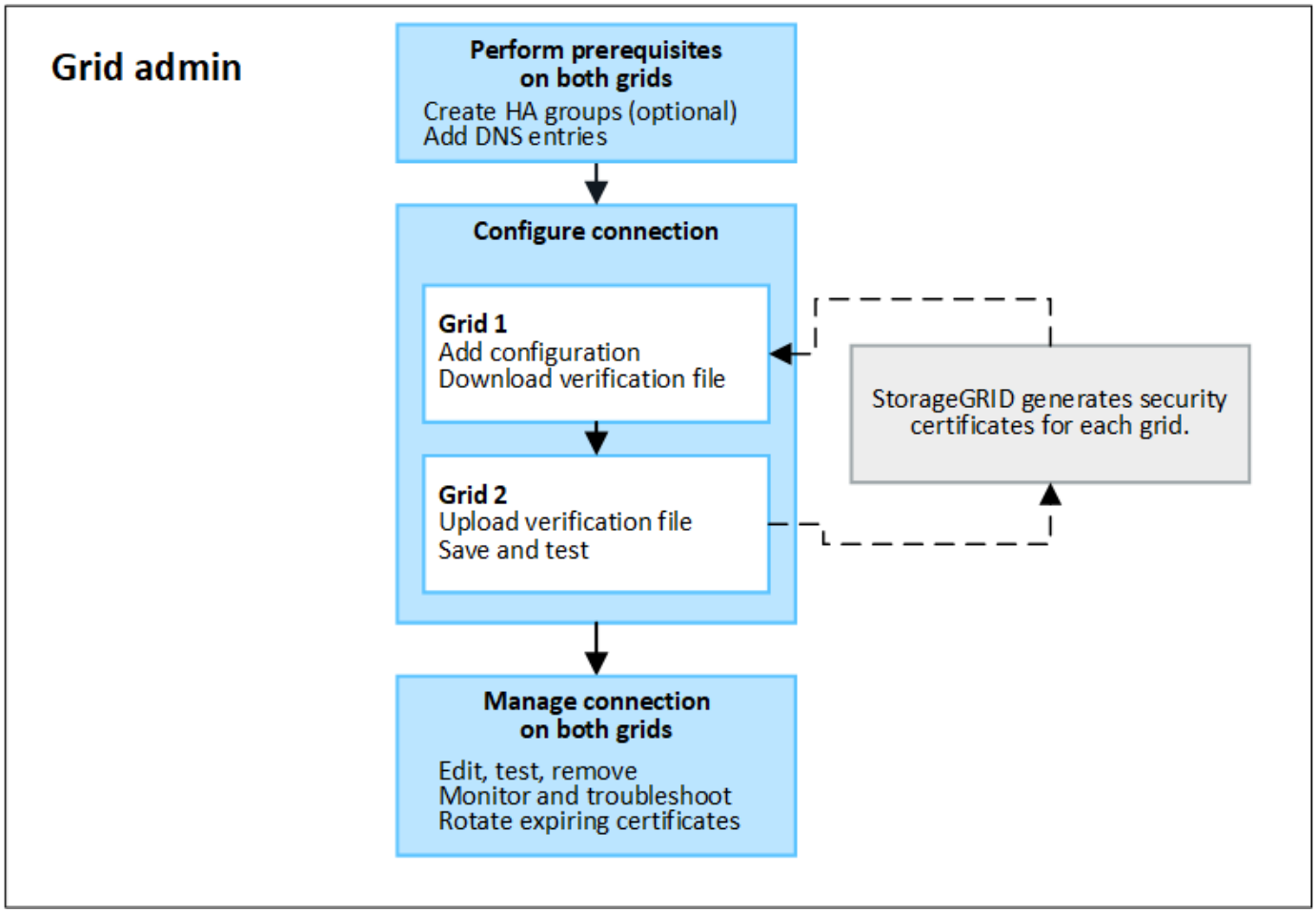
Vous pouvez utiliser la fédération de grilles pour cloner des locataires et répliquer leurs objets entre deux systèmes StorageGRID à des fins de reprise après sinistre.

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

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

Flux de travail pour la fédération de grid

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



Considérations et exigences relatives aux connexions de fédération de grid

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

  Pour plus de détails sur les exigences de version, consultez "Notes de version". Vous devez vous connecter avec votre compte NetApp ou en créer un pour accéder aux notes de version.

- Un grid peut avoir une ou plusieurs connexions de fédération avec d'autres grids. Chaque connexion de fédération de grid est indépendante des autres connexions. Par exemple, si Grid 1 a une connexion avec Grid 2 et une seconde connexion avec Grid 3, il n'existe aucune connexion implicite entre Grid 2 et Grid 3.
- Les connexions de fédération de grilles sont bidirectionnelles. Une fois la connexion établie, vous pouvez surveiller et gérer la connexion depuis l'une ou l'autre grille.
- Au moins une connexion de fédération de grille doit exister avant que vous puissiez utiliser "clone de compte" ou "réplication inter-grilles".

Exigences en matière de réseau et d'adresse IP

- Les connexions de fédération de grilles peuvent s'effectuer sur le réseau de grille, le réseau d'administration ou le réseau client.
- Une connexion de fédération de grilles relie une grille à une autre grille. La configuration de chaque grille spécifie un point de terminaison de fédération de grille sur l'autre grille, composé de nœuds d'administration, de nœuds de passerelle ou des deux.
- La bonne pratique consiste à connecter "groupes à haute disponibilité (HA)" les nœuds Gateway et Admin

sur chaque grille. L'utilisation de groupes HA permet de garantir que les connexions de fédération de grille resteront en ligne si des nœuds deviennent indisponibles. Si l'interface active dans l'un ou l'autre groupe HA échoue, la connexion peut utiliser une interface de secours.

- Il est déconseillé d'établir une connexion de fédération de grille utilisant l'adresse IP d'un seul nœud d'administration ou nœud de passerelle. Si ce nœud devient indisponible, la connexion de fédération de grille le sera également.
- "Réplication inter-grilles" L'accès aux objets nécessite que les nœuds de stockage de chaque grille puissent accéder aux nœuds Admin et Gateway configurés sur l'autre grille. Pour chaque grille, confirmez que tous les nœuds de stockage disposent d'une route à large bande passante vers les nœuds Admin ou Gateway utilisés pour la connexion.

Utilisez les FQDN (Fully Qualified Domain Names) pour équilibrer la charge de la connexion.

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

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

Lorsque vous utilisez plusieurs entrées DNS, les requêtes d'utilisation de la connexion sont réparties en charge, comme suit :

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

Exigences relatives aux ports

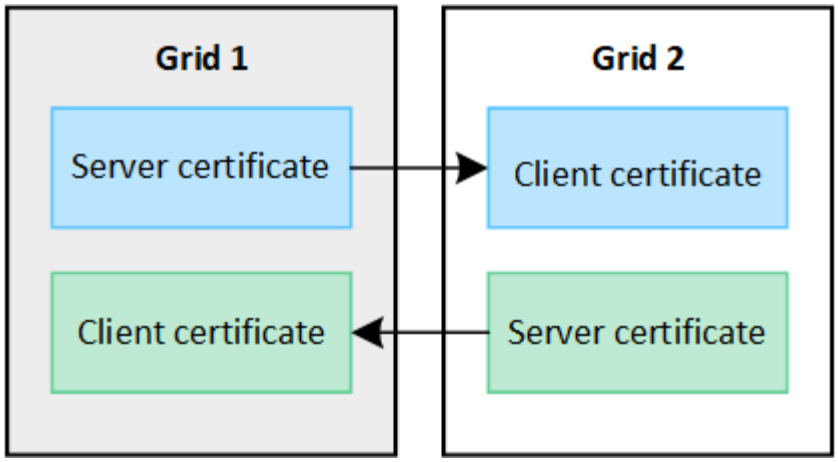
Lors de la création d'une connexion de fédération de grilles, vous pouvez spécifier n'importe quel numéro de port inutilisé compris entre 23000 et 23999. Les deux grilles de cette connexion utiliseront le même port.

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

Exigences relatives aux certificats

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

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



Par défaut, les certificats sont valides pendant 730 jours (2 ans). À l'approche de leur date d'expiration, l'alerte **Expiration of grid federation certificate** vous rappelle de renouveler les certificats, ce que vous pouvez faire à l'aide du Grid Manager.

> Si les certificats des deux extrémités de la connexion expirent, la connexion cessera 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"

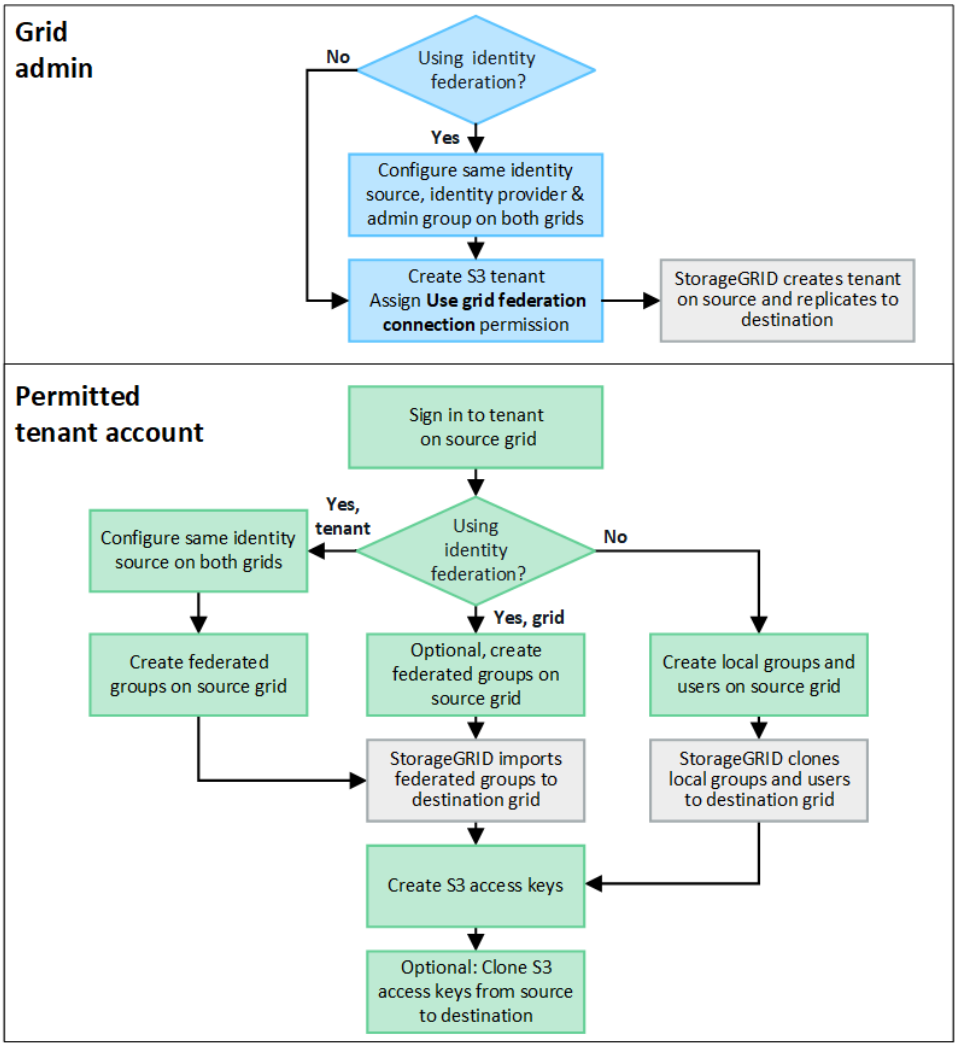
En savoir plus sur le clonage de compte dans StorageGRID

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

Flux de travail pour le clonage de compte

Le diagramme de flux de travail illustre les étapes que les administrateurs de grille et les locataires autorisés devront suivre pour configurer le clonage de compte. Ces étapes sont effectuées après le "La connexion de fédération de grille est configurée".



Flux de travail d'administration de la grille

Les étapes que les administrateurs de grille effectuent dépendent du fait que les systèmes StorageGRID dans le "connexion de fédération de grille" utilisent l'authentification unique (SSO) ou la fédération d'identités.

Configurer l'authentification unique pour le clonage de compte (facultatif)

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

Étapes

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

   Lors de la création du locataire, vous sélectionnerez ce groupe pour avoir l'autorisation d'accès Root initiale pour les comptes de locataire source et de destination.

Si ce groupe d'administrateurs n'existe pas sur les deux grilles avant que vous ne créiez le locataire, le locataire n'est pas répliqué vers la destination.

Configurer la fédération d'identités au niveau de la grille pour account clone (facultatif)

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

Étapes

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

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

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

Créer un compte locataire S3 autorisé

Après avoir éventuellement configuré l'authentification unique (SSO) ou la fédération d'identités, un administrateur de grille effectue ces étapes pour déterminer quels locataires peuvent répliquer les objets du compartiment vers d'autres systèmes StorageGRID.

Étapes

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

   La grille sur laquelle le locataire est initialement créé est appelée *grille source* du locataire. La grille sur laquelle le locataire est répliqué est appelée *grille de destination* du locataire.

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

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

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

   Lorsqu'un nouveau locataire disposant de 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 locataires possèdent le même identifiant de compte, le même nom, le même quota

de stockage et les mêmes autorisations attribuées.

- Si vous avez sélectionné un groupe fédéré disposant des autorisations d'accès racine pour le locataire, ce groupe est cloné dans le locataire de destination.
- Si vous avez sélectionné un utilisateur local disposant des droits d'accès Root pour le locataire, cet utilisateur est cloné dans le locataire de destination. Cependant, le mot de passe de cet utilisateur n'est pas cloné.

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

Flux de travail des comptes de locataire autorisé

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

Étapes

1. Connectez-vous au compte locataire sur la grille source du locataire.
2. Si cela est autorisé, configurez la fédération d'identité sur les comptes locataires source et de destination.
3. Créez des groupes et des utilisateurs sur le tenant source.

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

4. Créez des clés d'accès S3.
5. Vous pouvez, si vous le souhaitez, cloner les clés d'accès S3 du locataire source vers le locataire de destination.

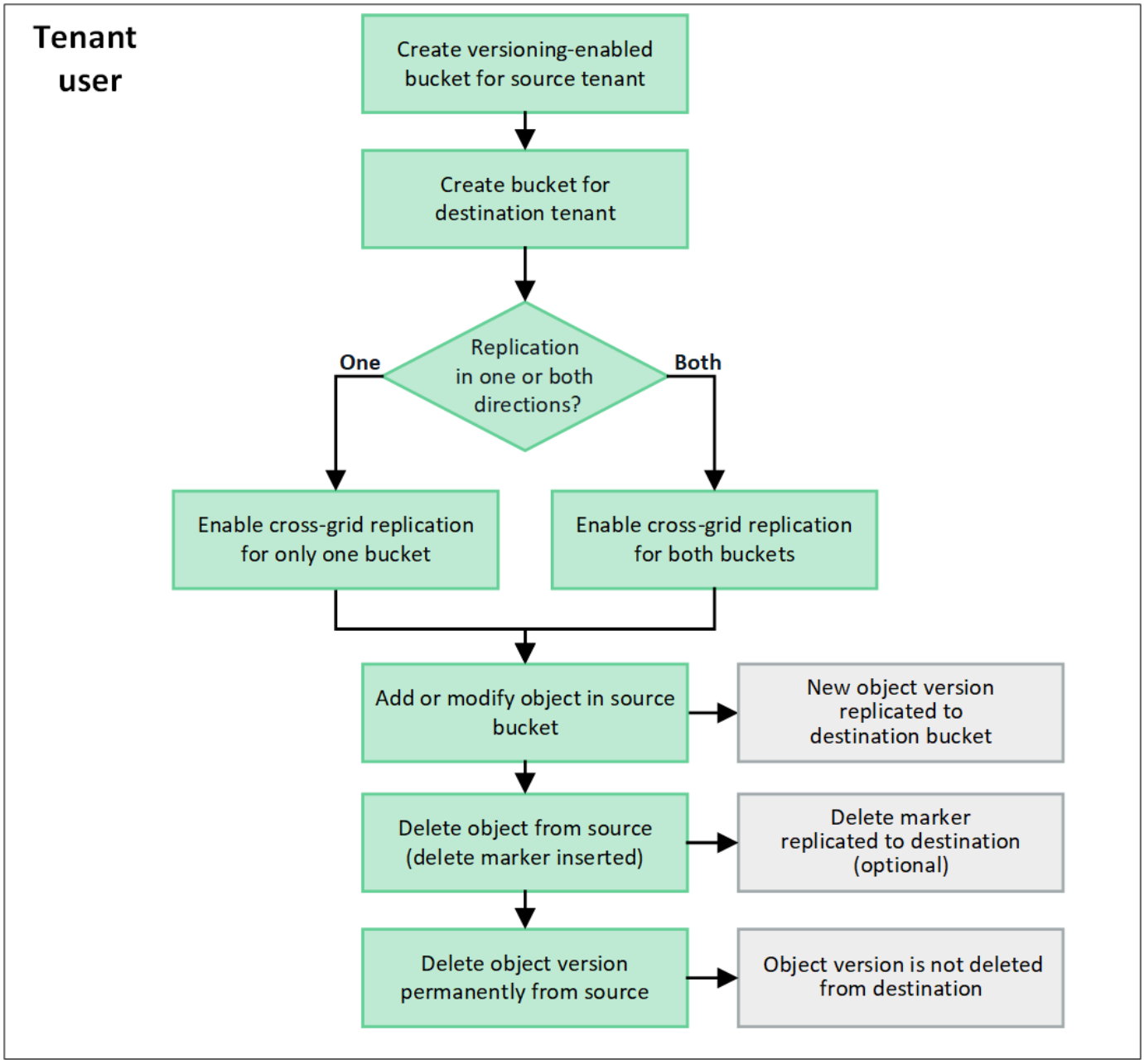
Pour plus de détails sur le flux de travail des comptes locataires autorisés et pour savoir comment les groupes, les utilisateurs et les clés d'accès S3 sont clonés, consultez "Cloner les groupes de locataires et les utilisateurs" et "Cloner les clés d'accès S3 à l'aide de l'API".

Découvrez la réplication inter-grilles dans StorageGRID

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

Flux de travail pour la réplication inter-grilles

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



Exigences pour la réplication inter-grilles

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

- Peuvent avoir des noms différents l'un de l'autre
- Peut avoir différentes régions
- La gestion des versions doit être activée
- Doit être vide

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

En savoir plus

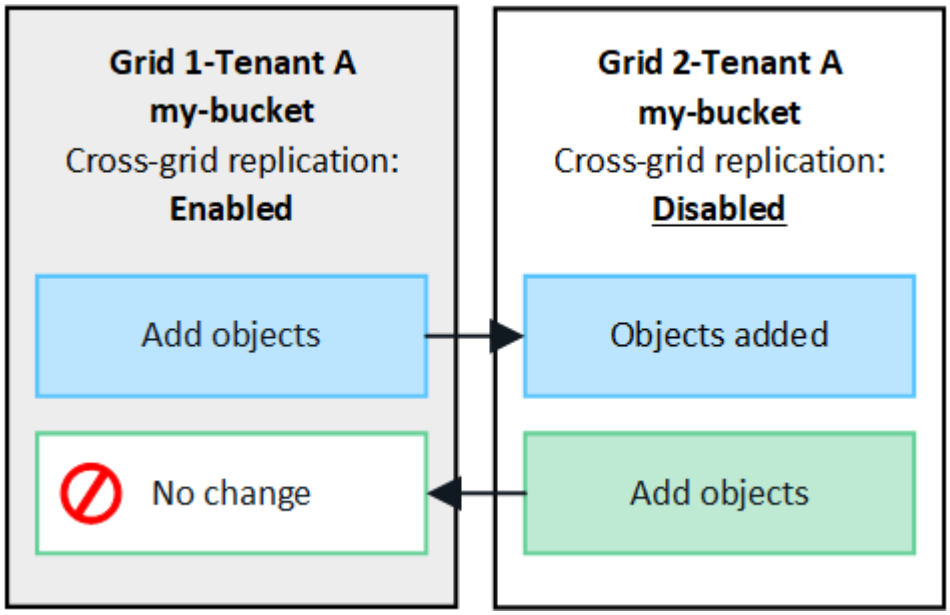
"Gérer la réplication inter-grilles"

Comment fonctionne la réplication inter-grilles

Vous pouvez configurer la réplication inter-grilles pour qu'elle s'effectue dans un seul sens ou dans les deux sens.

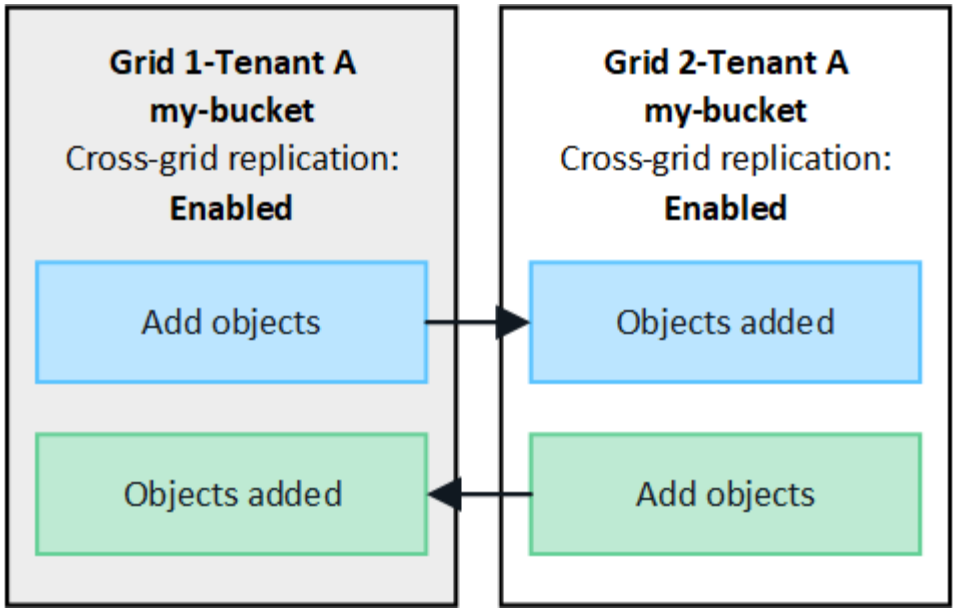
Réplication dans un seul sens

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



Réplication dans les deux sens

Si vous activez la réplication inter-grilles pour un même compartiment sur les deux grilles, les objets ajoutés à l'un des compartiments sont répliqués sur l'autre grille. Sur la figure, la réplication inter-grilles 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-grilles est activée, le processus suivant se déroule :

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

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

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

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

2. StorageGRID utilise les politiques 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 répliquée 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 requête de suppression.
- Un utilisateur de Tenant Manager sélectionne l'"Supprimer les objets dans le compartiment"option pour supprimer tous les objets d'un compartiment.
- Le compartiment possède une configuration de cycle de vie, qui expire.
- La dernière période définie dans la règle ILM pour l'objet arrive à son terme, et aucun autre placement n'est spécifié.

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

Pour comprendre ce qui se passe lorsqu'un client S3 supprime des objets d'un compartiment dont la réplication inter-grilles est activée, examinez comment les clients S3 suppriment des objets des compartiments dont le versionnage est activé, comme suit :

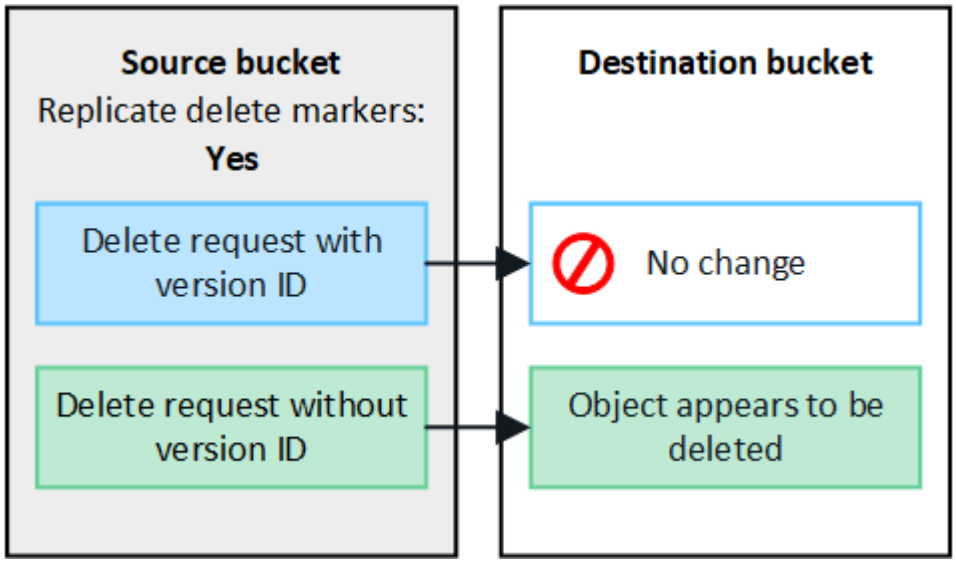
- Si un client S3 émet une requête de suppression incluant un ID de version, cette version de l'objet est définitivement supprimée. Aucun marqueur de suppression n'est ajouté au compartiment.
- Si un client S3 émet une requête de suppression sans inclure d'ID de version, StorageGRID ne supprime aucune version d'objet. À la place, il ajoute un marqueur de suppression au compartiment. Le marqueur de suppression fait en sorte que StorageGRID agisse comme si l'objet avait été supprimé :
  - Une requête GetObject sans identifiant de version échoue avec `404 No Object Found`
  - Une requête GetObject avec un ID de version valide aboutit et renvoie la version de l'objet demandée.

Lorsqu'un client S3 supprime un objet d'un compartiment sur lequel la réplication inter-grilles est activée, StorageGRID détermine s'il faut répliquer la requête de suppression vers la destination, comme suit :

- Si la requête de suppression inclut un identifiant de version, cette version de l'objet est définitivement supprimée de la grille source. Cependant, StorageGRID ne réplique pas les requêtes de suppression qui incluent un identifiant de version, de sorte que la même version de l'objet n'est pas supprimée de la destination.
- Si la demande de suppression ne contient pas d'identifiant de version, StorageGRID peut éventuellement répliquer le marqueur de suppression, en fonction de la configuration de la réplication inter-grilles pour le compartiment :
  - Si vous choisissez de répliquer les marqueurs de suppression (option par défaut), un marqueur de suppression est ajouté au compartiment source et répliqué dans le compartiment de destination. En conséquence, l'objet apparaît comme 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 n'est pas répliqué dans le compartiment de destination. En conséquence, les objets supprimés sur la grille source ne sont pas supprimés sur la grille de destination.

Dans la figure, **Répliquer les marqueurs de suppression** était défini sur **Oui** lorsque "La réplication inter-grilles a été activée". Les requêtes de suppression pour le compartiment source qui incluent un ID de version ne suppriment pas les objets du compartiment de destination. Les requêtes de suppression pour le

compartiment source qui n'incluent pas d'ID de version semblent supprimer les objets du compartiment de destination.



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

Comment les objets chiffrés sont répliqués

Lorsque vous utilisez la réplication inter-grilles pour répliquer des objets entre des grilles, vous pouvez chiffrer des objets individuellement, utiliser le chiffrement par défaut du compartiment ou configurer le chiffrement à l'échelle de la grille. Vous pouvez ajouter, modifier ou supprimer les paramètres de chiffrement par défaut du compartiment ou de la grille avant ou après avoir activé la réplication inter-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 requête et spécifiez `AES256`. Voir "Utilisez le chiffrement côté serveur".

L'utilisation de SSE-C (chiffrement côté serveur avec des clés fournies par le client) n'est pas prise en charge pour la réplication inter-grilles. L'opération d'ingestion échouera.

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

Pour utiliser le chiffrement au niveau du grid, définissez l'option **Chiffrement des objets stockés** sur **AES-256**. Le chiffrement au niveau du grid s'applique à tous les objets qui ne sont pas chiffrés au niveau du compartiment ou qui sont ingérés sans l'en-tête de requête `x-amz-server-side-encryption`. Voir "Configurer les options de réseau et d'objet".

SSE ne prend pas en charge AES-128. Si l'option **Chiffrement des objets stockés** est activée pour la grille source avec l'option **AES-128**, l'utilisation de l'algorithme AES-128 n'est pas propagée à l'objet répliqué. À la place, l'objet répliqué utilise le paramètre de chiffrement par défaut du compartiment ou de la grille de destination, si disponible.

Pour déterminer comment chiffrer les objets sources, StorageGRID applique les règles suivantes :

1. Utilisez l `x-amz-server-side-encryption`en-tête d'ingestion, s'il est présent.
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 global de la grille, s'il est configuré.
4. Si aucun paramètre global n'est présent, ne chiffrez pas l'objet source.

Pour déterminer comment chiffrer les objets répliqués, StorageGRID applique ces règles dans cet ordre :

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 s'il utilise AES-128, utilisez le paramètre de chiffrement par défaut du compartiment de destination, s'il est configuré.
3. Si le compartiment de destination ne dispose pas d'un paramètre de chiffrement, utilisez le paramètre de chiffrement global de la grille de destination, s'il est configuré.
4. Si aucun paramètre global n'est présent, ne chiffrez pas l'objet de destination.

Réplication inter-grilles avec S3 Object Lock

Vous pouvez configurer la réplication inter-grilles entre les compartiments StorageGRID avec le verrouillage d'objet S3 activé dans les circonstances suivantes.

Lorsque le verrouillage d'objet S3 sur le compartiment source est…	Et le verrouillage d'objet S3 sur le compartiment de destination est…
Activé	Activé
Désactivées	Activé

Lorsque le verrouillage d'objet S3 sur le compartiment source est activé :

- Les objets sont verrouillés avec des paramètres de rétention à destination dans cet ordre :
  a. Les valeurs d'en-tête de rétention de l'objet source pour :

     `x-amz-object-lock-mode`

     `x-amz-object-lock-retain-until-date`

  b. Durée de rétention par défaut du compartiment source, si elle est définie.
  c. La durée de rétention par défaut du compartiment de destination, si elle est définie.

  La durée de rétention par défaut du compartiment de destination ne remplace pas les paramètres de rétention répliqués à partir de l'objet source.

- Vous pouvez définir le statut de rétention légale de l'objet de destination en utilisant `x-amz-object-lock-legal-hold` lors du chargement de l'objet.
- Une erreur se produit si le locataire ou le compartiment de destination ne prend pas en charge les paramètres de S3 Object Lock de l'objet source. Consultez "Alertes et erreurs de réplication inter-grilles."

Lorsque le verrouillage d'objet S3 sur le compartiment source est désactivé :

- Vous pouvez configurer la rétention par défaut sur le compartiment de destination pour appliquer les paramètres de rétention S3 Object Lock à l'objet de destination.
- L'objet de destination ne peut pas définir de statut de rétention légale.

PutObjectTagging et DeleteObjectTagging ne sont pas pris en charge

PutObjectTagging et DeleteObjectTagging ne sont pas prises en charge pour les objets dans des compartiments ayant la réplication inter-grilles activée.

Si un client S3 émet une requête PutObjectTagging ou DeleteObjectTagging, `501 Not Implemented` est renvoyé. Le message est `Put(Delete) ObjectTagging isn't available for buckets that have cross-grid replication configured`.

PutObjectRetention et PutObjectLegalHold ne sont pas pris en charge

PutObjectRetention et PutObjectLegalHold ne sont pas entièrement prises en charge pour les objets dans des compartiments ayant la réplication inter-grilles activée.

Si un client S3 émet une requête PutObjectRetention ou une requête PutObjectLegalHold, les paramètres de l'objet source sont modifiés, mais les modifications ne sont pas appliquées à la destination.

Comment les objets segmentés sont répliqués

La taille maximale des segments de la grille source s'applique aux objets répliqués vers la grille de destination. Lorsque des objets sont répliqués vers une autre grille, le paramètre **Taille maximale des segments** (**Configuration** > **Système** > **Options de stockage**) de la grille source est utilisé sur les deux grilles. Par exemple, supposons que la taille maximale des segments de la grille source soit de 1 Go, tandis que la taille maximale des segments de la grille de destination soit de 50 Mo. Si vous ingérez un objet de 2 Go sur la grille source, cet objet est enregistré en deux segments de 1 Go. Il est également répliqué vers la grille de destination en deux segments de 1 Go, même si la taille maximale des segments de cette grille est de 50 Mo.

Comparer la réplication inter-grilles et la réplication CloudMirror dans StorageGRID

Lorsque vous commencez à utiliser la fédération de grilles, examinez les similitudes et les différences entre "réplication inter-grilles" et le "Service de réplication CloudMirror StorageGRID".

> Vous ne pouvez pas utiliser CloudMirror sur un bucket répliqué par réplication inter-grilles, et inversement.

	Réplication inter-grilles	CloudMirror service de réplication
Quel est l'objectif principal ?	Un système StorageGRID fait office de système de reprise après sinistre. Les objets d'un bucket peuvent être répliqués entre les grilles dans un sens ou dans les deux sens.	Permet à un locataire de répliquer automatiquement des objets d'un compartiment dans StorageGRID (source) vers un compartiment S3 externe (destination). CloudMirror replication crée une copie indépendante d'un objet dans une infrastructure S3 indépendante. Cette copie indépendante n'est pas utilisée comme sauvegarde, mais est souvent traitée ultérieurement dans le cloud.
Comment est-ce configuré ?	1. Configurez une connexion de fédération de grilles entre deux grilles. 2. Ajoutez de nouveaux comptes locataires, qui sont automatiquement clonés sur l'autre grille. 3. Ajoutez de nouveaux groupes de locataires et utilisateurs, qui sont également clonés. 4. Créez des compartiments correspondants sur chaque grille et activez la réplication inter-grilles dans un sens ou dans les deux sens.	1. Un utilisateur locataire configure la réplication CloudMirror en définissant un point de terminaison CloudMirror (adresse IP, informations d'identification, etc.) à l'aide du Tenant Manager ou de l'API S3. 2. Tout compartiment appartenant à ce compte locataire peut être configuré pour pointer vers le point de terminaison CloudMirror.
Qui est responsable de sa mise en place ?	• Un administrateur de grille configure la connexion et les tenants. • 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 de grille.	• Toute infrastructure S3 compatible (y compris Amazon S3). • Google Cloud Platform (GCP)
Le versionnage des objets est-il nécessaire ?	Oui, les compartiments source et de destination doivent tous deux avoir le versionnage des objets activé.	Non, la réplication CloudMirror prend en charge toute combinaison de compartiments non versionnés et versionnés, aussi bien à la source qu'à la destination.

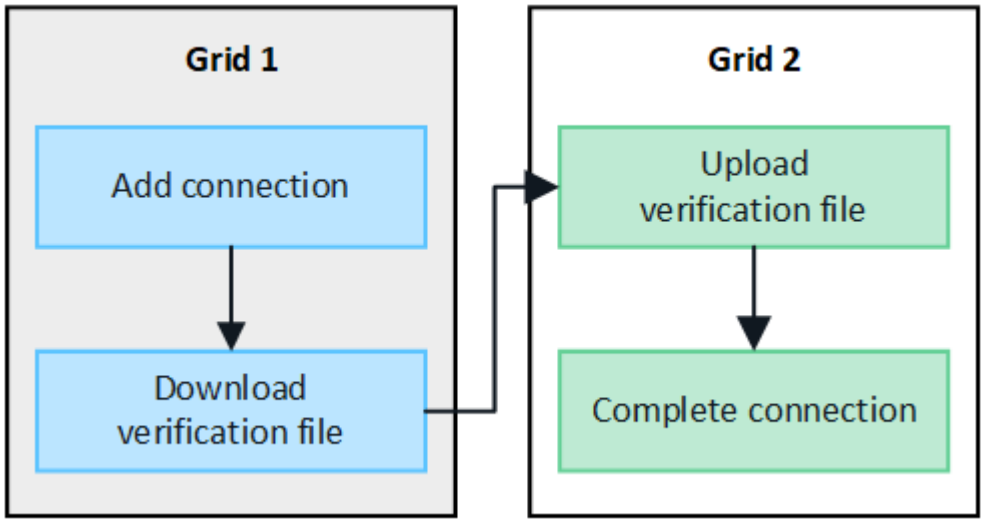
	Réplication inter-grilles	CloudMirror service de réplication
Qu'est-ce qui provoque le déplacement des objets vers la destination ?	Les objets sont automatiquement répliqués lorsqu'ils sont ajoutés à un compartiment qui a la réplication inter-grilles activée.	Les objets sont automatiquement répliqués lorsqu'ils sont ajoutés à un compartiment configuré avec un point de terminaison CloudMirror. Les objets présents dans le compartiment source avant que ce dernier ne soit configuré avec le point de terminaison CloudMirror ne sont pas répliqués, sauf s'ils sont modifiés.
Comment les objets sont-ils répliqués ?	La réplication inter-grilles crée des objets versionnés et réplique l'identifiant de version du compartiment source vers le compartiment de destination. Cela permet de conserver l'ordre des versions entre les deux grilles.	CloudMirror replication ne nécessite pas de compartiments avec versionnage activé, donc CloudMirror ne peut maintenir l'ordre d'une clé qu'au sein d'un site. Il n'y a aucune garantie que l'ordre sera maintenu pour les requêtes adressées à un objet sur un site différent.
Que se passe-t-il si un objet ne peut pas être répliqué ?	L'objet est mis en file d'attente pour réplication, sous réserve des limites de stockage des métadonnées.	L'objet est mis en file d'attente pour la réplication, sous réserve des limites des services de la plateforme (voir "Recommandations pour l'utilisation des services de la plateforme").
Les métadonnées système de l'objet sont-elles répliquées ?	Oui, lorsqu'un objet est répliqué sur l'autre grille, ses métadonnées système sont également répliquées. Les métadonnées seront identiques sur les deux grilles.	Non, lorsqu'un objet est répliqué dans le compartiment externe, ses métadonnées système sont mises à jour. Les métadonnées diffèrent selon l'emplacement, en fonction de l'heure d'ingestion et du comportement de l'infrastructure S3 indépendante.
Comment les objets sont-ils récupérés ?	Les applications peuvent récupérer ou lire des objets en effectuant une requête auprès du compartiment sur l'une ou l'autre grille.	Les applications peuvent récupérer ou lire des objets en effectuant une requête auprès de StorageGRID ou de la destination S3. Par exemple, supposons que vous utilisez la réplication CloudMirror pour dupliquer des objets vers une organisation partenaire. Le partenaire peut utiliser ses propres applications pour lire ou mettre à jour des objets directement depuis la destination S3. L'utilisation de StorageGRID n'est pas requise.

	Réplication inter-grilles	CloudMirror service de réplication
Que se passe-t-il si un objet est supprimé ?	• Les demandes de suppression incluant un ID de version ne sont jamais répliquées vers la grille de destination. • Les demandes de suppression qui n'incluent pas d'identifiant de version ajoutent un marqueur de suppression au compartiment source, qui peut éventuellement être répliqué vers la grille de destination. • Si la réplication inter-grille est configurée dans un seul sens, les objets du compartiment de destination peuvent être supprimés sans affecter la source.	Les résultats varieront en fonction de l'état de version des compartiments source et de destination (qui n'ont pas besoin d'être identiques) : • Si les deux compartiments sont versionnés, une demande de suppression ajoutera un marqueur de suppression dans les deux emplacements. • Si seul le compartiment source est versionné, une requête de suppression ajoutera un marqueur de suppression à la source mais pas à la destination. • Si aucun des deux compartiments n'est versionné, une requête de suppression supprimera 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 StorageGRID

Vous pouvez créer une connexion de fédération de grilles entre deux systèmes StorageGRID si vous souhaitez cloner les détails du locataire et répliquer les données des objets.

Comme illustré, la création d'une connexion de fédération de grilles nécessite des étapes sur les deux grilles. Vous ajoutez la connexion sur une grille et la complétez sur l'autre grille. Vous pouvez commencer à partir de l'une ou l'autre grille.



Avant de commencer

- Vous avez examiné la "considérations et exigences" pour la configuration des 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 possède les entrées appropriées.
- Vous utilisez un "navigateur Web pris en charge".
- Vous disposez des droits d'accès Root et de la phrase secrète de provisionnement pour les deux grilles.

Ajouter une connexion

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

Étapes

1. Connectez-vous au Gestionnaire de grille depuis le nœud d'administration principal de l'une ou l'autre grille.
2. Sélectionnez **Configuration** > **System** > **Grid federation**.
3. Sélectionnez **Ajouter une connexion**.
4. Saisissez les détails de la connexion.

Champ	Description
Nom de la connexion	Un nom unique pour vous aider à reconnaître cette connexion, par exemple, « Grid 1-Grid 2 ».
FQDN ou adresse IP pour cette grille	L'un des éléments suivants : • Le nom de domaine complet (FQDN) de la grille à laquelle vous êtes actuellement connecté • Adresse VIP d'un groupe HA sur cette grille • Adresse IP d'un nœud d'administration ou d'un nœud passerelle sur cette grille. L'adresse IP peut être sur n'importe quel réseau que la grille de destination peut atteindre.
Port	Le port que vous souhaitez utiliser pour cette connexion. Vous pouvez saisir n'importe quel numéro de port inutilisé entre 23000 et 23999. Les deux grilles de cette connexion utiliseront le même port. Vous devez vous assurer qu'aucun nœud dans l'une ou l'autre grille n'utilise ce port pour d'autres connexions.
Jours de validité du certificat pour cette grille	Le nombre de jours pendant lesquels vous souhaitez que les certificats de sécurité pour cette grille dans la connexion soient valides. La valeur par défaut est de 730 jours (2 ans), mais vous pouvez saisir 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	La phrase secrète de provisionnement pour la grille à laquelle vous êtes connecté.
FQDN ou adresse IP pour l'autre grid	L'un des éléments suivants : • Le domaine complet (FQDN) de la grille à laquelle vous souhaitez vous connecter • Une adresse VIP d'un groupe HA sur l'autre grille • Adresse IP d'un nœud d'administration ou d'un nœud passerelle sur l'autre grille. L'adresse IP peut être sur n'importe quel réseau que la grille source peut atteindre.

5. Sélectionnez **Enregistrer et continuer**.
6. Pour l'étape Télécharger le fichier de vérification, sélectionnez **Télécharger le fichier de vérification**.

   Une fois la connexion établie sur l'autre grid, vous ne pourrez plus télécharger le fichier de vérification depuis aucun des deux grids.

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

   > ⚠ Ce fichier contient des secrets (masqués comme *****) et d'autres informations sensibles et doit être stocké et transmis en toute sécurité.

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

Connexion complète

Effectuez ces étapes sur le système StorageGRID auquel vous vous connectez (l'autre grille).

Étapes

1. Connectez-vous au Gestionnaire de grille depuis le nœud d'administration principal.
2. Sélectionnez **Configuration** > **System** > **Grid federation**.
3. Sélectionnez **Téléverser un fichier de vérification** pour accéder à la page de téléversement.
4. Sélectionnez **Téléverser le fichier de vérification**. Ensuite, recherchez et sélectionnez le fichier téléchargé depuis la première grille (*`connection-name`*`.grid-federation`).

   Les détails de la connexion sont affichés.

5. Vous pouvez également saisir un nombre différent de jours de validité pour les certificats de sécurité de cette grille. Le champ **Durée de validité du certificat** reprend par défaut la valeur saisie dans la première grille, mais chaque grille peut utiliser une date d'expiration différente.

   En règle générale, utilisez le même nombre de jours pour les certificats des deux côtés de la connexion.

Si les certificats à l'une ou l'autre extrémité de la connexion expirent, la connexion cessera de fonctionner et les réplications seront en attente jusqu'à ce que les certificats soient mis à jour.

6. Saisissez la phrase secrète de provisionnement de 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 confirmation s'affiche et la nouvelle connexion est répertoriée sur la page de fédération Grid. L'état de la connexion sera **Connecté**.

   Si un message d'erreur apparaît, corrigez les problèmes rencontrés. Voir "Dépanner les erreurs de fédération de grille".

8. Accédez à la page de fédération de grilles de la première grille et actualisez le navigateur. Confirmez que l'état de la connexion est maintenant « Connecté ».
9. Une fois la connexion établie, supprimez en toute sécurité toutes les copies du fichier de vérification.

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

Après avoir terminé

- Examinez les éléments à prendre en compte pour "gestion des locataires autorisés".
- "Créez un ou plusieurs nouveaux comptes locataires", attribuez l'autorisation **Utiliser la connexion de fédération de grille** et sélectionnez la nouvelle connexion.
- "Gérer la connexion" si nécessaire. Vous pouvez modifier les valeurs de connexion, tester une connexion, renouveler les certificats de connexion ou supprimer une connexion.
- "Surveillez la connexion" dans le cadre de vos activités habituelles de surveillance StorageGRID.
- "Résoudre les problèmes de connexion", y compris la résolution de toute alerte et erreur liée au clonage de compte et à la réplication inter-grilles.

Gérer les connexions de fédération de grille StorageGRID

La gestion des connexions de fédération de grilles entre les systèmes StorageGRID comprend la modification des détails de connexion, la rotation des certificats, la suppression des autorisations des locataires et la suppression des connexions inutilisées.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille sur l'une ou l'autre grille à l'aide d'un "navigateur Web pris en charge".
- Vous disposez des "Autorisation d'accès root" pour la grille à laquelle vous êtes connecté.

Modifier une connexion de fédération de grille

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

Pendant la modification de la connexion, les demandes de clonage de compte ou de réplication entre grilles continueront d'utiliser les paramètres de connexion existants. Les modifications que vous apportez à la première grille sont enregistrées localement, mais ne sont utilisées qu'une fois qu'elles ont été téléchargées vers la seconde grille, enregistrées et testées.

Commencez à modifier la connexion

Étapes

1. Connectez-vous au Gestionnaire de grille depuis le nœud d'administration principal de l'une ou l'autre grille.
2. Sélectionnez **Nœuds** et vérifiez que tous les autres Admin Nodes de votre système sont en ligne.

   Lorsque vous modifiez une connexion de fédération de grilles, StorageGRID tente d'enregistrer un fichier de « configuration candidate » sur tous les nœuds d'administration de la première grille. Si ce fichier ne peut pas être enregistré sur tous les nœuds d'administration, un message d'avertissement s'affiche lorsque vous sélectionnez **Enregistrer et tester**.

3. Sélectionnez **Configuration** > **System** > **Grid federation**.
4. Modifiez les détails de la connexion à l'aide du menu **Actions** sur la page de fédération Grid ou sur la page de détails d'une connexion spécifique. Consultez "Créer des connexions de fédération de grille" pour savoir quoi saisir.

   Menu Actions

   a. Sélectionnez le bouton radio pour la connexion.
   b. Sélectionnez **Actions** > **Modifier**.
   c. Saisissez les nouvelles informations.

   Page de détails

   a. Sélectionnez un nom de connexion pour afficher ses détails.
   b. Sélectionnez **Modifier**.
   c. Saisissez les nouvelles informations.

5. Saisissez la phrase secrète de provisionnement pour la grille à laquelle vous êtes connecté.
6. Sélectionnez **Enregistrer et continuer**.

   Les nouvelles valeurs sont enregistrées, mais elles ne seront appliquées à la connexion que lorsque vous aurez téléchargé le nouveau fichier de vérification sur l'autre grid.

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`, puis enregistrez-le dans un emplacement sûr.

Le fichier de vérification contient des informations confidentielles et doit être stocké et transmis de manière sécurisée.

9. Sélectionnez **Fermer** pour revenir à la page de fédération Grid.
10. Confirmez 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. Transmettez le *connection-name*`.grid-federation` fichier à l'administrateur de l'autre grille.

Terminez la modification de la connexion

Terminez la modification de la connexion en téléchargeant le fichier de vérification sur l'autre grid.

Étapes

1. Connectez-vous au Gestionnaire de grille depuis le nœud d'administration principal.
2. Sélectionnez **Configuration** > **System** > **Grid federation**.
3. Sélectionnez **Téléverser le fichier de vérification** pour accéder à la page de téléversement.
4. Sélectionnez **Téléverser le fichier de vérification**. Ensuite, recherchez et sélectionnez le fichier téléchargé depuis la première grille.
5. Saisissez la phrase secrète de provisionnement de la grille à laquelle vous êtes actuellement connecté.
6. Sélectionnez **Enregistrer et tester**.

   Si la connexion peut être établie avec les valeurs modifiées, un message de confirmation s'affiche. Sinon, un message d'erreur s'affiche. Examinez le message et résolvez tout problème.

7. Fermez l'assistant pour revenir à la page de fédération Grid.
8. Confirmez que l'état de la **connexion** est **Connecté**.
9. Accédez à la page de fédération de grilles de la première grille et actualisez le navigateur. Confirmez que l'état de la connexion est maintenant « Connecté ».
10. Une fois la connexion établie, supprimez en toute sécurité toutes les copies du fichier de vérification.

Tester une connexion de fédération de grille

Étapes

1. Connectez-vous au Gestionnaire de grille depuis le nœud d'administration principal.
2. Sélectionnez **Configuration** > **System** > **Grid federation**.
3. Testez la connexion à l'aide du menu **Actions** sur la page de fédération Grid ou sur la page de détails d'une connexion spécifique.

Menu Actions

a. Sélectionnez le bouton radio pour la connexion.

b. Sélectionnez **Actions** > **Test**.

Page de détails

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

b. Sélectionnez **Test connection**.

4. Vérifiez l'état de la connexion :

État de la connexion	Description
Connecté	Les deux grids sont connectés 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.
En attente de modification	Vous avez modifié la connexion sur cette grille, mais celle-ci utilise toujours la configuration existante. Pour finaliser la modification, téléversez le nouveau fichier de vérification sur l'autre grille.
En attente de connexion	Vous avez configuré la connexion sur cette grille, mais celle-ci n'est pas encore établie sur l'autre grille. Téléchargez le fichier de vérification depuis cette grille et chargez-le sur l'autre grille.
Inconnu	La connexion est dans un état inconnu, probablement en raison d'un problème de réseau ou d'un nœud hors ligne.

5. Si l'état de la connexion est **Erreur**, résolvez tout problème. Ensuite, sélectionnez à nouveau **Tester la connexion** pour confirmer que le problème a été résolu.

Rotation des certificats de connexion

Chaque connexion de fédération de grilles utilise quatre certificats SSL générés automatiquement pour sécuriser la connexion. Lorsque les deux certificats de chaque grille approchent de leur date d'expiration, l'alerte **Expiration of grid federation certificate** vous rappelle de renouveler les certificats.

> Si les certificats à l'une ou l'autre extrémité de la connexion expirent, la connexion cessera de fonctionner et les réplications seront en attente jusqu'à ce que les certificats soient mis à jour.

Étapes

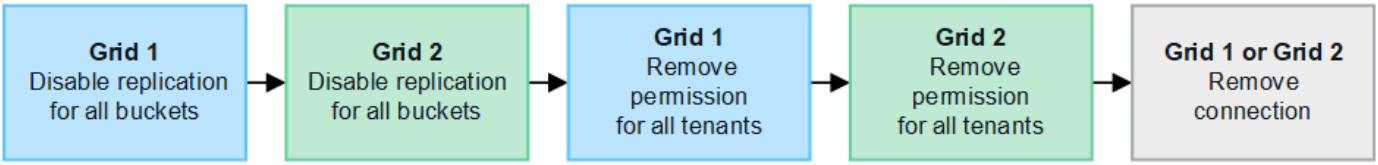
1. Connectez-vous au Gestionnaire de grille depuis le nœud d'administration principal de l'une ou l'autre grille.
2. Sélectionnez **Configuration** > **System** > **Grid federation**.
3. Depuis l'un ou l'autre onglet de la page de fédération Grid, sélectionnez le nom de la connexion pour afficher ses détails.

4. Sélectionnez l'onglet **Certificats**.
5. Sélectionnez **Faire pivoter les certificats**.
6. Indiquez combien de jours les nouveaux certificats doivent être valides.
7. Saisissez la phrase secrète de provisionnement pour la grille à laquelle vous êtes connecté.
8. Sélectionnez **Faire pivoter les certificats**.
9. Si nécessaire, répétez ces étapes sur l'autre grille de la connexion.

   En règle générale, utilisez le même nombre de jours pour les certificats des deux côtés de la connexion.

Supprimer une connexion de fédération de grille

Vous pouvez supprimer une connexion de fédération de grilles depuis l'une ou l'autre des grilles. Comme illustré, vous devez effectuer les étapes préalables sur les deux grilles pour vérifier que la connexion n'est utilisée par aucun 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 déjà copiés entre les grilles. Par exemple, les utilisateurs, groupes et objets du locataire présents dans les deux grilles ne sont supprimés d'aucune des deux grilles lorsque l'autorisation du locataire est supprimée. Si vous souhaitez supprimer ces éléments, vous devez les supprimer manuellement des deux grilles.
- Lorsque vous supprimez une connexion, tous les objets en attente de réplication (ingérés mais pas encore répliqués sur l'autre grille) verront leur réplication définitivement échouer.

Désactivez la réplication pour tous les compartiments locataires

Étapes

1. Depuis l'une ou l'autre grille, connectez-vous au Grid Manager depuis le nœud d'administration principal.
2. Sélectionnez **Configuration** > **System** > **Grid federation**.
3. Sélectionnez le nom de la connexion pour afficher ses détails.
4. Dans l'onglet **Locataires autorisés**, déterminez si la connexion est utilisée par des locataires.
5. Si des locataires sont répertoriés, demandez à tous les locataires de "désactiver la réplication inter-grilles" le faire pour tous leurs compartiments sur les deux grilles de la connexion.

> Vous ne pouvez pas supprimer l'autorisation **Utiliser la connexion de fédération de grilles** si des compartiments locataires ont la réplication inter-grilles activée. Chaque compte locataire doit désactiver la réplication inter-grilles pour ses compartiments sur les deux grilles.

Supprimez l'autorisation pour chaque locataire

Une fois la réplication inter-grilles désactivée pour tous les compartiments locataires, supprimez l'autorisation **Utiliser la fédération de grilles** de tous les locataires sur les deux grilles.

Étapes

1. Sélectionnez **Configuration** > **System** > **Grid federation**.
2. Sélectionnez le nom de la connexion pour afficher ses détails.
3. Pour chaque locataire figurant dans l'onglet **Locataires autorisés**, supprimez l'autorisation **Utiliser la connexion de fédération de grille** pour chaque locataire. Voir "Gérer les locataires autorisés".
4. Répétez ces étapes pour les locataires autorisés sur l'autre grille.

Supprimer la connexion

Étapes

1. Lorsque aucun locataire sur l'une ou l'autre grille n'utilise la connexion, sélectionnez **Supprimer**.
2. Vérifiez le message de confirmation, puis sélectionnez **Supprimer**.
   - Si la connexion peut être supprimée, un message de confirmation s'affiche. La connexion de fédération de grilles est désormais supprimée des deux grilles.
   - Si la connexion ne peut pas être supprimée (par exemple, si elle est toujours utilisée ou en cas d'erreur de connexion), un message d'erreur s'affiche. Vous pouvez effectuer l'une des actions suivantes :
     - Résolvez l'erreur (recommandé). Voir "Dépanner les erreurs de fédération de grille".
     - Supprimez la connexion de force. Voir la section suivante.

Supprimer de force une connexion de fédération de grille

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

La suppression forcée ne supprime la connexion que du grid local. Pour supprimer complètement la connexion, effectuez les mêmes étapes sur les deux grids.

Étapes

1. Dans la boîte de dialogue de confirmation, sélectionnez **Force remove**.

   Un message de confirmation s'affiche. Cette connexion de fédération de grilles ne peut plus être utilisée. Cependant, certains compartiments locataires peuvent encore avoir la réplication inter-grilles activée et certaines copies d'objets peuvent déjà avoir été répliquées entre les grilles de la connexion.

2. Depuis l'autre grille de la connexion, connectez-vous au Grid Manager depuis le nœud d'administration principal.
3. Sélectionnez **Configuration** > **System** > **Grid federation**.
4. Sélectionnez le nom de la connexion pour afficher ses détails.
5. Sélectionnez **Supprimer** et **Oui**.
6. Sélectionnez **Force remove** pour supprimer la connexion de cette grille.

Gérer les locataires autorisés pour la fédération de grilles StorageGRID

Vous pouvez autoriser les comptes locataires S3 à utiliser une connexion de fédération de grille entre deux systèmes StorageGRID. Lorsqu'un locataire est autorisé à utiliser une connexion, des étapes spécifiques sont nécessaires pour modifier les détails du locataire ou pour retirer définitivement l'autorisation d'utiliser la connexion.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille sur l'une ou l'autre grille à l'aide d'un "navigateur Web pris en charge".
- Vous disposez des "Autorisation d'accès root" pour la grille à laquelle vous êtes connecté.
- Vous avez "a créé une connexion de fédération de grille" entre deux grilles.
- Vous avez examiné les flux de travail pour "clone de compte" et "réplication inter-grilles".
- Comme requis, vous avez déjà configuré l'authentification unique (SSO) ou la fédération d'identité pour les deux grilles de la connexion. Voir "Qu'est-ce qu'un clone de compte".

Créer un locataire autorisé

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

- Vous pouvez créer le locataire à partir de l'une ou l'autre grille de la connexion. La grille sur laquelle un locataire est créé est la *grille source du locataire*.
- L'état de la connexion doit être **Connected**.
- Lorsqu'un locataire est créé ou modifié pour activer l'autorisation **Utiliser la connexion de fédération de grilles**, puis enregistré sur la première grille, un locataire identique est automatiquement répliqué sur l'autre grille. La grille sur laquelle le locataire est répliqué est la *grille de destination* du locataire.
- Les locataires des deux grilles auront le même identifiant de compte à 20 chiffres, le même nom, la même description, le même quota et les mêmes autorisations. Vous pouvez éventuellement utiliser le champ **Description** pour vous aider à identifier lequel est le locataire source et lequel est le locataire de destination. Par exemple, cette description pour un locataire créé sur la grille 1 apparaîtra également pour le locataire répliqué sur la grille 2 : « Ce locataire a été créé sur la grille 1. »
- Pour des raisons de sécurité, le mot de passe de l'utilisateur root local n'est pas copié sur la grille de destination.

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

- Une fois le locataire nouveau ou modifié disponible sur les deux grilles, les utilisateurs locataires peuvent effectuer les opérations suivantes :
  - À partir de 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 les groupes de locataires et les utilisateurs".
  - Créez de nouvelles clés d'accès S3, qui peuvent être clonées en option 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 de la connexion et activez la réplication inter-grilles dans un sens ou dans les deux sens. Voir "Gérer la réplication inter-grilles".

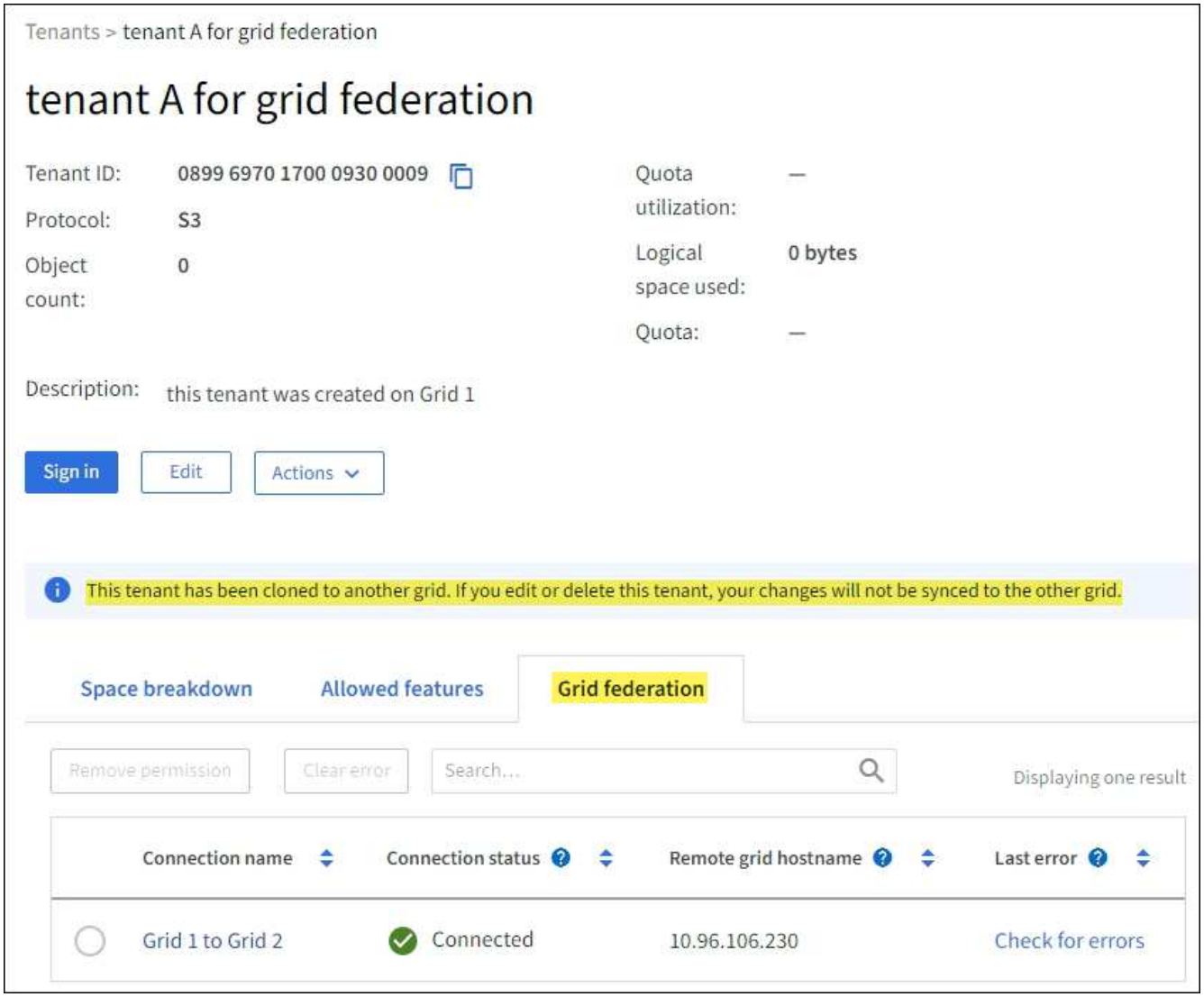
Afficher un locataire autorisé

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

Étapes

1. Sélectionnez **Tenants**.
2. Depuis la page Locataires, sélectionnez le nom du locataire pour afficher la page de détails du locataire.

   Si cette grille est la grille source du locataire (c'est-à-dire si le locataire a été créé sur cette grille), une bannière s'affiche pour vous rappeler que le locataire a été cloné sur une autre grille. Si vous modifiez ou supprimez ce locataire, vos modifications ne seront pas synchronisées avec l'autre grille.



3. Vous pouvez également sélectionner l'onglet **Fédération de grilles** pour "surveiller la connexion de la fédération du grid".

Modifier un locataire autorisé

Si vous devez modifier un locataire disposant de l'autorisation **Utiliser la connexion de fédération de grille**, suivez les instructions générales "modification d'un compte locataire" et tenez compte des points suivants :

- Si un locataire dispose de l'autorisation **Utiliser la connexion de fédération de grilles**, vous pouvez modifier les informations du locataire depuis l'une ou l'autre grille de la connexion. Cependant, toute modification que vous effectuez ne sera pas copiée sur l'autre grille. Si vous souhaitez que les informations du locataire restent synchronisées entre les grilles, vous devez effectuer les mêmes modifications sur les deux grilles.

- Vous ne pouvez pas supprimer l'autorisation **Utiliser la connexion de fédération de grille** lorsque vous modifiez un locataire.
- Vous ne pouvez pas sélectionner une connexion de fédération de grille différente lorsque vous modifiez un locataire.

Supprimer un locataire autorisé

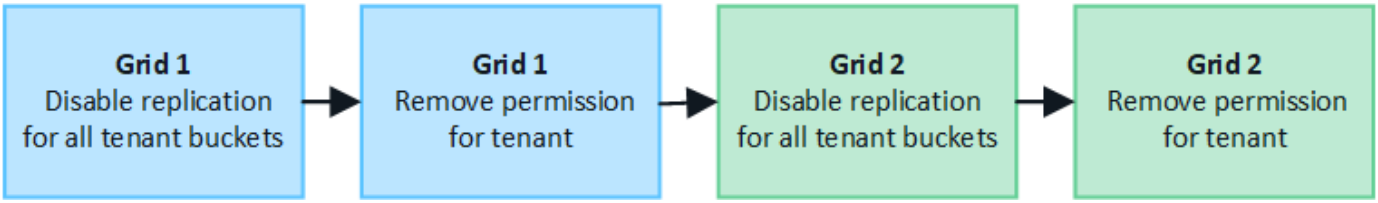
Si vous devez supprimer un locataire disposant de l'autorisation **Utiliser la connexion de fédération de grille**, suivez les instructions générales "suppression d'un compte locataire" et tenez compte des points suivants :

- Avant de pouvoir supprimer le locataire d'origine sur la grille source, vous devez supprimer tous les compartiments pour le compte sur la grille source.
- Avant de pouvoir supprimer le locataire cloné sur la grille de destination, vous devez supprimer tous les compartiments du compte sur la grille de destination.
- Si vous supprimez le locataire d'origine ou le locataire cloné, le compte ne pourra plus être utilisé pour la réplication inter-grille.
- Si vous supprimez le locataire d'origine sur la grille source, tous les groupes, utilisateurs ou clés de locataire clonés vers la grille de destination resteront inchangés. 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 produiront si de nouveaux groupes ou utilisateurs sont ajoutés au locataire d'origine.

  Pour éviter ces erreurs, supprimez l'autorisation du locataire d'utiliser la connexion de fédération de grille avant de supprimer le locataire de cette grille.

Supprimer l'autorisation d'utiliser la connexion à la fédération de grille

Pour empêcher un locataire d'utiliser une connexion de fédération de grille, vous devez supprimer l'autorisation **Utiliser une connexion de fédération de grille**.



Avant de retirer à un locataire l'autorisation 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 du locataire doit d'abord désactiver la réplication inter-grille pour tous ses compartiments.
- La suppression de l'autorisation « Utiliser la connexion de fédération de grilles » ne supprime pas les éléments déjà répliqués entre les grilles. Par exemple, les utilisateurs, groupes et objets du locataire présents sur les deux grilles ne sont supprimés d'aucune des deux grilles lorsque l'autorisation du locataire est retirée. 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 grilles » définit la grille locale comme grille source et déclenche le clonage vers la grille distante spécifiée par la connexion de fédération de grilles sélectionnée. Si le compte du locataire existe déjà sur la grille distante, le clonage entraînera une erreur de conflit.

Avant de commencer

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

Désactiver la réplication pour les compartiments locataires

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

Étapes

1. Depuis l'une ou l'autre grille, connectez-vous au Grid Manager depuis le nœud d'administration principal.
2. Sélectionnez **Configuration** > **System** > **Grid federation**.
3. Sélectionnez le nom de la connexion pour afficher ses détails.
4. Dans l'onglet **Locataires autorisés**, déterminez si le locataire utilise la connexion.
5. Si le locataire est répertorié, demandez-lui de "désactiver la réplication inter-grilles" le faire pour tous ses compartiments sur les deux grilles de la connexion.

Vous ne pouvez pas supprimer l'autorisation **Utiliser la connexion de fédération de grilles** si la réplication inter-grilles est activée pour au moins un compartiment locataire. Le locataire doit désactiver la réplication inter-grilles pour ses compartiments sur les deux grilles.

Supprimer l'autorisation du locataire

Une fois la réplication inter-grilles désactivée pour les compartiments de locataire, vous pouvez supprimer l'autorisation du locataire d'utiliser la connexion de fédération de grilles.

Étapes

1. Connectez-vous au Gestionnaire de grille depuis le nœud d'administration principal.
2. Supprimez l'autorisation depuis la page de fédération Grid ou la page des locataires.

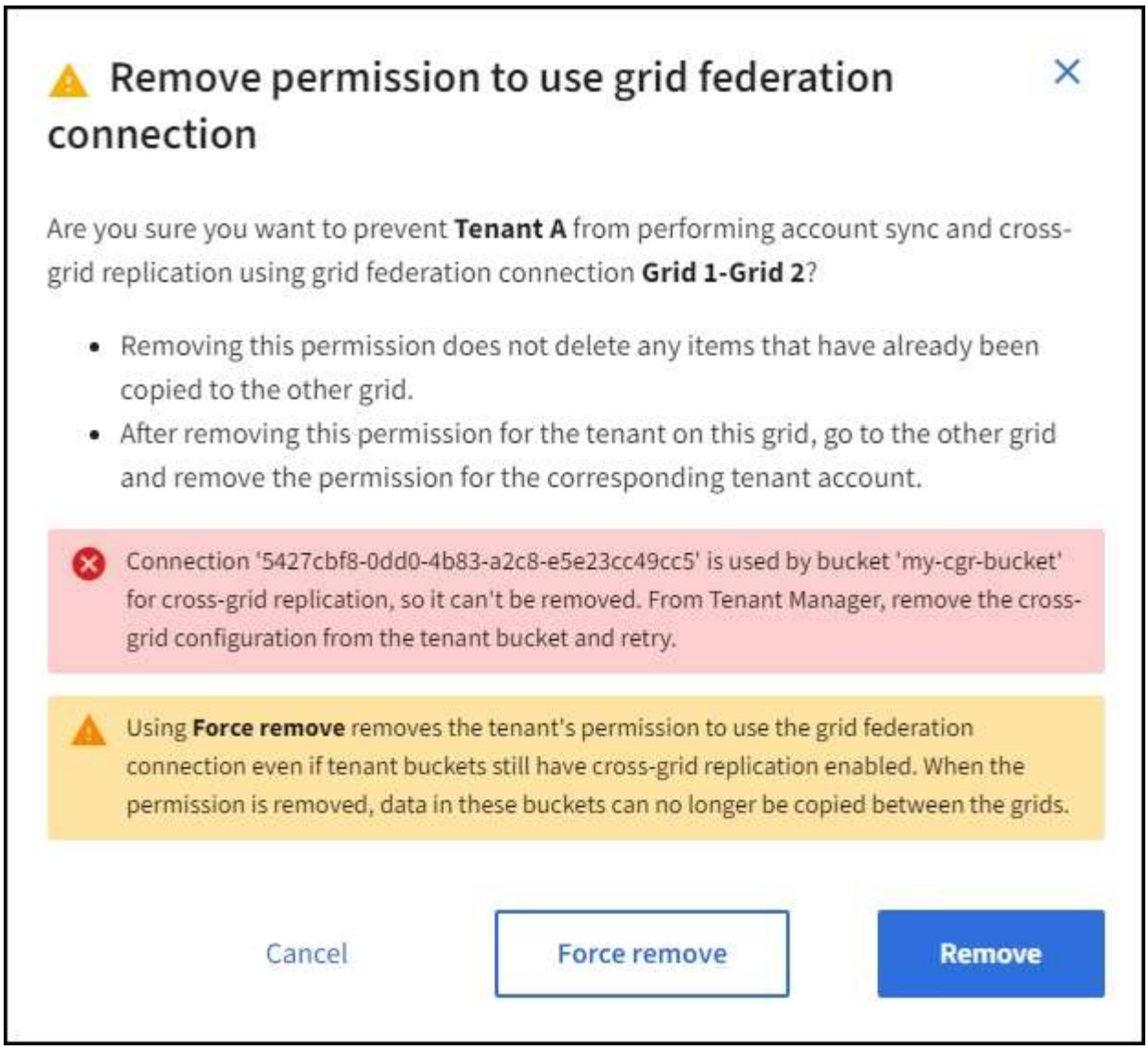
page de fédération de grille

a. Sélectionnez **Configuration** > **System** > **Grid federation**.
b. Sélectionnez le nom de la connexion pour afficher sa page de détails.
c. Dans l'onglet **Locataires autorisés**, sélectionnez le bouton radio correspondant au locataire.
d. Sélectionnez **Supprimer l'autorisation**.

Page des locataires

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

3. Examinez les avertissements dans la boîte de dialogue de confirmation et sélectionnez **Supprimer**.
   - Si l'autorisation peut être supprimée, vous êtes redirigé vers la page de détails et un message de confirmation s'affiche. Ce locataire ne peut plus utiliser la connexion de fédération de grille.
   - Si un ou plusieurs compartiments locataires ont encore la réplication inter-grille activée, une erreur s'affiche.



Vous pouvez faire l'une ou l'autre des choses suivantes :

- (Recommandé.) Connectez-vous au Tenant Manager et désactivez la réplication pour chaque compartiment du locataire. Voir "Gérer la réplication inter-grilles". Ensuite, répétez les étapes pour supprimer l'autorisation **Use grid connection**.
- Supprimez l'autorisation de force. Voir la section suivante.

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

Supprimer l'autorisation de force

Si nécessaire, vous pouvez forcer la suppression de l'autorisation d'un locataire à utiliser une connexion de fédération de grille, même si les compartiments du locataire ont la réplication inter-grille activée.

Avant de retirer de force l'autorisation d'un locataire, veuillez prendre en compte les considérations générales suppression de l'autorisation ainsi que les considérations supplémentaires suivantes :

- Si vous supprimez de force l'autorisation « Utiliser la connexion de fédération de grilles », 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 de traitement d'atteindre le compartiment de destination, vous devez

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

- 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 Gestionnaire de grille depuis le nœud d'administration principal.
2. Sélectionnez **Configuration** > **System** > **Grid federation**.
3. Sélectionnez le nom de la connexion pour afficher sa page de détails.
4. Dans l'onglet **Locataires autorisés**, sélectionnez le bouton radio correspondant au locataire.
5. Sélectionnez **Supprimer l'autorisation**.
6. Examinez les avertissements dans la boîte de dialogue de confirmation et sélectionnez **Force remove**.

   Un message de confirmation 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 supprimer de force l'autorisation du même compte client sur l'autre grille. Par exemple, vous devez répéter ces étapes sur l'autre grille pour empêcher les objets en cours de traitement d'atteindre le compartiment de destination.

Dépanner les erreurs de fédération de grille dans StorageGRID

Vous pourriez avoir besoin de résoudre des alertes et des erreurs liées aux connexions de fédération de grilles, au clonage de comptes et à la réplication inter-grilles.

Alertes et erreurs de connexion à la fédération de grilles

Vous pourriez recevoir des alertes ou rencontrer des erreurs concernant 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 redevient **Connecté**. Pour obtenir des instructions, consultez "Gérer les connexions de fédération de grille".

Alerte d'échec de connexion à la fédération de grille

Problème

L'alerte **Échec de la connexion à la fédération du grid** a été déclenchée.

Détails

Cette alerte indique que la connexion de fédération de grilles entre les grilles ne fonctionne pas.

Actions recommandées

1. Vérifiez les paramètres de la page Fédération de grilles pour les deux grilles. Assurez-vous 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 aucune alerte concernant l'expiration des certificats de fédération de grille et que les détails de chaque certificat sont valides. Consultez les instructions pour la rotation des certificats de connexion dans "Gérer les connexions de fédération de grille".
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 domaine complet (FQDN) pour la grille locale ou distante, vérifiez que le serveur DNS est en ligne et disponible. Voir "Qu'est-ce que la fédération de grilles ?" pour les exigences en matière de réseau, d'adresse IP et de DNS.

Alerte d'expiration du 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

Consultez les instructions pour la rotation des certificats de connexion dans "Gérer les connexions de fédération de grille".

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** : « Échec de la création d'un fichier de configuration candidat sur un ou plusieurs nœuds. »

Détails

Lorsque vous modifiez une connexion de fédération de grilles, StorageGRID tente d'enregistrer un fichier de « configuration candidate » sur tous les nœuds d'administration de la première grille. Un message d'avertissement s'affiche si ce fichier ne peut pas être enregistré sur tous les nœuds d'administration, par exemple si un nœud d'administration est hors ligne.

Actions recommandées

1. Dans la grille que vous utilisez pour modifier la connexion, sélectionnez **Nœuds**.
2. Vérifiez que tous les nœuds d'administration de cette grille sont en ligne.
3. Si des nœuds sont hors ligne, remettez-les en ligne et essayez de modifier à nouveau la connexion.

Erreurs de clonage de compte

Impossible de se connecter à un compte locataire cloné

Problème

Vous ne pouvez pas vous connecter à un compte locataire cloné. Le message d'erreur sur la page de connexion du Tenant Manager est « Vos identifiants pour ce compte étaient invalides. Veuillez réessayer. »

Détails

Pour des raisons de sécurité, lorsque vous clonez un compte client de la grille source du client vers la grille de destination du client, le mot de passe que vous définissez pour l'utilisateur racine local du client n'est pas cloné. De même, lorsqu'un client crée des utilisateurs locaux sur sa grille source, les mots de passe des utilisateurs locaux ne sont pas clonés vers la grille de destination.

Actions recommandées

Avant que l'utilisateur racine puisse se connecter à la grille de destination du locataire, un administrateur de grille doit d'abord "modifier le mot de passe de l'utilisateur root local" sur la grille de destination.

Avant qu'un utilisateur local cloné puisse se connecter à la grille de destination du locataire, l'utilisateur root du locataire cloné doit ajouter un mot de passe pour cet utilisateur sur la grille de destination. Pour obtenir des instructions, consultez "Gérer les utilisateurs" dans les instructions d'utilisation du Tenant Manager.

Locataire créé sans clone

Problème

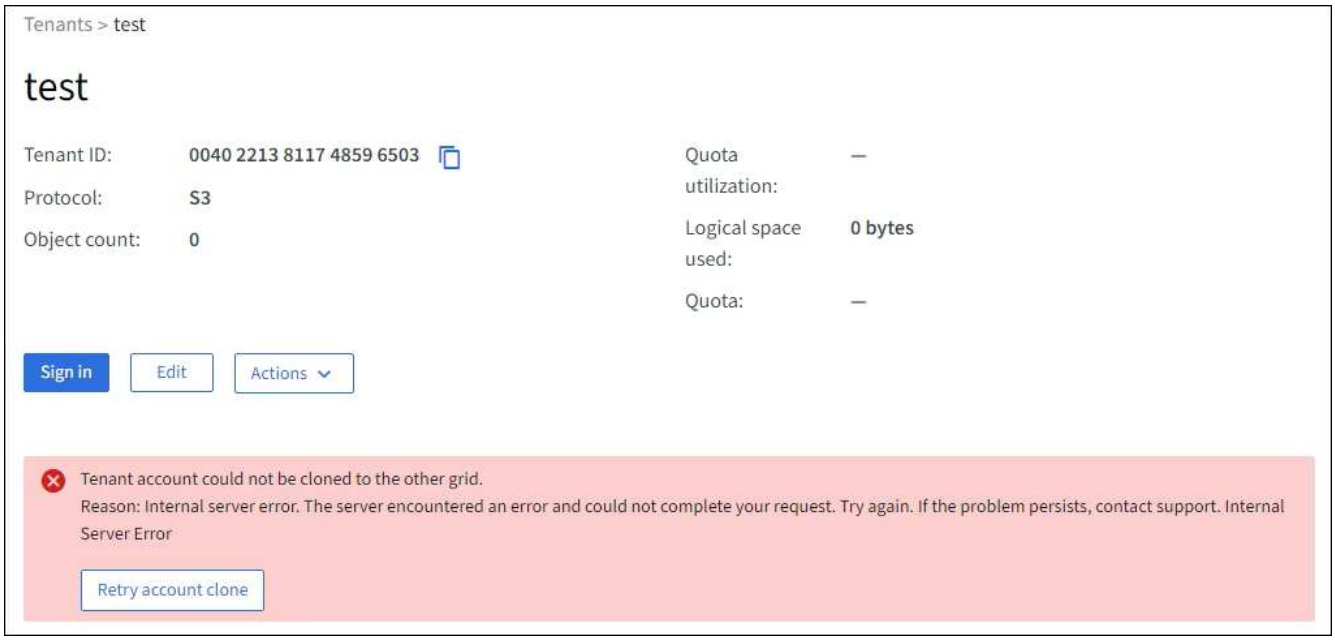
Vous voyez le message « Locataire créé sans clone » après avoir créé un nouveau locataire avec l'autorisation **Utiliser la connexion de fédération de grille**.

Détails

Ce problème peut survenir si les mises à jour de l'état de la connexion sont retardées, ce qui peut entraîner l'affichage d'une connexion défaillante comme **Connected**.

Actions recommandées

1. Examinez la raison indiquée dans le message d'erreur et résolvez tout problème de réseau ou autre pouvant empêcher la connexion de fonctionner. Voir Alertes et erreurs de connexion à la fédération de grille.
2. Suivez les instructions pour tester une connexion de fédération de grille dans "Gérer les connexions de fédération de grille" afin de confirmer que le problème a été résolu.
3. Depuis la grille source du locataire, sélectionnez **Tenants**.
4. Localisez le compte locataire qui n'a pas pu être cloné.
5. Sélectionnez le nom du locataire pour afficher la page de détails.
6. Sélectionnez **Réessayer le clonage du compte**.



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

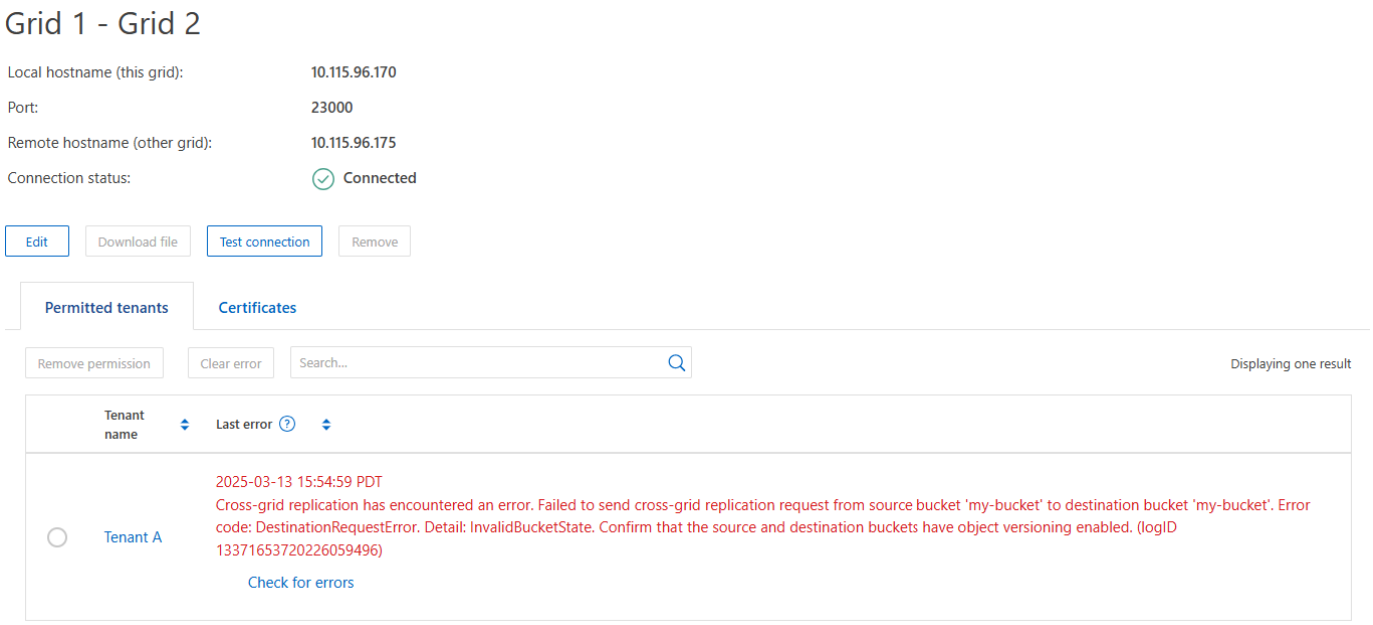
Alertes et erreurs de réplication inter-grilles

Dernière erreur affichée pour la connexion ou le tenant

Problème

Lorsque "visualisation d'une connexion de fédération de grille" (ou lorsque "gérer les locataires autorisés" pour

une connexion), vous constatez une erreur dans la colonne **Dernière erreur** sur la page des détails de la connexion. Par exemple :



Détails

Pour chaque connexion de fédération de grilles, la colonne **Dernière erreur** affiche la dernière erreur survenue, le cas échéant, lors de la réplication des données d'un locataire vers l'autre grille. Cette colonne n'affiche que la dernière erreur de réplication inter-grilles ; les erreurs précédentes qui auraient pu se produire ne sont pas affichées. Une erreur dans cette colonne peut survenir 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 compte différent.
- Le versionnage du bucket de destination est suspendu.
- Le compartiment de destination a été recréé par le même compte, mais il n'est plus versionné.
- L'objet source possède des paramètres de verrouillage d'objet S3 qui ne sont pas conformes aux paramètres de rétention au niveau du locataire de la grille de destination.
- L'objet source possède des paramètres de verrouillage d'objet S3 et le verrouillage d'objet S3 est désactivé sur le compartiment de destination.

Actions recommandées

Si un message d'erreur apparaît dans la colonne **Dernière erreur**, suivez ces étapes :

1. Veuillez vérifier le texte du message.
2. Effectuez les actions recommandées. Par exemple, si le versionnage a été suspendu sur le compartiment de destination pour la réplication inter-grilles, réactivez le versionnage pour ce compartiment.
3. Sélectionnez la connexion ou le compte locataire dans le tableau.
4. Sélectionnez **Effacer l'erreur**.
5. Sélectionnez **Oui** pour effacer le message et mettre à jour l'état du système.

6. Attendez 5 à 6 minutes, puis ajoutez un nouvel objet au bucket. Vérifiez que le message d'erreur ne réapparaît pas.

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

   Une fois l'erreur résolue, 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, consultez "Identifier et réessayer les opérations de réplication ayant échoué".

Alerte de défaillance permanente de la réplication inter-grid

Problème

L'alerte **Échec permanent de la réplication inter-grilles** a été déclenchée.

Détails

Cette alerte indique que la réplication des objets locataires entre les compartiments de deux grilles est impossible pour une raison nécessitant l'intervention de l'utilisateur. Cette alerte est généralement due à une modification apportée au compartiment source ou au compartiment de destination.

Actions recommandées

1. Connectez-vous à la grille où l'alerte a été déclenchée.
2. Accédez à **Configuration** > **Système** > **Fédération de grilles**, et repérez le nom de la connexion indiqué dans l'alerte.
3. Dans l'onglet Locataires autorisés, consultez la colonne **Dernière erreur** pour déterminer quels comptes locataires présentent des erreurs.
4. Pour en savoir plus sur cette défaillance, consultez les instructions dans "Surveiller les connexions de fédération de la grille" pour examiner les indicateurs de réplication inter-grilles.
5. Pour chaque compte locataire concerné :
   a. Consultez les instructions dans "Surveiller l'activité des locataires" pour confirmer que le locataire n'a pas dépassé son quota sur la grille de destination pour la réplication inter-grilles.
   b. Au besoin, augmentez le quota du locataire sur la grille de destination pour permettre l'enregistrement de nouveaux objets.
6. Pour chaque locataire concerné, connectez-vous à Tenant Manager sur les deux grilles afin de pouvoir comparer la liste des compartiments.
7. Pour chaque compartiment pour lequel la réplication inter-grilles est activée, confirmez les points suivants :
   - Il existe un compartiment correspondant pour le même locataire sur l'autre grille (vous devez utiliser le nom exact).
   - Les deux compartiments ont le versionnage des objets activé (le versionnage ne peut pas être suspendu sur aucune des deux grilles).
   - Aucun des deux compartiments n'est dans l'état **Suppression d'objets : lecture seule**.
8. Pour confirmer que le problème a été résolu, consultez les instructions dans "Surveiller les connexions de fédération de la grille" pour examiner les indicateurs de réplication inter-grilles, ou effectuez les étapes suivantes :

a. Revenez à la page Grid federation.

b. Sélectionnez le locataire concerné, puis sélectionnez **Effacer l'erreur** dans la colonne **Dernière erreur**.

c. Sélectionnez **Oui** pour effacer le message et mettre à jour l'état du système.

d. Attendez 5 à 6 minutes, puis ajoutez un nouvel objet au bucket. Vérifiez que le message d'erreur ne réapparaît pas.

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

> Il peut s'écouler jusqu'à une journée avant que l'alerte ne disparaisse après sa résolution.

a. Accédez à "Identifier et réessayer les opérations de réplication ayant échoué" pour identifier les objets ou les marqueurs de suppression qui n'ont pas pu être répliqués sur l'autre grille et pour réessayer la réplication si nécessaire.

Alerte de ressource de réplication inter-grilles indisponible

Problème

L'alerte **Ressource de réplication inter-grilles indisponible** a été déclenchée.

Détails

Cette alerte indique que des requêtes de réplication inter-réseaux sont en attente car une ressource est indisponible. Par exemple, il peut s'agir d'une erreur réseau.

Actions recommandées

1. Surveillez l'alerte pour voir si le problème se résout de lui-même.
2. Si le problème persiste, déterminez si l'une des grilles présente une alerte **Échec de la connexion à la fédération de grilles** pour la même connexion ou une alerte **Impossible de communiquer avec le nœud** pour un nœud. Cette alerte pourrait être résolue lorsque vous aurez résolu ces alertes.
3. Pour en savoir plus sur cette défaillance, consultez les instructions dans "Surveiller les connexions de fédération de la grille" pour examiner les indicateurs de réplication inter-grilles.
4. Si vous ne parvenez pas à résoudre l'alerte, contactez le support technique.

La réplication inter-grilles reprendra son cours normal une fois le problème résolu.

Identifier et réessayer les opérations de réplication StorageGRID ayant échoué

Après avoir résolu l'alerte « Échec permanent de la réplication inter-grilles », vous devez déterminer si des objets ou des marqueurs de suppression n'ont pas pu être répliqués vers l'autre grille. Vous pouvez ensuite réingérer ces objets ou utiliser l'API de gestion Grid Management pour réessayer la réplication.

L'alerte **Échec permanent de la réplication inter-grilles** indique que les objets locataires ne peuvent pas être répliqués entre les compartiments de deux grilles pour une raison nécessitant l'intervention de l'utilisateur. Cette alerte est généralement causée par une modification du compartiment source ou du compartiment de destination. Pour plus de détails, consultez "Dépanner les erreurs de fédération de grille".

Déterminez si des objets ont échoué à être répliqués

Pour déterminer si des objets ou des marqueurs de suppression n'ont pas été répliqués sur l'autre grille, vous pouvez rechercher dans le journal des audits les messages "CGRR (Demande de réplication inter-grilles)". Ce message est ajouté au journal lorsque StorageGRID ne parvient pas à répliquer un objet, un objet multipart ou un marqueur de suppression vers le compartiment de destination.

Vous pouvez utiliser le "outil audit-explain" pour traduire les résultats dans un format plus facile à lire.

Avant de commencer

- Vous disposez des droits d'accès root.
- 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. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.
   c. Saisissez la commande suivante pour passer en mode superutilisateur : `su -`
   d. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.

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

2. Recherchez les messages CGRR dans le journal des audits audit.log et utilisez l'outil audit-explain pour formater les résultats.

   Par exemple, cette commande recherche tous les messages CGRR des 30 dernières minutes et utilise l'outil audit-explain.

   ```
   # awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date { print }' audit.log | grep CGRR | audit-explain
   ```

   Les résultats de la commande ressembleront à cet exemple, qui contient les entrées de six messages CGRR. Dans l'exemple, toutes les requêtes de réplication inter-grilles ont renvoyé une erreur générale, car l'objet n'a pas pu être répliqué. Les trois premières erreurs concernent des opérations de « replicate object », et les trois dernières erreurs concernent des opérations de « 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 inter-grilles CGRR	Le nom de la demande
locataire	L'identifiant du compte du locataire
connexion	L'identifiant de la connexion de la fédération de grille
opération	Le type d'opération de réplication qui était en cours de tentative : • répliquer l'objet • répliquer le marqueur de suppression • répliquer un objet multipart
bucket	Le nom du compartiment
objet	Le nom de l'objet
version	L'identifiant de version de l'objet

Champ	Description
erreur	Type d'erreur. En cas d'échec de la réplication inter-grilles, l'erreur est « Erreur générale ».

Réessayer les réplications ayant échoué

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

- Réingérez chaque objet dans le compartiment source.
- Utilisez l'API privée de gestion de la grille, comme décrit.

Étapes

1. En haut du Grid Manager, sélectionnez l'icône d'aide et sélectionnez **API documentation**.
2. Sélectionnez **Accéder à la documentation de l'API privée**.

> Les points de terminaison de l'API StorageGRID marqués « Privé » sont susceptibles d'être modifiés sans préavis. Les points de terminaison privés de StorageGRID ignorent également la version de l'API de la requête.

3. Dans la section **cross-grid-replication-advanced**, sélectionnez l'endpoint suivant :

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

4. Sélectionnez **Try it out**.
5. Dans la zone de texte **corps**, remplacez l'exemple d'entrée pour **versionID** par un ID de version du journal des audits qui correspond à une requête de réplication inter-grille ayant échoué.

   Veillez à conserver les guillemets doubles autour de la chaîne de caractères.

6. Sélectionnez **Exécuter**.
7. Vérifiez que le code de réponse du serveur est **204**, ce qui indique que l'objet ou le marqueur de suppression a été marqué comme en attente de réplication inter-grille vers l'autre grille.

> « En attente » signifie que la demande de réplication inter-grille a été ajoutée à la file d'attente interne pour traitement.

Surveillez les tentatives de réplication

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

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

Vous pouvez surveiller les opérations de nouvelle tentative de deux manières :

- Utilisez une requête S3 "HeadObject" ou "GetObject". La réponse inclut l'en-tête de réponse spécifique à StorageGRID `x-ntap-sg-cgr-replication-status`, qui aura l'une des valeurs suivantes :

Grid	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 de manière permanente. Un utilisateur doit résoudre l'erreur.
Destination	**REPLICA** : L'objet a été répliqué à partir de la grille source.

- Utilisez l'API privée de gestion de la grille, comme décrit.

Étapes

1. Dans la section **cross-grid-replication-advanced** de la documentation de l'API privée, sélectionnez le point de terminaison suivant :

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

2. Sélectionnez **Try it out**.
3. Dans la section Paramètres, saisissez l'identifiant 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 de manière permanente. Un utilisateur doit résoudre l'erreur.

Gérer la sécurité

Gérer la sécurité dans StorageGRID

Vous pouvez configurer différents paramètres de sécurité depuis le Grid Manager pour contribuer à la sécurité de votre système StorageGRID.

Gérer le chiffrement

StorageGRID propose plusieurs options de chiffrement des données. Il vous appartient "examiner les méthodes de chiffrement disponibles" de déterminer celles qui répondent à vos exigences en matière de protection des données.

Gérer les certificats

Vous pouvez "configurer et gérer les certificats du serveur" utiliser pour les connexions HTTP ou les certificats clients utilisés pour authentifier l'identité d'un client ou d'un utilisateur auprès du serveur.

Configurer les serveurs de gestion des clés

L'utilisation d'une "serveur de gestion des clés" vous permet de protéger les données StorageGRID même si un dispositif est retiré du centre de données. Une fois les volumes du dispositif chiffrés, vous ne pouvez accéder à aucune donnée sur le dispositif à moins que le nœud puisse communiquer avec le KMS.

> Pour utiliser la gestion des clés de chiffrement, vous devez activer le paramètre **Chiffrement de nœud** pour chaque appareil lors de l'installation, avant que l'appareil ne soit ajouté à la grille.

Gérer les paramètres du proxy

Si vous utilisez les services de la plateforme S3 ou des Cloud Storage Pools, vous pouvez configurer une "serveur proxy de stockage" entre les nœuds de stockage et les points de terminaison S3 externes. Si vous envoyez des packages AutoSupport via HTTPS ou HTTP, vous pouvez configurer un "serveur proxy d'administration" entre les nœuds d'administration et le support technique.

Contrôlez les pare-feu

Pour renforcer la sécurité de votre système, vous pouvez contrôler l'accès aux nœuds d'administration StorageGRID en ouvrant ou fermant des ports spécifiques au "pare-feu externe". Vous pouvez également contrôler l'accès réseau à chaque nœud en configurant son "pare-feu interne". Vous pouvez bloquer l'accès sur tous les ports, à l'exception de ceux nécessaires à votre déploiement.

Passez en revue les méthodes de chiffrement de StorageGRID

StorageGRID propose plusieurs options de chiffrement des données. Vous devez examiner les méthodes disponibles afin de déterminer celles qui répondent à vos exigences en matière de protection des données.

Le tableau fournit un résumé général des méthodes de chiffrement disponibles dans StorageGRID.

Option de chiffrement	Comment ça marche	S'applique à
Serveur de gestion des clés (KMS) dans Grid Manager	Vous "configurer un serveur de gestion de clés" pour le site StorageGRID et "activer le chiffrement pour l'appliance". Ensuite, un nœud d'appliance se connecte au KMS pour demander une clé de chiffrement (KEK). Cette clé chiffre et déchiffre la clé de chiffrement (DEK) sur chaque volume.	Les nœuds d'appliance dont la fonction **Node Encryption** est activée lors de l'installation. Toutes les données sur l'appliance sont protégées contre toute perte physique ou tout retrait du centre de données. **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 ça marche	S'applique à
Page de chiffrement du disque dans l'installateur de l'appliance StorageGRID	Si l'appliance contient des disques prenant en charge le chiffrement matériel, vous pouvez définir une phrase secrète de disque lors de l'installation. Lorsque vous définissez une phrase secrète de disque, il est impossible pour quiconque de récupérer des données valides à partir de disques retirés du système, à moins de connaître la phrase secrète. Avant de commencer l'installation, allez dans **Configure Hardware** > **Drive Encryption** pour définir une phrase secrète de disque qui s'appliquera à tous les disques à chiffrement automatique gérés par StorageGRID dans un nœud.	Les appareils équipés de disques à chiffrement automatique. Toutes les données sur les disques sécurisés sont protégées contre la perte physique ou le retrait du centre de données. Le chiffrement des disques ne s'applique pas aux disques gérés par SANtricity. Si vous disposez d'un système de stockage avec des disques à chiffrement automatique et des contrôleurs SANtricity, vous pouvez activer la sécurité des disques dans SANtricity.
Sécurité des disques dans SANtricity System Manager	Si la fonction de sécurité des disques est activée pour votre StorageGRID appliance, vous pouvez utiliser "SANtricity System Manager" pour créer et gérer la clé de sécurité. La clé est requise pour accéder aux données des disques sécurisés.	Les appliances de stockage équipées de disques à chiffrement intégral (FDE) ou de disques à chiffrement automatique. Toutes les données sur les disques sécurisés sont protégées contre la perte physique ou le retrait du centre de données. Ne peut pas être utilisé avec certains appliances de stockage ni avec aucune appliance de services.
Chiffrement des objets stockés	Vous activez l'option "Chiffrement des objets stockés" dans le Gestionnaire de grille. Une fois activée, tous les nouveaux objets qui ne sont pas chiffrés au niveau du compartiment ou au niveau de l'objet sont chiffrés lors de l'ingestion.	Données d'objet S3 nouvellement ingérées. Les objets stockés existants ne sont pas chiffrés. Les métadonnées des objets et autres données sensibles ne sont pas chiffrées.

Option de chiffrement	Comment ça marche	S'applique à
chiffrement du compartiment S3	Vous envoyez une requête PutBucketEncryption pour activer le chiffrement du compartiment. Tous les nouveaux objets qui ne sont pas chiffrés au niveau de l'objet sont chiffrés lors de leur ingestion.	Données d'objet S3 nouvellement ingérées uniquement. Le chiffrement doit être spécifié pour le compartiment. Les objets existants du compartiment ne sont pas chiffrés. Les métadonnées des objets et autres données sensibles ne sont pas chiffrées. "Opérations sur les compartiments"
Chiffrement côté serveur des objets S3 (SSE)	Vous envoyez une requête S3 pour stocker un objet et incluez l `x-amz-server-side-encryption` en-tête de la requête.	Données d'objet S3 nouvellement ingérées uniquement. Le chiffrement doit être spécifié pour l'objet. Les métadonnées de l'objet et les autres données sensibles ne sont pas chiffrées. StorageGRID gère les clés. "Utilisez le chiffrement côté serveur"
Chiffrement côté serveur S3 des objets avec des clés fournies par le client (SSE-C)	Vous envoyez une requête S3 pour stocker un objet et incluez trois en-têtes de requête. • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	Données d'objet S3 nouvellement ingérées uniquement. Le chiffrement doit être spécifié pour l'objet. Les métadonnées de l'objet et les autres données sensibles ne sont pas chiffrées. Les clés sont gérées en dehors de StorageGRID. "Utilisez le chiffrement côté serveur"

Option de chiffrement	Comment ça marche	S'applique à
Chiffrement de volume ou de datastore externe	Vous utilisez une méthode de chiffrement externe à StorageGRID pour chiffrer un volume ou un datastore entier, si votre plateforme de déploiement le prend en charge.	Toutes les données d'objet, les métadonnées et les données de configuration système, en supposant que chaque volume ou banque de données soit chiffré. Une méthode de chiffrement externe offre un contrôle plus strict sur les algorithmes de chiffrement et les clés de chiffrement. Elle peut être combinée avec les autres méthodes mentionnées.
Chiffrement d'objet en dehors de StorageGRID	Vous utilisez une méthode de chiffrement externe à StorageGRID pour chiffrer les données et les métadonnées des objets avant leur ingestion dans StorageGRID.	Données et métadonnées de l'objet uniquement (les données de configuration système ne sont pas chiffrées). Une méthode de chiffrement externe offre un contrôle plus strict sur les algorithmes de chiffrement et les clés de chiffrement. Elle peut être combinée avec les autres méthodes mentionnées. "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 simultanément. Par exemple :

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

Si seule une petite partie de vos objets nécessite un chiffrement, envisagez de contrôler le chiffrement au niveau du compartiment ou de chaque objet à la place. L'activation de plusieurs niveaux de chiffrement engendre un coût supplémentaire en termes de performances.

Informations connexes

"Découvrez les options de chiffrement certifiées FIPS"

Gérer les certificats

Gérer les certificats de sécurité dans StorageGRID

Les certificats de sécurité sont de petits fichiers de données utilisés pour créer des connexions sécurisées et fiables entre les composants StorageGRID et entre les composants StorageGRID et les systèmes externes.

StorageGRID utilise deux types de certificats de sécurité :

- **Les certificats de serveur** sont requis lorsque vous utilisez des connexions HTTPS. Les certificats de serveur sont utilisés pour établir des connexions sécurisées entre les clients et les serveurs, authentifiant l'identité d'un serveur auprès de ses clients et fournissant un chemin de communication sécurisé pour les données. Le serveur et le client disposent chacun d'une copie du certificat.
- Les certificats clients authentifient l'identité d'un client ou d'un utilisateur auprès du serveur, offrant une authentification plus sécurisée que les mots de passe seuls. Les certificats clients ne 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 compare la signature du serveur à la signature sur sa copie du certificat. Si les signatures correspondent, le client démarre une session avec le serveur en utilisant la même clé publique.

StorageGRID fonctionne comme serveur pour certaines connexions (comme le point de terminaison de l'équilibreur de charge) ou comme client pour d'autres connexions (comme le service de réplication CloudMirror).

Certificat CA Grid par défaut

StorageGRID intègre une autorité de certification (CA) qui génère un certificat Grid CA interne lors de l'installation du système. Le certificat Grid CA est utilisé par défaut pour sécuriser le trafic interne de StorageGRID. Une autorité de certification (CA) externe peut émettre des certificats personnalisés, entièrement conformes aux politiques de sécurité informatique de votre organisation.

Utilisez le certificat de l'autorité de certification Grid pour les environnements hors production. Pour la production, utilisez des certificats personnalisés signés par une autorité de certification externe. Les connexions non sécurisées sans certificat sont prises en charge, mais ne sont pas recommandées.

- Les certificats d'autorité de certification personnalisés ne remplacent pas les certificats internes ; toutefois, ce sont les certificats personnalisés qui doivent être spécifiés pour vérifier les connexions au serveur.
- Tous les certificats personnalisés doivent respecter les "Recommandations de renforcement du système pour les certificats de serveur".
- StorageGRID prend en charge le regroupement des certificats d'une autorité de certification dans un seul fichier (appelé ensemble de certificats d'une autorité de certification).

> StorageGRID inclut également des certificats d'autorité de certification (CA) du système d'exploitation, identiques sur toutes les grilles. En environnement de production, veillez à spécifier un certificat personnalisé signé par une autorité de certification externe, en remplacement du certificat CA du système d'exploitation.

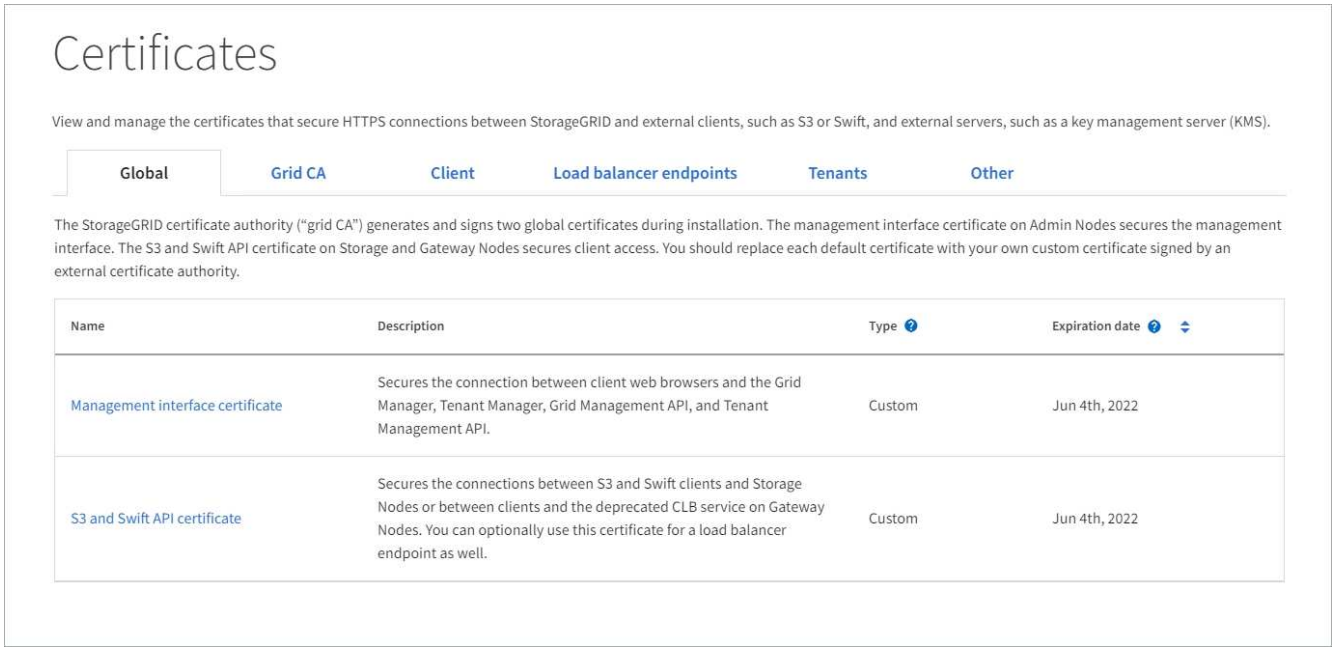
Les différents types de certificats serveur et client sont implémentés de plusieurs manières. Vous devez disposer de tous les certificats nécessaires à votre configuration StorageGRID avant de configurer le système.

Certificats de sécurité d'accès

Vous pouvez accéder aux informations concernant tous les certificats StorageGRID en un seul endroit, ainsi qu'aux liens vers le flux de travail de configuration de chaque certificat.

Étapes

1. Dans Grid Manager, sélectionnez **Configuration** > **Security** > **Certificates**.



2. Sélectionnez un onglet sur la page Certificats pour obtenir des informations sur chaque catégorie de certificat et accéder aux paramètres du certificat. Vous pouvez accéder à un onglet si vous avez le "autorisation appropriée".

   - **Global** : Sécurise l'accès à StorageGRID depuis les navigateurs web et les clients API externes.
   - **Autorité de certification Grid** : Sécurise le trafic interne de StorageGRID.
   - **Client** : Sécurise les connexions entre les clients externes et la base de données StorageGRID Prometheus.
   - **Points de terminaison de l'équilibreur de charge** : Sécurisent les connexions entre les clients S3 et l'équilibreur de charge StorageGRID.
   - **Locataires** : Sécurise les connexions aux serveurs de fédération d'identité ou depuis les points de terminaison de service de la plateforme vers les 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 supplémentaires sur le certificat.

Global

Les certificats globaux sécurisent l'accès à StorageGRID depuis les navigateurs web et les clients API S3 externes. Deux certificats globaux sont initialement générés par l'autorité de certification StorageGRID lors de l'installation. La bonne pratique pour un environnement de production consiste à utiliser des certificats personnalisés signés par une autorité de certification externe.

- Certificat d'interface de gestion: Sécurise les connexions des navigateurs web clients aux interfaces de gestion StorageGRID.
- Certificat API S3: Sécurise les connexions API client aux nœuds de stockage, aux nœuds d'administration et aux nœuds de passerelle, que les applications clientes S3 utilisent pour charger et télécharger des données d'objet.

Les informations relatives aux 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 une sécurité renforcée de la grille :
  - "Remplacez le certificat d'interface de gestion généré par défaut par StorageGRID" Utilisé pour les connexions de Grid Manager et de Tenant Manager.
  - "Remplacez le certificat de l'API S3"utilisé pour les connexions au nœud de stockage et au point de terminaison de l'équilibreur de charge (optionnel).
- "Restaurez le certificat d'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 "certificat d'interface de gestion" ou "Certificat API S3".

Grid CA

Le Certificat d'autorité de certification Grid généré par l'autorité de certification StorageGRID lors de l'installation de StorageGRID, sécurise tout le trafic interne de StorageGRID.

Les informations relatives au certificat comprennent la date d'expiration du certificat et le contenu du certificat.

Vous pouvez "Copiez ou téléchargez le certificat Grid CA", mais vous ne pouvez pas le changer.

Client

Certificats clients, générés par une autorité de certification externe, sécurisent les connexions entre les outils de surveillance externes et la base de données StorageGRID Prometheus.

Le tableau des certificats comporte une ligne pour chaque certificat client configuré et indique si le certificat peut être utilisé pour l'accès à la base de données Prometheus, ainsi que sa date d'expiration.

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 les autorisations d'accès à Prometheus."
  - "Téléchargez et remplacez le certificat client."
  - "Copiez ou téléchargez le certificat client."
  - "Supprimez le certificat client."
- Sélectionnez **Actions** pour "modifier", "attacher" ou "retirer" un certificat client rapidement. Vous pouvez sélectionner jusqu'à 10 certificats clients et les supprimer simultanément via **Actions** > **Supprimer**.

points de terminaison de l'équilibreur de charge

Certificats de point de terminaison de l'équilibreur de chargesécuriser les connexions entre les clients S3 et le service Load Balancer StorageGRID sur les nœuds de passerelle et les nœuds d'administration.

Le tableau des points de terminaison de l'équilibreur de charge comporte une ligne pour chaque point de terminaison configuré et indique si le certificat d'API S3 global ou un certificat personnalisé de point de terminaison d'équilibreur de charge est utilisé pour le point de terminaison. La date d'expiration de chaque certificat est également affichée.

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

Vous pouvez :

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

locataires

Les locataires peuvent utiliser certificats de serveur de fédération d'identité ou certificats de point de terminaison de service de plateforme pour sécuriser leurs connexions avec StorageGRID.

Le tableau des locataires comporte une ligne pour chaque locataire et indique si chaque locataire est autorisé à utiliser sa propre source d'identité ou ses propres services de plateforme.

Vous pouvez :

- "Sélectionnez un nom de locataire pour vous connecter au Tenant Manager"
- "Sélectionnez un nom de locataire pour afficher les détails de la fédération d'identité du locataire"
- "Sélectionnez un nom de locataire pour afficher les détails des services de la plateforme du locataire"
- "Spécifiez un certificat de point de terminaison de service de plateforme lors de la création du point de terminaison"

Autre

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

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

Les informations indiquent le type de certificat qu'une fonction utilise ainsi que les dates d'expiration de ses certificats serveur et client, le cas échéant. Sélectionner un nom de fonction ouvre un onglet du navigateur où vous pouvez consulter et modifier les détails du certificat.

> Vous ne pouvez consulter et accéder aux informations des autres certificats que si vous disposez du "autorisation appropriée".

Vous pouvez :

- "Spécifiez un certificat de Cloud Storage Pool 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"
- "Faites pivoter les certificats de connexion à la fédération de grille"
- "Afficher et modifier un certificat de fédération d'identité"
- "Téléversez les certificats serveur et client du serveur de gestion des clés (KMS)"
- "Spécifiez manuellement un certificat SSO pour une relation d'approbation de partie utilisatrice"

Détails du certificat de sécurité

Chaque type de certificat de sécurité est décrit ci-dessous, avec des liens vers les instructions de mise en œuvre.

Certificat d'interface de gestion

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les navigateurs web clients et l'interface de gestion StorageGRID, permettant aux utilisateurs d'accéder au Grid Manager et au Tenant Manager sans avertissement de sécurité. Ce certificat authentifie également les connexions à l'API de gestion de la grille et à 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 sélectionnez **Certificat d'interface de gestion**	"Configurer les certificats de l'interface de gestion"

Certificat API S3

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie les connexions client S3 sécurisées à un nœud de stockage et aux points de terminaison de l'équilibreur de charge (facultatif).	**Configuration** > **Sécurité** > **Certificats**, sélectionnez l'onglet **Global**, puis sélectionnez **S3 API certificate**	"Configurer les certificats de l'API S3"

Certificat d'autorité de certification Grid

Voir la Description du certificat d'autorité de certification Default Grid.

Certificat client administrateur

Type de certificat	Description	Emplacement de navigation	Détails
Client	Installé sur chaque client, il permet à StorageGRID d'authentifier l'accès des clients externes. • Permet aux clients externes autorisés d'accéder à la base de données Prometheus de StorageGRID. • Permet une surveillance sécurisée de StorageGRID à l'aide d'outils externes.	**Configuration** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Client**	"Configurer les certificats clients"

Certificat de point de terminaison de l'équilibreur de charge

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les clients S3 et le service d'équilibrage de charge StorageGRID sur les nœuds de passerelle et les nœuds d'administration. Vous pouvez télécharger ou générer un certificat d'équilibrage de charge lors de la configuration d'un point de terminaison d'équilibrage de charge. Les applications clientes utilisent le certificat d'équilibrage de charge lors de la connexion à StorageGRID pour enregistrer et récupérer des données d'objets. Vous pouvez également utiliser une version personnalisée du Certificat API S3 certificat global pour authentifier les connexions au service de Load Balancer. Si le certificat global est utilisé pour authentifier les connexions au Load Balancer, vous n'avez pas besoin de télécharger ou de générer un certificat distinct pour chaque point de terminaison du Load Balancer. **Remarque :** Le certificat utilisé pour l'authentification de l'équilibreur de charge est le certificat le plus fréquemment utilisé lors du fonctionnement normal de StorageGRID.	**Configuration** > **Réseau** > **Points de terminaison de l'équilibreur de charge**	• "Configurer les points de terminaison de l'équilibreur de charge" • "Créer un point de terminaison d'équilibrage de charge pour FabricPool"

certificat de point de terminaison Cloud Storage Pool

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

Certificat de notification d'alerte par courriel

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifie la connexion entre un serveur de messagerie SMTP et StorageGRID qui est utilisé pour les notifications d'alerte. • Si les communications avec le serveur SMTP nécessitent Transport Layer Security (TLS), vous devez spécifier le certificat d'autorité de certification (CA) du serveur de messagerie. • Spécifiez un certificat client uniquement si le serveur de messagerie SMTP exige des certificats clients pour l'authentification.	**Alertes** > **Configuration des e-mails**	"Configurer 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 enregistre les événements dans StorageGRID. **Remarque :** Un certificat de serveur syslog externe n'est pas requis pour les connexions TCP, RELP/TCP et UDP à un serveur syslog externe.	**Configuration** > **Surveillance** > **Serveur d'audit et de syslog**	"Utilisez un serveur syslog externe"

Certificat de connexion à la fédération Grid

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifiez et chiffrez les informations envoyées entre le système StorageGRID actuel et une autre grille dans une connexion de fédération de grilles.	**Configuration** > **Système** > **Fédération de grilles**	• "Créer des connexions de fédération de grille" • "Rotation des certificats de connexion"

certificat de fédération d'identité

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre StorageGRID et un fournisseur d'identité externe, tel qu'Active Directory, OpenLDAP ou Oracle Directory Server. Utilisé pour la fédération d'identité, ce qui permet aux groupes d'administrateurs et aux utilisateurs d'être gérés par un système externe.	**Configuration** > **Contrôle d'accès** > **Fédération d'identité**	"Utilisez la fédération d'identités"

certificat de serveur de gestion de clés (KMS)

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifie la connexion entre StorageGRID et un serveur de gestion de clés externe (KMS), qui fournit des clés de chiffrement aux nœuds de l'appliance StorageGRID.	**Configuration** > **Sécurité** > **Serveur de gestion des clés**	"Ajouter un serveur de gestion des clés (KMS)"

certificat de point de terminaison des services de plateforme

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion du service de plateforme StorageGRID à une ressource de stockage S3.	**Tenant Manager** > **STOCKAGE (S3)** > **Points de terminaison des services de plateforme**	"Créer un point de terminaison de services de plateforme" "Modifier le point de terminaison des services de plateforme"

Certificat d'authentification unique (SSO)

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les services de fédération d'identité, tels que les services de fédération Active Directory (AD FS), et StorageGRID utilisés pour les demandes d'authentification unique (SSO).	**Configuration** > **Contrôle d'accès** > **Authentification unique**	"Configurer l'authentification unique"

Exemples de certificats

Exemple 1 : Service d'équilibrage de charge

Dans cet exemple, StorageGRID fait office de serveur.

1. Vous configurez un point de terminaison d'équilibrage de charge et téléchargez ou générez un certificat de serveur dans StorageGRID.
2. Vous configurez une connexion client S3 au point de terminaison de l'équilibreur de charge et téléversez le même certificat sur le client.

3. Lorsque le client souhaite enregistrer ou récupérer des données, il se connecte au point de terminaison de l'équilibreur de charge via HTTPS.
4. StorageGRID répond avec le certificat du serveur, qui contient une clé publique, et avec une signature basée sur la clé privée.
5. Le client compare la signature du serveur à celle figurant sur sa copie du certificat. Si les signatures correspondent, le client établit une session en utilisant la même clé publique.
6. Le client envoie des données d'objet à StorageGRID.

Exemple 2 : Serveur de gestion de clés externe (KMS)

Dans cet exemple, StorageGRID fait office de client.

1. À l'aide d'un logiciel Key Management Server externe, vous configurez StorageGRID en tant que client KMS et obtenez un certificat serveur signé par une autorité de certification (CA), un certificat client public et la clé privée du 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 des données du certificat et une signature basée sur la clé privée.
4. Le serveur KMS valide la signature du certificat et décide qu'il peut faire confiance à StorageGRID.
5. Le serveur KMS répond en utilisant la connexion validée.

Types de certificats serveur pris en charge dans StorageGRID

Le système StorageGRID prend en charge les certificats personnalisés chiffrés avec RSA ou ECDSA (Elliptic Curve Digital Signature Algorithm).

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

Pour plus d'informations sur la manière dont StorageGRID sécurise les connexions client, consultez "Sécurité pour les clients S3".

Configurez les certificats d'interface de gestion dans StorageGRID

Vous pouvez remplacer le certificat d'interface de gestion par défaut par un certificat personnalisé unique permettant aux utilisateurs d'accéder au Grid Manager et au Tenant Manager sans rencontrer d'avertissements de sécurité. Vous pouvez également rétablir le certificat d'interface de gestion par défaut ou en générer un nouveau.

À propos de cette tâche

Par défaut, chaque nœud d'administration reçoit un certificat signé par la CA du grid. Ces certificats signés par la CA peuvent être remplacés par un certificat d'interface de gestion personnalisé commun et la clé privée correspondante.

Étant donné qu'un seul certificat d'interface de gestion personnalisé est utilisé pour tous les nœuds

d'administration, vous devez spécifier le certificat comme un certificat générique ou multidomaine si les clients doivent vérifier le nom d'hôte lors de la connexion au Grid Manager et au Tenant Manager. Définissez le certificat personnalisé de manière à ce qu'il corresponde à tous les nœuds d'administration de la grille.

Vous devez effectuer la configuration sur le serveur et, selon l'autorité de certification racine (CA) que vous utilisez, les utilisateurs devront peut-être également installer le certificat de l'autorité de certification Grid dans le navigateur web qu'ils utiliseront pour accéder au Grid Manager et au Tenant Manager.

> Pour éviter toute interruption de service due à une défaillance du certificat serveur, l'alerte **Expiration du certificat serveur pour l'interface de gestion** est déclenchée lorsque ce certificat est sur le point d'expirer. Au besoin, vous pouvez consulter la date d'expiration du certificat actuel en sélectionnant **Configuration** > **Sécurité** > **Certificats** et en vérifiant la date d'expiration du certificat de l'interface de gestion dans l'onglet Global.

> Si vous accédez au Gestionnaire de grille 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 possibilité de contournement si l'une des situations suivantes se produit :
>
> - Votre certificat d'interface de gestion personnalisée expire.
> - Vousrevenir d'un certificat d'interface de gestion personnalisé au certificat du serveur par défaut.

Ajouter un certificat d'interface de gestion personnalisé

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

Étapes

1. Sélectionnez **Configuration** > **Sécurité** > **Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat d'interface de gestion**.
3. Sélectionnez **Utiliser un certificat personnalisé**.
4. Téléchargez ou générez le certificat.

Télécharger le certificat

Téléversez les fichiers de certificat serveur requis.

a. Sélectionnez **Téléverser le certificat**.

b. Téléversez les fichiers de certificat serveur requis :

- **Certificat serveur** : Le fichier de certificat serveur personnalisé (encodé au format PEM).
- **Clé privée du certificat** : Le fichier de clé privée du certificat de serveur personnalisé (`.key`).

> Les clés privées EC doivent comporter au moins 224 bits. Les clés privées RSA doivent comporter au moins 2048 bits.

- **CA bundle** : Fichier optionnel unique contenant les certificats de chaque autorité de certification (CA) intermédiaire. Le fichier doit contenir chacun des fichiers de certificat CA encodés en 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 importé. Si vous avez importé un ensemble CA optionnel, chaque certificat s'affiche dans son propre onglet.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat ou sélectionnez **Télécharger le bundle CA** pour enregistrer le bundle de certificats.

  Spécifiez le nom du fichier de certificat et son emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

  Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier le certificat PEM** ou **Copier le bundle CA PEM** pour copier le contenu du certificat afin de le coller ailleurs.

d. Sélectionnez **Enregistrer**. + Le certificat d'interface de gestion personnalisé est utilisé pour toutes les nouvelles connexions ultérieures au Grid Manager, au Tenant Manager, à l'API Grid Manager ou à l'API Tenant Manager.

Générer un certificat

Générez les fichiers de certificat du serveur.

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

a. Sélectionnez **Générer un certificat**.

b. Spécifiez les informations du certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine complet à inclure dans le certificat. Utilisez un astérisque (*) comme caractère générique pour représenter plusieurs noms de domaine.
IP	Une ou plusieurs adresses IP à inclure dans le certificat.

Champ	Description
Sujet (facultatif)	Sujet X.509 ou nom unique (DN) du propriétaire du certificat. Si aucune valeur n'est saisie dans ce champ, le certificat généré utilise le premier nom de domaine ou la première adresse IP comme nom commun (CN) du sujet.
Jours valides	Nombre de jours après la création du certificat avant son expiration.
Ajouter des extensions d'utilisation de clé	Si cette option est sélectionnée (par défaut et recommandée), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré. Ces extensions définissent la finalité de la clé contenue dans le certificat. **Remarque** : 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 **Générer**.

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 son emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

   Par exemple : `storagegrid_certificate.pem`

   - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.

e. Sélectionnez **Enregistrer**. + Le certificat d'interface de gestion personnalisé est utilisé pour toutes les nouvelles connexions ultérieures au Grid Manager, au Tenant Manager, à l'API Grid Manager ou à l'API Tenant Manager.

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

> Après avoir téléchargé ou généré un nouveau certificat, prévoyez jusqu'à une journée pour que les alertes d'expiration de certificat associées disparaissent.

6. Après avoir ajouté un certificat d'interface de gestion personnalisé, la page du certificat d'interface de gestion affiche des informations détaillées sur les certificats utilisés. Vous pouvez télécharger ou copier le PEM du certificat si nécessaire.

Restaurez le certificat d'interface de gestion par défaut

Vous pouvez revenir à l'utilisation du certificat d'interface de gestion par défaut pour les connexions Grid Manager et Tenant Manager.

Étapes

1. Sélectionnez **Configuration** > **Sécurité** > **Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat d'interface de gestion**.
3. Sélectionnez **Utiliser le certificat par défaut**.

   Lorsque vous restaurez le certificat d'interface de gestion par défaut, les fichiers de certificat 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 ultérieures.

4. Actualisez la page pour vous assurer que le navigateur Web est 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.

À propos de cette tâche

La bonne 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. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.
   c. Saisissez la commande suivante pour passer en mode superutilisateur : `su -`
   d. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.

      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 valides pendant un an (365 jours) et doivent être recréés avant leur expiration. Vous pouvez utiliser l'argument `--days` pour remplacer la période de validité par défaut.

> La période de validité d'un certificat commence lorsque `make-certificate` est exécutée. Vous devez vous assurer que le client de gestion est synchronisé avec la même source de temps que StorageGRID ; sinon, le client risque de rejeter le certificat.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 720
```

Le résultat obtenu contient le certificat public nécessaire à votre client API de gestion.

4. Sélectionnez et copiez le certificat.

   Incluez les balises BEGIN et END dans votre sélection.

5. Déconnectez-vous de l'invite de commandes. `$ 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 **Certificat d'interface de gestion**.
7. Configurez votre client de gestion pour qu'il utilise le certificat public que vous avez copié. Incluez les balises BEGIN et END.

Téléchargez ou copiez le certificat de l'interface de gestion

Vous pouvez enregistrer ou copier le contenu du certificat d'interface de gestion pour l'utiliser ailleurs.

Étapes

1. Sélectionnez **Configuration** > **Sécurité** > **Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat d'interface de gestion**.
3. Sélectionnez l'onglet **Serveur** ou **CA bundle**, puis téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat ou le bundle CA

Téléchargez le certificat ou le fichier du bundle CA `.pem`. Si vous utilisez un bundle CA optionnel, chaque certificat du bundle s'affiche dans son propre sous-onglet.

a. Sélectionnez **Télécharger le certificat** ou **Télécharger le bundle CA**.

   Si vous téléchargez un ensemble d'autorités de certification, tous les certificats des onglets secondaires de l'ensemble d'autorités de certification sont téléchargés sous forme d'un seul fichier.

b. Spécifiez le nom du fichier de certificat et son emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

   Par exemple : `storagegrid_certificate.pem`

Copier le certificat ou le bundle d'autorités de certification PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un ensemble CA optionnel, chaque certificat de l'ensemble s'affiche dans son propre sous-onglet.

a. Sélectionnez **Copier le certificat PEM** ou **Copier le bundle CA PEM**.

   Si vous copiez un ensemble d'autorités de certification, tous les certificats des onglets secondaires de l'ensemble 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 dans StorageGRID

Vous pouvez remplacer ou restaurer le certificat serveur utilisé pour les connexions client S3 aux nœuds de stockage ou aux points de terminaison d'équilibrage de charge. Le certificat serveur personnalisé de remplacement est spécifique à votre organisation.

Les détails concernant Swift ont été supprimés de cette version du site de documentation. Voir "StorageGRID 11.8 : Configurez les certificats d'API S3 et Swift".

À propos de cette tâche

Par défaut, chaque nœud de stockage reçoit un certificat serveur X.509 signé par la CA du grid. Ces certificats signés par la CA peuvent être remplacés par un certificat serveur personnalisé unique et la clé privée correspondante.

Un seul certificat serveur personnalisé est utilisé pour tous les nœuds de stockage, donc vous devez spécifier le certificat comme un certificat générique ou multi-domaine si les clients doivent vérifier le nom d'hôte lors de la connexion au point de terminaison de stockage. Définissez le certificat personnalisé de sorte qu'il corresponde à tous les nœuds de stockage de la grille.

Une fois la configuration du serveur terminée, vous devrez peut-être également installer le certificat Grid CA

dans le client API S3 que vous utiliserez pour accéder au système, en fonction de l'autorité de certification racine (CA) que vous utilisez.

> Pour éviter toute interruption de service due à une défaillance du certificat serveur, l'alerte « Expiration du certificat serveur global pour l'API S3 » est déclenchée lorsque le certificat racine du serveur est sur le point d'expirer. Si nécessaire, vous pouvez voir quand le certificat actuel expire en sélectionnant **Configuration** > **Sécurité** > **Certificats** et en consultant la date d'expiration du certificat de l'API S3 dans l'onglet Global.

Vous pouvez télécharger ou générer un certificat d'API S3 personnalisé.

Ajouter un certificat d'API S3 personnalisé

Étapes

1. Sélectionnez **Configuration** > **Sécurité** > **Certificats**.
2. Dans l'onglet **Global**, sélectionnez **S3 API certificate**.
3. Sélectionnez **Utiliser un certificat personnalisé**.
4. Téléchargez ou générez le certificat.

Télécharger le certificat

Téléversez les fichiers de certificat serveur requis.

a. Sélectionnez **Téléverser le certificat**.

b. Téléversez les fichiers de certificat serveur requis :

- **Certificat serveur** : Le fichier de certificat serveur personnalisé (encodé au format PEM).
- **Clé privée du certificat** : Le fichier de clé privée du certificat de serveur personnalisé (`.key`).

> Les clés privées EC doivent comporter au moins 224 bits. Les clés privées RSA doivent comporter au moins 2048 bits.

- **Ensemble d'autorités de certification (CA bundle)** : Fichier optionnel unique contenant les certificats de chaque autorité de certification intermédiaire. Le fichier doit contenir chaque fichier de certificat d'autorité de certification au format PEM, concaténés dans l'ordre de la chaîne de certificats.

c. Sélectionnez les détails du certificat pour afficher les métadonnées et le PEM de chaque certificat d'API S3 personnalisé que vous avez chargé. Si vous avez chargé un bundle CA optionnel, chaque certificat s'affiche dans son propre onglet.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat ou sélectionnez **Télécharger le bundle CA** pour enregistrer le bundle de certificats.

  Spécifiez le nom du fichier de certificat et son emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

  Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier le certificat PEM** ou **Copier le bundle CA PEM** pour copier le contenu du certificat afin de le coller ailleurs.

d. Sélectionnez **Enregistrer**.

Le certificat serveur personnalisé est utilisé pour les connexions client S3 ultérieures.

Générer un certificat

Générez les fichiers de certificat du serveur.

a. Sélectionnez **Générer un certificat**.

b. Spécifiez les informations du certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine complet à inclure dans le certificat. Utilisez un astérisque (*) comme caractère générique pour représenter plusieurs noms de domaine.
IP	Une ou plusieurs adresses IP à inclure dans le certificat.

Champ	Description
Sujet (facultatif)	Sujet X.509 ou nom unique (DN) du propriétaire du certificat. Si aucune valeur n'est saisie dans ce champ, le certificat généré utilise le premier nom de domaine ou la première adresse IP comme nom commun (CN) du sujet.
Jours valides	Nombre de jours après la création du certificat avant son expiration.
Ajouter des extensions d'utilisation de clé	Si cette option est sélectionnée (par défaut et recommandée), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré. Ces extensions définissent la finalité de la clé contenue dans le certificat. **Remarque** : 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 **Générer**.

d. Sélectionnez **Détails du certificat** pour afficher les métadonnées et le PEM du certificat d'API S3 personnalisé qui a été généré.

   - Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

     Spécifiez le nom du fichier de certificat et son emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

     Par exemple : `storagegrid_certificate.pem`

   - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.

e. Sélectionnez **Enregistrer**.

   Le certificat serveur personnalisé est utilisé pour les connexions client S3 ultérieures.

5. Sélectionnez un onglet pour afficher les métadonnées du certificat serveur StorageGRID par défaut, d'un certificat signé par une autorité de certification qui a été téléchargé ou d'un certificat personnalisé qui a été généré.

   Après avoir téléchargé ou généré un nouveau certificat, prévoyez jusqu'à une journée pour que les alertes d'expiration de certificat associées disparaissent.

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

7. Après avoir ajouté un certificat d'API S3 personnalisé, la page du certificat d'API S3 affiche des informations détaillées sur le certificat d'API S3 personnalisé actuellement utilisé. Vous pouvez télécharger ou copier le PEM du certificat selon vos besoins.

Restaurez le certificat d'API S3 par défaut

Vous pouvez rétablir l'utilisation du certificat d'API S3 par défaut pour les connexions client S3 aux nœuds de stockage. Cependant, vous ne pouvez pas utiliser le certificat d'API S3 par défaut pour un point de terminaison d'équilibreur de charge.

Étapes

1. Sélectionnez **Configuration** > **Sécurité** > **Certificats**.
2. Dans l'onglet **Global**, sélectionnez **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 serveur personnalisés 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 ultérieures aux Storage Nodes.

4. Sélectionnez **OK** pour confirmer l'avertissement et restaurer le certificat API S3 par défaut.

   Si vous disposez des droits d'accès root et que le certificat API S3 personnalisé a été utilisé pour les connexions aux points de terminaison de l'équilibreur de charge, une liste des points de terminaison de l'équilibreur de charge qui ne seront plus accessibles avec le certificat API S3 par défaut s'affiche. Accédez à "Configurer les points de terminaison de l'équilibreur de charge" pour modifier ou supprimer les points de terminaison concernés.

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

Téléchargez ou copiez le certificat de l'API S3

Vous pouvez enregistrer ou copier le contenu du certificat S3 API pour l'utiliser ailleurs.

Étapes

1. Sélectionnez **Configuration** > **Sécurité** > **Certificats**.
2. Dans l'onglet **Global**, sélectionnez **S3 API certificate**.
3. Sélectionnez l'onglet **Serveur** ou **CA bundle**, puis téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat ou le bundle CA

Téléchargez le certificat ou le fichier du bundle CA `.pem`. Si vous utilisez un bundle CA optionnel, chaque certificat du bundle s'affiche dans son propre sous-onglet.

a. Sélectionnez **Télécharger le certificat** ou **Télécharger le bundle CA**.

   Si vous téléchargez un ensemble d'autorités de certification, tous les certificats des onglets secondaires de l'ensemble d'autorités de certification sont téléchargés sous forme d'un seul fichier.

b. Spécifiez le nom du fichier de certificat et son emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

   Par exemple : `storagegrid_certificate.pem`

Copier le certificat ou le bundle d'autorités de certification PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un ensemble CA optionnel, chaque certificat de l'ensemble s'affiche dans son propre sous-onglet.

a. Sélectionnez **Copier le certificat PEM** ou **Copier le bundle CA PEM**.

   Si vous copiez un ensemble d'autorités de certification, tous les certificats des onglets secondaires de l'ensemble sont copiés ensemble.

b. Collez le certificat copié dans un éditeur de texte.

c. Enregistrez le fichier texte avec l'extension `.pem`.

   Par exemple : `storagegrid_certificate.pem`

Informations connexes

- "Utilisez l'API REST S3"
- "Configurer les noms de domaine des points de terminaison S3"

Copiez le certificat d'autorité de certification (CA) StorageGRID Grid

StorageGRID utilise une autorité de certification interne (CA) pour sécuriser le trafic interne. Ce certificat ne change pas si vous importez 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".

À propos de cette tâche

Si un certificat serveur personnalisé a été configuré, les applications clientes doivent vérifier le serveur à l'aide de ce certificat serveur personnalisé. Elles ne doivent pas copier le certificat d'autorité de certification du système StorageGRID.

Étapes

1. Sélectionnez **Configuration** > **Security** > **Certificates** puis sélectionnez l'onglet **Grid CA**.
2. Dans la section **Certificat PEM**, téléchargez ou copiez le certificat.

Télécharger le fichier de certificat

Téléchargez le fichier de certificat `.pem`.

a. Sélectionnez **Télécharger le certificat**.
b. Spécifiez le nom du fichier de certificat et son emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

   Par exemple : `storagegrid_certificate.pem`

Copier le certificat PEM

Copiez le texte du certificat pour le coller ailleurs.

a. Sélectionnez **Copier le certificat PEM**.
b. Collez le certificat copié dans un éditeur de texte.
c. Enregistrez le fichier texte avec l'extension `.pem`.

   Par exemple : `storagegrid_certificate.pem`

Configurer les certificats StorageGRID pour FabricPool

Pour les clients S3 qui effectuent une validation stricte du nom d'hôte et ne prennent pas en charge la désactivation de cette validation stricte, tels que les clients ONTAP utilisant FabricPool, vous pouvez générer ou télécharger un certificat de serveur lors de la configuration du point de terminaison 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".

À propos de cette tâche

Lors de la création d'un point de terminaison d'équilibrage de charge, vous pouvez générer un certificat serveur auto-signé ou importer un certificat signé par une autorité de certification (CA) reconnue. Dans les environnements de production, vous devez utiliser un certificat signé par une CA reconnue. Les certificats signés par une CA peuvent être renouvelés sans interruption de service. Ils sont également plus sécurisés car ils offrent une meilleure protection contre les attaques de type homme du milieu.

Les étapes suivantes fournissent des instructions générales pour les clients S3 qui utilisent FabricPool. Pour plus d'informations et de procédures détaillées, consultez "Configurer StorageGRID pour FabricPool".

Étapes

1. Vous pouvez éventuellement configurer un groupe à haute disponibilité (HA) pour que FabricPool puisse l'utiliser.
2. Créez un point de terminaison d'équilibrage de charge S3 pour que FabricPool puisse l'utiliser.

Lorsque vous créez un point de terminaison d'équilibrage de charge HTTPS, vous êtes invité à télécharger votre certificat de serveur, votre clé privée de certificat et, éventuellement, le bundle d'autorité de certification.

3. Intégrez StorageGRID en tant que niveau cloud dans ONTAP.

   Veuillez indiquer le port du point de terminaison de l'équilibreur de charge et le nom de domaine complet utilisé dans le certificat d'autorité de certification que vous avez importé. Ensuite, fournissez le certificat d'autorité de certification.

> ⓘ Si le certificat StorageGRID a été émis par une autorité de certification intermédiaire, vous devez fournir le certificat de l'autorité de certification intermédiaire. Si le certificat StorageGRID a été émis directement par l'autorité de certification racine, vous devez fournir le certificat de l'autorité de certification racine.

Configurez les certificats clients dans StorageGRID

Les certificats clients permettent aux clients externes autorisés d'accéder à la base de données Prometheus de StorageGRID, offrant ainsi un moyen sécurisé pour les outils externes de surveiller StorageGRID.

Si vous devez accéder à StorageGRID à l'aide d'un outil de surveillance externe, vous devez télécharger ou générer un certificat client à l'aide de Grid Manager et copier les informations du certificat dans l'outil externe.

Voir "Gérer les certificats de sécurité" et "Configurer les certificats de serveur personnalisés".

> ⓘ Pour éviter toute interruption de service due à une défaillance du certificat serveur, l'alerte **Expiration des certificats clients configurés sur la page Certificats** est déclenchée lorsque ce certificat serveur est sur le point d'expirer. Au besoin, vous pouvez consulter la date d'expiration du certificat actuel en sélectionnant **Configuration** > **Sécurité** > **Certificats** et en regardant la date d'expiration du certificat client dans l'onglet Client.

> ⓘ Si vous utilisez un serveur de gestion de clés (KMS) pour protéger les données sur des nœuds d'appliance spécialement configurés, consultez les informations spécifiques concernant "téléchargement d'un certificat client KMS".

Avant de commencer

- Vous disposez des droits d'accès root.
- 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, vous disposez de l'autorité de certification, du certificat client et de la clé privée 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 sauvegardée ou enregistrée lors 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 (le cas échéant) sont disponibles sur votre ordinateur local.

Ajouter des certificats client

Pour ajouter le certificat client, utilisez l'une de ces procédures :

- Le certificat d'interface de gestion est déjà configuré
- Certificat client délivré par CA
- Certificat généré par Grid Manager

Le certificat d'interface de gestion est 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 **Add**.
3. Saisissez un nom de certificat.
4. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Allow prometheus**.
5. Sélectionnez **Continue**.
6. Pour l'étape **Joindre les certificats**, téléversez le certificat de l'interface de gestion.
   a. Sélectionnez **Téléverser le certificat**.
   b. Sélectionnez **Parcourir** et sélectionnez le fichier de certificat de l'interface de gestion (`.pem`.
      - Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.
      - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.
   c. Sélectionnez **Créer** pour enregistrer le certificat dans le Grid Manager.

      Le nouveau certificat apparaît dans l'onglet Client.
7. Configurer un outil de surveillance externe, comme Grafana.

Certificat client délivré par CA

Utilisez cette procédure pour ajouter un certificat client administrateur si aucun certificat d'interface de gestion n'a été configuré et que vous prévoyez d'ajouter un certificat client pour Prometheus qui utilise un certificat client et une clé privée émis par une autorité de certification (CA).

Étapes

1. Effectuez les étapes pour "configurer un certificat d'interface de gestion".
2. Dans le Gestionnaire de grille, sélectionnez **Configuration** > **Sécurité** > **Certificats**, puis sélectionnez

l'onglet **Client**.

3. Sélectionnez **Add**.
4. Saisissez un nom de certificat.
5. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Allow prometheus**.
6. Sélectionnez **Continue**.
7. Pour l'étape **Joindre les certificats**, téléchargez le certificat client, la clé privée et les fichiers du bundle d'autorité de certification :
   a. Sélectionnez **Téléverser le certificat**.
   b. Sélectionnez **Parcourir** et sélectionnez les fichiers du certificat client, de la clé privée et du bundle CA (`.pem`).
      - Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.
      - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.
   c. Sélectionnez **Créer** pour enregistrer le certificat dans le Grid Manager.

      Les nouveaux certificats apparaissent dans 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 administrateur si aucun certificat d'interface de gestion n'a été configuré et que vous prévoyez d'ajouter un certificat client pour Prometheus qui utilise la fonction de génération de certificat dans Grid Manager.

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **Configuration** > **Sécurité** > **Certificats**, puis sélectionnez l'onglet **Client**.
2. Sélectionnez **Add**.
3. Saisissez un nom de certificat.
4. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Allow prometheus**.
5. Sélectionnez **Continue**.
6. Pour l'étape **Joindre des certificats**, sélectionnez **Générer un certificat**.
7. Spécifiez les informations du certificat :
   - **Sujet** (facultatif) : sujet X.509 ou nom unique (DN) du propriétaire du certificat.
   - **Jours de validité** : Le nombre de jours pendant lesquels le certificat généré est valide, à partir du moment où il est généré.
   - **Ajouter les extensions d'utilisation de la clé** : Si cette option est sélectionnée (par défaut et recommandée), les extensions d'utilisation de la clé et d'utilisation étendue de la clé sont ajoutées au certificat généré.

     Ces extensions définissent la finalité 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 **Générer**.
9. Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.

   Vous ne pourrez plus consulter la clé privée du certificat après avoir fermé la boîte de dialogue. Copiez ou téléchargez la clé dans un emplacement sûr.

   - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.
   - Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

     Spécifiez le nom du fichier de certificat et son emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

     Par exemple : `storagegrid_certificate.pem`

   - Sélectionnez **Copier la clé privée** pour copier la clé privée du certificat afin de la coller ailleurs.
   - Sélectionnez **Télécharger la clé privée** pour enregistrer la clé privée dans un fichier.

     Spécifiez le nom du fichier de clé privée et l'emplacement de téléchargement.

10. Sélectionnez **Créer** pour enregistrer le certificat dans le Grid Manager.

    Le nouveau certificat apparaît dans l'onglet Client.

11. Dans le Grid Manager, sélectionnez **Configuration** > **Security** > **Certificates** puis sélectionnez l'onglet **Global**.
12. Sélectionnez **certificat d'interface de gestion**.
13. Sélectionnez **Utiliser un certificat personnalisé**.
14. Téléversez les fichiers certificate.pem et private_key.pem de l'Détails du certificat clientétape. Il n'est pas nécessaire de téléverser le bundle CA.
    a. Sélectionnez **Téléverser le certificat** puis **Continuer**.
    b. Téléchargez chaque fichier de certificat (`.pem`).
    c. Sélectionnez **Enregistrer** pour enregistrer le certificat dans le Grid Manager.

       Le nouveau certificat apparaît sur la page des certificats de l'interface de gestion.

15. Configurer un outil de surveillance externe, comme Grafana.

Configurer un outil de surveillance externe

Étapes

1. Configurez les paramètres suivants sur votre outil de surveillance externe, tel que Grafana.
   a. **Nom** : Saisissez un nom pour la connexion.

      StorageGRID n'a pas besoin de ces informations, mais vous devez fournir un nom pour tester la connexion.

b. **URL** : Saisissez le nom de domaine ou l'adresse IP du nœud d'administration. Spécifiez HTTPS et le port 9091.

   Par exemple : `https://admin-node.example.com:9091`

c. Activez **l'authentification client TLS** et **Avec certificat d'autorité de certification (CA)**.

d. Sous Détails d'authentification TLS/SSL, copiez et collez :
   - Le certificat CA de l'interface de gestion à **CA Cert**
   - Le certificat client à **Client Cert**
   - La clé privée de **Client Key**

e. **ServerName** : Entrez le nom de domaine du nœud d'administration.

   ServerName doit correspondre au nom de domaine tel qu'il apparaît dans le certificat de l'interface de gestion.

2. Enregistrez et testez le certificat et la clé privée que vous avez copiés depuis StorageGRID ou un fichier local.

   Vous pouvez désormais accéder aux métriques Prometheus de StorageGRID avec votre outil de surveillance externe.

   Pour plus d'informations sur les indicateurs, consultez le "Instructions pour la surveillance StorageGRID".

Modifier les certificats clients

Vous pouvez modifier un certificat client administrateur pour en changer le nom, activer ou désactiver l'accès Prometheus, ou télécharger un nouveau certificat lorsque le certificat actuel a expiré.

Étapes

1. Sélectionnez **Configuration** > **Security** > **Certificates** puis sélectionnez l'onglet **Client**.

   Le tableau indique les dates d'expiration des certificats et les autorisations d'accès à Prometheus. Si un certificat expire bientôt ou a déjà expiré, un message s'affiche dans le tableau et une alerte est déclenchée.

2. Sélectionnez le certificat que vous souhaitez modifier.
3. Sélectionnez **Modifier** puis **Modifier le nom et les permissions**
4. Saisissez un nom de certificat.
5. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Allow prometheus**.
6. Sélectionnez **Continuer** pour enregistrer le certificat dans le 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 le certificat actuel a expiré.

Étapes

1. Sélectionnez **Configuration** > **Security** > **Certificates** puis sélectionnez l'onglet **Client**.

   Le tableau indique les dates d'expiration des certificats et les autorisations d'accès à Prometheus. Si un certificat expire bientôt ou a déjà expiré, un message s'affiche dans le tableau et une alerte est déclenchée.

2. Sélectionnez le certificat que vous souhaitez modifier.
3. Sélectionnez **Modifier** puis sélectionnez une option de modification.

Télécharger le certificat

Copiez le texte du certificat pour le coller ailleurs.

a. Sélectionnez **Téléverser 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 PEM du certificat.

   - Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

     Spécifiez le nom du fichier de certificat et son emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

   Par exemple : `storagegrid_certificate.pem`

   - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.

c. Sélectionnez **Créer** pour enregistrer le certificat dans le Grid Manager.

   Le certificat mis à jour s'affiche dans l'onglet Client.

Générer un certificat

Générez le texte du certificat à coller ailleurs.

a. Sélectionnez **Générer un certificat**.

b. Spécifiez les informations du certificat :

   - **Sujet** (facultatif) : sujet X.509 ou nom unique (DN) du propriétaire du certificat.
   - **Jours de validité** : Le nombre de jours pendant lesquels le certificat généré est valide, à partir du moment où il est généré.
   - **Ajouter les extensions d'utilisation de la clé** : Si cette option est sélectionnée (par défaut et recommandée), les extensions d'utilisation de la clé et d'utilisation étendue de la clé sont ajoutées au certificat généré.

     Ces extensions définissent la finalité 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 **Générer**.

d. Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.

   Vous ne pourrez plus consulter la clé privée du certificat après avoir fermé la boîte de dialogue. Copiez ou téléchargez la clé dans un emplacement sûr.

   - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

  Spécifiez le nom du fichier de certificat et son emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

  Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier la clé privée** pour copier la clé privée du certificat afin de la coller ailleurs.
- Sélectionnez **Télécharger la clé privée** pour enregistrer la clé privée dans un fichier.

  Spécifiez le nom du fichier de clé privée et l'emplacement de téléchargement.

e. Sélectionnez **Créer** pour enregistrer le certificat dans le Grid Manager.

Le nouveau certificat apparaît dans l'onglet Client.

Télécharger ou copier les certificats clients

Vous pouvez télécharger ou copier un certificat client pour l'utiliser ailleurs.

Étapes

1. Sélectionnez **Configuration** > **Security** > **Certificates** puis sélectionnez l'onglet **Client**.
2. Sélectionnez le certificat que vous souhaitez copier ou télécharger.
3. Téléchargez ou copiez le certificat.

Télécharger le fichier de certificat

Téléchargez le fichier de certificat `.pem`.

a. Sélectionnez **Télécharger le certificat**.
b. Spécifiez le nom du fichier de certificat et son 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 clients

Si vous n'avez plus besoin d'un certificat client administrateur, vous pouvez le supprimer.

Étapes

1. Sélectionnez **Configuration** > **Security** > **Certificates** puis sélectionnez l'onglet **Client**.
2. Sélectionnez le certificat que vous souhaitez supprimer.
3. Sélectionnez **Supprimer** puis confirmez.

> Pour supprimer jusqu'à 10 certificats, sélectionnez chaque certificat à supprimer dans l'onglet Client, puis sélectionnez **Actions** > **Delete**.

Après la suppression d'un certificat, les clients qui utilisaient ce certificat doivent spécifier un nouveau certificat client pour accéder à la base de données StorageGRID Prometheus.

Configurer les paramètres de sécurité

Gérez la politique TLS et SSH dans StorageGRID

La politique TLS et SSH détermine les protocoles et les chiffrements utilisés pour établir des connexions TLS sécurisées avec les applications clientes et des connexions SSH sécurisées avec les services internes de StorageGRID.

La politique de sécurité détermine la façon dont TLS et SSH chiffrent les données en transit. En général, utilisez la politique Modern compatibility (par défaut), sauf si votre système doit être conforme aux Common Criteria ou si vous devez utiliser d'autres algorithmes de chiffrement.

> Certains services StorageGRID n'ont pas été mis à jour pour utiliser les algorithmes de chiffrement définis dans ces politiques.

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 root".

Sélectionnez une politique de sécurité

Étapes

1. Sélectionnez **Configuration** > **Sécurité** > **Paramètres de sécurité**.

   L'onglet **Stratégies TLS et SSH** affiche les stratégies disponibles. La stratégie actuellement active est indiquée par une coche verte sur la vignette de la stratégie.

2. Consultez les onglets pour en savoir plus sur les stratégies disponibles.

Compatibilité moderne (par défaut)

Utilisez la stratégie par défaut si vous avez besoin d'un chiffrement fort et que vous n'avez pas d'exigences particulières. Cette stratégie est compatible avec la plupart des clients TLS et SSH.

Compatibilité héritée

Utilisez la stratégie de compatibilité héritée si vous avez besoin d'options de compatibilité supplémentaires pour les anciens clients. Les options supplémentaires de cette stratégie peuvent la rendre moins sécurisée que la stratégie de compatibilité moderne.

Critères communs

Utilisez la politique Common Criteria si vous avez besoin d'une certification Common Criteria.

FIPS strict

Utilisez la politique FIPS stricte si vous avez besoin de la certification Critères communs et devez utiliser le NetApp Cryptographic Security Module (NCSM) 3.0.8 ou le module NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 pour les connexions client externes aux points de terminaison de l'équilibreur de charge, au Tenant Manager et au Grid Manager. L'utilisation de cette politique peut réduire les performances.

Les modules NCSM 3.0.8 et NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 sont utilisés dans les opérations suivantes :

- NCSM
  - Connexions TLS entre les services suivants : ADC, AMS, CMN, DDS, LDR, SSM, NMS, mgmt-api, nginx, nginx-gw et cache-svc
  - Connexions TLS entre les clients et le service nginx-gw (points de terminaison de l'équilibreur de charge)
  - Connexions TLS entre les clients et le service LDR
  - Chiffrement du contenu des objets pour SSE-S3, SSE-C et le paramètre de chiffrement des objets stockés
  - connexions SSH

  Pour plus d'informations, consultez le programme de validation des algorithmes cryptographiques du NIST "Certificat n° 4838".

- NetApp StorageGRID module API de chiffrement du noyau

  Le module API de chiffrement du noyau NetApp StorageGRID est présent uniquement sur les plateformes VM et les appliances StorageGRID.

  - Collecte d'entropie
  - Chiffrement du nœud

  Pour plus d'informations, consultez le programme de validation des algorithmes cryptographiques du NIST "Certificats n° A6242 à A6257" et "Certificat d'entropie n° E223".

Remarque : Après avoir sélectionné cette stratégie, "effectuer un redémarrage progressif" pour activer le NCSM sur tous les nœuds. Utilisez **Maintenance** > **Redémarrage progressif** pour lancer et surveiller les redémarrages.

Personnalisé

Créez une politique personnalisée si vous devez appliquer vos propres chiffrements.

Si votre StorageGRID est soumis à des exigences de cryptographie FIPS 140, vous pouvez activer la fonctionnalité de mode FIPS pour utiliser le module NCSM 3.0.8 et le module NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 :

a. Définissez le `fipsMode` paramètre sur `true`.

b. Lorsque vous y êtes invité, "effectuer un redémarrage progressif" pour activer les modules de cryptographie sur tous les nœuds. Utilisez **Maintenance** > **Rolling reboot** pour lancer et surveiller les redémarrages.

c. Sélectionnez **Support** > **Diagnostics** pour afficher les versions actives du module FIPS.

3. Pour consulter les détails des chiffrements, protocoles et algorithmes de chaque politique, sélectionnez **Afficher les détails**.
4. Pour modifier la politique actuelle, sélectionnez **Utiliser la politique**.

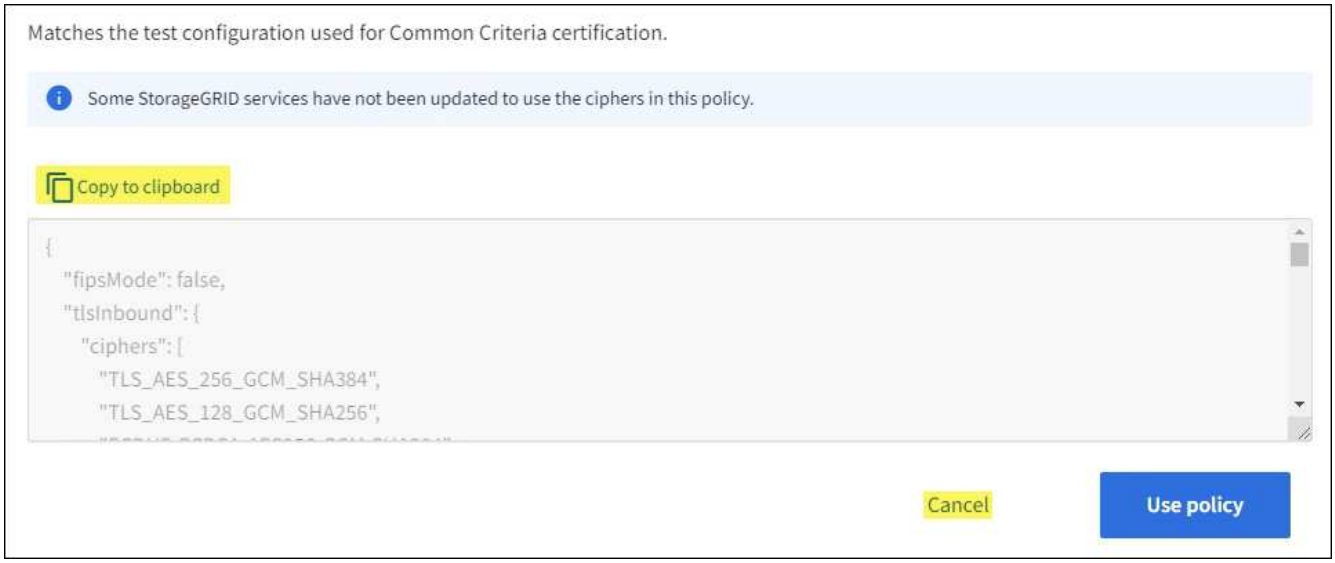
   Une coche verte apparaît à côté de **Current policy** sur la vignette de la politique.

Créer une politique de sécurité personnalisée

Vous pouvez créer une politique personnalisée si vous devez appliquer vos propres chiffrements.

Étapes

1. À partir de la vignette de la politique la plus similaire à la politique personnalisée que vous souhaitez créer, sélectionnez **Afficher les détails**.
2. Sélectionnez **Copier dans le presse-papiers**, puis sélectionnez **Annuler**.



3. Dans la vignette **Stratégie personnalisée**, sélectionnez **Configurer et utiliser**.
4. Collez le JSON que vous avez copié et apportez les modifications nécessaires.
5. Sélectionnez **Utiliser la stratégie**.

   Une coche verte apparaît à côté de **Police actuelle** sur la vignette **Police personnalisée**.

6. Vous pouvez également sélectionner **Modifier la configuration** pour apporter d'autres modifications à la nouvelle politique personnalisée.

Rétablir temporairement la politique de sécurité par défaut

Si vous avez configuré une stratégie de sécurité personnalisée, vous pourriez ne pas être en mesure de vous connecter au Grid Manager si la stratégie TLS configurée est incompatible avec le "certificat de serveur configuré".

Vous pouvez temporairement rétablir la politique de sécurité par défaut.

Étapes

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

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
2. Exécutez la commande suivante :

   ```
   restore-default-cipher-configurations
   ```
3. Depuis un navigateur Web, accédez au Grid Manager sur le même nœud d'administration.
4. Suivez les étapes décrites dans Sélectionnez une politique de sécurité pour configurer à nouveau la politique.

Configurer la sécurité du réseau et des objets StorageGRID

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 Storage Nodes à utiliser HTTP au lieu de HTTPS.

Chiffrement des objets stockés

Le chiffrement des objets stockés permet de chiffrer toutes les données des objets 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 chiffrement AES-128 ou AES-256. Lorsque vous activez ce paramètre, tous les nouveaux objets ingérés 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 nouveaux objets 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 au niveau de l'objet.

Pour plus de détails sur les méthodes de chiffrement StorageGRID, voir "Passez en revue les méthodes de chiffrement de StorageGRID".

Empêcher la modification du client

Empêcher la modification par le client est un paramètre à l'échelle du système. Lorsque l'option **Empêcher la modification par le client** est sélectionnée, les requêtes suivantes sont refusées.

API REST S3

- DeleteBucket demandes
- Toute demande de modification des données, des métadonnées définies par l'utilisateur ou du balisage d'objet S3 existant

Activer HTTP pour les connexions au nœud de stockage

Par défaut, les applications clientes utilisent le protocole réseau HTTPS pour toute connexion directe aux Storage Nodes. Vous pouvez activer le protocole HTTP pour ces connexions, par exemple lors du test d'une grille hors production.

Utilisez HTTP pour les connexions aux nœuds de stockage uniquement si les clients S3 doivent établir des connexions HTTP directes avec ces nœuds. Vous n'avez pas besoin d'utiliser cette option pour les clients qui utilisent uniquement des connexions HTTPS ou pour les clients qui se connectent au service Load Balancer (car vous pouvez "configurer chaque point de terminaison d'équilibrage de charge" utiliser HTTP ou HTTPS).

Consultez "Résumé : adresses IP et ports pour les connexions client" pour savoir quels ports les clients S3 utilisent lorsqu'ils se connectent 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 des droits d'accès root.

Étapes

1. Sélectionnez **Configuration** > **Sécurité** > **Paramètres de sécurité**.
2. Sélectionnez l'onglet **Réseau et objets**.
3. Pour le chiffrement des objets stockés, utilisez le paramètre **Aucun** (par défaut) si vous ne souhaitez pas que les objets stockés soient chiffrés, ou sélectionnez **AES-128** ou **AES-256** pour chiffrer les objets stockés.
4. Vous pouvez également sélectionner **Empêcher la modification du client** si vous souhaitez empêcher les clients S3 d'effectuer des requêtes spécifiques.

   Si vous modifiez ce paramètre, il faudra environ une minute pour que le nouveau paramètre soit appliqué. La valeur configurée est mise en cache pour optimiser les performances et la mise à l'échelle.

5. Vous pouvez également sélectionner **Activer HTTP pour les connexions aux nœuds de stockage** si les clients se connectent directement aux nœuds de stockage et que vous souhaitez utiliser des connexions HTTP.

   Soyez prudent lorsque vous activez le protocole HTTP pour une grille de production, car les requêtes seront envoyées sans chiffrement.

6. Sélectionnez **Enregistrer**.

Modifier les paramètres de sécurité de l'interface StorageGRID

Les paramètres de sécurité de l'interface vous permettent de contrôler si les utilisateurs sont déconnectés s'ils sont inactifs pendant une durée supérieure à celle spécifiée 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 root".

À propos de cette tâche

La page **Paramètres de sécurité** comprend les paramètres **Délai d'inactivité du navigateur** et **Trace de pile de l'API de gestion**.

Délai d'inactivité du navigateur

Indique la durée pendant laquelle le navigateur d'un utilisateur peut rester inactif avant que l'utilisateur ne soit déconnecté. La valeur par défaut est de 15 minutes.

Le délai d'inactivité du navigateur est également contrôlé par les éléments suivants :

- Un minuteur StorageGRID distinct et non configurable est 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) soit activée pour StorageGRID.

  Si l'authentification unique (SSO) est activée et que la session du navigateur d'un utilisateur expire, ce dernier doit saisir à nouveau ses identifiants SSO pour accéder de nouveau à StorageGRID. Voir "Fonctionnement de l'authentification unique (SSO)".

Trace de pile de l'API de gestion

Contrôle si une trace de pile est renvoyée dans les réponses d'erreur des API Grid Manager et Tenant Manager.

Cette option est désactivée par défaut, mais vous pouvez activer cette fonctionnalité pour un environnement de test. En règle générale, vous devez laisser la trace de pile désactivée dans les environnements de production afin d'éviter de révéler des détails internes du logiciel lorsque des erreurs d'API se produisent.

Étapes

1. Sélectionnez **Configuration** > **Sécurité** > **Paramètres de sécurité**.
2. Sélectionnez l'onglet **Interface**.
3. Pour modifier le paramètre de délai d'inactivité du navigateur :
   a. Déployez l'accordéon.
   b. Pour modifier le délai d'expiration, spécifiez une valeur comprise entre 60 secondes et 7 jours. Le délai d'expiration par défaut est de 15 minutes.

c. Pour désactiver cette fonctionnalité, décochez la case.

d. Sélectionnez **Enregistrer**.

Ce nouveau paramètre n'affecte pas les utilisateurs déjà connectés. Les utilisateurs doivent se reconnecter ou actualiser leur navigateur pour que le nouveau délai d'expiration prenne effet.

4. Pour modifier le paramètre de trace de pile de l'API de gestion :

a. Déployez l'accordéon.

b. Cochez la case pour afficher 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 afin d'éviter de révéler des détails internes du logiciel en cas d'erreurs d'API.

c. Sélectionnez **Enregistrer**.

Gérer l'accès SSH externe dans StorageGRID

Gérez l'accès SSH au trafic entrant dans la grille en bloquant ou en autorisant l'accès externe. La gestion de l'accès SSH externe n'a aucun impact sur le trafic entre les nœuds de la grille.

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 root".

À propos de cette tâche

Pour renforcer la sécurité du système, l'accès SSH externe est bloqué par défaut. Si vous devez effectuer des tâches nécessitant un accès SSH entrant, comme le dépannage, autorisez temporairement l'accès externe. Lorsque vous avez terminé la tâche, bloquez l'accès externe.

Étapes

1. Sélectionnez **Configuration** > **Sécurité** > **Paramètres de sécurité**.
2. Sélectionnez l'onglet **Bloquer SSH**.
3. Utilisez l'option **Bloquer l'accès SSH entrant** pour gérer l'accès SSH externe :

a. Cochez la case pour bloquer l'accès (par défaut).

b. Décochez la case pour autoriser l'accès.

Nécessite un accès au port 22 entre l'ordinateur portable de service et tous les autres nœuds du grid. Supprimez l'accès au port 22 une fois la tâche de maintenance terminée.

4. Sélectionnez **Enregistrer**.

Configurer les serveurs de gestion des clés

Découvrez les serveurs de gestion des clés dans StorageGRID

Un serveur de gestion de clés (KMS) est un système externe tiers qui fournit des clés de chiffrement aux nœuds d'appliance StorageGRID sur le site StorageGRID associé en utilisant le protocole d'interopérabilité de gestion de clés (KMIP).

StorageGRID ne prend en charge que certains serveurs de gestion de clés. Pour obtenir la liste des produits et des versions pris en charge, utilisez le "Outil de matrice d'interopérabilité (IMT) NetApp".

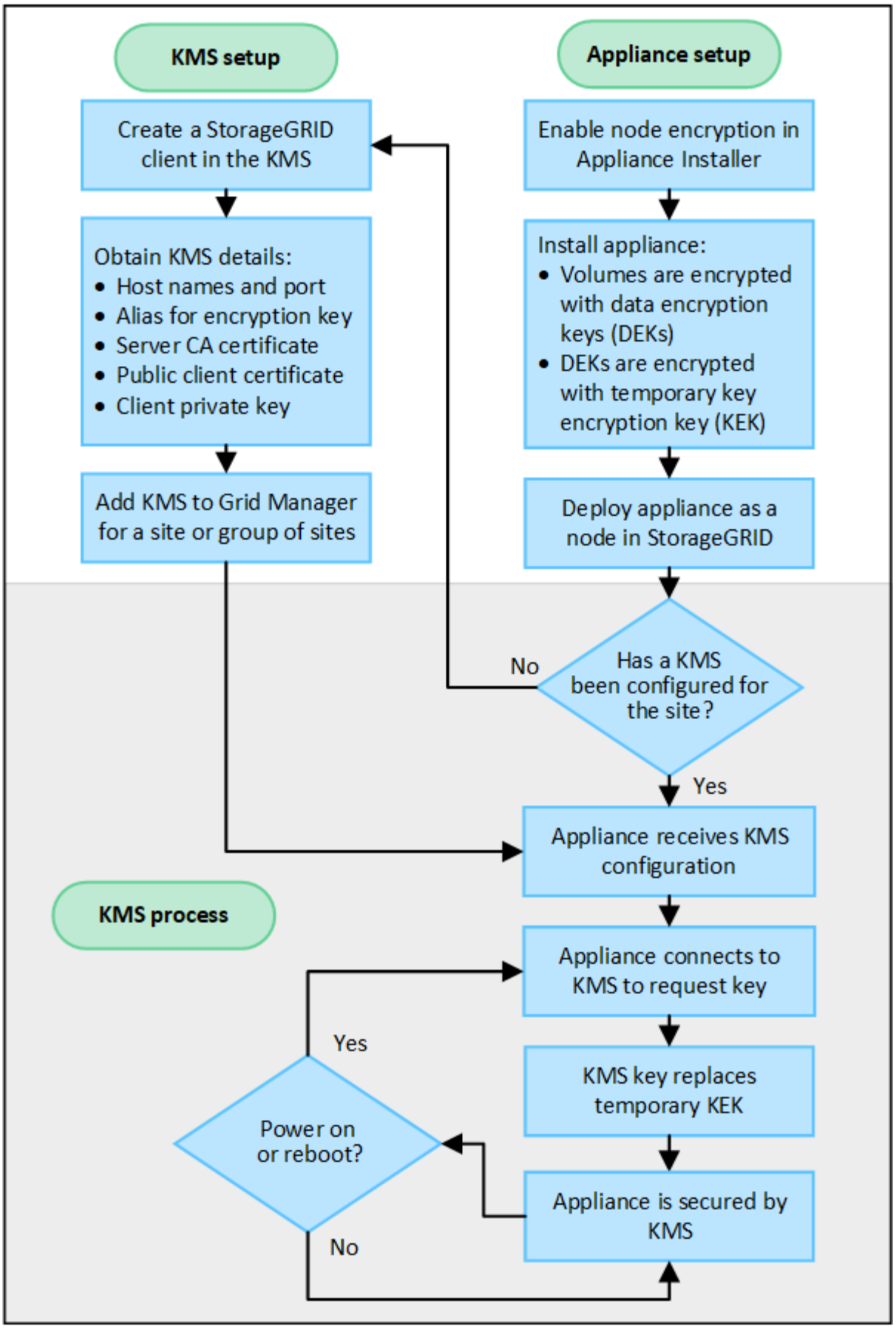
Vous pouvez utiliser un ou plusieurs serveurs de gestion de clés pour gérer les clés de chiffrement des nœuds StorageGRID dont l'option **Chiffrement des nœuds** est activée lors de l'installation. L'utilisation de serveurs de gestion de clés avec ces nœuds StorageGRID vous permet de protéger vos données même si un dispositif est retiré du centre de données. Une fois les volumes du dispositif chiffrés, vous ne pouvez accéder à aucune donnée sur le dispositif, sauf si le nœud peut communiquer avec le KMS.

> StorageGRID ne crée ni ne gère les clés externes utilisées pour chiffrer et déchiffrer les nœuds de l'appliance. Si vous prévoyez d'utiliser un serveur de gestion de clés externe pour protéger les données StorageGRID, vous devez comprendre comment configurer ce serveur et comment gérer les clés de chiffrement. L'exécution des tâches de gestion des clés dépasse le cadre de ces instructions. Si vous avez besoin d'aide, consultez la documentation de votre serveur de gestion de clés ou contactez le support technique.

Configuration du serveur de gestion des clés et de l'appliance StorageGRID

Avant de pouvoir utiliser un serveur de gestion de clés (KMS) pour sécuriser les données StorageGRID sur les nœuds de l'appliance, vous devez effectuer deux tâches de configuration : configurer un ou plusieurs serveurs KMS et activer le chiffrement des nœuds de l'appliance. Une fois ces deux tâches de configuration terminées, le processus de gestion des clés s'effectue automatiquement.

Le diagramme illustre les grandes étapes de l'utilisation d'un KMS pour sécuriser les données StorageGRID sur les nœuds de l'appliance.



Le diagramme montre que la configuration du KMS et celle de l'appliance se déroulent en parallèle ;

cependant, vous pouvez configurer les serveurs de gestion des clés avant ou après avoir activé le chiffrement pour les nouveaux nœuds de l'appliance, en fonction de vos besoins.

Configurer le serveur de gestion des clés (KMS)

La mise en place d'un serveur de gestion de clés comprend les étapes générales suivantes.

Étape	Consultez
Accédez au logiciel KMS et ajoutez un client pour StorageGRID à chaque KMS ou cluster KMS.	"Configurez StorageGRID en tant que client dans le KMS"
Obtenez les informations requises pour le client StorageGRID sur le KMS.	"Configurez StorageGRID en tant que client dans le KMS"
Ajoutez le KMS au Grid Manager, attribuez-le à un seul site ou à un groupe de sites par défaut, téléversez les certificats requis et enregistrez la configuration du KMS.	"Ajouter un serveur de gestion de clés (KMS)"

Configurez l'appareil

La configuration d'un nœud d'appliance pour une utilisation KMS comprend les étapes générales suivantes.

1. Lors de la phase de configuration matérielle de l'installation de l'appliance, utilisez le StorageGRID Appliance Installer pour activer le paramètre **Chiffrement de nœud** pour l'appliance.

   > Vous ne pouvez pas activer le paramètre **Chiffrement des nœuds** après l'ajout d'un appareil à la grille, et vous ne pouvez pas utiliser la gestion de clés externes pour les appareils qui n'ont pas le chiffrement des nœuds activé.

2. Exécutez le programme d'installation de l'appliance StorageGRID. Lors de l'installation, une clé de chiffrement de données (DEK) aléatoire est attribuée à chaque volume de l'appliance, comme suit :
   - Les clés DEK servent à chiffrer les données de chaque volume. Ces clés sont générées à l'aide du chiffrement de disque Linux Unified Key Setup (LUKS) dans le système d'exploitation de l'appliance et ne peuvent pas être modifiées.
   - Chaque DEK individuel est chiffré par une clé de chiffrement principale (KEK). La KEK initiale est une clé temporaire qui chiffre les DEK jusqu'à ce que l'appliance puisse se connecter au KMS.
3. Ajoutez le nœud de l'appliance à StorageGRID.

Voir "Activer le chiffrement des nœuds" pour plus de détails.

Processus de chiffrement de la gestion des clés (effectué automatiquement)

Le chiffrement avec gestion des clés comprend les étapes générales suivantes, qui sont exécutées automatiquement.

1. Lorsque vous installez dans la grille un appareil dont le chiffrement des nœuds est activé, 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 aucun KMS n'a encore été configuré pour le site, les données sur l'appliance continuent d'être chiffrées par la KEK temporaire jusqu'à ce que vous configuriez un KMS pour le site et que l'appliance reçoive la configuration KMS.

2. L'appareil utilise la configuration KMS pour se connecter au KMS et demander une clé de chiffrement.
3. Le KMS envoie une clé de chiffrement à l'appliance. La nouvelle clé provenant du KMS remplace la clé KEK temporaire et est désormais utilisée pour chiffrer et déchiffrer les clés DEK des volumes de l'appliance.

> Toutes les données existantes avant la connexion du nœud de l'appliance chiffrée 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 contre leur suppression du centre de données tant que la clé temporaire n'est pas remplacée par la clé de chiffrement KMS.

4. Si l'appareil est mis sous tension ou redémarré, il se reconnecte au KMS pour demander la clé. La clé, qui est enregistrée en mémoire volatile, ne peut pas survivre à une coupure de courant ou à un redémarrage.

Exigences et considérations relatives au serveur de gestion des clés StorageGRID

Avant de configurer un serveur de gestion de clés externe (KMS), vous devez comprendre les considérations et les exigences.

Quelle version de KMIP est prise en charge ?

StorageGRID prend en charge la version 1.4 de KMIP.

"Spécification du protocole d'interopérabilité de gestion des clés, version 1.4"

Quelles sont les considérations relatives au réseau ?

Les paramètres du pare-feu réseau doivent autoriser chaque nœud de l'appliance à communiquer via le port utilisé pour le protocole Key Management Interoperability Protocol (KMIP). Le port KMIP par défaut est 5696.

Vous devez vous assurer que chaque nœud d'appliance utilisant le chiffrement dispose d'un accès réseau au KMS ou au cluster KMS que vous avez configuré pour le site.

Quelles versions de TLS sont prises en charge ?

Les communications entre les nœuds de l'appliance et le KMS configuré utilisent des connexions TLS sécurisées. StorageGRID peut prendre en charge soit le protocole TLS 1.2, soit le protocole TLS 1.3 lors des connexions KMIP à un KMS ou un cluster KMS, en fonction de ce que le KMS prend en charge et de celui que "Politique TLS et SSH" vous utilisez.

StorageGRID négocie le protocole et le chiffrement (TLS 1.2) ou la suite de chiffrement (TLS 1.3) avec le KMS lors de l'établissement de la connexion. Pour connaître les versions de protocole et les chiffrements/suites de chiffrement disponibles, consultez la `tlsOutbound` section de la politique TLS et SSH active de la grille (**Configuration** > **Sécurité Paramètres de sécurité**).

Quels appareils sont pris en charge ?

Vous pouvez utiliser un serveur de gestion de clés (KMS) pour gérer les clés de chiffrement de tout appareil StorageGRID de votre grille dont l'option **Chiffrement des nœuds** est activée. Cette option ne peut être activée que lors de l'étape de configuration matérielle de l'installation de l'appareil, à l'aide de l'outil StorageGRID Appliance Installer.

Vous ne pouvez pas activer le chiffrement du nœud après l'ajout d'un appareil à la grille, et vous ne pouvez pas utiliser la gestion externe des clés pour les appareils qui n'ont pas le chiffrement du nœud activé.

Vous pouvez utiliser le KMS configuré pour les appliances StorageGRID et les nœuds d'appliance.

Vous ne pouvez pas utiliser le KMS configuré pour les nœuds logiciels (non-appliance), notamment les suivants :

- Nœuds déployés en tant que machines virtuelles (VM)
- Nœuds déployés au sein de moteurs de conteneurs sur des hôtes Linux

Les nœuds déployés sur ces autres plateformes peuvent utiliser le chiffrement en dehors de StorageGRID au niveau du datastore ou du disque.

Quand dois-je configurer les serveurs de gestion des clés ?

Lors d'une nouvelle installation, vous devez généralement configurer un ou plusieurs serveurs de gestion de clés dans Grid Manager avant de créer des locataires. Cet ordre garantit que les nœuds sont protégés avant que des données d'objets ne soient stockées dessus.

Vous pouvez configurer les serveurs de gestion des clés dans Grid Manager avant ou après l'installation des nœuds de l'appliance.

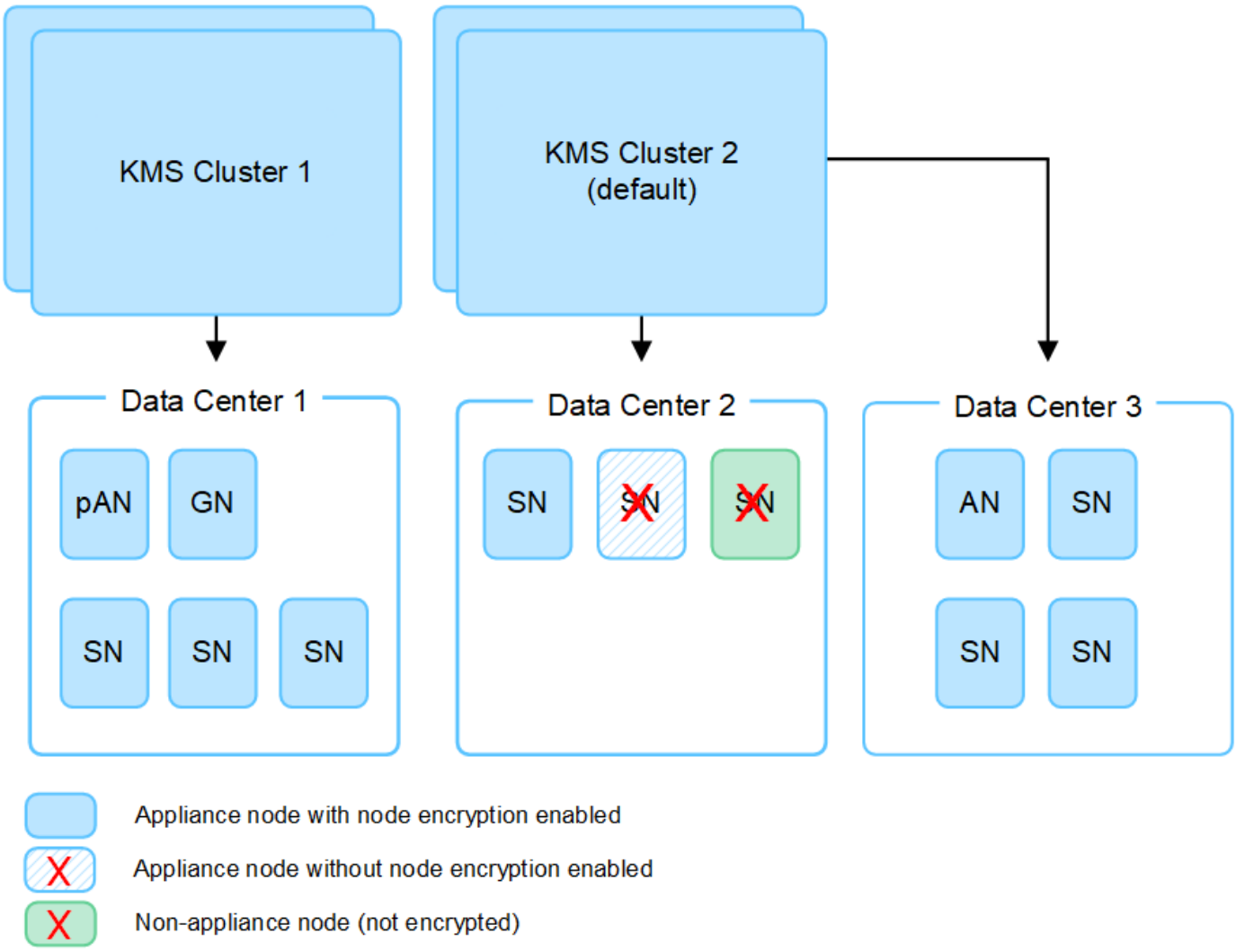
De combien de serveurs de gestion de clés avez-vous besoin ?

Vous pouvez configurer un ou plusieurs serveurs de gestion de clés externes pour fournir des clés de chiffrement aux nœuds d'appliance de votre système StorageGRID. Chaque KMS fournit une seule clé de chiffrement aux nœuds d'appliance StorageGRID d'un site ou d'un groupe de sites.

StorageGRID prend en charge l'utilisation de clusters KMS. Chaque cluster KMS contient plusieurs serveurs de gestion de clés répliqués qui partagent les paramètres de configuration et les clés de chiffrement. L'utilisation de clusters KMS pour la gestion des clés est recommandée car elle améliore les capacités de basculement d'une configuration à haute disponibilité.

Par exemple, supposons que votre système StorageGRID comporte trois centres de données. Vous pouvez configurer un cluster KMS pour fournir une clé à tous les nœuds d'appliance du Data Center 1 et un second cluster KMS pour fournir une clé à tous les nœuds d'appliance de tous 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 un KMS pour les nœuds non-appliance ou pour les nœuds d'appliance dont 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 bonne pratique de sécurité, vous devez périodiquement "faites pivoter la clé de chiffrement" utilisée par chaque KMS configuré.

Lorsque la nouvelle version de la clé sera disponible :

- Elle est automatiquement distribuée aux nœuds d'appliance chiffrés du ou des sites associés au KMS. La distribution doit avoir lieu dans l'heure suivant la rotation de la clé.
- Si le nœud de l'appliance chiffrée est hors ligne lors de la distribution de la nouvelle version de la clé, il recevra la nouvelle clé dès son redémarrage.
- Si la nouvelle version de la clé ne peut pas être utilisée pour chiffrer les volumes de l'appliance pour quelque raison que ce soit, l'alerte **KMS encryption key rotation failed** 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 son chiffrement ?

Si vous devez installer un dispositif chiffré dans un autre système StorageGRID, vous devez d'abord mettre hors service le nœud de la grille afin de déplacer les données d'objet vers un autre nœud. Ensuite, vous pouvez utiliser le StorageGRID Appliance Installer "effacer la configuration KMS". La suppression de la

configuration KMS désactive le paramètre **Node Encryption** et supprime l'association entre le nœud du dispositif et la configuration KMS pour le site StorageGRID.

> Sans accès à la clé de chiffrement KMS, toutes les données restant sur l'appareil ne peuvent plus être accessibles et sont définitivement verrouillées.

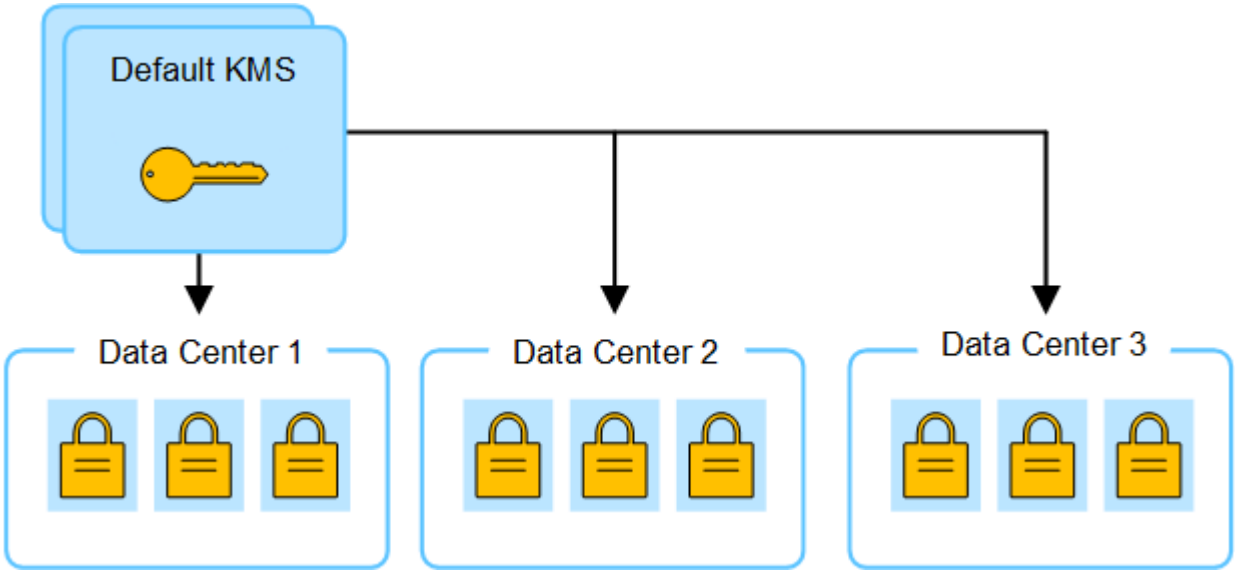
Considérations relatives à la modification du KMS pour un site StorageGRID

Chaque serveur de gestion de clés (KMS) ou cluster KMS fournit une clé de chiffrement à tous les nœuds d'appliance d'un site ou d'un groupe de sites. Si vous devez changer le KMS utilisé pour un site, vous devrez peut-être copier la clé de chiffrement d'un KMS à un autre.

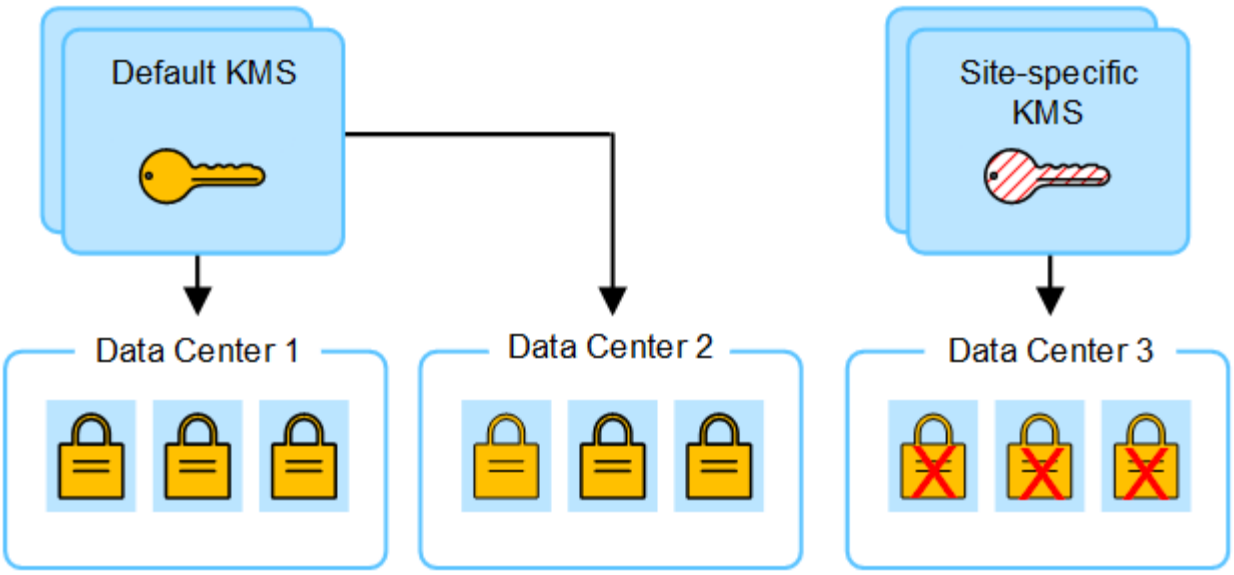
Si vous modifiez le KMS utilisé pour un site, vous devez vous assurer que les nœuds d'appliance précédemment chiffrés sur ce site peuvent être déchiffrés à l'aide de la clé stockée sur le nouveau KMS. Dans certains cas, vous pourriez avoir besoin de copier la version actuelle de la clé de chiffrement du KMS d'origine vers le nouveau KMS. Vous devez vous assurer que le KMS possède la clé correcte pour déchiffrer les nœuds d'appliance chiffrés sur le site.

Par exemple :

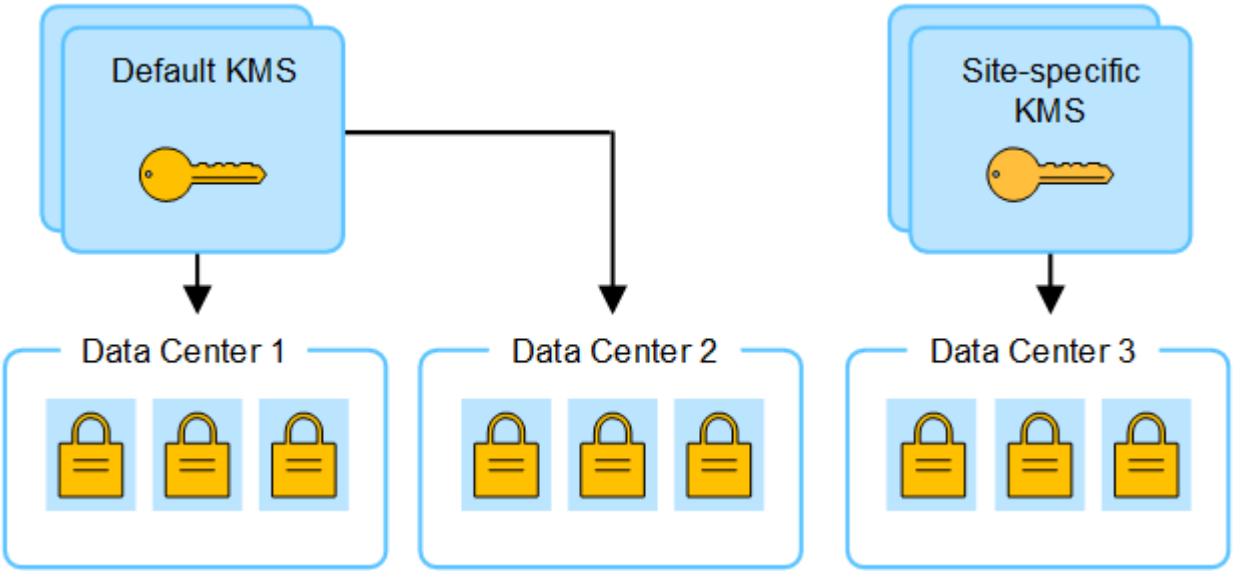
1. Vous configurez initialement un KMS par défaut qui s'applique à tous les sites ne disposant pas d'un KMS dédié.
2. Une fois le KMS enregistré, tous les nœuds d'appliance dont le paramètre **Chiffrement des nœuds** est activé se connectent au KMS et demandent la clé de chiffrement. Cette clé est utilisée pour chiffrer les nœuds d'appliance sur tous les sites. Cette même clé doit également être utilisée pour déchiffrer ces appliances.



3. Vous décidez d'ajouter un KMS spécifique au site (Data Center 3 sur la figure). Cependant, comme les nœuds de l'appliance sont déjà chiffrés, une erreur de validation se produit lorsque vous tentez d'enregistrer la configuration du KMS spécifique au site. L'erreur se produit parce que le KMS spécifique au site ne possède pas la clé correcte pour déchiffrer les nœuds de ce site.



4. Pour résoudre ce problème, vous copiez la version actuelle de la clé de chiffrement du KMS par défaut vers le nouveau KMS. (Techniquement, vous copiez la clé d'origine vers une nouvelle clé avec le même alias. La clé d'origine devient une version antérieure de la nouvelle clé.) Le KMS spécifique au site dispose désormais de la clé correcte pour déchiffrer les nœuds de l'appliance du Data Center 3, elle peut donc être enregistrée dans StorageGRID.



Cas d'utilisation pour la modification du KMS utilisé pour un site

Le tableau récapitule les étapes nécessaires pour les cas les plus courants de modification du KMS d'un site.

Cas d'utilisation pour la modification du KMS d'un site	Étapes requises
Vous disposez d'une ou plusieurs entrées KMS spécifiques au site, et vous souhaitez en utiliser une comme KMS par défaut.	Modifiez le KMS spécifique au site. Dans le champ **Gère les clés pour**, sélectionnez **Sites non gérés par un autre KMS (KMS par défaut)**. Le KMS spécifique au site sera désormais utilisé comme KMS par défaut. Il s'appliquera à tous les sites qui n'ont pas de KMS dédié. "Modifier un serveur de gestion de clés (KMS)"
Vous disposez d'un KMS par défaut et vous ajoutez un nouveau site lors d'une extension. Vous ne souhaitez pas utiliser le KMS par défaut pour le nouveau site.	1. Si les nœuds de l'appliance sur le nouveau site ont déjà été chiffrés par le KMS par défaut, utilisez le logiciel KMS pour copier la version actuelle de la clé de chiffrement du KMS par défaut vers un nouveau KMS. 2. À l'aide du Grid Manager, ajoutez le nouveau KMS et sélectionnez le site. "Ajouter un serveur de gestion de clés (KMS)"
Vous souhaitez que le KMS d'un site utilise un serveur différent.	1. Si les nœuds de l'appliance sur le site ont déjà été chiffrés par le KMS existant, utilisez le logiciel KMS pour copier la version actuelle de la clé de chiffrement du KMS existant vers le nouveau KMS. 2. À l'aide du Grid Manager, modifiez la configuration KMS existante et saisissez le nouveau nom de l'hôte ou la nouvelle adresse IP. "Ajouter un serveur de gestion de clés (KMS)"

Configurez StorageGRID en tant que client dans le KMS

Vous devez configurer StorageGRID en tant que client pour chaque serveur de gestion de clés externe ou cluster KMS avant de pouvoir ajouter le KMS à StorageGRID.

Ces instructions s'appliquent à Thales CipherTrust Manager et Hashicorp Vault. Pour obtenir la liste des produits et versions compatibles, utilisez le "Outil de matrice d'interopérabilité (IMT) NetApp".

Étapes

1. À partir du logiciel KMS, créez un client StorageGRID pour chaque KMS ou cluster KMS que vous prévoyez d'utiliser.

   Chaque KMS gère une seule clé de chiffrement pour les nœuds des appliances StorageGRID sur un seul site ou sur un groupe de sites.

2. Créez une clé en utilisant l'une des deux méthodes suivantes :
   - Utilisez la page de gestion des clés de votre produit KMS. Créez une clé de chiffrement AES pour chaque KMS ou cluster KMS.

     La clé de chiffrement doit comporter au moins 2 048 bits et être exportable.

   - Laissez StorageGRID créer la clé. Vous serez invité à le faire lors du test et de l'enregistrement après

"téléversement des certificats clients".

3. Enregistrez les informations suivantes pour chaque KMS ou cluster KMS.

   Vous aurez besoin de ces informations lorsque vous ajouterez le KMS à StorageGRID :

   - Nom d'hôte ou adresse IP pour chaque serveur.
   - Port KMIP utilisé par le KMS.
   - Alias de la clé de chiffrement dans le KMS.

4. Pour chaque KMS ou cluster KMS, obtenez un certificat serveur signé par une autorité de certification (CA) ou un ensemble de certificats contenant chacun des fichiers de certificat CA encodés au format 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 en Base-64 Privacy Enhanced Mail (PEM).
   - Le champ Subject Alternative Name (SAN) de chaque certificat de serveur doit inclure le domaine complet (FQDN) ou l'adresse IP auquel StorageGRID se connectera.

     > Lorsque vous configurez le KMS dans StorageGRID, vous devez saisir 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. Obtenez le certificat client public délivré à StorageGRID par le KMS externe et la clé privée du certificat client.

   Le certificat client permet à StorageGRID de s'authentifier auprès du KMS.

Ajouter un serveur de gestion de clés dans StorageGRID

Vous utilisez l'assistant du serveur de gestion de clés StorageGRID pour ajouter chaque KMS ou cluster KMS.

Avant de commencer

- Vous avez examiné le "Considérations et exigences relatives à l'utilisation d'un serveur de gestion de clés".
- Vous avez "configuré StorageGRID comme client dans le KMS", et vous disposez des informations requises pour chaque KMS ou cluster KMS.
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur Web pris en charge".
- Vous avez le "Autorisation d'accès root".

À propos de cette tâche

Si possible, configurez les serveurs de gestion de clés spécifiques à chaque site avant de configurer un KMS par défaut applicable à tous les sites non gérés par un autre KMS. Si vous créez d'abord le KMS par défaut, tous les équipements chiffrés au niveau des nœuds dans la grille seront chiffrés par le KMS par défaut. Si vous souhaitez créer un KMS spécifique à un site ultérieurement, vous devez d'abord copier la version actuelle de la clé de chiffrement du KMS par défaut vers le nouveau KMS. Voir "Considérations relatives à la modification du KMS d'un site" pour plus de détails.

Étape 1 : Détails du KMS

À l'étape 1 (détails KMS) de l'assistant Ajouter un serveur de gestion de clés, vous fournissez des détails sur le KMS ou le cluster KMS.

Étapes

1. Sélectionnez **Configuration** > **Security** > **Key management server**.

   La page du serveur de gestion des clés s'affiche avec l'onglet Détails de la configuration sélectionné.

2. Sélectionnez **Create**.

   L'étape 1 (détails KMS) de l'assistant Ajouter un serveur de gestion de clés apparaît.

3. Saisissez les informations suivantes concernant le KMS et le client StorageGRID que vous avez configuré dans ce KMS.

Champ	Description
Nom 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.
Gère les clés pour	Le site StorageGRID qui sera associé à ce KMS. Si possible, vous devez configurer les serveurs de gestion de clés spécifiques à un site avant de configurer un KMS par défaut qui s'applique à tous les sites non gérés par un autre KMS. • Sélectionnez un site si ce KMS doit gérer les clés de chiffrement des 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 ne disposant pas d'un KMS dédié et à tous les sites que vous ajouterez lors d'extensions ultérieures. **Remarque :** Une erreur de validation se produira lors de l'enregistrement de la configuration KMS si vous sélectionnez un site qui était précédemment chiffré par le KMS par défaut, mais que vous n'avez pas fourni la version actuelle de la clé de chiffrement d'origine au nouveau KMS.
Port	Le port que le serveur KMS utilise pour les communications Key Management Interoperability Protocol (KMIP). La valeur par défaut est 5696, qui est le port standard KMIP.

Champ	Description
Nom d'hôte	Le domaine complet ou l'adresse IP du KMS. **Remarque :** Le champ Nom alternatif du sujet (SAN) du certificat serveur doit inclure le domaine complet (FQDN) ou l'adresse IP que vous saisissez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ni 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 **Continue**.

Étape 2 : Télécharger le certificat du serveur

À l'étape 2 (Téléchargement du certificat serveur) de l'assistant Ajout d'un serveur de gestion de clés, vous téléchargez le certificat serveur (ou le lot de certificats) pour le KMS. Le certificat serveur permet au KMS externe de s'authentifier auprès de StorageGRID.

Étapes

1. À partir de l'**étape 2 (Télécharger le certificat du serveur)**, accédez à l'emplacement du certificat du serveur enregistré ou du bundle de certificats.
2. Téléchargez le fichier de certificat.

   Les métadonnées du certificat du serveur apparaissent.

   > Si vous avez importé un ensemble de certificats, les métadonnées de chaque certificat apparaissent dans son propre onglet.

3. Sélectionnez **Continue**.

Étape 3 : Téléversez les certificats clients

À l'étape 3 (Téléchargement des certificats clients) de l'assistant Ajout d'un serveur de gestion de clés, vous téléchargez le certificat client et la clé privée du certificat client. Le certificat client permet à StorageGRID de s'authentifier auprès du KMS.

Étapes

1. À partir de l'**étape 3 (Télécharger les certificats clients)**, accédez à l'emplacement du certificat client.
2. Téléchargez le fichier de certificat client.

   Les métadonnées du certificat client apparaissent.

3. Accédez à l'emplacement de la clé privée du certificat client.
4. Téléversez le fichier de clé privée.
5. Sélectionnez **Tester et enregistrer**.

   Si aucune clé n'existe, vous êtes invité à laisser StorageGRID en créer une.

   Les connexions entre le serveur de gestion des clés et les nœuds de l'appliance sont testées. Si toutes les connexions sont valides et que la clé correcte est trouvée sur le KMS, le nouveau serveur de gestion des

clés est ajouté au tableau 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. StorageGRID peut prendre jusqu'à 30 minutes pour obtenir l'état réel de chaque certificat. Vous devez actualiser votre navigateur web pour voir l'état actuel.

6. Si un message d'erreur apparaît lorsque vous sélectionnez **Tester et enregistrer**, consultez les détails du message, puis sélectionnez **OK**.

   Par exemple, vous pourriez recevoir une erreur 422 : Entité non traitable si un test de connexion a échoué.

7. Si vous devez enregistrer la configuration actuelle sans tester la connexion externe, sélectionnez **Forcer l'enregistrement**.

   > L'option **Forcer l'enregistrement** sauvegarde la configuration KMS, mais ne teste pas la connexion externe de chaque appliance à ce KMS. En cas de problème de configuration, il se peut que vous ne puissiez pas redémarrer les nœuds d'appliance dont le chiffrement de nœud est activé sur le site concerné. Vous pourriez perdre l'accès à vos données jusqu'à la résolution des problèmes.

8. Examinez 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 serveur de gestion de clés dans StorageGRID

La gestion d'un serveur de gestion de clés (KMS) implique la consultation ou la modification des détails, la gestion des certificats, la consultation 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 KMS

Vous pouvez consulter les informations relatives à chaque serveur de gestion de clés (KMS) dans votre système StorageGRID, notamment les détails des clés et l'état actuel des certificats du serveur et du client.

Étapes

1. Sélectionnez **Configuration** > **Security** > **Key management server**.

   La page du serveur de gestion des clés s'affiche et présente les informations suivantes :

   - L'onglet Détails de la configuration répertorie tous les serveurs de gestion des clés configurés.
   - L'onglet « Nœuds chiffrés » répertorie tous les nœuds dont le chiffrement de nœud est activé.

2. Pour consulter les détails d'un KMS spécifique et effectuer des opérations sur ce KMS, sélectionnez le nom du KMS. La page de détails du KMS affiche les informations suivantes :

Champ	Description
Gère les clés pour	Le site StorageGRID associé au KMS. Ce champ affiche le nom d'un site StorageGRID spécifique ou **des sites non gérés par un autre KMS (KMS par défaut).**
Nom d'hôte	Le domaine complet ou l'adresse IP du KMS. S'il existe un cluster de deux serveurs de gestion de clés, le domaine complet ou l'adresse IP des deux serveurs est indiqué. S'il existe plus de deux serveurs de gestion de clés dans un cluster, le domaine complet ou l'adresse IP du premier KMS est indiqué, ainsi que le nombre de serveurs de gestion de clés supplémentaires dans le cluster. Par exemple : `10.10.10.10 and 10.10.10.11` ou `10.10.10.10 and 2 others`. Pour afficher tous les noms d'hôte d'un cluster, 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	L'alias de clé pour le client StorageGRID dans le KMS.
UID de la clé	L'identifiant unique de la dernière version de la clé.	Dernière modification
Date et heure de la dernière version de la clé.	Certificat serveur	Métadonnées
Les métadonnées du certificat, telles que le numéro de série, la date et l'heure d'expiration, et le certificat PEM.	Certificat PEM	Le contenu du fichier PEM (privacy enhanced mail) pour le certificat.
Certificat client	Métadonnées	Les métadonnées du certificat, telles que le numéro de série, la date et l'heure d'expiration, et le certificat PEM.

4. Aussi souvent que nécessaire selon les pratiques de sécurité de votre organisation, sélectionnez **Rotate key** ou utilisez le logiciel KMS pour créer une nouvelle version de la clé.

   Lorsque la rotation de la clé réussit, les champs Key UID 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 cette même clé. Ne faites pas pivoter vers une clé totalement différente.

Ne tentez jamais de faire tourner une clé en modifiant son nom (alias) auprès du KMS. StorageGRID exige que toutes les versions de clés précédemment utilisées (ainsi que les futures) soient accessibles depuis le KMS avec le même alias de clé. Si vous modifiez l'alias de clé pour un KMS configuré, StorageGRID pourrait ne pas être en mesure de déchiffrer vos données.

Gérer les certificats

Réglez rapidement tout problème lié aux certificats serveur ou client. Si possible, remplacez les certificats avant leur expiration.

Vous devez régler tout problème de certificat dès que possible afin de maintenir l'accès aux données.

Étapes

1. Sélectionnez **Configuration** > **Security** > **Key management server**.
2. Dans le tableau, consultez la valeur de l'expiration du certificat pour chaque KMS.
3. Si la date d'expiration du certificat de n'importe quel KMS est inconnue, attendez jusqu'à 30 minutes, puis actualisez votre navigateur web.
4. Si la colonne « Expiration du certificat » indique qu'un certificat a expiré ou est sur le point d'expirer, sélectionnez le KMS pour accéder à la page de détails du KMS.
   a. Sélectionnez **Certificat serveur** et vérifiez la valeur du champ « Expire le ».
   b. Pour remplacer le certificat, sélectionnez **Modifier le certificat** pour télécharger un nouveau certificat.
   c. Répétez ces sous-étapes et sélectionnez **Certificat client** au lieu de **Certificat serveur**.
5. Lorsque les alertes **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 jusqu'à 30 minutes pour mettre à jour la date d'expiration du certificat. Actualisez votre navigateur web pour voir les valeurs actuelles.

Si vous obtenez le statut **Statut du certificat serveur inconnu**, assurez-vous que votre KMS permette d'obtenir un certificat serveur sans exiger de certificat client.

Afficher les nœuds chiffrés

Vous pouvez consulter les informations relatives aux nœuds d'appliance de votre système StorageGRID dont le paramètre **Chiffrement des nœuds** est activé.

Étapes

1. Sélectionnez **Configuration** > **Security** > **Key management server**.

   La page Serveur de gestion des clés s'affiche. L'onglet Détails de la configuration présente les serveurs de gestion des clés configurés.

2. En haut de la page, sélectionnez l'onglet **Nœuds chiffrés**.

   L'onglet Nœuds chiffrés répertorie les nœuds d'appliance de votre système StorageGRID dont le paramètre **Chiffrement des nœuds** est activé.

3. Consultez les informations du tableau pour chaque nœud d'appliance.

Colonne	Description
Nom du nœud	Le nom du nœud de l'appliance.
Type de nœud	Le type de nœud : Storage, Admin ou Gateway.
Site	Le nom du site StorageGRID où le nœud est installé.
Nom KMS	Nom descriptif du KMS utilisé pour le nœud. Si aucun KMS n'est répertorié, sélectionnez l'onglet Détails de configuration pour ajouter un KMS. "Ajouter un serveur de gestion de clés (KMS)"
UID de la clé	L'identifiant unique de la clé de chiffrement utilisée pour chiffrer et déchiffrer les données sur le nœud de l'appliance. Pour afficher l'UID complet de la clé, sélectionnez le texte. Un tiret (--) indique que l'UID de la clé est inconnu, probablement en raison d'un problème de connexion entre le nœud de l'appliance et le KMS.
Statut	État de la connexion entre le KMS et le nœud de l'appliance. Si le nœud est connecté, l'horodatage est mis à jour toutes les 30 minutes. La mise à jour de l'état de la connexion peut prendre plusieurs minutes après une modification de la configuration du KMS. **Remarque :** Actualisez votre navigateur Web pour voir les nouvelles valeurs.

4. Si la colonne « Status » indique un problème KMS, résolvez le problème immédiatement.

   Lors des opérations normales du KMS, le statut sera **Connecté au KMS**. Si un nœud est déconnecté du grid, l'état de connexion du nœud est affiché (Administrativement hors service ou Inconnu).

   D'autres messages d'état correspondent à des alertes StorageGRID portant les mêmes noms :

   - Échec du chargement de la configuration KMS
   - Erreur de connectivité KMS
   - Nom de clé de chiffrement KMS introuvable
   - La rotation de la clé de chiffrement KMS a échoué
   - La clé KMS n'a pas pu déchiffrer le volume de l'appliance.
   - KMS n'est pas configuré

Veuillez effectuer les actions recommandées pour ces alertes.

> Vous devez remédier immédiatement à tout problème afin de garantir la protection intégrale de vos données.

Modifier un KMS

Vous pourriez avoir besoin de modifier la configuration d'un serveur de gestion de clés, par exemple si un certificat est sur le point d'expirer.

Avant de commencer

- Si vous prévoyez de mettre à jour le site sélectionné pour un KMS, vous avez examiné le "considérations relatives à la modification du KMS d'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 root".

Étapes

1. Sélectionnez **Configuration** > **Security** > **Key management server**.

   La page du serveur de gestion des clés s'affiche et présente tous les serveurs de gestion des clés configurés.

2. Sélectionnez le KMS que vous souhaitez modifier, puis sélectionnez **Actions** > **Edit**.

   Vous pouvez également modifier un KMS en sélectionnant le nom du KMS dans le tableau et en sélectionnant **Modifier** sur la page de détails du KMS.

3. Vous pouvez également mettre à jour les détails à l'étape 1 (détails KMS) de l'assistant Modifier un Key Management Server.

Champ	Description
Nom 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. Vous n'avez besoin de modifier le nom de la clé que dans de rares cas. Par exemple, vous devez modifier le nom de la clé si l'alias est renommé dans le KMS ou si toutes les versions de l'ancienne clé ont été copiées dans l'historique des versions du nouvel alias.

Champ	Description
Gère les clés pour	Si vous modifiez un KMS spécifique à un site et que vous n'avez pas encore de KMS par défaut, vous pouvez sélectionner **Sites non gérés par un autre KMS (KMS par défaut)**. Cette sélection convertit un KMS spécifique à un 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 lors d'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 que le serveur KMS utilise pour les communications Key Management Interoperability Protocol (KMIP). La valeur par défaut est 5696, qui est le port standard KMIP.
Nom d'hôte	Le domaine complet ou l'adresse IP du KMS. **Remarque :** Le champ Nom alternatif du sujet (SAN) du certificat serveur doit inclure le domaine complet (FQDN) ou l'adresse IP que vous saisissez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ni 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 **Continue**.

   L'étape 2 (Télécharger le certificat du serveur) de l'assistant Modifier un Key Management Server apparaît.

6. Si vous devez remplacer le certificat du serveur, sélectionnez **Parcourir** et importez le nouveau fichier.
7. Sélectionnez **Continue**.

   L'étape 3 (Télécharger les certificats clients) de l'assistant Modifier un serveur de gestion de clés apparaît.

8. Si vous devez remplacer le certificat client et la clé privée du certificat client, sélectionnez **Parcourir** et téléversez les nouveaux fichiers.
9. Sélectionnez **Tester et enregistrer**.

   Les connexions entre le serveur de gestion des clés et tous les nœuds des appliances chiffrées sur les sites concernés 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 au tableau de la page Serveur de gestion des clés.

10. Si un message d'erreur apparaît, consultez les détails du message et sélectionnez **OK**.

    Par exemple, vous pourriez recevoir une erreur 422 : Entité non traitable si le site que vous avez sélectionné pour ce KMS est déjà géré par un autre KMS ou si un test de connexion a échoué.

11. Si vous devez enregistrer la configuration actuelle avant de résoudre les erreurs de connexion, sélectionnez **Force save**.

L'option **Forcer l'enregistrement** sauvegarde la configuration KMS, mais ne teste pas la connexion externe de chaque appliance à ce KMS. En cas de problème de configuration, il se peut que vous ne puissiez pas redémarrer les nœuds d'appliance dont le chiffrement de nœud est activé sur le site concerné. Vous pourriez perdre l'accès à vos données jusqu'à la résolution des problèmes.

La configuration KMS est enregistrée.

12. Examinez l'avertissement de confirmation et sélectionnez **OK** si vous êtes sûr de vouloir forcer l'enregistrement de la configuration.

    La configuration KMS est enregistrée, mais la connexion au KMS n'est pas testée.

Supprimer un serveur de gestion de clés (KMS)

Vous pourriez vouloir supprimer un serveur de gestion de clés dans certains cas. Par exemple, vous pourriez vouloir supprimer un KMS spécifique à un site si vous avez mis ce site hors service.

Avant de commencer

- Vous avez examiné le "Considérations et exigences relatives à l'utilisation d'un serveur de gestion de clés".
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur Web pris en charge".
- Vous avez le "Autorisation d'accès root".

À propos de cette tâche

Vous pouvez supprimer un KMS dans les cas suivants :

- Vous pouvez supprimer un KMS spécifique à un site si celui-ci a été mis hors service ou s'il ne comprend aucun nœud d'appliance avec chiffrement de nœud activé.
- Vous pouvez supprimer le KMS par défaut si un KMS spécifique au site existe déjà pour chaque site comportant des nœuds d'appliance avec chiffrement de nœud activé.

Étapes

1. Sélectionnez **Configuration** > **Security** > **Key management server**.

   La page du serveur de gestion des clés s'affiche et présente tous les serveurs de gestion des clés configurés.

2. Sélectionnez le KMS que vous souhaitez supprimer, puis sélectionnez **Actions** > **Remove**.

   Vous pouvez également supprimer un KMS en sélectionnant le nom du KMS dans le tableau et en sélectionnant **Supprimer** sur la page de détails du KMS.

3. Veuillez confirmer que ce qui suit est vrai :
   - Vous supprimez un KMS spécifique à un site pour un site qui ne possède aucun nœud d'appliance avec chiffrement de nœud activé.
   - Vous supprimez le KMS par défaut, mais un KMS spécifique au site existe déjà pour chaque site avec chiffrement de nœud.
4. Sélectionnez **Oui**.

   La configuration KMS est supprimée.

Gérer les paramètres du proxy

Configurer un proxy de stockage StorageGRID

Si vous utilisez des services de plateforme ou des pools de stockage cloud, vous pouvez configurer un proxy non transparent entre les nœuds de stockage et les points de terminaison S3 externes. Par exemple, vous pourriez avoir besoin d'un proxy non transparent pour permettre l'envoi de messages des services de plateforme vers des points de terminaison externes, tels qu'un point de terminaison sur Internet.

> Les paramètres de proxy de stockage configurés ne s'appliquent pas aux points de terminaison des services de la plateforme Kafka.

Avant de commencer

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

À propos de cette tâche

Vous pouvez configurer les paramètres d'un seul proxy de stockage.

Étapes

1. Sélectionnez **Configuration** > **Sécurité** > **Paramètres du proxy**.
2. Dans l'onglet **Stockage**, cochez la case **Activer le proxy de stockage**.
3. Sélectionnez le protocole pour le proxy de stockage.
4. Saisissez 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, de nouveaux points de terminaison pour les services de plateforme ou les Cloud Storage Pools peuvent être configurés et testés.

   > Les modifications de proxy peuvent prendre jusqu'à 10 minutes pour prendre effet.

7. Vérifiez les paramètres de votre serveur proxy pour vous assurer que les messages relatifs au service de la plateforme provenant de StorageGRID ne seront pas bloqués.
8. Si vous devez désactiver un proxy de stockage, décochez la case et sélectionnez **Enregistrer**.

Configurez les paramètres du proxy d'administration dans StorageGRID

Si vous envoyez des packages AutoSupport en utilisant 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".

À propos de cette tâche

Vous pouvez configurer les paramètres d'un seul proxy d'administration.

Étapes

1. Sélectionnez **Configuration** > **Sécurité** > **Paramètres du proxy**.

   La page Paramètres du proxy s'affiche. Par défaut, Stockage est sélectionné dans le menu des onglets.

2. Sélectionnez l'onglet **Admin**.
3. Cochez la case **Activer le proxy d'administration**.
4. Saisissez le nom d'hôte ou l'adresse IP du serveur proxy.
5. Saisissez le port utilisé pour vous connecter au serveur proxy.
6. Vous pouvez éventuellement saisir un nom d'utilisateur et un mot de passe pour le serveur proxy.

   Laissez ces champs vides si votre serveur proxy ne requiert ni nom d'utilisateur ni mot de passe.

7. Sélectionnez l'une des options suivantes :

   - Pour sécuriser la connexion au proxy d'administration, sélectionnez **Vérifier le certificat du proxy**. Chargez un bundle 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 de mise à niveau StorageGRID ne fonctionneront pas si un certificat proxy est vérifié.

   Après que vous ayez téléchargé le paquet CA, ses métadonnées apparaissent.

   - Si vous ne souhaitez pas valider les certificats lors de la communication avec le serveur proxy d'administration, sélectionnez **Ne pas vérifier le certificat proxy**.

8. Sélectionnez **Enregistrer**.

   Une fois le proxy d'administration enregistré, le serveur proxy entre les nœuds d'administration et le support technique est configuré.

   Les modifications de proxy peuvent prendre jusqu'à 10 minutes pour prendre effet.

9. Si vous devez désactiver le proxy d'administration, décochez la case **Activer le proxy d'administration**, puis sélectionnez **Enregistrer**.

Contrôlez les pare-feu

Contrôlez l'accès à StorageGRID à un pare-feu externe

Vous pouvez ouvrir ou fermer des ports spécifiques au niveau du pare-feu externe.

Vous pouvez contrôler l'accès aux interfaces utilisateur et aux API sur les nœuds d'administration StorageGRID en ouvrant ou en fermant des ports spécifiques au niveau du pare-feu externe. Par exemple, vous pouvez empêcher les locataires de se connecter au Grid Manager au niveau du pare-feu, en plus d'utiliser d'autres méthodes pour contrôler l'accès au système.

Si vous souhaitez configurer le pare-feu interne de StorageGRID, consultez "Configurer le pare-feu interne".

Port	Description	Si le port est ouvert…
443	Port HTTPS par défaut pour les nœuds d'administration	Les navigateurs Web et les clients API de gestion peuvent accéder au Grid Manager, à l'API de gestion du Grid, au Tenant Manager et à l'API de gestion du Tenant. **Remarque :** Le port 443 est également utilisé pour une partie du trafic interne.
8443	Port restreint du Grid Manager sur les nœuds d'administration	• Les navigateurs Web et les clients API de gestion peuvent accéder au Grid Manager et à l'API de gestion du Grid à l'aide de HTTPS. • Les navigateurs Web et les clients API de gestion ne peuvent pas accéder au Tenant Manager ni à l'API de gestion des locataires. • Les demandes de contenu interne seront rejetées.
9443	Port restreint du gestionnaire de locataires sur les nœuds d'administration	• Les navigateurs Web et les clients API de gestion peuvent accéder au Tenant Manager et à l'API de gestion des locataires via HTTPS. • Les navigateurs Web et les clients de l'API de gestion ne peuvent pas accéder au Grid Manager ni à l'API de gestion du Grid. • Les demandes de contenu interne seront rejetées.

L'authentification unique (SSO) n'est pas disponible sur les ports restreints de Grid Manager ou de Tenant Manager. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec l'authentification unique.

Informations connexes

- "Connectez-vous au Grid Manager"
- "Créer un compte locataire"
- "Communications externes"

Gérez les contrôles de pare-feu internes dans StorageGRID

StorageGRID intègre un pare-feu interne sur chaque nœud, renforçant ainsi la sécurité de votre grid en vous permettant de contrôler l'accès réseau au nœud. Utilisez le pare-feu pour empêcher l'accès réseau sur tous les ports, sauf ceux nécessaires au

déploiement spécifique de votre grid. Les modifications de configuration que vous effectuez sur la page de contrôle du pare-feu sont déployées sur chaque nœud.

Utilisez les trois onglets de la page de contrôle du pare-feu pour personnaliser l'accès dont vous avez besoin pour votre grid.

- **Liste d'adresses privilégiées** : utilisez cet onglet pour autoriser l'accès à des ports fermés sélectionnés. Vous pouvez ajouter des adresses IP ou des sous-réseaux au format CIDR qui peuvent accéder aux ports fermés à l'aide de l'onglet Gérer l'accès externe.
- **Gérer l'accès externe** : Utilisez cet onglet pour fermer les ports ouverts par défaut ou rouvrir les ports précédemment fermés.
- **Réseau client non approuvé** : Utilisez cet onglet pour spécifier si un nœud fait confiance au trafic entrant provenant du réseau client.

  Les paramètres de cet onglet prévalent sur ceux de l'onglet Gérer l'accès externe.

  - Un nœud doté d'un Client Network non fiable n'acceptera que les connexions sur les ports de point de terminaison de l'équilibreur de charge configurés sur ce nœud (points de terminaison globaux, d'interface de nœud et liés au type de nœud).
  - Les ports des points de terminaison de l'équilibreur de charge *sont les seuls ports ouverts* sur les réseaux clients non approuvés, quels que soient les paramètres de l'onglet Manage external networks.
  - Une fois approuvés, tous les ports ouverts sous l'onglet Gérer l'accès externe sont accessibles, ainsi que tous les points de terminaison d'équilibrage de charge ouverts sur le réseau client.

> Les paramètres que vous définissez dans un onglet peuvent affecter les modifications d'accès que vous effectuez dans un autre onglet. Assurez-vous de vérifier les paramètres de tous les onglets pour que votre réseau se comporte comme vous l'attendez.

Pour configurer les contrôles du pare-feu interne, consultez "Configurer les contrôles du pare-feu".

Pour plus d'informations sur les pare-feu externes et la sécurité réseau, consultez "Contrôler l'accès au niveau du pare-feu externe".

Onglets Liste d'adresses privilégiées et Gérer l'accès externe

L'onglet « Liste des adresses privilégiées » vous permet d'enregistrer une ou plusieurs adresses IP autorisées à accéder à des ports de la grille fermés. L'onglet « Gérer l'accès externe » vous permet de fermer l'accès externe à certains ports externes ou à tous les ports externes ouverts (les ports externes sont des ports accessibles par défaut aux nœuds non-grille). Ces deux onglets peuvent souvent être utilisés conjointement pour personnaliser précisément l'accès réseau dont vous avez besoin pour votre grille.

> Les adresses IP privilégiées n'ont pas accès par défaut aux ports internes de la grille.

Exemple 1 : Utilisez un serveur de rebond pour les tâches de maintenance

Supposons que vous souhaitiez utiliser un serveur de rebond (un hôte sécurisé) pour l'administration du réseau. Vous pouvez suivre les étapes générales suivantes :

1. Utilisez l'onglet Liste des adresses privilégiées pour ajouter l'adresse IP de l'hôte de rebond.
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 des adresses privilégiées.

Une fois votre configuration enregistrée, tous les ports externes du nœud d'administration de votre grille seront bloqués pour tous les hôtes, à l'exception du jump host. Vous pouvez alors utiliser le jump host pour effectuer des tâches de maintenance sur votre grille de manière plus sécurisée.

Exemple 2 : Verrouillez les ports sensibles

Supposons que vous souhaitiez verrouiller les ports sensibles et le service sur ce port. Vous pouvez suivre les étapes générales suivantes :

1. Utilisez l'onglet Liste d'adresses privilégiées pour n'accorder l'accès qu'aux hôtes qui ont besoin d'accéder au service.
2. Utilisez l'onglet Gérer l'accès externe pour bloquer tous les ports.

> Ajoutez l'adresse IP privilégiée avant de bloquer l'accès à tout port attribué à l'accès à Grid Manager et Tenant Manager (les ports prédéfinis sont 443 et 8443). Tout utilisateur actuellement connecté à un port bloqué, y compris vous, perdra l'accès à Grid Manager à moins que son adresse IP n'ait été ajoutée à la liste des adresses privilégiées.

Une fois votre configuration enregistrée, le port sensible et le service associé sont accessibles aux hôtes figurant dans la liste d'adresses privilégiées. L'accès au service est refusé à tous les autres hôtes, quelle que soit l'interface d'où provient la requête.

Exemple 3 : Désactivez 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 HTTP des clients S3, vous utiliseriez le bouton bascule de l'onglet Gérer l'accès externe pour bloquer le port 18084.

Onglet Réseaux clients non approuvés

Si vous utilisez un réseau client, vous pouvez contribuer à sécuriser StorageGRID contre les attaques hostiles en n'acceptant le trafic client entrant que sur les points de terminaison explicitement configurés.

Par défaut, le réseau client de chaque nœud de la grille est *de confiance*. Autrement dit, par défaut, StorageGRID fait confiance aux connexions entrantes vers chaque nœud de la grille sur tous les "ports externes disponibles".

Vous pouvez réduire le risque d'attaques hostiles sur votre système StorageGRID en spécifiant que le réseau client de chaque nœud soit *non fiable*. Si le réseau client d'un nœud est non fiable, le nœud n'accepte les connexions entrantes que sur les ports explicitement configurés comme points de terminaison d'équilibrage de charge. Voir "Configurer les points de terminaison de l'équilibreur de charge" et "Configurer les contrôles du pare-feu".

Exemple 1 : Le nœud passerelle accepte uniquement les requêtes HTTPS S3

Supposons que vous souhaitiez qu'un nœud Gateway refuse tout le trafic entrant sur le réseau client, à l'exception des requêtes HTTPS S3. Vous effectueriez les étapes générales suivantes :

1. À partir de la page "points de terminaison de l'équilibreur de charge", configurez un point de terminaison

d'équilibrage de charge pour S3 via 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 de passerelle n'est pas approuvé.

Après avoir enregistré votre configuration, tout le trafic entrant sur le réseau client du nœud de passerelle est bloqué, à l'exception des requêtes HTTPS S3 sur le port 443 et des requêtes d'écho ICMP (ping).

Exemple 2 : Un nœud de stockage envoie des requêtes de services de plateforme S3

Supposons que vous souhaitiez autoriser le trafic sortant des services de la plateforme S3 depuis un nœud de stockage, mais empêcher toute connexion entrante vers ce nœud de stockage sur le réseau client. Vous effectueriez l'étape générale suivante :

- Dans l'onglet Réseaux clients non approuvés de la page de contrôle du pare-feu, indiquez que le réseau client sur le nœud de stockage n'est pas approuvé.

Une fois votre configuration enregistrée, le nœud de stockage n'accepte plus aucun trafic entrant sur le réseau client, mais il continue d'autoriser les requêtes sortantes vers les destinations des services de plateforme configurés.

Exemple 3 : Limiter 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. Vous effectueriez les étapes suivantes :

1. Connectez le réseau client de vos nœuds d'administration au sous-réseau.
2. Utilisez l'onglet Untrusted Client Network pour configurer le réseau client comme non approuvé.
3. Lorsque vous créez un point de terminaison d'équilibreur de charge d'interface de gestion, saisissez le port et sélectionnez l'interface de gestion à laquelle le port accédera.
4. Sélectionnez **Oui** pour Réseau client non approuvé.
5. Utilisez l'onglet Gérer l'accès externe pour bloquer tous les ports externes (avec ou sans adresses IP privilégiées définies pour les hôtes situés en dehors de ce sous-réseau).

Une fois votre configuration enregistrée, seuls les hôtes du sous-réseau que vous avez spécifié peuvent accéder au Grid Manager. Tous les autres hôtes sont bloqués.

Configurer le pare-feu interne de StorageGRID

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 du pare-feu" et "Directives de mise en réseau".
- Si vous souhaitez qu'un nœud d'administration ou un nœud de passerelle n'accepte le trafic entrant que sur les points de terminaison explicitement configurés, vous avez défini les points de terminaison de l'équilibreur de charge.

Lors de la modification de la configuration du réseau client, les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.

À propos de cette tâche

StorageGRID intègre 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 les ports qui sont ouverts par défaut sur le réseau de la grille, le réseau d'administration et le réseau client. Vous pouvez également créer une liste d'adresses IP privilégiées pouvant accéder aux ports de la grille qui sont fermés. Si vous utilisez un réseau client, vous pouvez spécifier si un nœud fait confiance au trafic entrant provenant du réseau client, et vous pouvez configurer l'accès à des ports spécifiques sur le réseau client.

Limiter le nombre de ports ouverts aux adresses IP extérieures à votre grid aux seuls ports strictement nécessaires renforce la sécurité de votre grid. 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 du pare-feu, y compris des exemples, consultez "Gérer les contrôles du pare-feu".

Pour plus d'informations sur les pare-feu externes et la sécurité réseau, consultez "Contrôler l'accès au niveau du pare-feu externe".

Contrôler l'accès au pare-feu

Étapes

1. Sélectionnez **Configuration** > **Sécurité** > **Contrôle du pare-feu**.

   Les trois onglets de cette page sont décrits dans "Gérer les contrôles du pare-feu".

2. Sélectionnez un onglet pour configurer les contrôles du pare-feu.

   Vous pouvez utiliser ces onglets dans n'importe quel ordre. Les configurations que vous définissez dans un onglet n'empêchent pas ce que vous pouvez faire dans les autres onglets ; cependant, les modifications de configuration que vous effectuez dans un onglet peuvent modifier le comportement des ports configurés dans les autres onglets.

Liste d'adresses privilégiées

Vous utilisez l'onglet Liste d'adresses privilégiées pour accorder aux hôtes l'accès aux ports fermés par défaut ou fermés par les paramètres de l'onglet Gérer l'accès externe.

Les adresses IP et les sous-réseaux privilégiés n'ont pas accès au grid interne par défaut. De plus, les points de terminaison de l'équilibreur de charge et les ports supplémentaires ouverts dans l'onglet Liste des adresses privilégiées sont accessibles même s'ils sont bloqués dans l'onglet Gérer l'accès externe.

Les paramètres de l'onglet « Liste des adresses privilégiées » ne peuvent pas remplacer les paramètres de l'onglet « Réseau client non approuvé ».

Étapes

1. Dans l'onglet Liste des adresses privilégiées, saisissez l'adresse ou le sous-réseau IP auquel vous souhaitez accorder l'accès aux ports fermés.

2. Vous pouvez également sélectionner **Ajouter une autre adresse IP ou un sous-réseau au format CIDR** pour ajouter des clients privilégiés supplémentaires.

   Ajoutez le moins d'adresses possible à la liste privilégiée.

3. Vous pouvez également sélectionner **Autoriser les adresses IP privilégiées à accéder aux ports internes de StorageGRID**. Voir "Ports internes de StorageGRID".

   Cette option désactive certaines protections des services internes. Laissez-la désactivée si possible.

4. Sélectionnez **Enregistrer**.

Gérer l'accès externe

Lorsqu'un port est fermé dans l'onglet Gérer l'accès externe, le port ne peut pas être accessible par une adresse IP non-grid, sauf si vous ajoutez l'adresse IP à la liste des adresses privilégiées. Vous pouvez uniquement fermer les ports ouverts par défaut et uniquement ouvrir les ports que vous avez fermés.

Les paramètres de l'onglet « Gérer l'accès externe » ne peuvent pas prévaloir sur ceux de l'onglet « Réseau client non fiable ». Par exemple, si un nœud est non fiable, 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 fiable » prévalent sur les ports fermés (tels que 443, 8443, 9443) sur le réseau client.

Étapes

1. Sélectionnez **Gérer l'accès externe**. L'onglet affiche un tableau répertoriant tous les ports externes (ports accessibles par défaut aux nœuds hors grille) des nœuds de votre grille.
2. Configurez les ports que vous souhaitez ouvrir et fermer à l'aide des options suivantes :
   - Utilisez le bouton à bascule situé à côté de chaque port pour ouvrir ou fermer le port sélectionné.
   - Sélectionnez **Ouvrir tous les ports affichés** pour ouvrir tous les ports répertoriés dans le tableau.
   - Sélectionnez **Fermer tous les ports affichés** pour fermer tous les ports listés dans le tableau.

     Si vous fermez les ports 443 ou 8443 de Grid Manager, tous les utilisateurs actuellement connectés sur un port bloqué, y compris vous, perdront l'accès à Grid Manager à moins que leur adresse IP n'ait été ajoutée à la liste des adresses privilégiées.

     Utilisez la barre de défilement à droite du tableau pour vous assurer d'avoir visualisé tous les ports disponibles. Utilisez le champ de recherche pour trouver les paramètres de n'importe quel port externe en saisissant un numéro de port. Vous pouvez saisir un numéro de port partiel. Par exemple, si vous saisissez **2**, tous les ports dont le nom contient la chaîne « 2 » seront affichés.

3. Sélectionnez **Save**

Réseau de clients non fiables

Si le réseau client d'un nœud n'est pas approuvé, le nœud n'accepte le trafic entrant que sur les ports configurés comme points de terminaison d'équilibrage de charge et, éventuellement, sur les ports

supplémentaires que vous sélectionnez dans cet onglet. Vous pouvez également utiliser cet onglet pour définir le paramètre par défaut des nouveaux nœuds ajoutés lors d'une extension.

> Les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.

Les modifications de configuration que vous effectuez dans l'onglet **Réseau client non approuvé** remplacent les paramètres de l'onglet **Gérer l'accès externe**.

Étapes

1. Sélectionnez **Réseau client non approuvé**.
2. Dans la section Définir la valeur par défaut des nouveaux nœuds, spécifiez le paramètre par défaut qui doit être appliqué lorsque de nouveaux nœuds sont ajoutés à la grille lors d'une procédure d'expansion.
   - **Fiable** (par défaut) : lorsqu'un nœud est ajouté dans une extension, son réseau client est fiable.
   - **Non fiable** : Lorsqu'un nœud est ajouté lors d'une extension, son réseau client est non fiable.

     Au besoin, vous pouvez revenir à cet onglet pour modifier le paramètre d'un nouveau nœud spécifique.

     > Ce paramètre n'affecte pas les nœuds existants de votre système StorageGRID.
3. Utilisez les options suivantes pour sélectionner les nœuds qui doivent autoriser les connexions client uniquement sur les points de terminaison d'équilibrage de charge explicitement configurés ou sur des ports supplémentaires sélectionnés :
   - Sélectionnez **Ne pas faire confiance aux nœuds affichés** pour ajouter tous les nœuds affichés dans le tableau à la liste Untrusted Client Network.
   - Sélectionnez **Faire confiance aux nœuds affichés** pour supprimer tous les nœuds affichés dans le tableau de la liste Untrusted Client Network.
   - Utilisez le bouton bascule situé à côté de chaque nœud pour définir le réseau client comme étant de confiance ou non de confiance pour le nœud sélectionné.

     Par exemple, vous pouvez sélectionner **Ne pas faire confiance aux nœuds affichés** pour ajouter tous les nœuds à la liste Réseau client non fiable, puis utiliser le bouton bascule situé à côté d'un nœud individuel pour ajouter ce nœud à la liste Réseau client fiable.

     > Utilisez la barre de défilement à droite du tableau pour vous assurer d'avoir visualisé tous les nœuds disponibles. Utilisez le champ de recherche pour trouver les paramètres de n'importe quel nœud en saisissant le nom du nœud. Vous pouvez saisir un nom partiel. Par exemple, si vous saisissez **GW**, tous les nœuds dont le nom contient la chaîne "GW" seront affichés.
4. Sélectionnez **Enregistrer**.

   Les nouveaux paramètres du 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

Comptes locataires dans StorageGRID

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

Les détails concernant Swift ont été supprimés de cette version du site de documentation. Voir "StorageGRID 11.8 : Gérer les locataires".

En tant qu'administrateur de grille, vous créez et gérez les comptes locataires que les clients S3 utilisent pour stocker et récupérer des objets.

Chaque compte locataire possède des groupes fédérés ou locaux, des utilisateurs, des compartiments S3 et des objets.

Les comptes locataires permettent de segmenter les objets stockés par différentes entités. Par exemple, plusieurs comptes locataires peuvent être utilisés dans les deux cas suivants :

- **Cas d'utilisation en entreprise :** Si vous administrez un système StorageGRID dans une application d'entreprise, vous pouvez vouloir segmenter le stockage d'objets de la grille en fonction des différents services de votre organisation. Dans ce cas, vous pouvez créer des comptes locataires pour le service Marketing, le service Support Client, le service Ressources Humaines, etc.

  Si vous utilisez le protocole client S3, vous pouvez utiliser les compartiments S3 et les stratégies de compartiment pour segmenter les objets entre les services d'une entreprise. Vous n'avez pas besoin d'utiliser des comptes locataires. Consultez les instructions pour implémenter "Compartiments S3 et politiques de compartiment" pour plus d'informations.

- **Cas d'utilisation pour un fournisseur de services :** Si vous administrez un système StorageGRID en tant que fournisseur de services, vous pouvez segmenter le stockage d'objets de la grille en fonction des différentes entités qui loueront le stockage sur votre grille. Dans ce cas, vous créeriez des comptes clients pour Company A, Company B, Company C, etc.

Pour plus d'informations, consultez "Utilisez un compte locataire".

Comment créer un compte locataire ?

Utilisez le gestionnaire Grid pour créer un compte locataire. Lorsque vous créez un compte locataire, vous spécifiez les informations suivantes :

- Informations de base, notamment le nom du locataire, le type de client (S3) et le quota de stockage facultatif.
- Les autorisations du compte locataire, telles que la possibilité pour ce dernier d'utiliser les services de la plateforme S3, de configurer sa propre source d'identité, d'utiliser S3 Select ou d'utiliser une connexion de fédération de grille.
- L'accès racine initial du locataire, en fonction de la manière dont le système StorageGRID utilise les groupes et utilisateurs locaux, la fédération d'identités ou l'authentification unique (SSO).

De plus, vous pouvez activer le paramètre S3 Object Lock pour le système StorageGRID si les comptes locataires S3 doivent se conformer aux exigences réglementaires. Lorsque S3 Object Lock est activé, tous les comptes locataires S3 peuvent créer et gérer des compartiments conformes.

À quoi sert Tenant Manager ?

Une fois le compte locataire créé, les utilisateurs locataires peuvent se connecter au Gestionnaire de locataires pour effectuer des tâches telles que les suivantes :

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

> Bien que les utilisateurs d'un locataire S3 puissent créer et gérer des clés d'accès S3 et des compartiments avec le Tenant Manager, ils doivent utiliser une application cliente S3 pour ingérer et gérer les objets. Voir "Utilisez l'API REST S3" pour plus de détails.

Créer un compte locataire StorageGRID

Vous devez créer au moins un compte locataire pour contrôler l'accès au stockage dans votre système StorageGRID.

Les étapes de création d'un compte locataire varient selon que "fédération d'identité" et "authentification unique" sont configurés et selon que le compte Grid Manager que vous utilisez pour créer le compte locataire appartient à un groupe d'administrateurs disposant de l'autorisation d'accès Root.

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 root ou autorisation de comptes locataires".
- Si le compte locataire utilise la source d'identité configurée pour le Grid Manager et que vous souhaitez accorder l'autorisation d'accès Root à un groupe fédéré pour ce compte, vous avez importé ce groupe fédéré dans le Grid Manager. Vous n'avez pas besoin d'attribuer d'autorisations Grid Manager à ce groupe d'administrateurs. Voir "Gérer les groupes d'administrateurs".
- Si vous souhaitez autoriser un locataire S3 à cloner les données d'un compte et à répliquer les objets d'un compartiment vers une autre grille à l'aide d'une connexion de fédération de grilles :
  - Vous avez "configuré la connexion de fédération de grille".
  - L'état de la connexion est **Connecté**.
  - Vous disposez des droits d'accès root.
  - Vous avez examiné les éléments à prendre en compte pour "gestion des locataires autorisés pour la fédération de grid".
  - Si le compte locataire utilisera la source d'identité qui a été configurée pour Grid Manager, vous avez importé le même groupe fédéré dans Grid Manager sur les deux grilles.

    Lors de la création du locataire, vous sélectionnerez ce groupe pour avoir l'autorisation d'accès Root initiale pour les comptes de locataire source et de destination.

Si ce groupe d'administrateurs n'existe pas sur les deux grilles avant que vous ne créiez le locataire, le locataire n'est pas répliqué vers la destination.

Accédez à l'assistant

Étapes

1. Sélectionnez **Tenants**.
2. Sélectionnez **Create**.

Saisissez les détails

Étapes

1. Saisissez les informations concernant le locataire.

Champ	Description
Nom	Nom du compte locataire. Les noms de locataire n'ont pas besoin d'être uniques. Lors de la création du compte locataire, il reçoit un identifiant de compte unique à 20 chiffres.
Description (facultatif)	Une description permettant d'identifier le locataire. Si vous créez un locataire qui utilisera une connexion de fédération de grilles, vous pouvez éventuellement utiliser ce champ pour vous aider à identifier lequel est le locataire source et lequel est le locataire de destination. Par exemple, cette description pour un locataire créé sur Grid 1 apparaîtra également pour le locataire répliqué sur Grid 2 : « Ce locataire a été créé sur Grid 1. »
Type de client	Doit être **S3**.
Quota de stockage (facultatif)	Si vous souhaitez attribuer un quota de stockage à ce locataire, indiquez une valeur numérique pour le quota et les unités.

2. Sélectionnez **Continue**.

Sélectionnez les autorisations

Étapes

1. Vous pouvez également sélectionner les autorisations de base que vous souhaitez que ce locataire ait.

Certaines de ces autorisations comportent des exigences supplémentaires. Pour plus de détails, sélectionnez l'icône d'aide pour chaque autorisation.

Autorisation	Si sélectionné…
Autoriser les services de plateforme	Le locataire peut utiliser les services de la plateforme S3 tels que CloudMirror. Voir "Gérer les services de plateforme pour les comptes locataires S3".

Autorisation	Si sélectionné…
Utiliser votre propre source d'identité	Le locataire peut configurer et gérer sa propre source d'identité pour les groupes et utilisateurs fédérés. Cette option est désactivée si vous avez "SSO configuré" pour votre système StorageGRID.
Autoriser S3 Select	Le locataire peut émettre des requêtes API S3 SelectObjectContent pour filtrer et récupérer les données d'objet. Voir "Gérer S3 Select pour les comptes locataires". **Important** : les requêtes SelectObjectContent peuvent dégrader les performances de l'équilibreur de charge pour tous les clients et locataires S3. N'activez cette fonctionnalité qu'en cas de besoin et uniquement pour les locataires de confiance.

2. Vous pouvez également sélectionner les autorisations avancées que vous souhaitez que ce locataire possède.

Autorisation	Si sélectionné…
Connexion de fédération de grille	Le locataire peut utiliser une connexion de fédération de grille, qui : • Fait en sorte que ce locataire, ainsi que tous les groupes de locataires et les utilisateurs ajoutés au compte, soient clonés 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 inter-grilles entre les compartiments correspondants sur chaque grille. Voir "Gérer les locataires autorisés pour la fédération de grid".
Verrouillage d'objet S3	Autorisez le locataire à utiliser certaines fonctionnalités de S3 Object Lock : • **Définir la période de rétention maximale** définit la durée pendant laquelle les nouveaux objets ajoutés à ce compartiment doivent être conservés, à compter de leur ingestion. • **Autoriser le mode de conformité** empêche les utilisateurs d'écraser ou de supprimer les versions d'objets protégés pendant la période de conservation.

3. Sélectionnez **Continue**.

Définissez l'accès root et créez un locataire

Étapes

1. Définissez l'accès racine pour le compte locataire, selon que votre système StorageGRID utilise la fédération d'identités, l'authentification unique (SSO) ou les deux.

Option	Faites ceci
Si la fédération d'identités n'est pas activée	Spécifiez le mot de passe à utiliser pour vous connecter au locataire en tant qu'utilisateur root local.
Si la fédération d'identité est activée	a. Sélectionnez un groupe fédéré existant pour avoir l'autorisation d'accès Root pour le locataire. b. Vous pouvez également spécifier le mot de passe à utiliser lors de la connexion au locataire en tant qu'utilisateur racine local.
Si la fédération d'identités et l'authentification unique (SSO) sont toutes deux activées	Sélectionnez un groupe fédéré existant auquel vous accordez l'autorisation d'accès Root pour le locataire. Aucun utilisateur local ne peut se connecter.

2. Sélectionnez **Créer un locataire**.

   Un message de confirmation s'affiche et le nouveau locataire est répertorié sur la page Locataires. Pour savoir comment consulter les détails d'un locataire et suivre son activité, voir "Surveiller l'activité des locataires".

   > L'application des paramètres locataires à l'ensemble de la grille peut prendre 15 minutes ou plus en fonction de la connectivité réseau, de l'état des nœuds et des opérations Cassandra.

3. Si vous avez sélectionné l'autorisation **Utiliser la connexion de fédération de grille** pour le locataire :

   a. Vérifiez qu'un locataire identique a bien été répliqué sur l'autre grille de la connexion. Les locataires des deux grilles auront le même identifiant de compte à 20 chiffres, le même nom, la même description, le même quota et les mêmes autorisations.

      > Si vous voyez le message d'erreur « Tenant created without a clone », reportez-vous aux instructions dans "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, "modifier le mot de passe de l'utilisateur root local" pour le locataire répliqué.

      > Un utilisateur racine local ne peut pas se connecter à Tenant Manager sur la grille de destination tant que le mot de passe n'est pas modifié.

Se connecter au locataire (facultatif)

Selon vos besoins, vous pouvez vous connecter dès maintenant au nouveau tenant pour terminer la configuration, ou vous pouvez vous connecter au tenant ultérieurement. Les étapes de connexion dépendent du fait que vous êtes connecté à Grid Manager en utilisant le port par défaut (443) ou un port restreint. Voir "Contrôler l'accès au niveau du pare-feu externe".

Connectez-vous maintenant

Si vous utilisez…	Faites ceci…
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 apparaissent pour configurer les compartiments, la fédération d'identités, les groupes et les utilisateurs. 2. Sélectionnez les liens pour configurer le compte tenant. Chaque lien ouvre la page correspondante dans le Tenant Manager. Pour compléter la page, consultez le "instructions pour l'utilisation des comptes locataires".
Le port 443 et vous n'avez pas défini de mot de passe pour l'utilisateur root local	Sélectionnez **Se connecter**, puis saisissez les informations d'identification d'un utilisateur du groupe fédéré d'accès racine.
Un port restreint	1. Sélectionnez **Terminer** 2. Sélectionnez **Restreint** dans le tableau Tenant pour en savoir plus sur l'accès à ce compte locataire. L'URL du Tenant Manager a le format suivant : `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* est un domaine complet ou l'adresse IP d'un nœud d'administration ◦ *port* est le port réservé aux locataires ◦ *20-digit-account-id* est l'identifiant unique du compte du locataire

Se connecter plus tard

Si vous utilisez…	Effectuez l'une de ces actions…
Port 443	• Dans le Grid Manager, sélectionnez **Tenants**, puis **Sign in** à droite du nom du tenant. • Saisissez l'URL du locataire dans un navigateur Web : `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* est un domaine complet ou l'adresse IP d'un nœud d'administration ◦ *20-digit-account-id* est l'identifiant unique du compte du locataire

Si vous utilisez…	Effectuez l'une de ces actions…
Un port restreint	• Dans le Grid Manager, sélectionnez **Tenants**, puis **Restricted**. • Saisissez l'URL du locataire dans un navigateur Web : `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ *FQDN_or_Admin_Node_IP* est un domaine complet ou l'adresse IP d'un nœud d'administration ◦ *port* est le port réservé aux locataires ◦ *20-digit-account-id* est l'identifiant unique du compte du locataire

Configurer le locataire

Suivez les instructions dans "Utilisez un compte locataire" pour gérer les groupes de locataires et les utilisateurs, les clés d'accès S3, les compartiments, les services de plateforme, ainsi que le clonage de compte et la réplication inter-grilles.

Modifier un compte locataire StorageGRID

Vous pouvez modifier un compte locataire pour changer le nom d'affichage, le quota de stockage ou les autorisations du locataire.

Si un locataire dispose de l'autorisation **Utiliser la connexion de fédération de grilles**, vous pouvez modifier les informations du locataire depuis l'une ou l'autre des grilles de la connexion. Cependant, toute modification effectuée sur une grille de la connexion ne sera pas copiée sur l'autre grille. Si vous souhaitez que les informations du locataire restent parfaitement synchronisées entre les grilles, effectuez les mêmes modifications sur les deux grilles. Voir "Gérer les locataires autorisés pour la connexion à la fédération de grid".

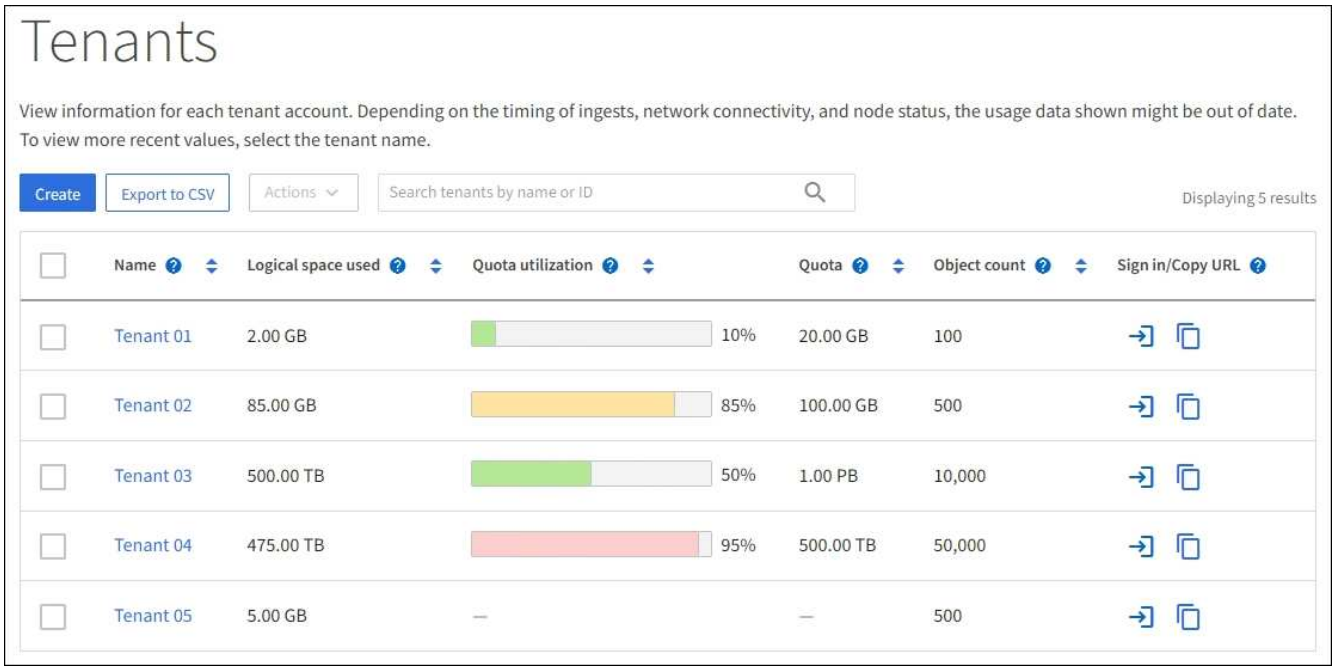
Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur Web pris en charge".
- Vous avez le "Autorisation d'accès root ou autorisation de comptes locataires".

L'application des paramètres locataires à l'ensemble de la grille peut prendre 15 minutes ou plus en fonction de la connectivité réseau, de l'état des nœuds et des opérations Cassandra.

Étapes

1. Sélectionnez **Tenants**.



2. Localisez le compte locataire que vous souhaitez modifier.

   Utilisez le champ de recherche pour rechercher un locataire par son nom ou son identifiant de locataire.

3. Sélectionnez le locataire. Vous pouvez procéder de l'une des manières suivantes :
   - Sélectionnez la case à cocher du locataire, puis sélectionnez **Actions** > **Edit**.
   - Sélectionnez le nom du locataire pour afficher la page de détails, puis sélectionnez **Modifier**.
4. Vous pouvez éventuellement modifier les valeurs de ces champs :
   - **Nom**
   - **Description**
   - **Quota de stockage**
5. Sélectionnez **Continue**.
6. Sélectionnez ou désélectionnez les autorisations du compte locataire.
   - Si vous désactivez les **Services de plateforme** pour un locataire qui les utilise déjà, les services qu'il a configurés pour ses compartiments S3 cesseront de fonctionner. Aucun message d'erreur n'est envoyé au locataire. Par exemple, si le locataire a configuré la réplication CloudMirror pour un compartiment S3, il pourra toujours stocker des objets dans le compartiment, mais des copies de ces objets ne seront plus créées dans le compartiment S3 externe qu'il a configuré comme point de terminaison. Voir "Gérer les services de plateforme pour les comptes locataires S3".
   - Modifiez le paramètre **Utiliser sa propre source d'identité** pour déterminer si le compte locataire utilisera sa propre source d'identité ou la source d'identité configurée pour Grid Manager.

     Si **Utiliser votre propre source d'identité** est :

     - Désactivé et sélectionné, le locataire a déjà activé sa propre source d'identité. Un locataire doit désactiver sa source d'identité avant de pouvoir utiliser la source d'identité configurée pour le Grid Manager.
     - Désactivé et non sélectionné, l'authentification unique (SSO) est activée pour le système StorageGRID. Le locataire doit utiliser la source d'identité qui a été configurée pour le Grid

Manager.

- Sélectionnez ou désactivez l'autorisation **Allow S3 Select** selon vos besoins. Voir "Gérer S3 Select pour les comptes locataires".
- Pour supprimer l'autorisation **Utiliser la connexion de fédération de grille** :
  i. Sélectionnez l'onglet **Fédération de grilles**.
  ii. Sélectionnez **Supprimer l'autorisation**.
- Pour ajouter l'autorisation **Utiliser la connexion de fédération de grille** :
  i. Sélectionnez l'onglet **Fédération de grilles**.
  ii. Cochez la case **Utiliser la connexion de fédération de grille**.
  iii. Vous pouvez également sélectionner **Cloner les utilisateurs et groupes locaux existants** pour les cloner sur la grille distante. Si vous le souhaitez, vous pouvez interrompre le clonage en cours ou réessayer de cloner si certains utilisateurs ou groupes locaux n'ont pas pu être clonés après la dernière opération de clonage.
- Pour définir une durée de conservation maximale ou autoriser le mode de conformité :

> Le verrouillage d'objet S3 doit être activé sur la grille avant que vous puissiez utiliser ces paramètres.

  i. Sélectionnez l'onglet **Verrouillage d'objet S3**.
  ii. Pour **Définir la période de conservation maximale**, saisissez une valeur et sélectionnez la période dans le menu déroulant.
  iii. Pour **Allow compliance mode**, cochez la case.

Modifier le mot de passe de l'utilisateur root local d'un locataire StorageGRID

Vous devrez peut-être modifier le mot de passe de l'utilisateur racine local d'un locataire si l'utilisateur racine est verrouillé hors de son compte.

Avant de commencer

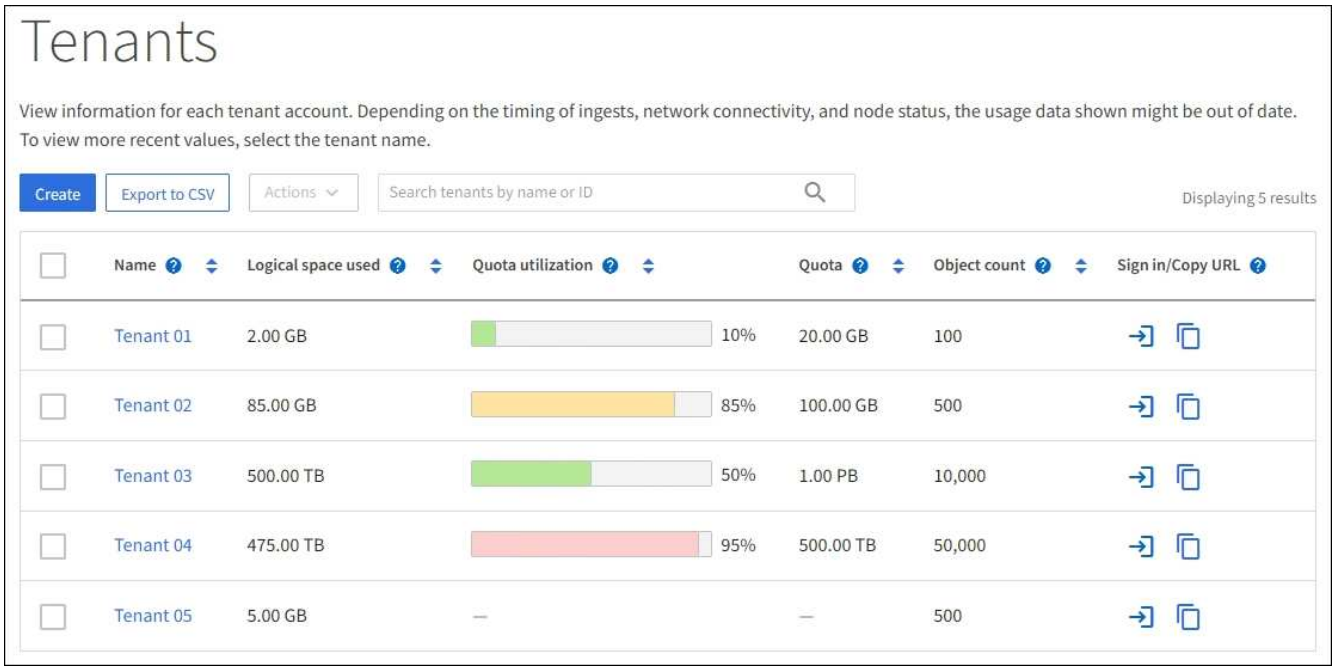
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur Web pris en charge".
- Vous avez "autorisations d'accès spécifiques".

À propos de cette tâche

Si l'authentification unique (SSO) est activée pour votre système StorageGRID, l'utilisateur root local ne peut pas se connecter au compte du locataire. Pour effectuer des tâches d'utilisateur root, les utilisateurs doivent appartenir à un groupe fédéré disposant de l'autorisation d'accès Root pour le locataire.

Étapes

1. Sélectionnez **Tenants**.



2. Sélectionnez le compte locataire. Vous pouvez effectuer l'une des actions suivantes :
   - Sélectionnez la case à cocher correspondant au locataire, puis sélectionnez **Actions** > **Modifier le mot de passe racine**.
   - Sélectionnez le nom du locataire pour afficher la page de détails, puis sélectionnez **Actions** > **Changer le mot de passe racine**.
3. Saisissez le nouveau mot de passe du compte locataire.
4. Sélectionnez **Enregistrer**.

Supprimer un compte locataire StorageGRID

Vous pouvez supprimer un compte locataire si vous souhaitez supprimer définitivement l'accès du locataire 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 les objets associés au compte du 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 disposant de l'autorisation « Utiliser la connexion de fédération de grille »".

Étapes

1. Sélectionnez **Tenants**.
2. Localisez le ou les comptes locataires que vous souhaitez supprimer.

   Utilisez le champ de recherche pour rechercher un locataire par son nom ou son identifiant de locataire.

3. Pour supprimer plusieurs locataires, cochez les cases et sélectionnez **Actions** > **Supprimer**.
4. Pour supprimer un seul locataire, procédez de l'une des manières suivantes :

- Cochez la case, puis sélectionnez **Actions** > **Supprimer**.
- Sélectionnez le nom du locataire pour afficher la page de détails, puis sélectionnez **Actions** > **Delete**.

5. Sélectionnez **Oui**.

Gérer les services de plateforme

Découvrez les services de la plateforme StorageGRID

Les services de la plateforme incluent la réplication CloudMirror, les notifications d'événements et le service d'intégration de recherche.

Si vous activez les services de plateforme pour les comptes locataires S3, vous devez configurer votre grille afin que les locataires puissent accéder aux ressources externes nécessaires à l'utilisation de ces services.

Les services de plateforme ne sont pas pris en charge pour "seaux de branches".

Réplication CloudMirror

Le service de réplication CloudMirror StorageGRID est utilisé pour mettre en miroir des objets spécifiques d'un compartiment StorageGRID vers une destination externe spécifiée.

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

La réplication CloudMirror présente des similitudes et des différences importantes avec la fonctionnalité de réplication inter-grilles. Pour en savoir plus, consultez "Comparez la réplication inter-grilles et la réplication CloudMirror".

> CloudMirror replication n'est pas prise en charge si le compartiment source a le verrouillage d'objet S3 activé.

Notifications

Les notifications d'événements par compartiment sont utilisées pour envoyer des notifications concernant des actions spécifiques effectuées sur des objets à un cluster Kafka externe spécifié, à un point de terminaison webhook ou à Amazon Simple Notification Service.

Par exemple, vous pouvez configurer des alertes pour qu'elles soient envoyées aux administrateurs concernant chaque objet ajouté à un compartiment, où les objets représentent des fichiers journaux associés à un événement système critique.

> Bien que la notification d'événements puisse être configurée sur un compartiment avec S3 Object Lock activé, les métadonnées S3 Object Lock (y compris Retain Until Date et Legal Hold status) des objets ne seront pas incluses dans les messages de notification.

service d'intégration de recherche

Le service d'intégration de recherche est utilisé pour envoyer les métadonnées d'objets S3 à un index Elasticsearch spécifié où les métadonnées peuvent être recherchées ou analysées à l'aide du service externe.

Par exemple, vous pouvez configurer vos compartiments pour envoyer les métadonnées des objets S3 à un service Elasticsearch distant. Vous pouvez ensuite utiliser Elasticsearch pour effectuer des recherches dans

vos compartiments et réaliser des analyses sophistiquées des tendances présentes dans les métadonnées de vos objets.

> Bien que l'intégration d'Elasticsearch puisse être configurée sur un compartiment avec le S3 Object Lock activé, les métadonnées S3 Object Lock (y compris la date de conservation et le statut de Legal Hold) 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 est généralement externe à votre déploiement StorageGRID, vous devez décider si vous souhaitez autoriser les locataires à utiliser ces services. Si tel est le cas, vous devez activer l'utilisation des services de plateforme lors de la création ou de la modification des comptes locataires. Vous devez également configurer votre réseau afin que les messages des services de plateforme générés par les locataires puissent atteindre leurs destinations.

Recommandations pour l'utilisation des services de la plateforme

Avant d'utiliser les services de la plateforme, veuillez prendre connaissance des recommandations suivantes :

- Si un compartiment S3 dans le système StorageGRID a à la fois le versionnage et la réplication CloudMirror activés, vous devez également activer le versionnage du compartiment S3 pour le point de terminaison de destination. Cela permet à la réplication CloudMirror de générer des versions d'objets similaires sur le point de terminaison.
- Il est déconseillé d'utiliser plus de 100 locataires actifs pour les requêtes S3 nécessitant la réplication CloudMirror, les notifications et l'intégration à la recherche. Un nombre supérieur à 100 locataires actifs peut entraîner une baisse des performances du client S3.
- Les requêtes vers un point de terminaison qui ne peuvent être traitées seront mises en file d'attente, dans la limite de 500 000 requêtes. Cette limite est répartie équitablement entre les locataires actifs. Les nouveaux locataires sont autorisés à dépasser temporairement cette limite de 500 000 afin que les locataires nouvellement créés ne soient pas injustement pénalisés.

Informations connexes

- "Gérer les services de plateforme"
- "Configurer les paramètres du proxy de stockage"
- "Surveiller StorageGRID"

Réseau et ports pour les services de plateforme StorageGRID

Si vous autorisez un locataire S3 à utiliser les services de plateforme, vous devez configurer le réseau pour la grille afin de garantir que les messages des services de plateforme puissent être livrés à leurs destinations.

Vous pouvez activer les services de plateforme pour un compte locataire S3 lors de la création ou de la mise à jour du compte locataire. Si les services de plateforme sont activés, le locataire peut créer des points de terminaison servant de destination pour la réplication CloudMirror, les notifications d'événements ou les messages d'intégration de recherche provenant de ses compartiments S3. Ces messages de services de plateforme sont envoyés des nœuds de stockage exécutant le service ADC vers les points de terminaison de destination.

Par exemple, les locataires peuvent configurer les types de points de terminaison de destination suivants :

- Un cluster Elasticsearch hébergé localement
- Une application locale qui prend en charge la réception des messages Amazon Simple Notification Service
- Un cluster Kafka hébergé localement
- Un point de terminaison webhook externe ou hébergé localement qui prend en charge les requêtes de notification HTTP POST.

  Ce point de terminaison peut être hébergé sur divers serveurs web, frameworks ou outils de traitement des données tels que Fluentd.

- Un compartiment S3 hébergé localement sur la même instance ou une autre instance de StorageGRID
- Un point de terminaison externe, tel qu'un point de terminaison sur Amazon Web Services.

Pour garantir la transmission des messages des services de plateforme, vous devez configurer le ou les réseaux contenant les nœuds de stockage ADC. Vous devez vous assurer que les ports suivants peuvent être utilisés pour envoyer les messages des services de plateforme aux points de terminaison de destination.

Par défaut, les messages des services de la plateforme sont envoyés sur les ports suivants :

- **80** : Pour les URI de point de terminaison qui commencent par http (la plupart des points de terminaison)
- **443** : Pour les URI de points de terminaison qui commencent par https (la plupart des points de terminaison)
- **9092** : Pour les URI d'endpoint qui commencent par http ou https (endpoints Kafka uniquement)

Les locataires peuvent spécifier un port différent lorsqu'ils créent ou modifient un point de terminaison.

> Si un déploiement StorageGRID est utilisé comme destination pour la réplication CloudMirror, les messages de réplication peuvent être reçus sur un port autre que 80 ou 443. Assurez-vous que le port utilisé pour S3 par le déploiement StorageGRID de destination est spécifié dans le point de terminaison.

Si vous utilisez un serveur proxy non transparent, vous devez également "configurer les paramètres du proxy de stockage" autoriser l'envoi de messages vers des points de terminaison externes, tels qu'un point de terminaison sur Internet.

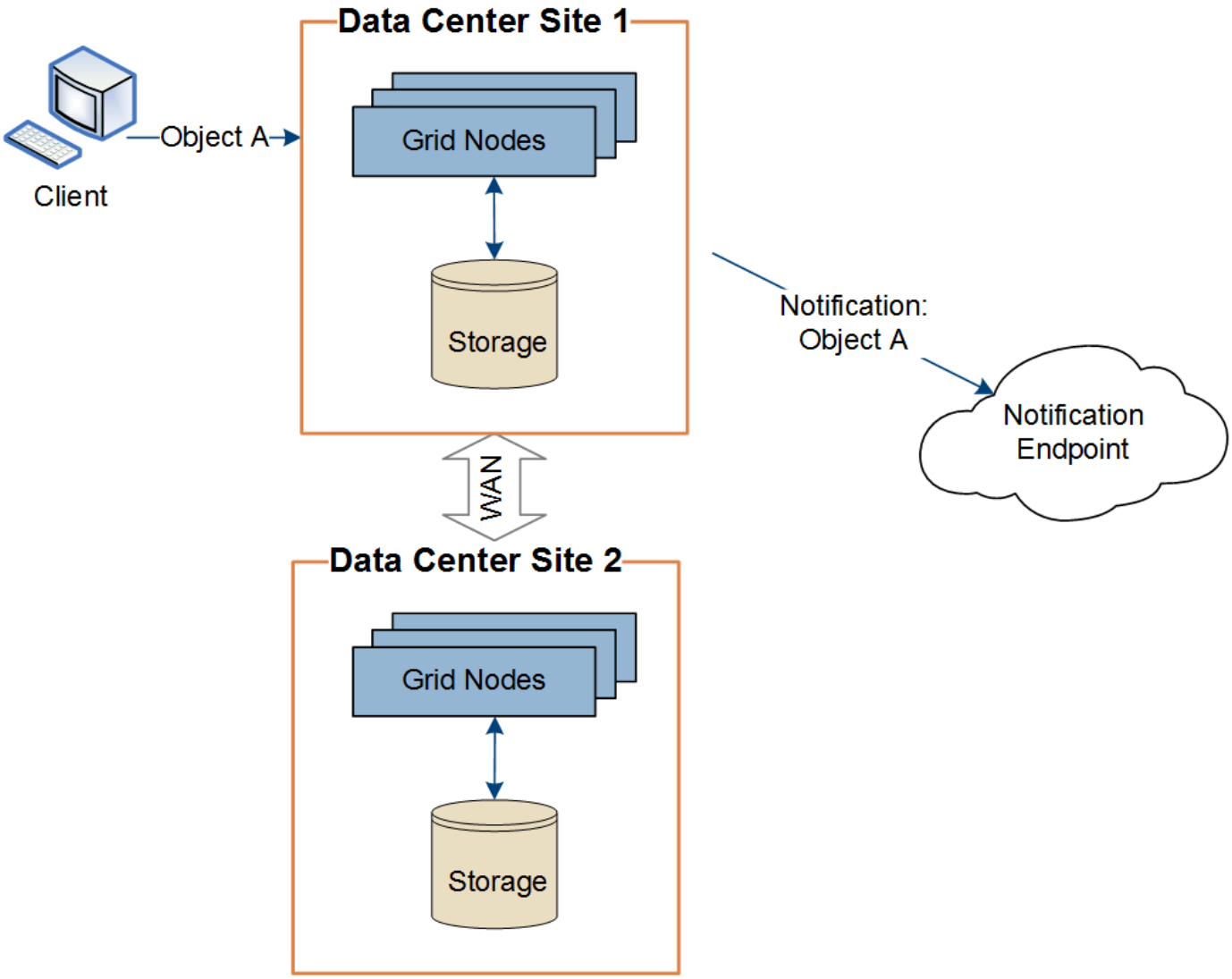
Informations connexes

"Utilisez un compte locataire"

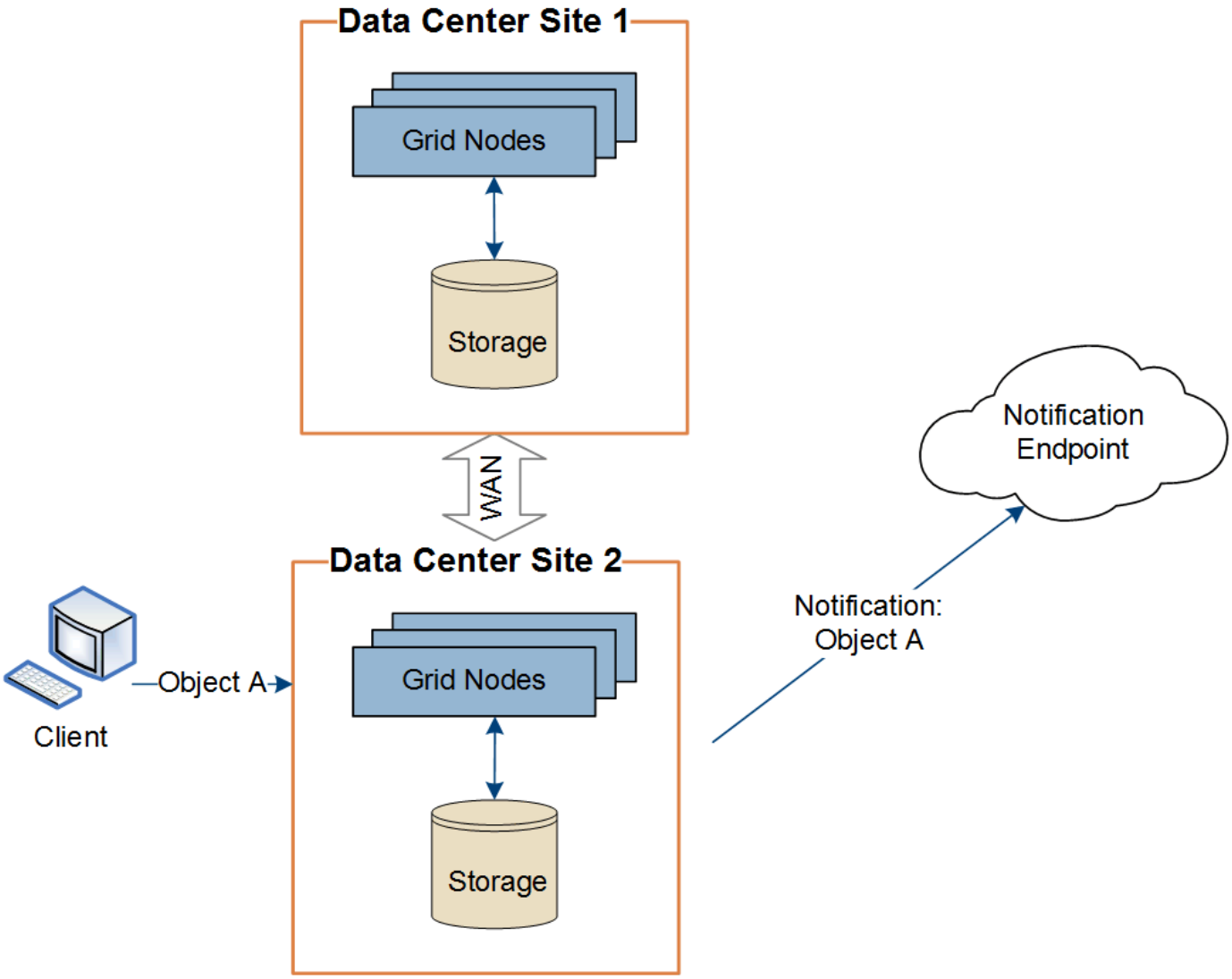
Livraison par site des messages des services de plateforme StorageGRID

Toutes les opérations des services de la plateforme sont effectuées site par site.

Autrement dit, si un locataire utilise un client pour effectuer une opération de création d'API S3 sur un objet en se connectant à un nœud de passerelle du Data Center Site 1, la notification concernant cette action est déclenchée et envoyée depuis le Data Center Site 1.



Si le client effectue ultérieurement une opération Delete de l'API S3 sur ce même objet depuis Data Center Site 2, la notification concernant l'action de suppression est déclenchée et envoyée depuis Data Center Site 2.



Assurez-vous que le réseau de chaque site est configuré de manière à ce que les messages des services de la plateforme puissent être acheminés vers leurs destinations.

Dépanner les services de plateforme StorageGRID

Les points de terminaison utilisés dans les services de la plateforme sont créés et gérés par les utilisateurs locataires dans le Tenant Manager. Cependant, si un locataire rencontre des difficultés pour configurer ou utiliser les services de la plateforme, vous pouvez utiliser le Grid Manager pour aider à résoudre le problème.

Problèmes liés aux nouveaux points de terminaison

Avant qu'un locataire puisse utiliser les services de la plateforme, il doit créer un ou plusieurs points de terminaison à l'aide du Tenant Manager. Chaque point de terminaison représente une destination externe pour un service de la plateforme, telle qu'un compartiment StorageGRID S3, un compartiment Amazon Web Services, un sujet Amazon Simple Notification Service, un sujet Kafka ou un cluster Elasticsearch hébergé localement ou sur AWS. Chaque point de terminaison inclut à la fois l'emplacement de la ressource externe et les informations d'identification nécessaires pour accéder à cette ressource.

Lorsqu'un locataire crée un point de terminaison, le système StorageGRID vérifie que le point de terminaison existe et qu'il est accessible à l'aide des identifiants spécifiés. La connexion au point de terminaison est

validée à partir d'un nœud sur chaque site.

En cas d'échec de la validation du point de terminaison, un message d'erreur explique la raison de cet échec. L'utilisateur du locataire doit résoudre le problème, puis essayer de créer à nouveau le point de terminaison.

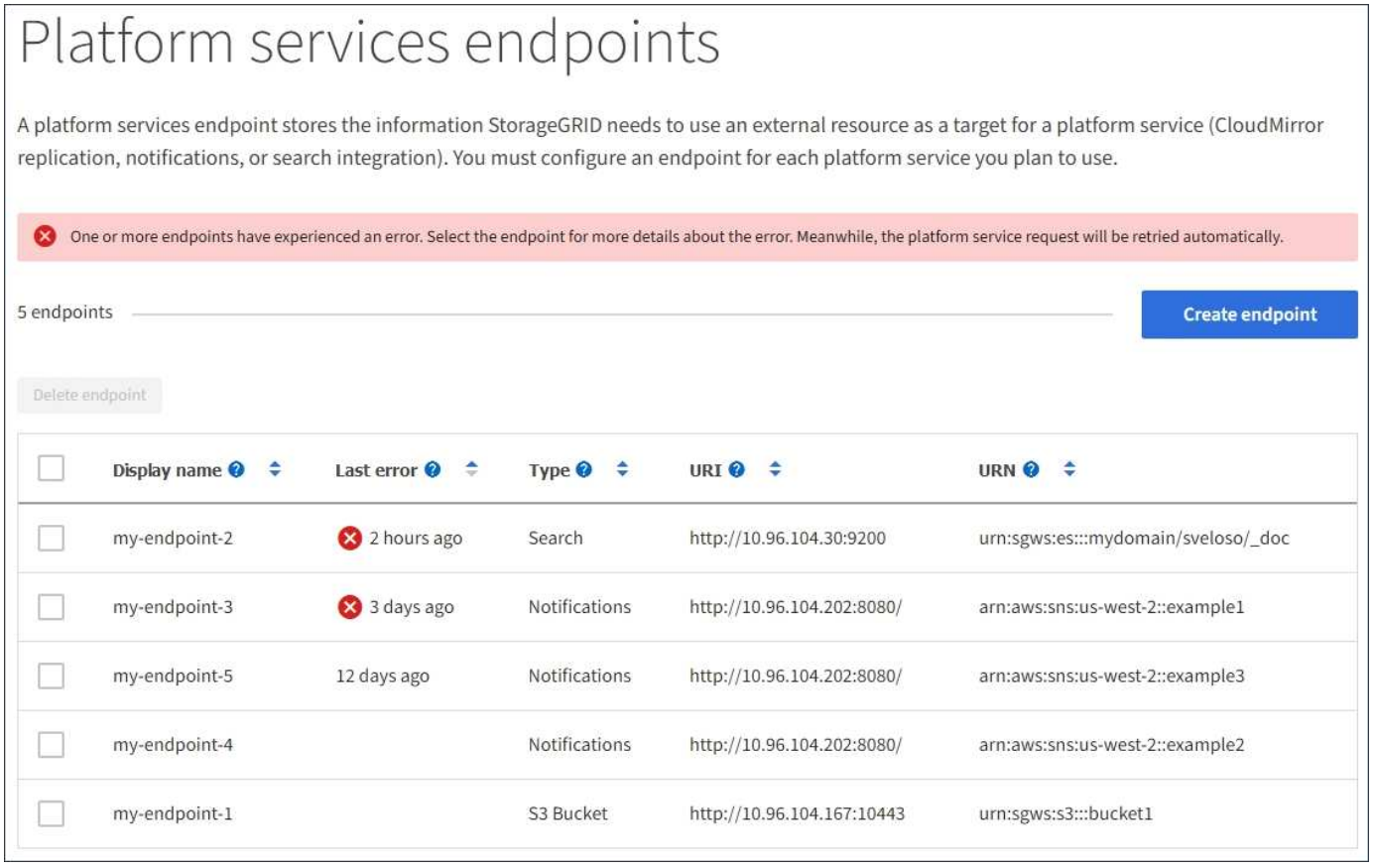
> La création du point de terminaison échouera si les services de la plateforme ne sont pas activés pour le compte du locataire.

Problèmes liés aux points de terminaison existants

Si une erreur se produit lorsque StorageGRID tente d'atteindre un point de terminaison existant, un message s'affiche sur le tableau de bord du Tenant Manager.

> One or more endpoints have experienced an error and might not be functioning properly. Go to the Endpoints page to view the error details. The last error occurred 2 hours ago.

Les utilisateurs locataires peuvent accéder à la page « Points de terminaison » pour examiner le message d'erreur le plus récent pour chaque point de terminaison et déterminer depuis combien de temps l'erreur s'est produite. La colonne « Dernière erreur » affiche le message d'erreur le plus récent pour chaque point de terminaison et indique depuis combien de temps l'erreur s'est produite. Les erreurs qui incluent l'icône ⊗ se sont produites au cours des 7 derniers jours.



> Certains messages d'erreur de la colonne **Dernière erreur** peuvent contenir un logID entre parenthèses. Un administrateur de grille ou le support technique peut utiliser ce logID pour trouver des informations plus détaillées sur l'erreur dans le fichier bycast.log.

Problèmes liés aux serveurs proxy

Si vous avez configuré un "proxy de stockage" entre les nœuds de stockage et les points de terminaison des services de la plateforme, des erreurs peuvent survenir si votre service proxy n'autorise pas les messages provenant de StorageGRID. Pour résoudre ces problèmes, vérifiez les paramètres de votre serveur proxy afin de vous assurer que les messages relatifs aux services de la plateforme ne sont pas bloqués.

Déterminez si une erreur s'est produite

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

Les opérations du client échouent

Certains problèmes liés aux services de la plateforme peuvent entraîner l'échec des opérations client sur le compartiment S3. Par exemple, les opérations client S3 échoueront si le service interne Replicated State Machine (RSM) s'arrête ou si un trop grand nombre de messages de services de plateforme sont en attente de livraison.

Pour vérifier l'état des services :

1. Sélectionnez **Nodes** > ***site*** > ***Storage Node*** > **Overview**.
2. Vérifiez les alertes actives dans le tableau des alertes.
3. Résolvez les alertes en cours. Au besoin, contactez le support technique.

Erreurs de point de terminaison récupérables et irrécupérables

Une fois les points de terminaison créés, des erreurs de requête de service de la plateforme peuvent survenir pour diverses raisons. Certaines erreurs sont récupérables avec l'intervention de l'utilisateur. Par exemple, des erreurs récupérables peuvent survenir pour les raisons suivantes :

- Les identifiants de l'utilisateur ont été supprimés ou ont expiré.
- Le compartiment de destination n'existe pas.
- La notification ne peut pas être transmise.

Si StorageGRID rencontre une erreur récupérable, la requête de service de la plateforme sera réessayée jusqu'à ce qu'elle réussisse.

D'autres erreurs sont irrécupérables. Par exemple, des erreurs irrécupérables peuvent survenir pour les raisons suivantes :

- Le point de terminaison a été supprimé.
- Un point de terminaison webhook de destination répond à une requête de notification par une erreur `400 Bad Request`.

Si StorageGRID rencontre une erreur de point de terminaison irrécupérable :

- Dans le Gestionnaire de grille, accédez à **Support** > **Outils** > **Métriques** > **Grafana** > **Platform Services Overview** pour afficher les détails de l'erreur.
- Dans le Gestionnaire de locataires, accédez à **STOCKAGE (S3)** > **Points de terminaison des services de plateforme** pour afficher les détails de l'erreur.

- Vérifiez la `/var/local/log/bycast-err.log` pour les erreurs associées. Les nœuds de stockage disposant du service ADC contiennent ce fichier journal.

Les messages des services de la plateforme ne peuvent pas être remis.

Si la destination rencontre un problème l'empêchant de recevoir les messages des services de plateforme, l'opération client sur le compartiment réussit, mais le message des services de plateforme n'est pas transmis. Par exemple, cette erreur peut se produire si les informations d'identification sont mises à jour sur la destination et que StorageGRID ne peut plus s'authentifier auprès du service de destination.

Vérifiez les alertes associées.

Performances ralenties pour les requêtes de service de la plateforme

Le logiciel StorageGRID peut limiter le nombre de requêtes S3 entrantes pour un compartiment si le débit d'envoi des requêtes dépasse le débit auquel le point de terminaison de destination peut les recevoir. La limitation ne se produit que lorsqu'il y a un retard d'envoi des requêtes en attente vers le point de terminaison de destination.

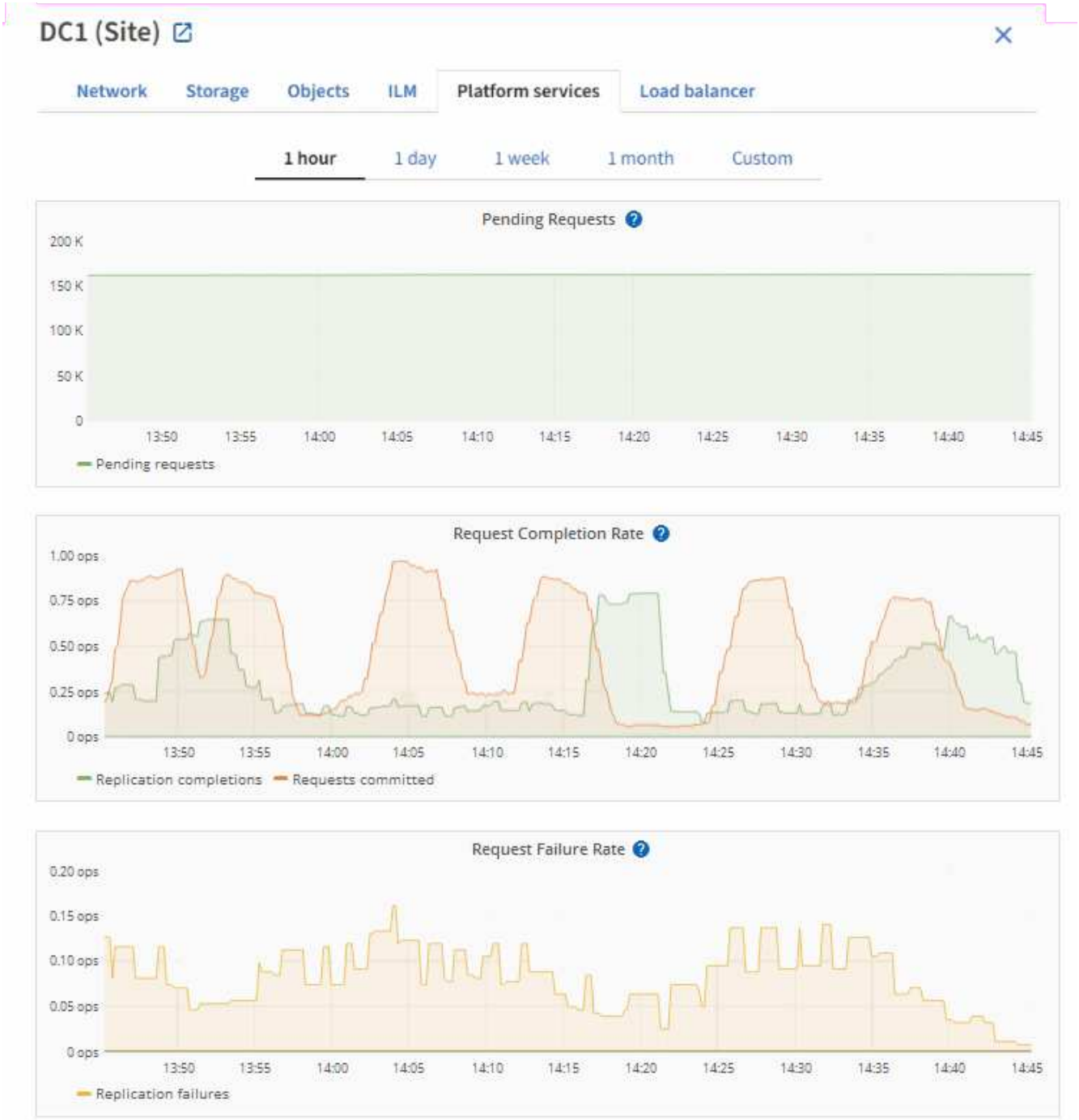
Le seul effet visible est un allongement du temps d'exécution des requêtes S3 entrantes. Si vous constatez un ralentissement significatif des performances, vous devez réduire le débit d'ingestion ou utiliser un point de terminaison offrant une capacité supérieure. Si le nombre de requêtes en attente continue d'augmenter, les opérations S3 côté client (telles que les requêtes PUT) finiront par échouer.

CloudMirror Les requêtes sont plus susceptibles d'être affectées par les performances du point de terminaison de destination, car elles impliquent généralement plus de transfert de données que les requêtes d'intégration de recherche ou de notification d'événements.

Les requêtes de service de la plateforme échouent

Pour consulter le taux d'échec des requêtes pour les services de la plateforme :

1. Sélectionnez **Nœuds**.
2. Sélectionnez ***site*** > **Services de plateforme**.
3. Consultez le graphique du taux d'erreur des requêtes.



Alerte d'indisponibilité des services de la plateforme

L'alerte **Services de plateforme indisponibles** indique qu'aucune opération de service de plateforme ne peut être effectuée sur un site, car trop peu de nœuds de stockage avec le service RSM sont en cours d'exécution ou disponibles.

Le service RSM garantit que les requêtes de service de la plateforme sont envoyées à leurs points de terminaison respectifs.

Pour résoudre cette alerte, identifiez les nœuds de stockage du site qui hébergent le service RSM. (Le service RSM est présent sur les nœuds de stockage qui hébergent également le service ADC.) Ensuite, assurez-vous qu'une majorité simple de ces nœuds de stockage sont en cours d'exécution et disponibles.

Si plusieurs nœuds de stockage contenant le service RSM tombent en panne sur un site, vous perdez toutes les requêtes de service de plateforme en attente pour ce site.

Conseils de dépannage supplémentaires pour les points de terminaison des services de plateforme

Pour plus d'informations, voir **Utiliser un compte locataire › Dépanner les points de terminaison des services de la plateforme**.

Informations connexes

"Dépanner le système StorageGRID"

Gérer S3 Select pour les comptes locataires dans StorageGRID

Vous pouvez autoriser certains locataires S3 à utiliser S3 Select pour émettre des requêtes SelectObjectContent sur des objets individuels.

S3 Select offre une solution efficace pour effectuer des recherches dans de grands volumes de données sans nécessiter le déploiement d'une base de données et des ressources associées. Il permet également de réduire le coût et la latence de récupération des données.

Qu'est-ce que S3 Select ?

S3 Select permet aux clients S3 d'utiliser des requêtes SelectObjectContent pour filtrer et récupérer uniquement les données nécessaires d'un objet. L'implémentation StorageGRID de S3 Select inclut un sous-ensemble des commandes et fonctionnalités de S3 Select.

Considérations et exigences relatives à l'utilisation de S3 Select

Exigences d'administration du grid

L'administrateur de la grille doit accorder aux locataires l'autorisation S3 Select. Sélectionnez **Autoriser S3 Select** lorsque "création d'un locataire" ou "modification d'un locataire".

Exigences relatives au format des objets

L'objet que vous souhaitez interroger doit être dans l'un des formats suivants :

- **CSV**. Peut être utilisé tel quel ou compressé dans des archives GZIP ou BZIP2.
- **Parquet**. Exigences supplémentaires pour les objets Parquet :
  - S3 Select prend uniquement en charge la compression par colonnes via GZIP ou Snappy. S3 Select ne prend pas en charge la compression de l'objet entier pour les objets Parquet.
  - S3 Select ne prend pas en charge la sortie Parquet. Vous devez spécifier le format de sortie comme CSV ou JSON.
  - La taille maximale d'un groupe de lignes non compressé est de 512 Mo.
  - Vous devez utiliser les types de données spécifiés dans le schéma de l'objet.
  - Vous ne pouvez pas utiliser les types logiques INTERVAL, JSON, LIST, TIME ou UUID.

Exigences relatives aux points de terminaison

La requête SelectObjectContent doit être envoyée à un "Point de terminaison de l'équilibreur de charge

StorageGRID".

Les nœuds d'administration et de passerelle utilisés par le point de terminaison doivent être l'un des suivants :

- Un nœud d'appliance de services
- Un nœud logiciel basé sur VMware
- Un nœud bare metal exécutant un noyau avec cgroup v2 activé

Considérations générales

Les requêtes ne peuvent pas être envoyées directement aux nœuds de stockage.

> SelectObjectContent requests peuvent dégrader les performances de l'équilibreur de charge pour tous les clients S3 et tous les locataires. N'activez cette fonctionnalité qu'en cas de besoin et uniquement pour les locataires de confiance.

Voir la "Instructions d'utilisation de S3 Select".

Pour consulter "Graphiques Grafana" pour les opérations S3 Select au fil du temps, sélectionnez **Support** > **Outils** > **Métriques** dans le Grid Manager.

Configurer les connexions client

Configurer les connexions client S3 à StorageGRID

En tant qu'administrateur de grille, vous gérez les options de configuration qui contrôlent la manière dont les applications clientes S3 se connectent à votre système StorageGRID pour stocker et récupérer des données.

> Les détails concernant Swift ont été supprimés de cette version du site de documentation. Voir "StorageGRID 11.8 : Configurez les connexions client S3 et Swift".

Tâches de configuration

1. Effectuez les tâches préalables dans StorageGRID, en fonction de la manière dont l'application cliente se connectera à StorageGRID.

Tâches requises

Vous devez obtenir :

- adresses IP
- Noms de domaine
- certificat SSL

Tâches facultatives

Configurez éventuellement :

- Fédération d'identité
- SSO

1. Utilisez StorageGRID pour obtenir les valeurs dont l'application a besoin pour se connecter à la grille. Vous pouvez soit utiliser l'assistant de configuration S3, soit configurer chaque entité StorageGRID manuellement.

Utilisez l'assistant de configuration S3

Suivez les étapes de l'assistant de configuration S3.

Configurer manuellement

1. Créer un groupe à haute disponibilité
2. Créer un point de terminaison d'équilibrage de charge
3. Créer un compte locataire
4. Créer un compartiment et des clés d'accès
5. Configurer la règle et la stratégie ILM

1. Utilisez l'application S3 pour établir la connexion à StorageGRID. Créez des entrées DNS pour associer les adresses IP aux 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 pour gérer et surveiller le stockage d'objets au fil du temps.

Informations nécessaires pour connecter StorageGRID à une application cliente

Avant de pouvoir connecter StorageGRID à une application cliente S3, vous devez effectuer des étapes de configuration dans StorageGRID et obtenir certaines valeurs.

De quelles valeurs avez-vous besoin ?

Le tableau suivant présente les valeurs que vous devez configurer dans StorageGRID et indique où ces valeurs sont utilisées par l'application S3 et le serveur DNS.

Valeur	Où la valeur est configurée	Là où la valeur est utilisée
Adresses IP virtuelles (VIP)	StorageGRID > Groupe HA	Entrée DNS
Port	StorageGRID > Point de terminaison de l'équilibreur de charge	Application cliente
certificat SSL	StorageGRID > Point de terminaison de l'équilibreur de charge	Application cliente
Nom du serveur (FQDN)	StorageGRID > Point de terminaison de l'équilibreur de charge	• Application cliente • Entrée DNS
ID de clé d'accès S3 et clé d'accès secrète	StorageGRID > Locataire et compartiment	Application cliente
Nom du compartiment/conteneur	StorageGRID > Locataire et compartiment	Application cliente

Comment obtenir ces valeurs ?

Selon vos besoins, vous pouvez procéder de l'une ou l'autre des manières suivantes pour obtenir les informations nécessaires :

- **Utilisez le "Assistant de configuration S3"**. L'assistant de configuration S3 vous aide à configurer rapidement les valeurs requises dans StorageGRID et génère un ou deux fichiers que vous pouvez utiliser lors de la configuration de l'application S3. L'assistant vous guide à travers les étapes nécessaires et vous aide à garantir que vos paramètres respectent les bonnes pratiques de StorageGRID.

  > Si vous configurez une application S3, il est recommandé d'utiliser l'assistant de configuration S3, sauf si vous avez des exigences particulières ou si votre implémentation nécessite une personnalisation importante.

- **Utilisez le "FabricPool assistant de configuration"**. Similaire à l'assistant de configuration S3, l'assistant de configuration FabricPool vous aide à configurer rapidement les valeurs requises et génère un fichier que vous pouvez utiliser lors de la configuration d'un niveau cloud FabricPool dans ONTAP.

  > Si vous prévoyez d'utiliser StorageGRID comme système de stockage d'objets pour un niveau cloud FabricPool, il est recommandé d'utiliser l'assistant de configuration FabricPool, sauf si vous savez que vous avez des exigences particulières ou si votre implémentation nécessite une personnalisation importante.

- **Configurez les éléments manuellement**. Si vous vous connectez à une application S3 et préférez ne pas utiliser l'assistant de configuration S3, vous pouvez obtenir les valeurs requises en effectuant la configuration manuellement. Procédez comme suit :

  a. Configurez le groupe de haute disponibilité (HA) que vous souhaitez utiliser pour l'application S3. Voir "Configurer les groupes à haute disponibilité".

b. Créez le point de terminaison de l'équilibreur de charge que l'application S3 utilisera. Voir "Configurer les points de terminaison de l'équilibreur de charge".

c. Créez le compte locataire que l'application S3 utilisera. Voir "Créer un compte locataire".

d. Pour un locataire S3, connectez-vous au compte du locataire et générez un ID de clé d'accès et une clé d'accès secrète pour chaque utilisateur qui accédera à l'application. Voir "Créez vos propres clés d'accès".

e. Créez un ou plusieurs compartiments S3 dans le compte du locataire. Pour S3, voir "Créer un compartiment S3".

f. Pour ajouter des instructions de placement spécifiques aux objets appartenant au nouveau locataire ou compartiment/conteneur, créez une nouvelle règle ILM et activez une nouvelle stratégie ILM pour utiliser cette règle. Voir "Créer une règle ILM" et "Créer une stratégie ILM".

Sécurité des clients S3 dans StorageGRID

Les comptes locataires StorageGRID utilisent des applications clientes S3 pour enregistrer les données d'objets dans StorageGRID. Vous devez examiner les mesures de sécurité mises en œuvre pour les applications clientes.

Résumé

La liste suivante résume la manière dont la sécurité est mise en œuvre pour l'API REST S3 :

Sécurité de la connexion
: TLS

Authentification du serveur
: Certificat serveur X.509 signé par l'autorité de certification système ou certificat serveur personnalisé fourni par l'administrateur

Authentification du client
: ID de clé d'accès au compte S3 et clé d'accès secrète

Autorisation du client
: Propriété du compartiment et toutes les politiques de contrôle d'accès applicables

Comment StorageGRID assure la sécurité des applications clientes

Les applications clientes S3 peuvent se connecter au service d'équilibrage de charge sur les nœuds de passerelle ou les nœuds d'administration, ou directement aux nœuds de stockage.

- Les clients qui se connectent au service Load Balancer peuvent utiliser HTTPS ou HTTP, selon la façon dont vous "configurer le point de terminaison de l'équilibreur de charge".

  Le protocole HTTPS assure une communication sécurisée et chiffrée (TLS) et est recommandé. Vous devez associer un certificat de sécurité au point de terminaison.

  Le protocole HTTP offre une communication moins sécurisée et non chiffrée et ne devrait être utilisé que pour les environnements hors production ou de test.

- Les clients qui se connectent aux nœuds de stockage peuvent également utiliser HTTPS ou HTTP.

HTTPS est le protocole par défaut et est recommandé.

Le protocole HTTP offre une communication moins sécurisée et non chiffrée, mais peut être utilisé en option "activé" pour les environnements hors production ou de test.

- Les communications entre StorageGRID et le client sont chiffrées à l'aide de TLS.
- Les communications entre le service d'équilibrage de charge et les nœuds de stockage au sein de la grille sont chiffrées, que le point de terminaison de l'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 des opérations REST API.

Certificats de sécurité et applications clientes

Dans tous les cas, les applications clientes peuvent établir des connexions TLS en utilisant soit un certificat serveur personnalisé téléchargé par l'administrateur de la grille, soit un certificat généré par le système StorageGRID :

- Lorsque les applications clientes se connectent au service d'équilibrage de charge, elles utilisent le certificat configuré pour le point de terminaison de l'équilibreur de charge. Chaque point de terminaison d'équilibrage de charge possède son propre certificat—soit un certificat serveur personnalisé chargé par l'administrateur de la grille, soit un certificat généré par l'administrateur de la grille dans StorageGRID lors de la configuration du point de terminaison.

  Voir "Considérations relatives à l'équilibrage de charge".

- Lorsque des applications clientes se connectent directement à un nœud de stockage, elles utilisent soit les certificats serveur générés par le système pour les nœuds de stockage lors de l'installation du système StorageGRID (qui sont signés par l'autorité de certification du système), soit un certificat serveur personnalisé unique fourni pour la grille par un administrateur de la grille. Voir "ajoutez un certificat d'API S3 personnalisé".

Les clients doivent être configurés pour faire confiance à l'autorité de certification qui a signé le certificat qu'ils utilisent pour établir des connexions TLS.

Algorithmes de hachage et de chiffrement pris en charge pour les bibliothèques TLS

Le système StorageGRID prend en charge un ensemble de suites de chiffrement que les applications clientes peuvent utiliser lors de l'établissement d'une session TLS. Pour configurer les suites de chiffrement, accédez à **Configuration** > **Sécurité** > **Paramètres de sécurité** et sélectionnez **Stratégies TLS et SSH**.

Versions de TLS prises en charge

StorageGRID prend en charge TLS 1.2 et TLS 1.3.

SSLv3 et TLS 1.1 (ou versions antérieures) ne sont plus pris en charge.

Utilisez l'assistant de configuration S3

Considérations et exigences de l'assistant de configuration StorageGRID S3

Vous pouvez utiliser l'assistant de configuration S3 pour configurer StorageGRID comme système de stockage d'objets pour une application S3.

Quand utiliser l'assistant de configuration S3

L'assistant de configuration S3 vous guide à chaque étape de la configuration de StorageGRID pour une utilisation avec une application S3. Dans le cadre de l'utilisation 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 StorageGRID.

Si vous disposez de l'"Autorisation d'accès root", vous pouvez compléter l'assistant de configuration S3 lors de la première utilisation de StorageGRID Grid Manager, ou y accéder et le compléter ultérieurement. Selon vos besoins, vous pouvez également configurer manuellement tout ou partie des éléments requis, puis utiliser l'assistant pour assembler les valeurs nécessaires à une application S3.

Avant d'utiliser l'assistant

Avant d'utiliser l'assistant, assurez-vous d'avoir rempli ces conditions préalables.

Obtenez des adresses IP et configurez des interfaces VLAN

Si vous configurez un groupe à haute disponibilité (HA), vous savez à quels nœuds l'application S3 se connectera et quel réseau StorageGRID sera utilisé. Vous savez également quelles valeurs saisir pour le CIDR du sous-réseau, l'adresse IP de la passerelle et les adresses IP virtuelles (VIP).

Si vous prévoyez d'utiliser un réseau local virtuel (VLAN) pour isoler le trafic de l'application S3, vous avez déjà configuré l'interface VLAN. Voir "Configurer les interfaces VLAN".

Configurer la fédération d'identité et l'authentification unique (SSO)

Si vous prévoyez d'utiliser la fédération d'identité ou l'authentification unique (SSO) pour votre système StorageGRID, vous avez activé ces fonctionnalités. Vous savez également quel groupe fédéré doit disposer d'un accès root pour le compte locataire que l'application S3 utilisera. Voir "Utilisez la fédération d'identités" et "Configurer l'authentification unique".

Obtenir et configurer les noms de domaine

Vous savez quel nom de domaine complet (FQDN) utiliser pour StorageGRID. Les entrées du serveur de noms de domaine (DNS) associeront ce FQDN aux adresses IP virtuelles (VIP) du groupe HA 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 points de terminaison S3 configurés". L'utilisation de requêtes de type hébergement virtuel est recommandée.

Passez en revue les exigences relatives à l'équilibreur de charge et au certificat de sécurité

Si vous prévoyez d'utiliser l'équilibreur de charge StorageGRID, vous avez pris connaissance des considérations générales relatives à l'équilibrage de charge. Vous disposez des certificats à importer ou des valeurs nécessaires à la génération d'un certificat.

Si vous prévoyez d'utiliser un point de terminaison d'équilibreur de charge externe (tiers), vous disposez du domaine complet (FQDN), du port et du certificat pour cet équilibreur de charge.

Configurez les connexions de fédération de grille

Si vous souhaitez autoriser le locataire S3 à cloner les données du compte et à répliquer les objets du compartiment vers une autre grille à l'aide d'une connexion de fédération de grilles, confirmez les points suivants avant de démarrer l'assistant :

- Vous avez "configuré la connexion de fédération de grille".

- L'état de la connexion est **Connecté**.
- Vous disposez des droits d'accès root.

Accédez et complétez l'assistant de configuration S3 dans StorageGRID

Vous pouvez utiliser l'assistant de configuration S3 pour configurer StorageGRID afin de l'utiliser avec une application S3. L'assistant de configuration fournit les valeurs dont l'application a besoin pour accéder à un compartiment StorageGRID et y enregistrer des objets.

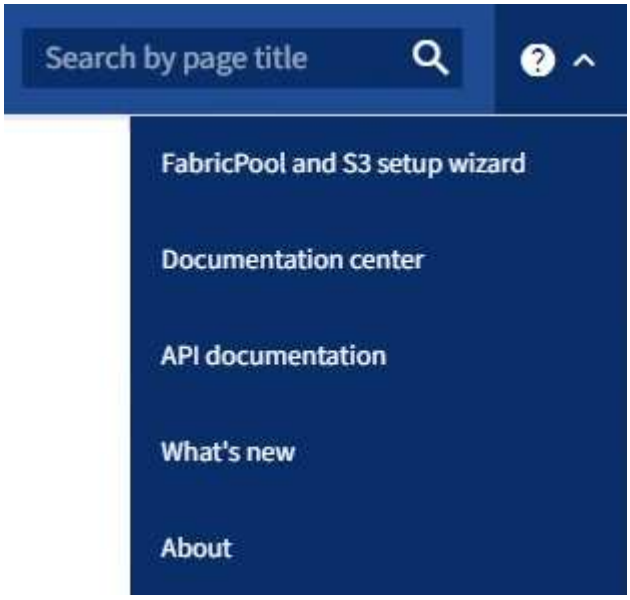
Avant de commencer

- Vous avez le "Autorisation d'accès root".
- Vous avez consulté les "considérations et exigences" instructions pour utiliser l'assistant.

Accédez à l'assistant

Étapes

1. Connectez-vous au Gestionnaire de grille en utilisant 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 n'apparaît plus, sélectionnez l'icône d'aide dans la barre d'en-tête du Grid Manager et sélectionnez **FabricPool and S3 setup wizard**.



3. Dans la section application S3 de la page de l'assistant de configuration FabricPool et S3, sélectionnez **Configurer maintenant**.

Étape 1 sur 6 : Configurer le groupe HA

Un groupe HA est un ensemble de nœuds qui contiennent chacun le service d'équilibrage de charge StorageGRID. Un groupe HA peut contenir des nœuds de passerelle, des nœuds d'administration, ou les deux.

Vous pouvez utiliser un groupe HA pour garantir la disponibilité des connexions de données S3. Si l'interface active du groupe HA tombe en panne, une interface de secours peut gérer la charge de travail avec peu d'impact sur les opérations S3.

Pour plus de détails sur cette tâche, voir "Gérer les groupes à haute disponibilité".

Étapes

1. Si vous prévoyez d'utiliser un équilibreur de charge externe, vous n'avez pas besoin de créer un groupe HA. Sélectionnez **Ignorer cette étape** et accédez à Étape 2 sur 6 : Configurer le point de terminaison de l'équilibreur de charge.
2. Pour utiliser l'équilibreur de charge StorageGRID, vous pouvez créer un nouveau groupe HA ou utiliser un groupe HA existant.

Créer un groupe HA

a. Pour créer un nouveau groupe HA, sélectionnez **Créer un groupe HA**.

b. Pour l'étape **Saisir les détails**, complétez les champs suivants.

Champ	Description
nom de groupe HA	Un nom d'affichage unique pour ce groupe HA.
Description (facultatif)	La description de ce groupe HA.

c. À l'étape **Ajouter des interfaces**, sélectionnez les interfaces de nœud que vous souhaitez utiliser dans ce groupe HA.

Utilisez les en-têtes de colonnes pour trier les lignes ou saisissez un terme de recherche pour localiser plus rapidement les interfaces.

Vous pouvez sélectionner un ou plusieurs nœuds, mais vous ne pouvez sélectionner qu'une seule interface par nœud.

d. Pour l'étape **Prioriser les interfaces**, déterminez l'interface principale et toute interface de secours pour ce groupe HA.

Faites glisser les 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 panne.

Si le groupe HA comprend plusieurs interfaces et que l'interface active tombe en panne, les adresses IP virtuelles (VIP) sont transférées vers la première interface de secours par ordre de priorité. Si cette interface tombe en panne à son tour, les adresses VIP sont transférées vers l'interface de secours suivante, et ainsi de suite. Une fois les pannes résolues, les adresses VIP sont réaffectées à l'interface prioritaire disponible.

e. Pour l'étape **Saisir les adresses IP**, complétez les champs suivants.

Champ	Description
CIDR du sous-réseau	L'adresse du sous-réseau VIP en notation CIDR — une adresse IPv4 suivie d'une barre oblique et de la longueur du sous-réseau (0-32). L'adresse réseau ne doit comporter aucun bit d'hôte activé. Par exemple, `192.16.0.0/22`.
Adresse IP de la passerelle (facultatif)	Si les adresses IP S3 utilisées pour accéder à StorageGRID ne se trouvent pas sur le même sous-réseau que les adresses VIP de StorageGRID, saisissez l'adresse IP de la passerelle locale VIP de StorageGRID. L'adresse IP de la passerelle locale doit appartenir au sous-réseau VIP.

Champ	Description
Adresse IP virtuelle	Saisissez au moins une et au plus dix adresses VIP pour l'interface active du groupe HA. Toutes les adresses VIP doivent appartenir au sous-réseau VIP. Au moins une adresse doit être de type IPv4. Vous pouvez également spécifier des adresses IPv4 et IPv6 supplémentaires.

f. Sélectionnez **Créer un groupe HA** puis **Terminer** pour revenir à l'assistant de configuration S3.

g. Sélectionnez **Continuer** pour passer à l'étape de l'équilibreur de charge.

Utiliser le groupe HA existant

a. Pour utiliser un groupe HA existant, sélectionnez le nom du groupe HA dans **Sélectionner un groupe HA**.

b. Sélectionnez **Continuer** pour passer à l'étape de l'équilibreur de charge.

Étape 2 sur 6 : Configurer le point de terminaison de l'équilibreur de charge

StorageGRID utilise un équilibreur de charge pour gérer la charge de travail des applications clientes. L'équilibrage de charge optimise la vitesse et la capacité de connexion sur plusieurs nœuds de stockage.

Vous pouvez utiliser le service d'équilibrage de charge StorageGRID, présent sur tous les nœuds Gateway et Admin, ou vous connecter à un équilibreur de charge externe (tiers). L'utilisation de l'équilibreur de charge StorageGRID est recommandée.

Pour plus de détails sur cette tâche, voir "Considérations relatives à l'équilibrage de charge".

Pour utiliser le service d'équilibrage de charge StorageGRID, sélectionnez l'onglet **StorageGRID load balancer**, puis créez ou sélectionnez le point de terminaison d'équilibrage de charge que vous souhaitez utiliser. Pour utiliser un équilibreur de charge externe, sélectionnez l'onglet **External load balancer** et fournissez les détails concernant le système que vous avez déjà configuré.

Créer un point de terminaison

Étapes

1. Pour créer un point de terminaison d'équilibrage de charge, sélectionnez **Créer un point de terminaison**.
2. Pour l'étape **Saisir les détails du point de terminaison**, complétez les champs suivants.

Champ	Description
Nom	Un nom descriptif pour le point de terminaison.
Port	Le port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est défini par défaut sur 10433 pour le premier point de terminaison que vous créez, mais vous pouvez saisir n'importe quel port externe inutilisé. Si vous saisissez 80 ou 443, le point de terminaison est configuré uniquement sur les nœuds de passerelle, car ces ports sont réservés sur les nœuds d'administration. **Remarque :** Les ports utilisés par d'autres services de grille ne sont pas autorisés. Voir "Ports internes de StorageGRID".
Type de client	Doit être **S3**.
Protocole réseau	Sélectionnez **HTTPS**. **Remarque** : La communication avec StorageGRID sans chiffrement TLS est prise en charge, mais n'est pas recommandée.

3. À l'étape **Sélectionnez le mode de liaison**, spécifiez le mode de liaison. Le mode de liaison contrôle la façon dont le point de terminaison est accessible, soit via n'importe quelle adresse IP, soit via des adresses IP et des interfaces réseau spécifiques.

Mode	Description
Global (par défaut)	Les clients peuvent accéder au point de terminaison en utilisant l'adresse IP de n'importe quel Gateway Node ou Admin Node, l'adresse IP virtuelle (VIP) de n'importe quel groupe HA sur n'importe quel réseau, ou un FQDN correspondant. Utilisez le paramètre **Global** (par défaut) sauf si vous devez restreindre l'accessibilité de ce point de terminaison.

Mode	Description
Adresses IP virtuelles des groupes HA	Les clients doivent utiliser une adresse IP virtuelle (ou un nom de domaine complet correspondant) d'un groupe HA pour accéder à ce point de terminaison. Les points de terminaison dotés de ce mode de liaison peuvent tous utiliser le même numéro de port, à condition que les groupes HA que vous sélectionnez pour les points de terminaison ne se chevauchent pas.
Interfaces de nœud	Les clients doivent utiliser les adresses IP (ou les noms de domaine complets correspondants) des interfaces de nœud sélectionnées pour accéder à ce point de terminaison.
Type de nœud	En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel Admin Node, soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel Gateway Node pour accéder à ce point de terminaison.

4. Pour l'étape d'accès du locataire, sélectionnez l'une des options suivantes :

Champ	Description
Autoriser tous les locataires (par défaut)	Tous les comptes locataires peuvent utiliser ce point de terminaison pour accéder à leurs compartiments.
Autoriser les locataires sélectionnés	Seuls les comptes locataires sélectionnés peuvent utiliser ce point de terminaison pour accéder à leurs compartiments.
Bloquer les locataires sélectionnés	Les comptes locataires sélectionnés ne peuvent pas utiliser ce point de terminaison pour accéder à leurs compartiments. Tous les autres locataires peuvent utiliser ce point de terminaison.

5. Pour l'étape **Joindre le certificat**, sélectionnez l'une des options suivantes :

Champ	Description
Télécharger le certificat (recommandé)	Utilisez cette option pour télécharger un certificat de serveur signé par une autorité de certification, la clé privée du certificat et, éventuellement, un ensemble de certificats d'autorité de certification.
Générer un certificat	Utilisez cette option pour générer un certificat auto-signé. Consultez "Configurer les points de terminaison de l'équilibreur de charge" pour plus de détails sur les informations à saisir.

Champ	Description
Utiliser le certificat StorageGRID S3	N'utilisez cette option que si vous avez déjà importé ou généré une version personnalisée du certificat global StorageGRID. Consultez "Configurer les certificats de l'API S3" pour plus de détails.

6. Sélectionnez **Terminer** pour revenir à l'assistant de configuration S3.
7. Sélectionnez **Continuer** pour passer à l'étape du locataire et du compartiment.

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

Utilisez le point de terminaison de l'équilibreur de charge existant

Étapes

1. Pour utiliser un point de terminaison existant, sélectionnez son nom dans **Sélectionner un point de terminaison d'équilibrage de charge**.
2. Sélectionnez **Continuer** pour passer à l'étape du locataire et du compartiment.

Utiliser un équilibreur de charge externe

Étapes

1. Pour utiliser un équilibreur de charge externe, complétez les champs suivants.

Champ	Description
FQDN	Le domaine complet (FQDN) de l'équilibreur de charge externe.
Port	Le numéro de port que l'application S3 utilisera pour se connecter à l'équilibreur de charge externe.
Certificat	Copiez le certificat du serveur pour l'équilibreur de charge externe et collez-le dans ce champ.

2. Sélectionnez **Continuer** pour passer à l'étape du locataire et du compartiment.

Étape 3 sur 6 : Créez un locataire et un compartiment

Un locataire est une entité qui peut utiliser les applications S3 pour stocker et récupérer des objets dans StorageGRID. Chaque locataire possède ses propres utilisateurs, clés d'accès, compartiments, objets et un ensemble spécifique de fonctionnalités.

Un bucket est un conteneur utilisé pour stocker les objets d'un locataire et les métadonnées des objets. Bien que les locataires puissent avoir plusieurs buckets, l'assistant vous aide à créer un locataire et un bucket de la manière la plus rapide et la plus simple. Si vous devez ajouter des buckets ou définir des options ultérieurement, vous pouvez utiliser le Tenant Manager.

Pour plus de détails sur cette tâche, consultez "Créer un compte locataire" et "Créer un compartiment S3".

Étapes

1. Saisissez un nom pour le compte locataire.

   Les noms des locataires n'ont pas besoin d'être uniques. Lors de la création du compte locataire, il reçoit un identifiant numérique unique.

2. Définissez l'accès racine pour le compte locataire, selon que votre système StorageGRID utilise "fédération d'identité", "authentification unique (SSO)" ou les deux.

Option	Faites ceci
Si la fédération d'identités n'est pas activée	Spécifiez le mot de passe à utiliser pour vous connecter au locataire en tant qu'utilisateur root local.
Si la fédération d'identité est activée	a. Sélectionnez un groupe fédéré existant pour avoir "Autorisation d'accès root" pour le locataire. b. Vous pouvez également spécifier le mot de passe à utiliser lors de la connexion au locataire en tant qu'utilisateur racine local.
Si la fédération d'identités et l'authentification unique (SSO) sont toutes deux activées	Sélectionnez un groupe fédéré existant pour avoir "Autorisation d'accès root" pour le locataire. Aucun utilisateur local ne peut se connecter.

3. Si vous souhaitez que l'assistant crée l'ID de clé d'accès et la clé d'accès secrète pour l'utilisateur racine, sélectionnez **Créer automatiquement la clé d'accès S3 de l'utilisateur racine**.

   Sélectionnez cette option si le seul utilisateur du locataire est l'utilisateur racine. Si d'autres utilisateurs utiliseront ce locataire, "utilisez Tenant Manager" pour configurer les clés et les autorisations.

4. Si vous souhaitez créer un compartiment pour ce locataire maintenant, sélectionnez **Créer un compartiment pour ce locataire**.

   Si le S3 Object Lock est activé pour la grille, le compartiment créé à cette étape n'a pas le S3 Object Lock activé. Si vous devez utiliser un compartiment S3 Object Lock pour cette application S3, ne sélectionnez pas la création d'un compartiment maintenant. Utilisez plutôt Tenant Manager pour "créer le compartiment" ultérieurement.

   a. Saisissez 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`) sauf si vous prévoyez d'utiliser ILM à l'avenir pour filtrer les objets en fonction de la région du bucket.

5. Sélectionnez **Créer et continuer**.

Étape 4 sur 6 : Télécharger les données

Lors de l'étape de téléchargement des données, vous pouvez télécharger un ou deux fichiers pour enregistrer les détails de ce que vous venez de configurer.

Étapes

1. Si vous avez sélectionné **Créer automatiquement une clé d'accès S3 pour l'utilisateur racine**, effectuez une ou les deux opérations suivantes :
   - Sélectionnez **Télécharger les clés d'accès** pour télécharger un `.csv` fichier contenant le nom du compte tenant, l'ID de la clé d'accès et la clé d'accès secrète.
   - Sélectionnez l'icône de copie ( ) pour copier l'ID de clé d'accès et la clé d'accès secrète dans le presse-papiers.
2. Sélectionnez **Télécharger les valeurs de configuration** pour télécharger un `.txt` fichier contenant les paramètres du point de terminaison de l'équilibreur de charge, du tenant, du bucket et de l'utilisateur root.
3. Conservez ces informations dans un endroit sûr.

> Ne fermez pas cette page tant que vous n'avez pas copié les deux clés d'accès. Les clés ne seront plus disponibles après la fermeture de cette page. Veillez à conserver ces informations en lieu sûr, car elles peuvent être utilisées pour obtenir des données à partir de votre système StorageGRID.

4. Si le système vous y invite, cochez la case pour confirmer que vous avez téléchargé ou copié les clés.
5. Sélectionnez **Continuer** pour passer à l'étape relative à la règle et à la stratégie ILM.

Étape 5 sur 6 : Examiner la règle ILM et la politique ILM pour S3

Les règles de gestion du cycle de vie des informations (ILM) contrôlent l'emplacement, la durée de conservation et le comportement d'ingestion de tous les objets dans votre système StorageGRID. La stratégie ILM incluse avec StorageGRID crée deux copies répliquées de tous les objets. Cette stratégie reste en vigueur jusqu'à ce que vous activiez au moins une nouvelle stratégie.

Étapes

1. Examinez 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 nouvelle règle et une nouvelle stratégie. Voir "Créer une règle ILM" et "Utilisez les politiques ILM".
3. Sélectionnez **J'ai pris connaissance de ces étapes et je comprends ce que je dois faire**.
4. Cochez la case pour indiquer que vous comprenez ce que vous devez faire ensuite.
5. Sélectionnez **Continuer** pour accéder au **Résumé**.

Étape 6 sur 6 : Récapitulatif

Étapes

1. Consultez le résumé.
2. Prenez note des détails des étapes suivantes, qui décrivent la configuration supplémentaire pouvant être nécessaire avant de vous connecter au client S3. Par exemple, en sélectionnant **Se connecter en tant que root**, vous accédez au Tenant Manager, où vous pouvez ajouter des utilisateurs de locataire, créer des compartiments supplémentaires et mettre à jour les paramètres des compartiments.
3. Sélectionnez **Terminer**.
4. Configurez l'application à l'aide du fichier que vous avez téléchargé depuis StorageGRID ou des valeurs que vous avez obtenues manuellement.

Gérer les groupes HA

Découvrez les groupes de haute disponibilité StorageGRID

Les groupes à haute disponibilité (HA) fournissent des connexions de données à haute disponibilité pour les clients S3 et des connexions à haute disponibilité au Grid Manager et au Tenant Manager.

Vous pouvez regrouper les interfaces réseau de plusieurs nœuds Admin et Gateway dans un groupe à haute disponibilité (HA). Si l'interface active du groupe HA tombe en panne, une interface de secours peut gérer la charge de travail.

Chaque groupe HA donne accès aux services partagés sur les nœuds sélectionnés.

- Les groupes HA qui incluent des nœuds de passerelle, des nœuds d'administration ou les deux fournissent des connexions de données hautement disponibles pour les clients S3.
- Les groupes HA qui incluent uniquement des nœuds d'administration offrent des connexions à haute disponibilité au Grid Manager et au Tenant Manager.
- Un groupe HA composé uniquement d'appliances de services et de nœuds logiciels basés sur VMware peut fournir des connexions à haute disponibilité pour "Les locataires S3 qui utilisent S3 Select". Les groupes HA sont recommandés lors de l'utilisation de S3 Select, mais ne sont pas obligatoires.

Comment créer un groupe HA ?

1. Vous sélectionnez une interface réseau pour un ou plusieurs nœuds d'administration ou nœuds de passerelle. Vous pouvez utiliser une interface Grid Network (eth0), une interface Client Network (eth2), une interface VLAN ou une interface d'accès que vous avez ajoutée au nœud.

   > Vous ne pouvez pas ajouter une interface à un groupe HA si elle possède une adresse IP attribuée par DHCP.

2. Vous désignez une interface comme interface principale. L'interface principale est l'interface active sauf en cas de panne.
3. Vous déterminez l'ordre de priorité des interfaces de sauvegarde.
4. Vous attribuez de une à dix adresses IP virtuelles (VIP) au groupe. Les applications clientes peuvent utiliser n'importe laquelle de ces adresses VIP pour se connecter à StorageGRID.

Pour obtenir des instructions, consultez "Configurer les groupes à haute disponibilité".

Qu'est-ce que l'interface active ?

En fonctionnement normal, toutes les adresses VIP du groupe HA sont ajoutées à l'interface principale, qui est la première interface par ordre de priorité. Tant que l'interface principale reste disponible, elle est utilisée lorsque des clients se connectent à une adresse VIP du groupe. Autrement dit, en fonctionnement normal, l'interface principale est l'interface « active » du groupe.

De même, en fonctionnement normal, les interfaces de priorité inférieure du groupe HA servent d'interfaces de secours. Ces interfaces de secours ne sont utilisées que si l'interface principale (actuellement active) devient indisponible.

Afficher l'état actuel du groupe HA d'un nœud

Pour voir si un nœud est affecté à un groupe HA et déterminer son état actuel, sélectionnez **Nodes** > ***node***.

Si l'onglet **Aperçu** comporte une entrée pour les **groupes HA**, le nœud est affecté aux groupes HA listés. La valeur après le nom du groupe correspond à l'état actuel du nœud dans le groupe HA :

- **Actif** : Le groupe HA est actuellement hébergé sur ce nœud.
- **Sauvegarde** : Le groupe HA n'utilise pas actuellement ce nœud ; il s'agit d'une interface de sauvegarde.
- **Arrêté** : Le groupe HA ne peut pas être hébergé sur ce nœud car le service de haute disponibilité (keepalived) a été arrêté manuellement.
- **Erreur** : Le groupe HA ne peut pas être hébergé sur ce nœud en raison d'un ou de plusieurs des éléments suivants :
  - Le service Load Balancer (nginx-gw) n'est pas en cours d'exécution sur le nœud.
  - L'interface eth0 ou VIP du nœud est hors service.
  - Le nœud est hors service.

Dans cet exemple, le nœud d'administration principal a été ajouté à deux groupes HA. Ce nœud est actuellement l'interface active pour le groupe des clients d'administration et une interface de secours pour le groupe des 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 HA comprend plus d'une interface et que l'interface active tombe en panne, les adresses VIP sont transférées vers la première interface de secours disponible selon l'ordre de priorité. Si cette interface tombe en panne, les adresses VIP sont transférées vers l'interface de secours suivante, et ainsi de suite.

Le basculement peut être déclenché pour l'une des raisons suivantes :

- Le nœud sur lequel l'interface est configurée tombe en panne.
- Le nœud sur lequel l'interface est configurée perd la connectivité avec tous les autres nœuds pendant au moins 2 minutes.
- L'interface active tombe en panne.
- Le service d'équilibrage de charge s'arrête.
- Le service de haute disponibilité s'arrête.

> Le basculement peut ne pas être déclenché par des pannes réseau externes au nœud hébergeant l'interface active. De même, le basculement n'est pas déclenché par les services du Grid Manager ou du Tenant Manager.

Le processus de basculement ne prend généralement que quelques secondes et est suffisamment rapide pour que les applications clientes ne subissent que peu d'impact et puissent compter sur des comportements de nouvelle tentative normaux pour continuer à fonctionner.

Lorsque la panne est résolue et qu'une interface de priorité supérieure redevient disponible, les adresses VIP sont automatiquement déplacées vers l'interface de priorité la plus élevée disponible.

Comment les groupes HA de StorageGRID assurent une haute disponibilité

Vous pouvez utiliser des groupes à haute disponibilité (HA) pour fournir des connexions hautement disponibles à StorageGRID pour les données d'objets et pour une utilisation administrative.

- Un groupe HA peut fournir des connexions administratives hautement disponibles au Grid Manager ou au Tenant Manager.
- Un groupe HA peut fournir des connexions de données à haute disponibilité pour les clients S3.
- Un groupe HA ne contenant qu'une seule interface vous permet de fournir de nombreuses adresses VIP et de définir explicitement des adresses IPv6.

Un groupe HA ne peut garantir une haute disponibilité que si tous les nœuds qui le composent fournissent les mêmes services. Lorsque vous créez un groupe HA, ajoutez des interfaces provenant des types de nœuds qui fournissent les services dont vous avez besoin.

- **Nœuds d'administration** : Incluez le service Load Balancer et activez l'accès au Grid Manager ou au Tenant Manager.
- **Nœuds de passerelle** : Incluent le service Load Balancer.

Objectif du groupe HA	Ajoutez les nœuds de ce type au groupe HA
Accès à Grid Manager	• Nœud d'administration principal (**Primary**) • Nœuds d'administration non principaux **Remarque :** Le nœud d'administration principal doit être l'interface principale. Certaines procédures de maintenance ne peuvent être effectuées qu'à partir du nœud d'administration principal.

Objectif du groupe HA	Ajoutez les nœuds de ce type au groupe HA
Accès uniquement à Tenant Manager	• Nœuds d'administration principaux ou non principaux
Accès client S3—Service Load Balancer	• Nœuds d'administration • Nœuds de passerelle
Accès client S3 pour "S3 Select"	• Appareils de services • Nœuds logiciels basés sur VMware **Remarque** : Les groupes HA sont recommandés lors de l'utilisation de S3 Select, mais ne sont pas requis.

Limitations liées à l'utilisation des groupes HA avec Grid Manager ou Tenant Manager

Si un service Grid Manager ou Tenant Manager tombe en panne, le basculement du groupe HA n'est pas déclenché.

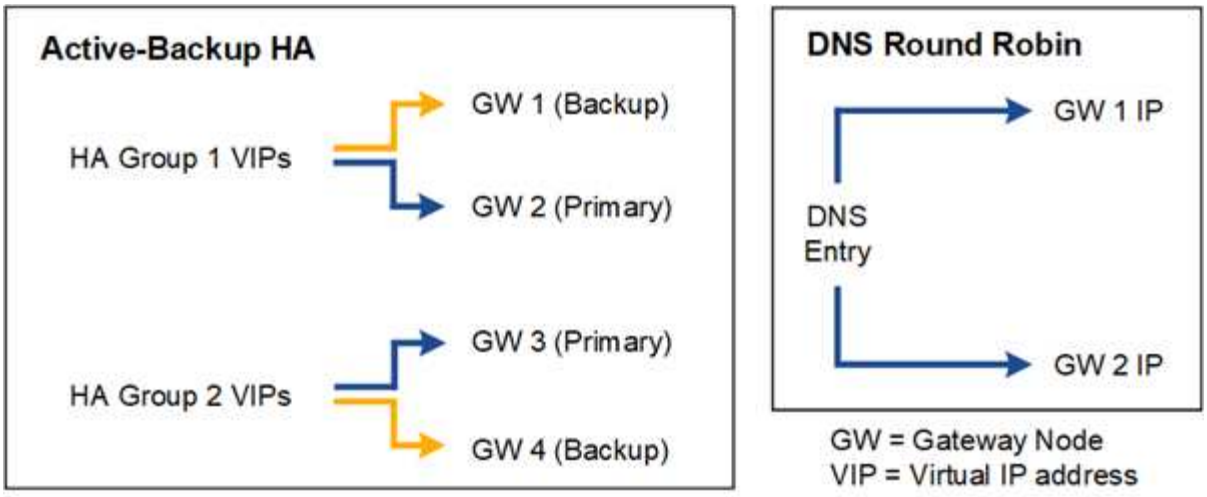
Si vous êtes connecté à Grid Manager ou à Tenant Manager lors d'un basculement, vous êtes déconnecté et devez vous reconnecter pour reprendre votre tâche.

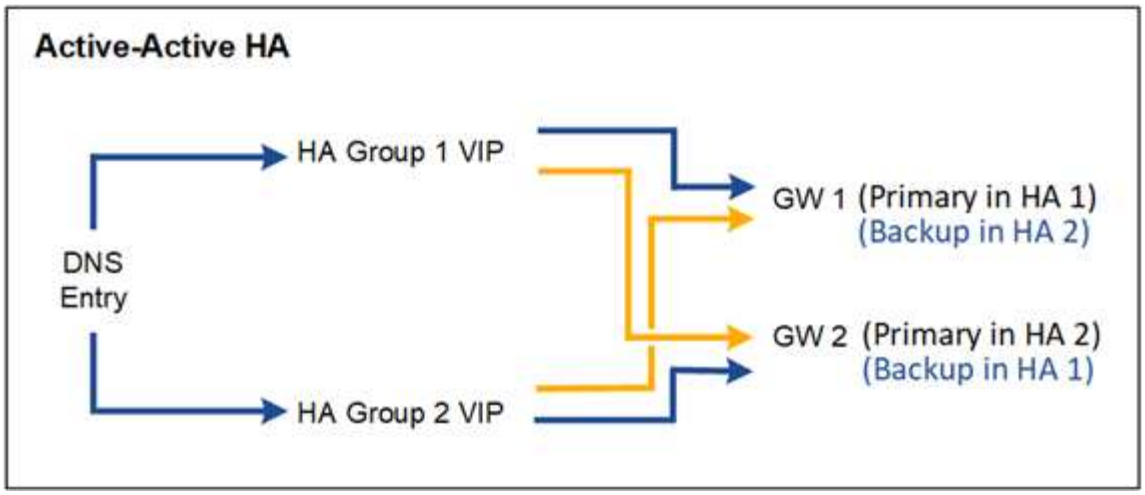
Certaines opérations de maintenance sont impossibles lorsque le nœud d'administration principal est indisponible. En cas de basculement, vous pouvez utiliser le Grid Manager pour surveiller votre système StorageGRID.

Options de configuration pour les groupes à haute disponibilité StorageGRID

Les schémas suivants présentent des exemples de différentes façons dont vous pouvez configurer des groupes à haute disponibilité (HA). Chaque option comporte des avantages et des inconvénients.

Sur les schémas, le bleu indique l'interface principale du groupe HA et le jaune indique l'interface de secours du groupe HA.





Le tableau récapitule les avantages de chaque configuration HA présentée dans le schéma.

Configuration	Avantages	Inconvénients
HA actif-sauvegarde	• Géré par StorageGRID sans aucune dépendance externe. • Basculement rapide.	• Dans un groupe HA, un seul nœud est actif. Au moins un nœud par groupe HA est inactif.
DNS Round Robin	• Augmentation du débit global. • Aucun hôte inactif.	• Basculement lent, pouvant dépendre du comportement du client. • Nécessite une configuration matérielle en dehors de StorageGRID. • Nécessite une vérification de l'état.
HA actif-actif	• Le trafic est réparti sur plusieurs groupes HA. • Débit agrégé élevé qui évolue avec le nombre de groupes HA. • Basculement rapide.	• Plus complexe à configurer. • Nécessite une configuration matérielle en dehors de StorageGRID. • Nécessite une vérification de l'état.

Configurez des groupes de haute disponibilité dans StorageGRID

Vous pouvez configurer des groupes à haute disponibilité (HA) pour fournir un accès hautement disponible aux services sur les nœuds d'administration ou les nœuds de passerelle.

Un système StorageGRID peut comporter un maximum de 255 groupes HA.

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 root".
- Si vous prévoyez d'utiliser une interface VLAN dans un groupe HA, vous avez créé l'interface VLAN. Voir "Configurer les interfaces VLAN".
- Si vous prévoyez d'utiliser une interface d'accès pour un nœud dans un groupe HA, vous avez créé l'interface :
  - **Linux (avant l'installation du nœud)** : "Créer des fichiers de configuration de nœud"
  - **Linux (après installation du nœud)** : "Ajouter des interfaces de tronc ou d'accès à un nœud"
  - **VMware (après l'installation du nœud)** : "Ajouter des interfaces de tronc ou d'accès à un nœud"

« Linux » désigne un déploiement RHEL, Ubuntu ou Debian. Pour obtenir la liste des versions prises en charge, consultez le "Outil de matrice d'interopérabilité (IMT) NetApp".

Créer un groupe à haute disponibilité

Lorsque vous créez un groupe à haute disponibilité, vous sélectionnez une ou plusieurs interfaces et les organisez par ordre de priorité. Ensuite, vous attribuez une ou plusieurs adresses VIP au groupe.

Pour être incluse dans un groupe HA, une interface doit être dédiée à un nœud Gateway ou à un nœud Admin. Un groupe HA ne peut utiliser qu'une seule interface pour un nœud donné ; cependant, d'autres interfaces du même nœud peuvent être utilisées dans d'autres groupes HA.

Accédez à l'assistant

Étapes

1. Sélectionnez **Configuration** > **Réseau** > **Groupes de haute disponibilité**.
2. Sélectionnez **Create**.

Saisissez les détails du groupe HA

Étapes

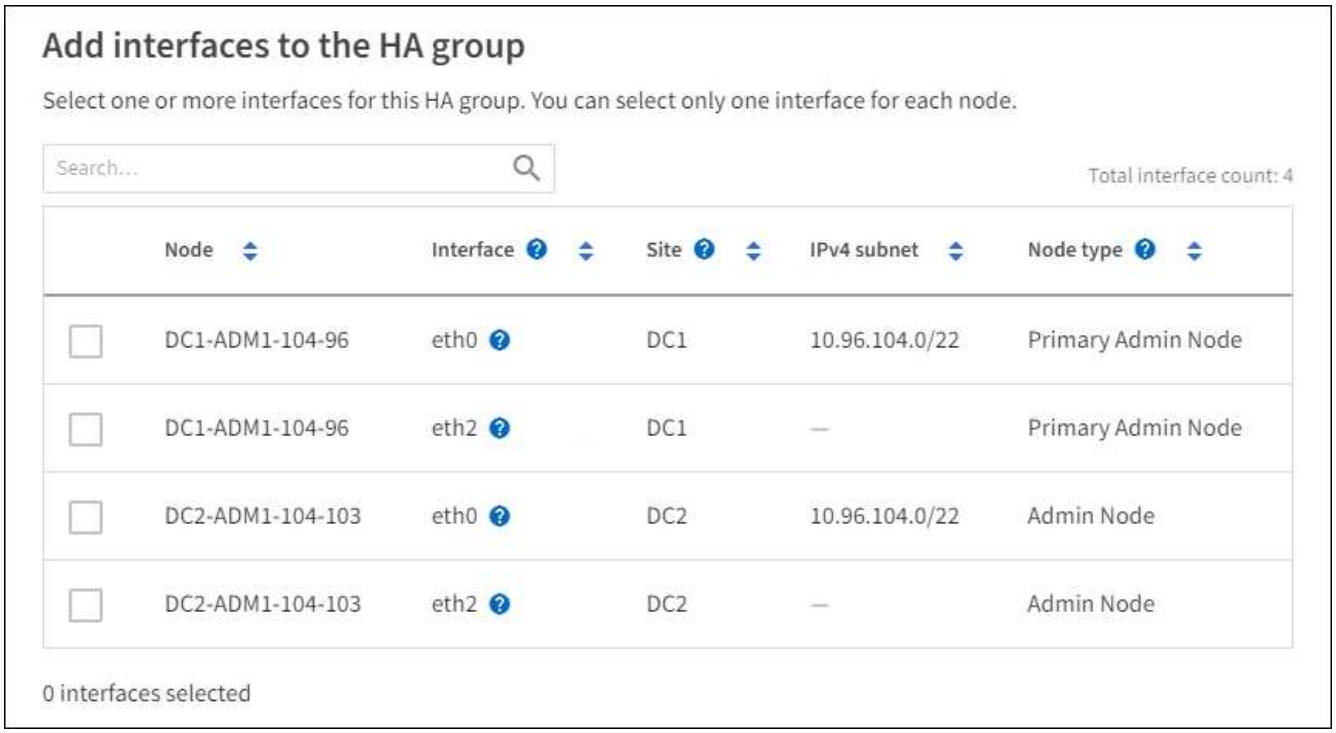
1. Donnez un nom unique au groupe HA.
2. Vous pouvez éventuellement saisir une description pour le groupe HA.
3. Sélectionnez **Continue**.

Ajouter des interfaces au groupe HA

Étapes

1. Sélectionnez une ou plusieurs interfaces à ajouter à ce groupe HA.

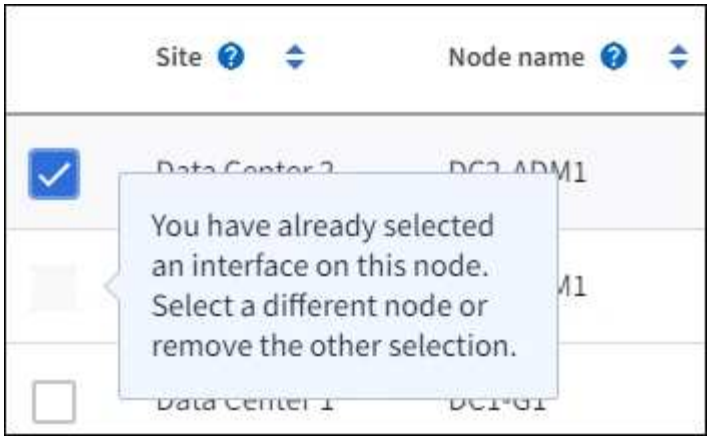
Utilisez les en-têtes de colonnes pour trier les lignes ou saisissez un terme de recherche pour localiser plus rapidement les interfaces.



Après avoir créé une interface VLAN, attendez jusqu'à 5 minutes pour que la nouvelle interface apparaisse dans le tableau.

Recommandations pour la sélection des interfaces

- Vous devez sélectionner au moins une interface.
- Vous ne pouvez sélectionner qu'une seule interface pour un nœud.
- Si le groupe HA est destiné à la protection HA des services du nœud d'administration, qui incluent le Grid Manager et le Tenant Manager, sélectionnez uniquement les interfaces sur les nœuds d'administration.
- Si le groupe HA est destiné à la protection HA du trafic client S3, sélectionnez des interfaces sur les nœuds Admin, les nœuds Gateway ou les deux.
- Si vous sélectionnez des interfaces sur différents types de nœuds, une note d'information s'affiche. Il vous est rappelé qu'en cas de basculement, les services fournis par le nœud précédemment actif pourraient ne pas être disponibles sur le nœud nouvellement actif. Par exemple, un nœud Gateway de secours ne peut pas assurer la protection HA des services du nœud Admin. De même, un nœud Admin de secours ne peut pas effectuer toutes les procédures de maintenance que le nœud Admin principal peut fournir.
- Si vous ne pouvez pas sélectionner une interface, sa case à cocher est désactivée. L'infobulle fournit plus d'informations.



- Vous ne pouvez pas sélectionner une 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 **Continue**.

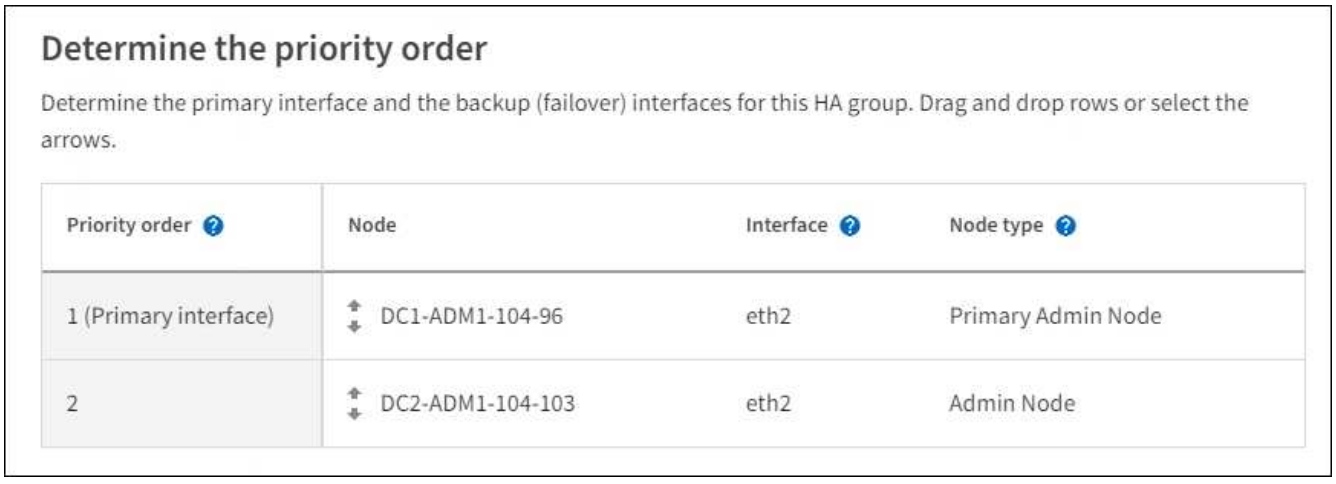
Déterminez l'ordre de priorité

Si le groupe HA comprend plusieurs interfaces, vous pouvez déterminer quelle est l'interface principale et quelles sont les interfaces de secours (basculement). Si l'interface principale tombe en panne, les adresses VIP sont transférées vers l'interface prioritaire la plus élevée disponible. Si cette interface tombe en panne, les adresses VIP sont transférées vers l'interface prioritaire suivante disponible, et ainsi de suite.

Étapes

1. Faites glisser les lignes de la colonne **Ordre de priorité** pour déterminer l'interface principale et les interfaces de secours.

   La première interface de la liste est l'interface principale. L'interface principale est l'interface active sauf en cas de panne.



Si le groupe HA donne accès au Grid Manager, vous devez sélectionner une interface sur le nœud d'administration principal comme interface principale. Certaines opérations de maintenance ne peuvent être effectuées que depuis le nœud d'administration principal.

2. Sélectionnez **Continue**.

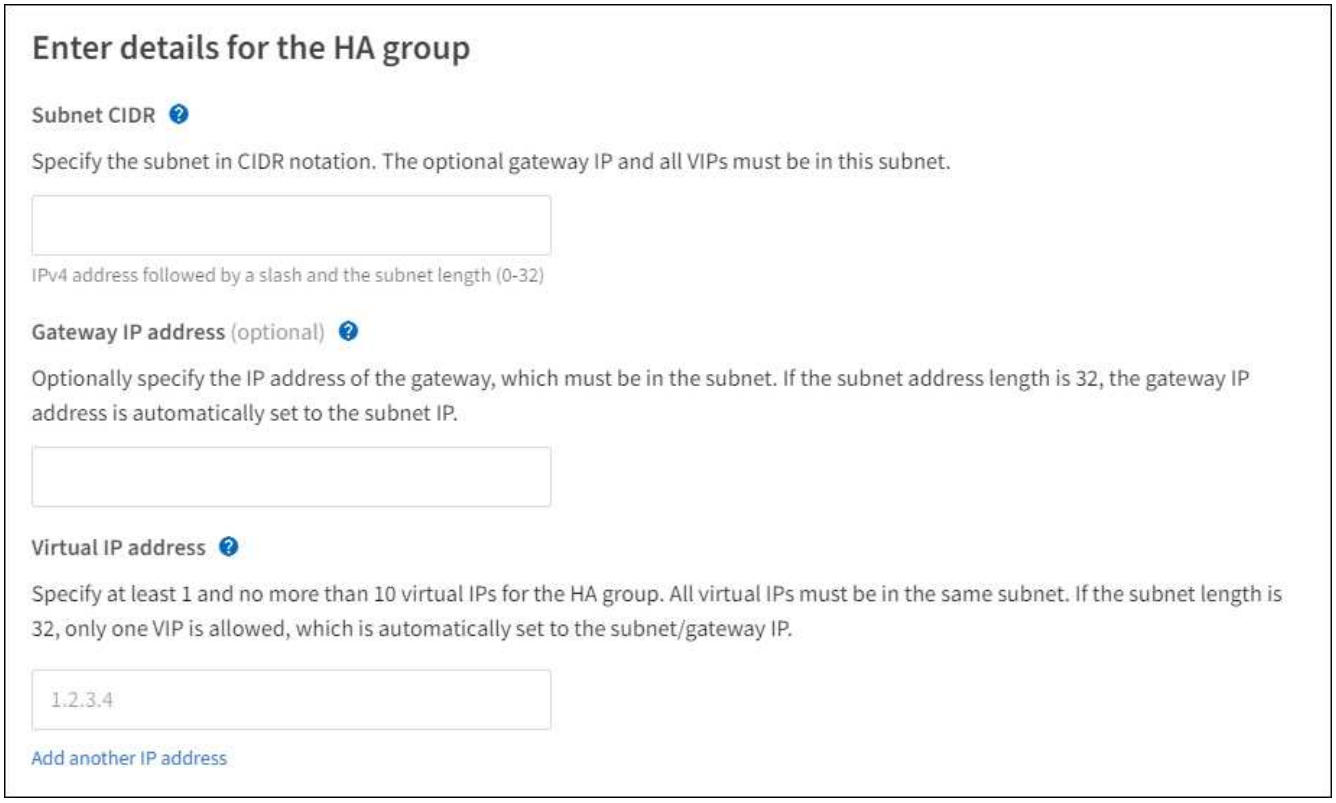
Saisissez les adresses IP

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).

   L'adresse réseau ne doit comporter aucun bit d'hôte activé. 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 des clients administrateurs ou locataires S3 doivent accéder à ces adresses VIP depuis un sous-réseau différent, indiquez l'adresse IP de la passerelle. L'adresse de la passerelle doit se trouver dans le même sous-réseau VIP.

   Les utilisateurs clients et administrateurs utiliseront cette passerelle pour accéder aux adresses IP virtuelles.

3. Saisissez au moins une et au plus dix adresses VIP pour l'interface active du groupe HA. Toutes les adresses VIP doivent appartenir au sous-réseau VIP et seront toutes actives simultanément sur l'interface active.

   Vous devez fournir au moins une adresse IPv4. Vous pouvez également spécifier des adresses IPv4 et IPv6 supplémentaires.

4. Sélectionnez **Créer un groupe HA** et sélectionnez **Terminer**.

   Le groupe HA est créé et vous pouvez désormais utiliser les adresses IP virtuelles configurées.

Prochaines étapes

Si vous utilisez ce groupe HA pour l'équilibrage de charge, créez un point de terminaison d'équilibrage de charge afin de déterminer le port et le protocole réseau et d'y associer les certificats requis. Voir "Configurer les points de terminaison de l'équilibreur de charge".

Modifier un groupe à haute disponibilité

Vous pouvez modifier un groupe à haute disponibilité (HA) pour changer son nom et sa description, ajouter ou supprimer des interfaces, modifier l'ordre de priorité ou ajouter ou mettre à jour des adresses IP virtuelles.

Par exemple, vous pourriez avoir besoin de modifier un groupe HA si vous souhaitez supprimer le nœud associé à une interface sélectionnée lors d'une procédure de mise hors service de site ou de nœud.

Étapes

1. Sélectionnez **Configuration** > **Réseau** > **Groupes de haute disponibilité**.

   La page des groupes de haute disponibilité affiche tous les groupes HA existants.

2. Cochez la case correspondant au groupe HA que vous souhaitez modifier.
3. Procédez comme suit, 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. Mettez à jour les adresses IP virtuelles du groupe HA.
   b. Sélectionnez **Enregistrer**.
   c. Sélectionnez **Terminer**.
5. Si vous avez sélectionné **Modifier le groupe HA** :
   a. Vous pouvez éventuellement mettre à jour le nom ou la description du groupe.
   b. Vous pouvez, si vous le souhaitez, sélectionner ou désélectionner les cases à cocher pour ajouter ou supprimer des interfaces.

      > Si le groupe HA donne accès au Grid Manager, vous devez sélectionner une interface sur le nœud d'administration principal comme interface principale. Certaines procédures de maintenance ne peuvent être effectuées que depuis le nœud d'administration principal.

   c. Vous pouvez également faire glisser les lignes pour modifier l'ordre de priorité de l'interface principale et de toute interface de secours pour ce groupe HA.
   d. Vous pouvez éventuellement mettre à jour les adresses IP virtuelles.
   e. Sélectionnez **Enregistrer** puis sélectionnez **Terminer**.

Supprimer un groupe à haute disponibilité

Vous pouvez supprimer un ou plusieurs groupes à haute disponibilité (HA) à la fois.

Vous ne pouvez pas supprimer un groupe HA s'il est lié à un point de terminaison d'équilibreur de charge. Pour supprimer un groupe HA, vous devez le retirer de tous les points de terminaison d'équilibreur de charge qui l'utilisent.

Pour éviter toute interruption de service, mettez à jour les applications clientes S3 concernées avant de supprimer un groupe HA. Mettez à jour chaque client pour qu'il se connecte à l'aide d'une autre adresse IP, par exemple l'adresse IP virtuelle d'un autre groupe HA ou l'adresse IP qui a été configurée pour une interface lors de l'installation.

Étapes

1. Sélectionnez **Configuration** > **Réseau** > **Groupes de haute disponibilité**.
2. Consultez la colonne **Points de terminaison de l'équilibreur de charge** pour chaque groupe HA que vous souhaitez supprimer. Si des points de terminaison de l'équilibreur de charge sont répertoriés :
   a. Accédez à **Configuration** > **Réseau** > **Points de terminaison de l'équilibreur de charge**.
   b. Cochez la case correspondant au point de terminaison.
   c. Sélectionnez **Actions** > **Modifier le mode de liaison du point de terminaison**.
   d. Mettez à jour le mode de liaison pour supprimer le groupe HA.
   e. Sélectionnez **Save changes**.
3. Si aucun point de terminaison d'équilibrage de charge n'est répertorié, cochez la case pour chaque groupe HA que vous souhaitez supprimer.
4. Sélectionnez **Actions** > **Supprimer le groupe HA**.
5. Vérifiez le message et sélectionnez **Supprimer le groupe HA** pour confirmer votre sélection.

   Tous les groupes HA que vous avez sélectionnés sont supprimés. Une bannière verte de succès apparaît sur la page Groupes de haute disponibilité.

Gérer l'équilibrage de charge

Découvrez l'équilibrage de charge StorageGRID

Vous pouvez utiliser l'équilibrage de charge pour gérer les charges de travail d'ingestion et de récupération des clients S3.

Qu'est-ce que l'équilibrage de charge ?

Lorsqu'une application cliente enregistre ou récupère des données depuis un système StorageGRID, StorageGRID utilise un équilibreur de charge pour gérer la charge de travail d'ingestion et de récupération. L'équilibrage de charge optimise la vitesse et la capacité de connexion en répartissant la charge de travail sur plusieurs nœuds de stockage.

Le service d'équilibrage de charge StorageGRID est installé sur tous les nœuds d'administration et tous les nœuds de passerelle et assure l'équilibrage de charge de couche 7. Il effectue la terminaison TLS (Transport Layer Security) des requêtes client, les inspecte et établit de nouvelles connexions sécurisées avec les nœuds de stockage.

Le service d'équilibrage de charge de chaque nœud fonctionne indépendamment lors de la répartition du trafic client vers les nœuds de stockage. Grâce à un processus de pondération, le service d'équilibrage de charge achemine davantage de requêtes vers les nœuds de stockage disposant d'une plus grande disponibilité de

processeur.

> Bien que le service StorageGRID Load Balancer soit le mécanisme d'équilibrage de charge recommandé, vous pouvez également intégrer un équilibreur de charge tiers. Pour plus d'informations, contactez votre représentant de compte NetApp ou consultez "Utilisez des équilibreurs de charge tiers avec StorageGRID".

De combien de nœuds d'équilibrage de charge avez-vous besoin ?

En bonne pratique, chaque site de votre système StorageGRID devrait comporter au moins deux nœuds avec le service d'équilibrage de charge. Par exemple, un site peut inclure deux nœuds de passerelle ou à la fois un nœud d'administration et un nœud de passerelle. Assurez-vous de disposer d'une infrastructure réseau, matérielle ou de virtualisation adéquate pour chaque nœud d'équilibrage de charge, que vous utilisiez des appliances de services, des nœuds bare metal ou des nœuds basés sur des machines virtuelles (VM).

Qu'est-ce qu'un point de terminaison d'équilibrage de charge ?

Un point de terminaison d'équilibrage de charge définit le port et le protocole réseau (HTTPS ou HTTP) que les requêtes entrantes et sortantes des applications clientes utiliseront pour accéder aux nœuds qui contiennent le service Load Balancer. Ce point de terminaison définit également le type de client (S3), le mode de liaison et, éventuellement, une liste de locataires autorisés ou bloqués.

Pour créer un point de terminaison d'équilibrage de charge, utilisez Grid Manager ou terminez la configuration S3 et les assistants FabricPool :

- "Configurer les points de terminaison de l'équilibreur de charge"
- "Utilisez l'assistant de configuration S3"
- "Utilisez l'assistant de configuration FabricPool"

Considérations relatives à la mise en cache de l'équilibreur de charge

La mise en cache améliore considérablement les performances lorsqu'une charge de travail traite un sous-ensemble de données et accède plusieurs fois aux objets. De plus, la mise en cache permet un accès distant au stockage d'objets sans déploiement complet de la grille. La mise en cache de l'équilibreur de charge est disponible uniquement pour les Gateway Nodes.

Lors de la création des points de terminaison de l'équilibreur de charge :

- N'activez la mise en cache que pour les charges de travail pouvant être mises en cache. Les charges de travail accédant plus fréquemment aux données non mises en cache qu'aux données mises en cache auront des performances inférieures à celles qui n'auraient pas été prises en charge par le cache. Dans certains cas, les charges de travail avec des taux élevés de réécriture et d'éviction peuvent également dépasser l'endurance d'écriture garantie du disque.
- Envisagez d'ajouter des points de terminaison ou des nœuds supplémentaires pour la mise en cache des charges de travail individuelles qui sont de bons candidats pour la mise en cache.
- Utilisez des points de terminaison distincts pour les charges de travail pouvant être mises en cache et celles qui ne le peuvent pas. Cette séparation garantit que les mécanismes de mise en cache sont appliqués correctement et n'interfèrent pas avec le traitement des données non mises en cache.
- Évaluez la pertinence d'une charge de travail pouvant être mise en cache en la dirigeant vers le point de terminaison compatible avec la mise en cache. Surveillez et vérifiez le taux d'accès au cache afin de déterminer si la charge de travail est adaptée à la mise en cache. Cette évaluation contribue à optimiser les performances et à garantir une utilisation efficace des ressources du cache.

- "Examiner les journaux d'audit" pour déterminer si une charge de travail existante serait un bon candidat pour la mise en cache. Pour une période donnée, déterminez quel pourcentage des requêtes GET concerne des objets uniques. Pour être adaptée à la mise en cache, cette valeur doit être inférieure à 50 %.

Exemples de charges de travail qui pourraient être de bons candidats pour la mise en cache

- lacs de données
- Calcul haute performance (HPC)
- Entraînement IA/ML
- Réseaux de distribution de contenu (CDN)
- gestion des ressources média
- Production vidéo

- Plusieurs versions d'un même objet peuvent être mises en cache.
- Les opérations de lecture de plage sont prises en charge.

Exemples de charges de travail qui ne sont pas de bons candidats pour la mise en cache

- FabricPool
- Applications de sauvegarde
- hiérarchisation du stockage

Si un contenu quelconque à servir par le cache nécessite un chiffrement au repos, "activer le chiffrement du nœud ou du disque" sur le nœud de cache.

Types d'objets et de requêtes qui ne seront pas mis en cache

- Le `response-content-encoding` paramètre de requête
- Le `partNumber` paramètre de requête
- En-têtes conditionnels
  - `If-Match`
  - `If-Modified-Since`
  - `If-None-Match`
  - `If-Unmodified-Since`
- Les requêtes qui ont été chiffrées au repos avec l'un des éléments suivants :
  - SSE (chiffrement côté serveur avec des clés gérées par StorageGRID)
  - SSE-C (chiffrement côté serveur avec clés fournies par le client)
  - Chiffrement des objets stockés

Toute requête qui n'est pas mise en cache est transmise à un LDR en amont comme si le cache n'était pas activé.

Informations connexes

- "Dépannez la mise en cache de l'équilibreur de charge"
- Pour plus d'informations sur la mise en cache de l'équilibreur de charge, contactez le support technique.

Considérations relatives au port

Le port d'un point de terminaison d'équilibrage de charge est par défaut 10433 pour le premier point de terminaison que vous créez, mais vous pouvez spécifier n'importe quel port externe inutilisé entre 1 et 65535. Si vous utilisez le port 80 ou 443, le point de terminaison utilisera le service Load Balancer uniquement sur les Gateway Nodes. Ces ports sont réservés sur les Admin Nodes. Si vous utilisez le même port pour plus d'un point de terminaison, vous devez spécifier un mode de liaison différent pour chaque point de terminaison.

Les ports utilisés par d'autres services de grid ne sont pas autorisés. Voir "Ports internes de StorageGRID".

Considérations relatives au protocole réseau

Dans la plupart des cas, les connexions entre les applications clientes et StorageGRID doivent utiliser le chiffrement Transport Layer Security (TLS). La connexion à StorageGRID sans chiffrement TLS est possible, mais déconseillée, notamment en environnement de production. Lorsque vous sélectionnez le protocole réseau pour le point de terminaison de l'équilibreur de charge StorageGRID, vous devez choisir **HTTPS**.

Considérations relatives aux certificats des points de terminaison de l'équilibreur de charge

Si vous sélectionnez **HTTPS** comme protocole réseau pour le point de terminaison de l'équilibreur de charge, vous devez fournir un certificat de sécurité. Vous pouvez utiliser l'une de ces trois options lors de la création du point de terminaison de l'équilibreur de charge :

- **Téléchargez un certificat signé (recommandé)**. Ce certificat peut être signé par une autorité de certification (CA) publique ou privée. Utiliser un certificat de serveur CA public pour sécuriser la connexion est la bonne pratique. Contrairement aux certificats générés, les certificats signés par une CA peuvent être renouvelés sans interruption, ce qui permet d'éviter les problèmes d'expiration.

  Vous devez obtenir les fichiers suivants avant de créer le point de terminaison de l'équilibreur de charge :

  - Le fichier de certificat serveur personnalisé.
  - Le fichier de clé privée du certificat serveur personnalisé.
  - En option, un ensemble de certificats CA provenant de chaque autorité de certification émettrice intermédiaire.
- **Générez un certificat auto-signé**.
- **Utilisez le certificat S3 global StorageGRID**. Vous devez importer ou générer une version personnalisée de ce certificat avant de pouvoir le sélectionner pour le point de terminaison de l'équilibreur de charge. Voir "Configurer les certificats de l'API S3".

De quelles valeurs avez-vous besoin ?

Pour créer le certificat, vous devez connaître tous les noms de domaine et adresses IP que les applications clientes S3 utiliseront pour accéder au point de terminaison.

L'entrée **Subject DN** (Nom distinctif) du certificat doit inclure le nom de domaine complet que l'application cliente utilisera pour StorageGRID. Par exemple :

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

Conformément aux exigences, le certificat peut utiliser des caractères génériques pour représenter les noms de domaine complets de tous les nœuds d'administration et les 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 **Nom alternatif** pour chaque "nom de domaine du terminal S3" que vous avez configuré, y compris tout nom générique. Par exemple :

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

> ⓘ Si vous utilisez des caractères génériques pour les noms de domaine, consultez la "Recommandations pour le renforcement de la sécurité des certificats de serveur".

Vous devez également définir une entrée DNS pour chaque nom figurant dans le certificat de sécurité.

Comment gérer les certificats qui expirent ?

> ⚠ 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 de certificat, suivez ces bonnes pratiques :

- Surveillez attentivement toutes les alertes signalant l'approche des dates d'expiration des certificats, telles que les alertes **Expiration of load balancer endpoint certificate** et **Expiration of global server certificate for S3 API**.
- Veillez à toujours synchroniser les versions du certificat de StorageGRID et de l'application S3. Si vous remplacez ou renouvelez le certificat utilisé pour un point de terminaison d'équilibrage de charge, vous devez également remplacer ou renouveler le certificat équivalent utilisé par l'application S3.
- Utilisez un certificat signé par une autorité de certification (CA) publique. Si vous utilisez un certificat signé par une CA, vous pouvez remplacer les certificats arrivant bientôt à expiration sans interruption de service.
- Si vous avez généré un certificat StorageGRID auto-signé et que ce certificat est sur le point d'expirer, vous devez le remplacer manuellement à la fois dans StorageGRID et dans l'application S3 avant l'expiration du certificat existant.

Considérations relatives au mode de liaison

Le mode de liaison permet de contrôler les adresses IP qui peuvent être utilisées pour accéder à un point de terminaison d'équilibreur de charge. Si un point de terminaison utilise un mode de liaison, les applications clientes ne peuvent accéder au point de terminaison que si elles utilisent une adresse IP autorisée ou son domaine complet (FQDN) correspondant. Les applications clientes utilisant toute autre adresse IP ou tout autre FQDN ne peuvent pas accéder au point de terminaison.

Vous pouvez spécifier l'un des modes de liaison suivants :

- **Global** (par défaut) : les applications clientes peuvent accéder au point de terminaison via l'adresse IP de n'importe quel nœud de passerelle ou nœud d'administration, l'adresse IP virtuelle (VIP) de n'importe quel groupe HA sur n'importe quel réseau, ou un domaine complet (FQDN) correspondant. Utilisez ce paramètre sauf si vous devez restreindre l'accessibilité d'un point de terminaison.
- **Adresses IP virtuelles des groupes HA**. Les applications clientes doivent utiliser une adresse IP virtuelle (ou le nom de domaine complet correspondant) d'un groupe HA.
- **Interfaces de nœud**. Les clients doivent utiliser les adresses IP (ou les domaines complets correspondants) des interfaces de nœud sélectionnées.
- **Type de nœud**. En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser soit l'adresse IP (ou le domaine complet correspondant) de n'importe quel nœud d'administration, soit l'adresse IP (ou le domaine complet correspondant) de n'importe quel nœud de passerelle.

Considérations relatives à l'accès des locataires

Le contrôle d'accès des locataires est une fonctionnalité de sécurité optionnelle qui vous permet de contrôler quels comptes locataires StorageGRID peuvent utiliser un point de terminaison d'équilibrage de charge pour accéder à leurs compartiments. Vous pouvez autoriser tous les locataires à accéder à un point de terminaison (par défaut), ou spécifier une liste de locataires autorisés ou bloqués pour chaque point de terminaison.

Vous pouvez utiliser cette fonctionnalité pour offrir une meilleure isolation de sécurité entre les locataires et leurs terminaux. Par exemple, vous pouvez utiliser cette fonctionnalité pour garantir que les documents ultra-confidentiels ou hautement classifiés appartenant à un locataire restent totalement inaccessibles aux autres locataires.

> Aux fins du contrôle d'accès, le locataire est déterminé à partir des clés d'accès utilisées dans la requête du client ; si aucune clé d'accès n'est fournie dans le cadre de la requête (comme dans le cas d'accès anonyme), le propriétaire du compartiment est utilisé pour déterminer le locataire.

Exemple d'accès locataire

Pour comprendre le fonctionnement de cette fonction de sécurité, considérez l'exemple suivant :

1. Vous avez créé deux points de terminaison d'équilibrage de charge, comme suit :
   - Point de terminaison **public** : utilise le port 10443 et permet l'accès à tous les tenants.
   - Point d'accès **Top secret** : utilise le port 10444 et autorise l'accès uniquement au locataire **Top secret**. Tous les autres locataires sont bloqués de l'accès à ce point d'accès.
2. Le `top-secret.pdf` se trouve dans un compartiment appartenant au locataire **Top secret**.

Pour accéder à `top-secret.pdf`, un utilisateur du locataire **Top secret** peut envoyer une requête GET à `https://w.x.y.z:10444/top-secret.pdf`. Ce locataire étant autorisé à utiliser le point de terminaison 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 immédiatement un message Accès refusé. L'accès est refusé même si les identifiants et la signature sont valides.

disponibilité du processeur

Le service d'équilibrage de charge sur chaque nœud d'administration et de passerelle fonctionne indépendamment lors de l'acheminement du trafic S3 vers les nœuds de stockage. Grâce à un processus de pondération, le service d'équilibrage de charge dirige davantage de requêtes vers les nœuds de stockage disposant d'une plus grande disponibilité CPU. Les informations sur la charge CPU des nœuds sont mises à jour toutes les quelques minutes, mais la pondération peut être actualisée plus fréquemment. Tous les nœuds

de stockage se voient attribuer une valeur de poids minimale, même si un nœud signale 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 de Load Balancer.

Configurer les points de terminaison de l'équilibreur de charge StorageGRID

Les points de terminaison de l'équilibreur de charge déterminent les ports et les protocoles réseau que les clients S3 peuvent utiliser pour se connecter à l'équilibreur de charge StorageGRID sur les nœuds Gateway et Admin. Vous pouvez également utiliser ces points de terminaison pour accéder au Grid Manager, au Tenant Manager ou aux deux.

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 root".
- 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 point de terminaison de l'équilibreur de charge, vous avez "suppression du remappage de port".
- Vous avez créé les groupes de haute disponibilité (HA) que vous prévoyez d'utiliser. Les groupes HA sont recommandés, mais non obligatoires. Voir "Gérer les groupes à haute disponibilité".
- Si le point de terminaison de l'équilibreur de charge sera utilisé par "Locataires S3 pour S3 Select", il ne doit pas utiliser les adresses IP ni les FQDN de nœuds bare-metal. Seuls les appliances de services et les nœuds logiciels basés sur VMware sont autorisés pour les points de terminaison de l'équilibreur de charge utilisés pour S3 Select.
- Vous avez configuré les interfaces VLAN que vous prévoyez d'utiliser. Voir "Configurer les interfaces VLAN".
- Si vous créez un point de terminaison HTTPS (recommandé), vous disposez des informations pour le certificat du serveur.

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

  - Pour télécharger un certificat, vous avez besoin du certificat serveur, de la clé privée du certificat et, éventuellement, d'un bundle d'autorité de certification (CA bundle).
  - Pour générer un certificat, vous avez besoin de tous les noms de domaine et adresses IP que les clients S3 utiliseront pour accéder au point de terminaison. Vous devez également connaître le sujet (Distinguished Name).
  - Si vous souhaitez utiliser le certificat de l'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 de l'API S3".

Créer un point de terminaison d'équilibrage de charge

Chaque point de terminaison d'équilibrage de charge client S3 spécifie un port, un type de client (S3) et un protocole réseau (HTTP ou HTTPS). Les points de terminaison d'équilibrage de charge de l'interface de gestion spécifient un port, un type d'interface et un réseau Client Network non approuvé.

Accédez à l’assistant

Étapes

1. Sélectionnez **Configuration** > **Réseau** > **Points de terminaison de l’équilibreur de charge**.
2. Pour créer un point de terminaison pour un client S3, sélectionnez l’onglet **S3 client**.
3. Pour créer un point de terminaison permettant d’accéder au Grid Manager, au Tenant Manager ou aux deux, sélectionnez l’onglet **Management interface**.
4. Sélectionnez **Create**.

Saisissez les détails du point de terminaison

Étapes

1. Sélectionnez les instructions appropriées pour saisir les détails du type de point de terminaison que vous souhaitez créer.

Client S3

Champ	Description
Nom	Un nom descriptif pour le point de terminaison, qui apparaîtra dans le tableau de la page des points de terminaison de l'équilibreur de charge.
Port	Le port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est défini par défaut sur 10433 pour le premier point de terminaison que vous créez, mais vous pouvez saisir n'importe quel port externe inutilisé compris entre 1 et 65535. Si vous saisissez **80** ou **8443**, le point de terminaison est configuré uniquement sur les nœuds de passerelle, sauf si vous avez libéré le port 8443. Vous pouvez alors utiliser le port 8443 comme point de terminaison S3, et le port sera configuré à la fois sur les nœuds de passerelle et d'administration.
Type de client	Doit être **S3**.
Protocole réseau	Le protocole réseau que les clients utiliseront lorsqu'ils se connecteront à ce point de terminaison. • Sélectionnez **HTTPS** pour une communication sécurisée et chiffrée TLS (recommandé). Vous devez associer un certificat de sécurité avant de pouvoir enregistrer le point de terminaison. • Sélectionnez **HTTP** pour une communication moins sécurisée et non chiffrée. Utilisez HTTP uniquement pour une grille hors production.
Activer la mise en cache	Activer ou désactiver "mise en cache sur les nœuds de passerelle" pour ce point de terminaison d'équilibrage de charge. En cas de problème de mise en cache, veuillez vous référer à "Dépannez la mise en cache de l'équilibreur de charge".

Interface de gestion

Champ	Description
Nom	Un nom descriptif pour le point de terminaison, qui apparaîtra dans le tableau de la page des points de terminaison de l'équilibreur de charge.

Champ	Description
Port	Le port StorageGRID que vous souhaitez utiliser pour accéder au Grid Manager, au Tenant Manager ou aux deux. • Gestionnaire de grille : **8443** • Gestionnaire de locataires : **9443** • Gestionnaire de grille et gestionnaire de locataires : **443** **Remarque** : Vous pouvez utiliser ces ports prédéfinis ou d'autres ports disponibles.
Type d'interface	Sélectionnez le bouton radio pour l'interface StorageGRID à laquelle vous accéderez à l'aide de ce point de terminaison.
Réseau de clients non fiables	Sélectionnez **Oui** si ce point de terminaison doit être accessible aux réseaux clients non approuvés. Sinon, sélectionnez **Non**. Lorsque vous sélectionnez **Oui**, le port est ouvert sur tous les réseaux clients non approuvés. **Remarque** : Vous ne pouvez configurer un port pour qu'il soit ouvert ou fermé aux réseaux clients non approuvés que lors de la création du point de terminaison de l'équilibreur de charge.

1. Sélectionnez **Continue**.

Sélectionnez un mode de liaison

Étapes

1. Sélectionnez un mode de liaison pour le point de terminaison afin de contrôler la manière dont le point de terminaison est accessible en utilisant n'importe quelle adresse IP ou en utilisant des adresses IP et des interfaces réseau spécifiques.

   Certains modes de liaison sont disponibles pour les points de terminaison clients ou les points de terminaison d'interface de gestion. Tous les modes pour les deux types de points de terminaison sont répertoriés ici.

Mode	Description
Global (par défaut pour les points de terminaison clients)	Les clients peuvent accéder au point de terminaison en utilisant l'adresse IP de n'importe quel Gateway Node ou Admin Node, l'adresse IP virtuelle (VIP) de n'importe quel groupe HA sur n'importe quel réseau, ou un FQDN correspondant. Utilisez le paramètre **Global** sauf si vous devez restreindre l'accessibilité de ce point de terminaison.

Mode	Description
Adresses IP virtuelles des groupes HA	Les clients doivent utiliser une adresse IP virtuelle (ou un nom de domaine complet correspondant) d'un groupe HA pour accéder à ce point de terminaison. Les points de terminaison dotés de ce mode de liaison peuvent tous utiliser le même numéro de port, à condition que les groupes HA que vous sélectionnez pour les points de terminaison ne se chevauchent pas.
Interfaces de nœud	Les clients doivent utiliser les adresses IP (ou les noms de domaine complets correspondants) des interfaces de nœud sélectionnées pour accéder à ce point de terminaison.
Type de nœud (points de terminaison clients uniquement)	En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel Admin Node, soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel Gateway Node pour accéder à ce point de terminaison.
Tous les nœuds d'administration (par défaut pour les points de terminaison de l'interface de gestion)	Les clients doivent utiliser l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel nœud d'administration pour accéder à ce point de terminaison.

Si plusieurs points de terminaison utilisent le même port, StorageGRID utilise cet ordre de priorité pour décider quel point de terminaison utiliser : **Virtual IPs of HA groups** > **Interfaces de nœud** > **Type de nœud** > **Global**.

Si vous créez des points de terminaison d'interface de gestion, seuls les nœuds d'administration sont autorisés.

2. Si vous avez sélectionné **Virtual IPs of HA groups**, sélectionnez un ou plusieurs groupes HA.

   Si vous créez des points de terminaison d'interface de gestion, sélectionnez les VIP associés uniquement aux Admin Nodes.

3. Si vous avez sélectionné **Interfaces de nœud**, sélectionnez une ou plusieurs interfaces de nœud pour chaque nœud d'administration ou nœud de passerelle que vous souhaitez associer à ce point de terminaison.
4. Si vous avez sélectionné **Type de nœud**, sélectionnez soit Admin Nodes, qui comprend à la fois le primary Admin Node et tous les non-primary Admin Nodes, soit Gateway Nodes.

Contrôler l'accès des locataires

> Un point de terminaison d'interface de gestion ne peut contrôler l'accès des locataires que lorsque le point de terminaison possède le type d'interface de Tenant Manager.

Étapes

1. Pour l'étape **Accès locataire**, sélectionnez l'une des options suivantes :

Champ	Description
Autoriser tous les locataires (par défaut)	Tous les comptes locataires peuvent utiliser ce point de terminaison pour accéder à leurs compartiments. Vous devez sélectionner cette option si vous n'avez pas encore créé de comptes locataires. Après avoir ajouté des comptes locataires, vous pouvez modifier le point de terminaison de l'équilibreur de charge pour autoriser ou bloquer des comptes spécifiques.
Autoriser les locataires sélectionnés	Seuls les comptes locataires sélectionnés peuvent utiliser ce point de terminaison pour accéder à leurs compartiments.
Bloquer les locataires sélectionnés	Les comptes locataires sélectionnés ne peuvent pas utiliser ce point de terminaison pour accéder à leurs compartiments. Tous les autres locataires peuvent utiliser ce point de terminaison.

2. Si vous créez un point de terminaison **HTTP**, vous n'avez pas besoin d'associer un certificat. Sélectionnez **Créer** pour ajouter le nouveau point de terminaison d'équilibrage de charge. Ensuite, accédez à Après avoir terminé. Sinon, sélectionnez **Continuer** pour associer le certificat.

Joindre le certificat

Étapes

1. Si vous créez un point de terminaison **HTTPS**, sélectionnez le type de certificat de sécurité que vous souhaitez associer au point de terminaison.

   Le certificat sécurise les connexions entre les clients S3 et le service Load Balancer sur le nœud d'administration ou les nœuds de passerelle.

   - **Téléverser un certificat**. Sélectionnez cette option si vous avez des certificats personnalisés à téléverser.
   - **Générer un certificat**. Sélectionnez cette option si vous disposez des informations nécessaires pour générer un certificat personnalisé.
   - **Utiliser le certificat StorageGRID S3**. Sélectionnez cette option si vous souhaitez utiliser le certificat global de l'API S3, qui peut également être utilisé pour les connexions directes aux nœuds de stockage.

     Vous ne pouvez pas sélectionner cette option à moins d'avoir remplacé le certificat API S3 par défaut, qui est signé par l'AC du grid, par un certificat personnalisé signé par une autorité de certification externe. Voir "Configurer les certificats de l'API S3".

   - **Utiliser le certificat d'interface de gestion**. Sélectionnez cette option si vous souhaitez utiliser le certificat d'interface de gestion global, qui peut également être utilisé pour les connexions directes aux nœuds d'administration.
2. Si vous n'utilisez pas le certificat S3 StorageGRID, téléchargez-le ou générez-le.

Télécharger le certificat

a. Sélectionnez **Téléverser le certificat**.

b. Téléversez les fichiers de certificat serveur requis :

- **Certificat serveur** : Le fichier de certificat serveur personnalisé au format PEM.
- **Clé privée du certificat** : Le fichier de clé privée du certificat de serveur personnalisé (`.key`).

> Les clés privées EC doivent comporter au moins 224 bits. Les clés privées RSA doivent comporter au moins 2048 bits.

- **CA bundle** : Fichier optionnel unique contenant les certificats de chaque autorité de certification (CA) intermédiaire. Le fichier doit contenir chacun des fichiers de certificat CA encodés en 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 importé. Si vous avez importé un ensemble CA optionnel, chaque certificat s'affiche dans son propre onglet.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat ou sélectionnez **Télécharger le bundle CA** pour enregistrer le bundle de certificats.

  Spécifiez le nom du fichier de certificat et son emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

  Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier le certificat PEM** ou **Copier le bundle CA PEM** pour copier le contenu du certificat afin de le coller ailleurs.

d. Sélectionnez **Créer**. + Le point de terminaison de l'équilibreur de charge est créé. Le certificat personnalisé est utilisé pour toutes les nouvelles connexions ultérieures entre les clients S3 ou l'interface de gestion et le point de terminaison.

Générer un certificat

a. Sélectionnez **Générer un certificat**.

b. Spécifiez les informations du certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine complet à inclure dans le certificat. Utilisez un astérisque (*) comme caractère générique pour représenter plusieurs noms de domaine.
IP	Une ou plusieurs adresses IP à inclure dans le certificat.
Sujet (facultatif)	Sujet X.509 ou nom unique (DN) du propriétaire du certificat. Si aucune valeur n'est saisie dans ce champ, le certificat généré utilise le premier nom de domaine ou la première adresse IP comme nom commun (CN) du sujet.

Champ	Description
Jours valides	Nombre de jours après la création du certificat avant son expiration.
Ajouter des extensions d'utilisation de clé	Si cette option est sélectionnée (par défaut et recommandée), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré. Ces extensions définissent la finalité de la clé contenue dans le certificat. **Remarque** : 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 **Générer**.

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 son emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

  Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.

e. Sélectionnez **Create**.

Le point de terminaison de l'équilibreur de charge est créé. Le certificat personnalisé est utilisé pour toutes les nouvelles connexions ultérieures entre les clients S3 ou l'interface de gestion et ce point de terminaison.

Après avoir terminé

Étapes

1. Si vous utilisez un DNS, assurez-vous que celui-ci inclut un enregistrement permettant d'associer le nom de domaine complet (FQDN) de StorageGRID à chaque adresse IP que les clients utiliseront pour établir des connexions.

   L'adresse IP que vous saisissez dans l'enregistrement DNS dépend du fait que vous utilisiez ou non un groupe HA de nœuds d'équilibrage de charge :

   - Si vous avez configuré un groupe HA, les clients se connecteront aux adresses IP virtuelles de ce groupe HA.
   - Si vous n'utilisez pas de groupe HA, les clients se connecteront au service d'équilibrage de charge StorageGRID en utilisant l'adresse IP d'un nœud de passerelle ou d'un nœud d'administration.

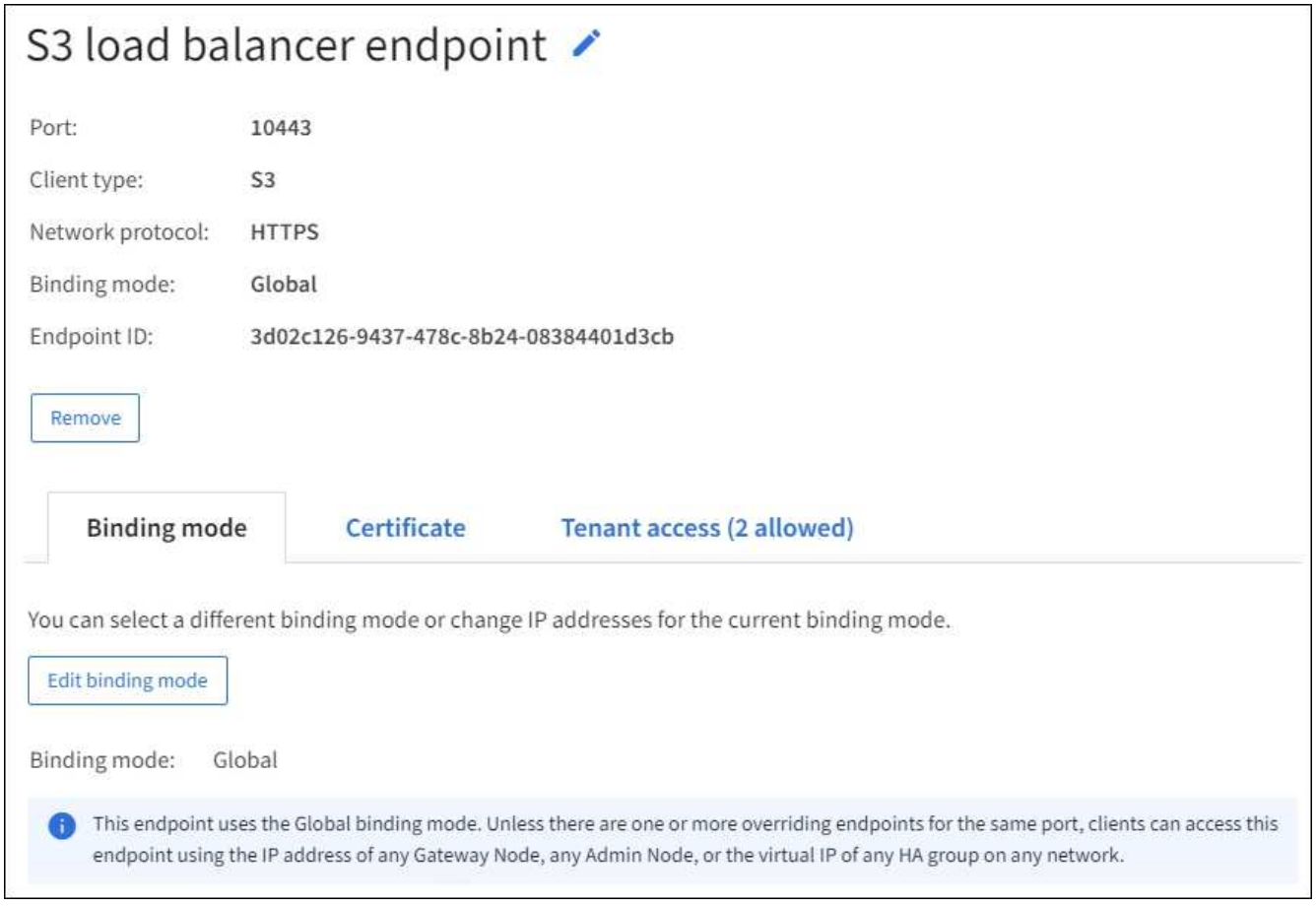
   Vous devez également vous assurer que l'enregistrement DNS référence tous les noms de domaine de point de terminaison requis, y compris les noms génériques.

2. Fournissez aux clients S3 les informations nécessaires pour se connecter au point de terminaison :
    - Numéro de port
    - nom de domaine complet ou adresse IP
    - Tous les détails de certificat requis

Afficher et modifier les points de terminaison de l'équilibreur de charge

Vous pouvez consulter les détails des points de terminaison d'équilibrage de charge existants, y compris les métadonnées du certificat d'un point de terminaison sécurisé. Vous pouvez modifier certains paramètres d'un point de terminaison.

- Pour consulter les informations de base de tous les points de terminaison de l'équilibreur de charge, consultez les tableaux de la page Points de terminaison de l'équilibreur de charge.
- Pour afficher tous les détails d'un point de terminaison spécifique, y compris les métadonnées du certificat, sélectionnez le nom du point de terminaison dans le tableau. Les informations affichées varient selon le type de point de terminaison et la façon dont il est configuré.



- Pour modifier un point de terminaison, utilisez le menu **Actions** sur la page des points de terminaison de l'équilibreur de charge.

> Si vous perdez l'accès à Grid Manager lors de la modification du port d'un point de terminaison d'interface de gestion, mettez à jour l'URL et le port pour rétablir l'accès.

Après avoir modifié un point de terminaison, vous devrez peut-être attendre jusqu'à 15 minutes pour que vos modifications soient appliquées à tous les nœuds.

Tâche	Menu Actions	Page de détails
Modifier le nom du point de terminaison	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez **Actions** > **Modifier le nom du point de terminaison**. c. Saisissez le nouveau nom. d. Sélectionnez **Enregistrer**.	a. Sélectionnez le nom du point de terminaison pour afficher les détails. b. Sélectionnez l'icône de modification . c. Saisissez le nouveau nom. d. Sélectionnez **Enregistrer**.
Modifier le port du point de terminaison	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez **Actions** > **Modifier le port du point de terminaison** c. Veuillez saisir un numéro de port valide. d. Sélectionnez **Enregistrer**.	*n/a*
Modifier le mode de liaison du point de terminaison	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez **Actions** > **Modifier le mode de liaison du point de terminaison**. c. Mettez à jour le mode de liaison si nécessaire. d. Sélectionnez **Save changes**.	a. Sélectionnez le nom du point de terminaison pour afficher les détails. b. Sélectionnez **Modifier le mode de liaison**. c. Mettez à jour le mode de liaison si nécessaire. d. Sélectionnez **Save changes**.
Modifier le certificat du point de terminaison	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez **Actions** > **Modifier le certificat du point de terminaison**. c. Téléchargez ou générez un nouveau certificat personnalisé ou commencez à utiliser le certificat S3 global, selon les besoins. d. Sélectionnez **Save changes**.	a. Sélectionnez le nom du point de terminaison pour afficher les détails. b. Sélectionnez l'onglet **Certificat**. c. Sélectionnez **Modifier le certificat**. d. Téléchargez ou générez un nouveau certificat personnalisé ou commencez à utiliser le certificat S3 global, selon les besoins. e. Sélectionnez **Save changes**.

Tâche	Menu Actions	Page de détails
Modifier l'accès du locataire	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez **Actions** > **Modifier l'accès du locataire**. c. Choisissez une autre option d'accès, sélectionnez ou supprimez des locataires de la liste, ou faites les deux. d. Sélectionnez **Save changes**.	a. Sélectionnez le nom du point de terminaison pour afficher les détails. b. Sélectionnez l'onglet **Accès locataire**. c. Sélectionnez **Modifier l'accès du locataire**. d. Choisissez une autre option d'accès, sélectionnez ou supprimez des locataires de la liste, ou faites les deux. e. Sélectionnez **Save changes**.

Supprimez les points de terminaison de l'équilibreur de charge

Vous pouvez supprimer un ou plusieurs points de terminaison à l'aide du menu **Actions**, ou vous pouvez supprimer un seul point de terminaison à partir de la page de détails.

> Pour éviter toute interruption de service client, mettez à jour les applications clientes S3 concernées avant de supprimer un point de terminaison d'équilibreur de charge. Mettez à jour chaque client pour qu'il se connecte à l'aide d'un port attribué à un autre point de terminaison d'équilibreur de charge. Veillez également à mettre à jour les informations de certificat requises.

> Si vous perdez l'accès à Grid Manager lors de la suppression d'un point de terminaison d'interface de gestion, mettez à jour l'URL.

- Pour supprimer un ou plusieurs points de terminaison :
  a. Sur la page de l'équilibreur de charge, cochez la case correspondant à chaque point de terminaison que vous souhaitez supprimer.
  b. Sélectionnez **Actions** > **Supprimer**.
  c. Sélectionnez **OK**.
- Pour supprimer un point de terminaison de la page de détails :
  a. Sur la page de l'équilibreur de charge, sélectionnez le nom du point de terminaison.
  b. Sélectionnez **Supprimer** sur la page de détails.
  c. Sélectionnez **OK**.

Configurez les noms de domaine des points de terminaison S3 dans StorageGRID

Pour prendre en charge les requêtes de type hébergement virtuel S3, vous devez utiliser le Grid Manager pour configurer la liste des noms de domaine des points de terminaison S3 auxquels les clients S3 se connectent.

> L'utilisation d'une adresse IP comme nom de domaine d'endpoint n'est pas prise en charge. Les prochaines versions 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'aucune mise à niveau de la grille n'est en cours.

> Ne modifiez pas la configuration du nom de domaine pendant une mise à niveau du grid.

À propos de cette tâche

Pour permettre aux clients d'utiliser les noms de domaine des points de terminaison S3, vous devez effectuer toutes les opérations suivantes :

- Utilisez Grid Manager pour ajouter les noms de domaine des points de terminaison S3 au système StorageGRID.
- Assurez-vous que le "certificat que le client utilise pour les connexions HTTPS à StorageGRID" est signé pour tous les noms de domaine requis par le client.

  Par exemple, si le point de terminaison est `s3.company.com`, vous devez vous assurer que le certificat utilisé pour les connexions HTTPS inclut le `s3.company.com` point de terminaison et le nom alternatif de sujet générique (SAN) du point de terminaison : `*.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 ces enregistrements référencent tous les noms de domaine de point de terminaison S3 requis, y compris tout nom générique (wildcard).

> Les clients peuvent se connecter à StorageGRID via l'adresse IP d'un nœud de passerelle, d'un nœud d'administration ou d'un nœud de stockage, ou via l'adresse IP virtuelle d'un groupe à haute disponibilité. Vous devez comprendre comment les applications clientes se connectent à la grille afin d'inclure les adresses IP correctes dans les enregistrements DNS.

Les clients qui utilisent des connexions HTTPS (recommandées) à la grille peuvent utiliser l'un ou l'autre de ces certificats :

- Les clients qui se connectent à un point de terminaison d'équilibreur de charge peuvent utiliser un certificat personnalisé pour ce point de terminaison. Chaque point de terminaison d'équilibreur de charge peut être configuré pour reconnaître différents noms de domaine de point de terminaison S3.
- Les clients qui se connectent à un point de terminaison d'équilibreur 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 point de terminaison S3 requis.

> Si vous n'ajoutez pas de noms de domaine de point de terminaison S3 et que la liste est vide, la prise en charge des requêtes de type hébergement virtuel S3 est désactivée.

Ajouter un nom de domaine de point de terminaison S3

Étapes

1. Sélectionnez **Configuration** > **Réseau** > **Noms de domaine des endpoints S3**.
2. Saisissez le nom de domaine dans le champ **Nom de domaine 1**. Sélectionnez **Ajouter un autre nom de domaine** pour ajouter d'autres noms de domaine.

3. Sélectionnez **Enregistrer**.
4. Assurez-vous que les certificats serveur utilisés par les clients correspondent aux noms de domaine des points de terminaison S3 requis.
   - Si les clients se connectent à un point de terminaison d'équilibreur de charge qui utilise son propre certificat, "mettre à jour le certificat associé au point de terminaison".
   - Si les clients se connectent à un point de terminaison d'équilibreur de charge qui utilise le certificat d'API S3 global ou directement aux nœuds de stockage, "mettre à jour le certificat global de l'API S3".
5. Ajoutez les enregistrements DNS nécessaires pour garantir que les requêtes de nom de domaine des points de terminaison puissent être résolues.

Résultat

Désormais, lorsque les clients utilisent le point de terminaison `bucket.s3.company.com`, le serveur DNS résout le point de terminaison correct et le certificat authentifie le point de terminaison comme prévu.

Renommer un nom de domaine d'endpoint S3

Si vous modifiez un nom utilisé par les applications S3, les requêtes de type hébergement virtuel échoueront.

Étapes

1. Sélectionnez **Configuration** > **Réseau** > **Noms de domaine des endpoints S3**.
2. Sélectionnez le champ du nom de domaine que vous souhaitez modifier et apportez les modifications nécessaires.
3. Sélectionnez **Enregistrer**.
4. Sélectionnez **Oui** pour confirmer votre modification.

Supprimer un nom de domaine de point de terminaison S3

Si vous supprimez un nom utilisé par les applications S3, les requêtes de type hébergement virtuel échoueront.

Étapes

1. Sélectionnez **Configuration** > **Réseau** > **Noms de domaine des endpoints S3**.
2. Sélectionnez l'icône de suppression ✕ à côté du nom de domaine.
3. Sélectionnez **Oui** pour confirmer la suppression.

Informations connexes

- "Utilisez l'API REST S3"
- "Afficher les adresses IP"
- "Configurer les groupes à haute disponibilité"

Adresses IP et ports pour les connexions client StorageGRID

Pour stocker ou récupérer des objets, les applications clientes S3 se connectent au service Load Balancer, qui est inclus sur tous les Admin Nodes et Gateway Nodes, ou au service Local Distribution Router (LDR), qui est inclus sur tous les Storage Nodes.

Les applications clientes peuvent se connecter à StorageGRID en utilisant l'adresse IP d'un nœud du réseau

et le numéro de port du service sur ce nœud. Vous pouvez également créer des groupes de haute disponibilité (HA) de nœuds d'équilibrage de charge afin de fournir des connexions hautement disponibles utilisant des adresses IP virtuelles (VIP). Si vous souhaitez vous connecter à StorageGRID à l'aide d'un domaine complet (FQDN, fully qualified domain name) plutôt que d'une adresse IP ou VIP, vous pouvez configurer des entrées DNS.

Ce tableau récapitule les différents modes de connexion des clients à StorageGRID ainsi que les adresses IP et les ports utilisés pour chaque type de connexion. Si vous avez déjà créé des points de terminaison d'équilibrage de charge et des groupes de haute disponibilité (HA), consultez Où trouver des adresses IP pour localiser ces valeurs dans le Grid Manager.

Là où la connexion est établie	Service auquel le client se connecte	Adresse IP	Port
Groupe HA	Équilibreur de charge	Adresse IP virtuelle d'un groupe HA	Port attribué au point de terminaison de l'équilibreur de charge
Nœud d'administration	Équilibreur de charge	Adresse IP du nœud d'administration	Port attribué au point de terminaison de l'équilibreur de charge
Nœud de passerelle	Équilibreur de charge	Adresse IP du nœud passerelle	Port attribué au point de terminaison de l'équilibreur de charge
Nœud de stockage	LDR	Adresse IP du nœud de stockage	Ports S3 par défaut : • HTTPS: 18082 • HTTP: 18084

Exemples d'URL

Pour connecter une application cliente au point de terminaison de l'équilibreur de charge d'un groupe HA de nœuds de passerelle, utilisez une URL structurée comme indiqué ci-dessous :

`https://VIP-of-HA-group:LB-endpoint-port`

Par exemple, si l'adresse IP virtuelle du groupe HA est 192.0.2.5 et que le numéro de port du point de terminaison de l'équilibreur de charge est 10443, une application peut utiliser l'URL suivante pour se connecter à StorageGRID :

`https://192.0.2.5:10443`

Où trouver des adresses IP

1. Connectez-vous au Gestionnaire de grille en utilisant un "navigateur Web pris en charge".
2. Pour trouver l'adresse IP d'un nœud de grille :
   a. Sélectionnez **Nœuds**.
   b. Sélectionnez le nœud d'administration, le nœud de passerelle ou le nœud de stockage auquel vous souhaitez vous connecter.

c. Sélectionnez l'onglet **Overview**.

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 correspondances d'interface.

Vous pouvez établir des connexions depuis des applications clientes vers n'importe laquelle des adresses IP de la liste :

- **eth0:** Réseau Grid
- **eth1:** Réseau d'administration (facultatif)
- **eth2:** Réseau client (facultatif)

> Si vous consultez un nœud d'administration ou un nœud de passerelle et qu'il s'agit du nœud actif dans un groupe à haute disponibilité, l'adresse IP virtuelle du groupe HA est affichée sur eth2.

3. Pour trouver l'adresse IP virtuelle d'un groupe à haute disponibilité :
   a. Sélectionnez **Configuration** > **Réseau** > **Groupes de haute disponibilité**.
   b. Dans le tableau, notez l'adresse IP virtuelle du groupe HA.
4. Pour trouver le numéro de port d'un point de terminaison d'équilibreur de charge :
   a. Sélectionnez **Configuration** > **Réseau** > **Points de terminaison de l'équilibreur de charge**.
   b. Notez le numéro de port du point de terminaison que vous souhaitez utiliser.

> Si le numéro de port est 80 ou 443, le point de terminaison est configuré uniquement sur les nœuds de passerelle, car ces ports sont réservés sur les nœuds d'administration. Tous les autres ports sont configurés sur les nœuds de passerelle et les nœuds d'administration.

   c. Sélectionnez le nom du point de terminaison dans le tableau.
   d. Vérifiez que le **type de client** (S3) correspond à l'application cliente qui utilisera le point de terminaison.

Gérer les réseaux et les connexions

Configurer les paramètres réseau de StorageGRID

Vous pouvez configurer différents paramètres réseau depuis le Grid Manager afin d'optimiser le fonctionnement de votre système StorageGRID.

Configurer les interfaces VLAN

Vous pouvez "créer des interfaces de réseau local virtuel (VLAN)" isoler et partitionner le trafic pour des raisons de sécurité, de flexibilité et de performance. Chaque interface VLAN est associée à une ou plusieurs interfaces parentes sur les Admin Nodes et les Gateway Nodes. Vous pouvez utiliser les interfaces VLAN dans les groupes HA et dans les points de terminaison d'équilibrage de charge pour séparer le trafic client ou d'administration par application ou locataire.

Politiques de classification du trafic

Vous pouvez utiliser "politiques de classification du trafic" pour identifier et gérer différents types de trafic réseau, y compris le trafic lié à des compartiments spécifiques, des locataires, des sous-réseaux clients ou des points de terminaison d'équilibrage de charge. Ces politiques peuvent aider à limiter et à surveiller le trafic.

Directives pour les réseaux StorageGRID

Vous pouvez utiliser Grid Manager pour configurer et gérer les réseaux et les connexions StorageGRID.

Consultez "Configurer les connexions client S3" pour savoir comment connecter des clients S3.

Réseaux StorageGRID par défaut

Par défaut, StorageGRID prend en charge trois interfaces réseau par nœud de grille, ce qui vous permet de configurer le réseau de chaque nœud de grille individuel afin de répondre à vos exigences de sécurité et d'accès.

Pour plus d'informations sur la topologie du réseau, consultez "Directives de mise en réseau".

Réseau Grid

Obligatoire. Le réseau Grid est utilisé pour tout le trafic interne de StorageGRID. Il assure la connectivité entre tous les nœuds de la grille, sur l'ensemble des 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 aux protocoles clients. Le réseau d'administration 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 clientes S3, afin que le réseau Grid puisse être isolé et sécurisé. Le réseau client peut communiquer avec tout sous-réseau accessible via la passerelle locale.

Lignes directrices

- Chaque nœud StorageGRID nécessite une interface réseau dédiée, une adresse IP, un masque de sous-réseau et une passerelle pour chaque réseau auquel il est affecté.
- Un nœud de grille ne peut pas avoir plus d'une interface sur un réseau.
- Une seule passerelle par réseau et par nœud de grille est prise en charge, et elle doit se trouver sur le même sous-réseau que le nœud. Vous pouvez implémenter un routage plus complexe au niveau de la passerelle, si nécessaire.
- Sur chaque nœud, chaque réseau est associé à une interface réseau spécifique.

Réseau	Nom de l'interface
Grid	eth0

Réseau	Nom de l'interface
Administrateur (facultatif)	eth1
Client (facultatif)	eth2

- Si le nœud est connecté à un StorageGRID appliance, des ports spécifiques sont utilisés pour chaque réseau. Pour plus de détails, consultez les instructions d'installation de votre appliance.
- La route par défaut est générée automatiquement, par nœud. Si eth2 est activé, alors 0.0.0.0/0 utilise le réseau client sur eth2. Si eth2 n'est pas activé, alors 0.0.0.0/0 utilise le réseau Grid sur eth0.
- Le réseau client ne devient opérationnel que lorsque le nœud de grille a rejoint la grille
- Le réseau d'administration peut être configuré lors du déploiement du nœud de la grille pour permettre l'accès à l'interface utilisateur d'installation avant que la grille ne soit entièrement installée.

Interfaces optionnelles

Vous pouvez éventuellement ajouter des interfaces supplémentaires à un nœud. Par exemple, vous pourriez vouloir ajouter une interface trunk à un nœud Admin ou Gateway, afin de pouvoir utiliser "Interfaces VLAN" pour segmenter le trafic appartenant à différentes applications ou locataires. Ou, vous pourriez vouloir ajouter une interface d'accès à utiliser dans un "groupe à haute disponibilité (HA)".

Pour ajouter des interfaces trunk ou d'accès, consultez les informations suivantes :

- **VMware (après installation du nœud)** : "VMware : Ajouter des interfaces trunk ou d'accès à un nœud"
  - **Linux (avant l'installation du nœud)** : "Créer des fichiers de configuration de nœud"
  - **Linux (après installation du nœud)** : "Ajouter des interfaces de tronc ou d'accès à un nœud"

> « Linux » désigne un déploiement RHEL, Ubuntu ou Debian. Pour obtenir la liste des versions prises en charge, consultez le "Outil de matrice d'interopérabilité (IMT) NetApp".

Afficher les adresses IP dans StorageGRID

Vous pouvez consulter l'adresse IP de chaque nœud de votre système StorageGRID. Vous pouvez ensuite utiliser cette adresse IP pour vous connecter au nœud via la ligne de commandes et effectuer diverses opérations de maintenance.

Avant de commencer

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

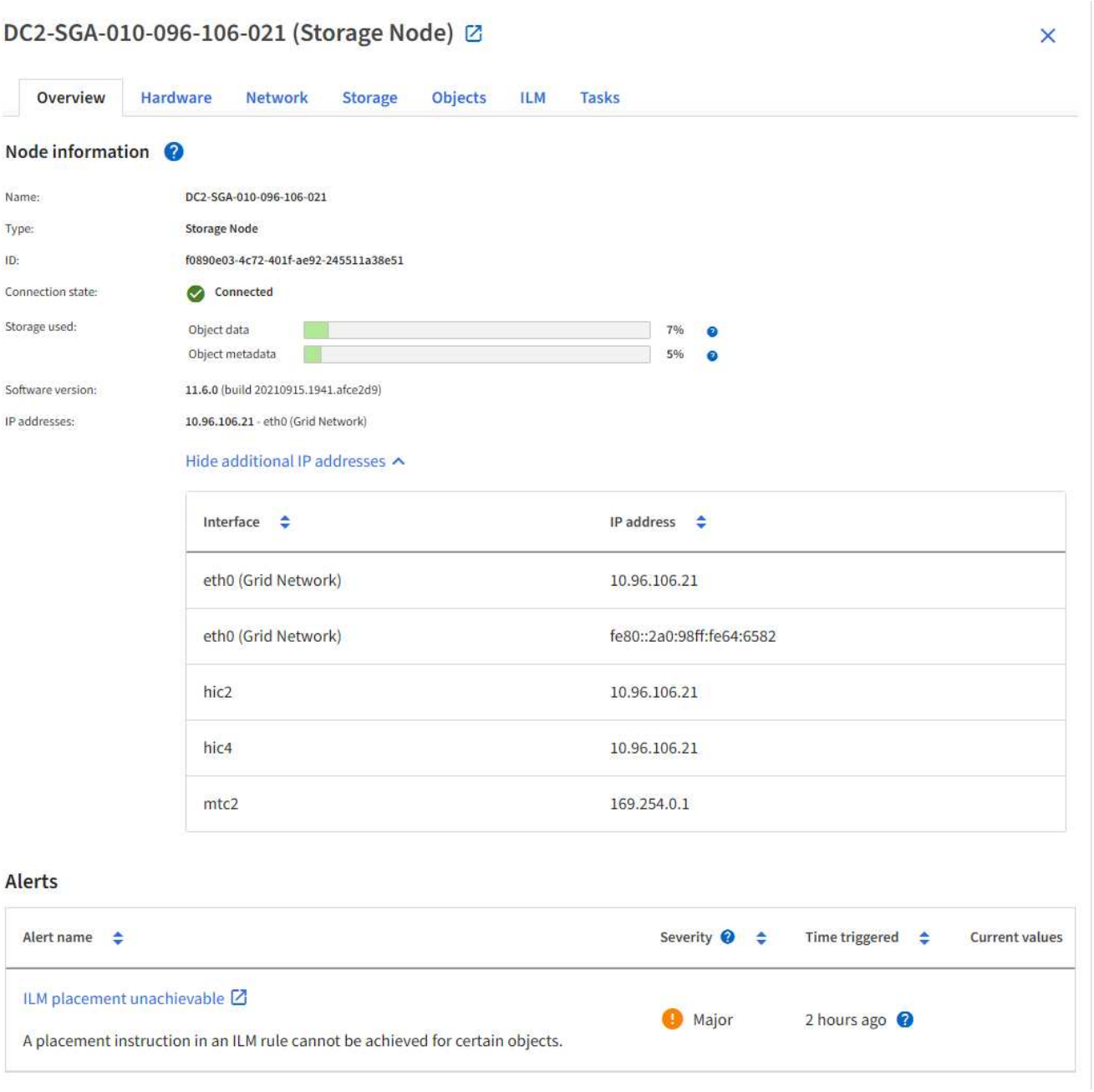
À propos de cette tâche

Pour plus d'informations sur la modification des adresses IP, consultez "Configurer les adresses IP".

Étapes

1. Sélectionnez **Nodes** > ***grid node*** > **Overview**.
2. Sélectionnez **Afficher plus** à droite du titre IP Addresses.

   Les adresses IP de ce nœud de grille sont répertoriées dans un tableau.



Configurez les interfaces VLAN dans StorageGRID

Créez des interfaces VLAN (réseau local virtuel) sur les nœuds d'administration et les nœuds passerelle, puis utilisez-les dans des groupes HA et des points de terminaison d'équilibrage de charge afin d'isoler et de partitionner le trafic pour la sécurité, la flexibilité et la performance. Les nœuds sélectionnés dans le groupe HA peuvent utiliser les interfaces VLAN pour partager jusqu'à 10 adresses IP virtuelles, de sorte que si un nœud tombe en panne, un autre nœud prend en charge le trafic à destination et en provenance des adresses IP virtuelles.

Considérations relatives aux interfaces VLAN

- Vous créez une interface VLAN en saisissant un ID de VLAN et en choisissant une interface parente sur un

ou plusieurs nœuds.

- Une interface parente doit être configurée comme interface trunk au niveau du commutateur.
- Une interface parente peut être le Grid Network (eth0), le Client Network (eth2) ou une interface trunk supplémentaire pour la VM ou l'hôte bare-metal (par exemple, ens256).
- Pour chaque interface VLAN, vous ne pouvez sélectionner qu'une seule interface parente pour un nœud donné. Par exemple, vous ne pouvez pas utiliser à la fois l'interface Grid Network et l'interface Client Network sur le même Gateway Node comme interface parente pour un même VLAN.
- Si l'interface VLAN est destinée au trafic du nœud d'administration, y compris le trafic lié au Grid Manager et au Tenant Manager, sélectionnez uniquement les interfaces des 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 devez ajouter des interfaces de tronc, consultez les informations suivantes :
  - **VMware (après installation du nœud)** : "VMware : Ajouter des interfaces trunk ou d'accès à un nœud"
  - **Linux (avant l'installation du nœud)** : "Créer des fichiers de configuration de nœud"
  - **Linux (après installation du nœud)** : "Ajouter des interfaces de tronc ou d'accès à un nœud"

> « Linux » désigne un déploiement RHEL, Ubuntu ou Debian. Pour obtenir la liste des versions prises en charge, consultez le "Outil de matrice d'interopérabilité (IMT) NetApp".

Créer 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 root".
- Une interface trunk a été configurée sur le réseau et connectée à la machine virtuelle ou au nœud Linux. Vous connaissez le nom de l'interface trunk.
- Vous connaissez l'identifiant du VLAN que vous configurez.

À propos de cette tâche

Votre administrateur réseau a peut-être configuré une ou plusieurs interfaces trunk et un ou plusieurs VLAN afin de séparer le trafic client ou d'administration appartenant à différentes applications ou locataires. Chaque VLAN est identifié par un identifiant numérique ou un tag. 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 permettant aux clients d'accéder à StorageGRID sur un VLAN spécifique. Lorsque vous créez des interfaces VLAN, vous spécifiez l'ID du VLAN et sélectionnez les interfaces parentes (trunk) sur un ou plusieurs nœuds.

Accédez à l'assistant

Étapes

1. Sélectionnez **Configuration** > **Réseau** > **Interfaces VLAN**.
2. Sélectionnez **Create**.

Saisissez les détails des interfaces VLAN

Étapes

1. Spécifiez l'ID du VLAN sur votre réseau. Vous pouvez saisir n'importe quelle valeur comprise entre 1 et 4094.

   Les ID de VLAN n'ont pas besoin d'être uniques. Par exemple, vous pouvez utiliser l'ID de VLAN 200 pour le trafic d'administration sur un site et le même ID pour le trafic client sur un autre site. Vous pouvez créer des interfaces VLAN distinctes avec des ensembles d'interfaces parentes différents sur chaque site. Cependant, deux interfaces VLAN ayant 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 éventuellement saisir une brève description pour l'interface VLAN.
3. Sélectionnez **Continue**.

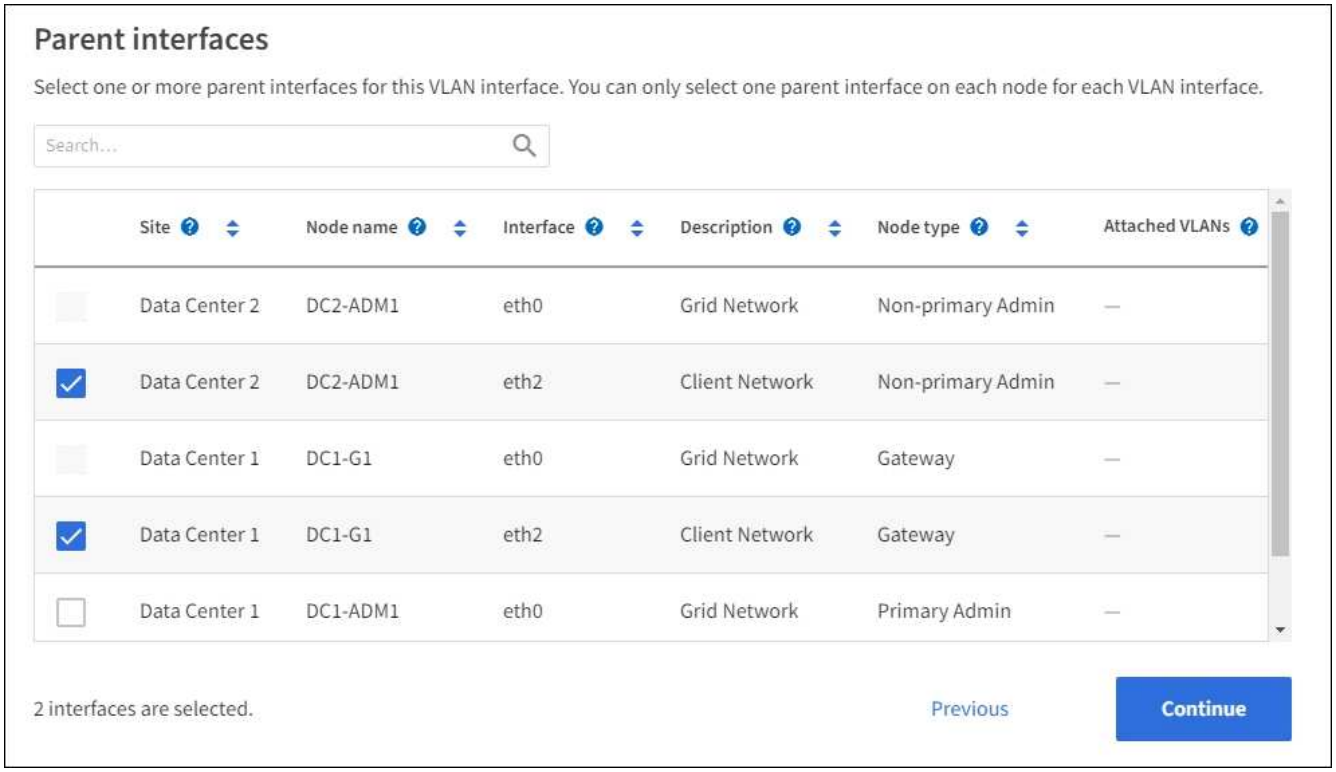
Choisissez les interfaces parentes

Le tableau répertorie les interfaces disponibles pour tous les nœuds d'administration et les nœuds passerelle à chaque site de votre grille. Les interfaces du réseau d'administration (eth1) ne peuvent pas être utilisées comme interfaces parentes et ne sont pas affichées.

Étapes

1. Sélectionnez une ou plusieurs interfaces parentes auxquelles associer ce VLAN.

   Par exemple, vous pourriez vouloir attacher un VLAN à l'interface Client Network (eth2) pour un Gateway Node et un Admin Node.



2. Sélectionnez **Continue**.

Confirmez les paramètres

Étapes

1. Vérifiez la configuration et apportez les modifications nécessaires.
   - Si vous devez modifier l'ID ou la description du VLAN, sélectionnez **Saisir les détails du VLAN** en haut de la page.
   - Si vous devez modifier une interface parente, sélectionnez **Choisir les interfaces parentes** en haut de la page ou sélectionnez **Précédent**.
   - Si vous devez supprimer une interface parente, sélectionnez l'icône de la corbeille .
2. Sélectionnez **Enregistrer**.
3. Attendez jusqu'à 5 minutes pour que la nouvelle interface apparaisse comme sélection sur la page des groupes de haute disponibilité et soit répertoriée dans le tableau **Interfaces réseau** pour le nœud (**Nœuds** > ***parent interface node*** > **Réseau**).

Modifier une interface VLAN

Lorsque vous modifiez une interface VLAN, vous pouvez effectuer les types de modifications suivants :

- Modifiez l'ID VLAN ou la description.
- Ajouter ou supprimer des interfaces parentes.

Par exemple, vous pourriez vouloir supprimer une interface parente d'une interface VLAN si vous prévoyez de mettre hors service le nœud associé.

Remarque :

- Vous ne pouvez pas modifier l'ID d'un VLAN si l'interface VLAN est utilisée dans un groupe HA.
- Vous ne pouvez pas supprimer une interface parente si celle-ci est utilisée dans un groupe HA.

  Par exemple, supposons que le VLAN 200 soit connecté aux interfaces parentes des nœuds A et B. Si un groupe HA utilise l'interface VLAN 200 pour le nœud A et l'interface eth2 pour le nœud B, vous pouvez supprimer l'interface parente inutilisée du nœud B, mais vous ne pouvez pas supprimer l'interface parente utilisée du nœud A.

Étapes

1. Sélectionnez **Configuration** > **Réseau** > **Interfaces VLAN**.
2. Cochez la case correspondant à l'interface VLAN que vous souhaitez modifier. Ensuite, sélectionnez **Actions** > **Modifier**.
3. Vous pouvez éventuellement mettre à jour l'ID du VLAN ou la description. Ensuite, sélectionnez **Continuer**.

   Vous ne pouvez pas mettre à jour un ID de VLAN si le VLAN est utilisé dans un groupe HA.

4. Vous pouvez cocher ou décocher les cases pour ajouter des interfaces parentes ou supprimer les interfaces inutilisées. Ensuite, sélectionnez **Continuer**.
5. Vérifiez la configuration et apportez les modifications nécessaires.
6. Sélectionnez **Enregistrer**.

Supprimer une interface VLAN

Vous pouvez supprimer une ou plusieurs interfaces VLAN.

Vous ne pouvez pas supprimer une interface VLAN si elle est actuellement utilisée dans un groupe HA. Vous devez retirer l'interface VLAN du groupe HA avant de pouvoir la supprimer.

Pour éviter toute interruption du trafic client, envisagez de faire l'une des actions suivantes :

- Ajoutez une nouvelle interface VLAN au groupe HA avant de supprimer cette interface VLAN.
- Créez un nouveau groupe HA qui n'utilise pas cette interface VLAN.
- Si l'interface VLAN que vous souhaitez supprimer est actuellement l'interface active, modifiez le groupe HA. Déplacez l'interface VLAN que vous souhaitez supprimer en bas de la liste de priorité. Attendez que la communication soit établie sur la nouvelle interface principale, puis supprimez l'ancienne interface du groupe HA. Enfin, supprimez l'interface VLAN sur ce nœud.

Étapes

1. Sélectionnez **Configuration** > **Réseau** > **Interfaces VLAN**.
2. Cochez la case correspondant à chaque interface VLAN que vous souhaitez supprimer. Ensuite, sélectionnez **Actions** > **Supprimer**.
3. Sélectionnez **Oui** pour confirmer votre sélection.

   Toutes les interfaces VLAN que vous avez sélectionnées sont supprimées. Une bannière verte de succès apparaît sur la page des interfaces VLAN.

Activez StorageGRID CORS pour une interface de gestion

En tant qu'administrateur de grille, vous pouvez activer le partage de ressources entre origines (CORS) pour les requêtes d'API de gestion vers StorageGRID, si vous souhaitez que les données dans StorageGRID soient accessibles via les API de gestion à un autre domaine.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur Web pris en charge".
- Le "Autorisation d'accès root" permet d'accéder à toutes les requêtes de configuration CORS.

À propos de cette tâche

CORS est un mécanisme de sécurité qui permet aux applications web clientes d'un domaine d'accéder aux ressources d'un autre domaine. Par exemple, supposons que vous souhaitiez créer un tableau de bord de surveillance pour StorageGRID dans le domaine `http://www.example.com`. En activant CORS dans StorageGRID pour `http://www.example.com` et « Grid Manager », le domaine StorageGRID répond aux requêtes de l'API Grid Management provenant de `http://www.example.com`.

Les requêtes Management API (mgmt-api) avec `application/json` ou `multipart/formdata` requêtes pour `Content-Type` sont prises en charge pour CORS.

Étapes

1. Dans Grid Manager, accédez à **CONFIGURATION** > **Réseau** > **Paramètres CORS de l'interface de gestion**.

2. Sélectionnez **Grid Manager**, **Tenant Manager** ou les deux options.
   - **Gestionnaire de grille** : Active CORS pour les requêtes API de gestion de grille interdomaines.
   - **Gestionnaire de locataires** : Active CORS pour les requêtes API de gestion de locataires interdomaines.
3. Saisissez l'URL de l'autre domaine dans le champ **Domains**.

   Sélectionnez **Ajouter un autre domaine** si vous souhaitez activer CORS dans StorageGRID pour plus d'un domaine.

4. Sélectionnez **Enregistrer**.

Informations connexes

"Configurer StorageGRID CORS pour les compartiments et les objets"

Gérer les politiques de classification du trafic

Politiques de classification du trafic dans StorageGRID

Les politiques de classification du trafic permettent d'identifier et de surveiller différents types de trafic réseau. Ces politiques peuvent faciliter la limitation et la surveillance du trafic afin d'améliorer vos offres de qualité de service (QoS).

Les politiques de classification du trafic sont appliquées aux points de terminaison du service d'équilibrage de charge StorageGRID pour les nœuds de passerelle et les nœuds d'administration. Pour créer des politiques de classification du trafic, vous devez avoir préalablement créé des points de terminaison d'équilibrage de charge.

Règles de correspondance

Chaque politique de classification du trafic contient une ou plusieurs règles de correspondance permettant d'identifier le trafic réseau lié à une ou plusieurs des entités suivantes :

- Compartiments
- Sous-réseau
- Locataire
- points de terminaison de l'équilibreur de charge

StorageGRID surveille le trafic correspondant à toute règle au sein de la politique, conformément aux objectifs de la règle. Tout trafic correspondant à une règle d'une politique est traité par cette politique. Inversement, vous pouvez définir des règles pour faire correspondre tout le trafic, à l'exception d'une entité spécifiée.

Limitation du trafic

Vous pouvez également ajouter les types de limites suivants à une politique :

- Bande passante de l'agrégat
- Bande passante par requête
- Requêtes simultanées
- Taux de requêtes

Les valeurs limites sont appliquées à chaque équilibreur de charge. Si le trafic est réparti simultanément entre plusieurs équilibreurs de charge, les débits maximaux totaux correspondent à un multiple des limites de débit que vous spécifiez.

> Vous pouvez créer des règles pour limiter la bande passante de l'agrégat ou 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 de l'agrégat peuvent avoir un impact mineur supplémentaire sur les performances du trafic non limité.

Pour les limites de bande passante de l'agrégat ou par requête, les requêtes sont traitées au débit que vous avez défini. StorageGRID ne peut imposer qu'une seule vitesse, donc la règle la plus spécifique, selon le type de correspondance, est celle qui est appliquée. La bande passante consommée par la requête n'est pas prise en compte dans le calcul des autres règles de correspondance moins spécifiques contenant des politiques de limite de bande passante de l'agrégat. Pour tous les autres types de limites, les requêtes client sont retardées de 250 millisecondes et reçoivent une réponse 503 Slow Down pour les requêtes qui dépassent une limite définie par une règle correspondante.

Dans le Gestionnaire de grille, vous pouvez consulter les graphiques de trafic et vérifier que les politiques appliquent les limites de trafic attendues.

Utilisez des politiques de classification du trafic avec des SLA

Vous pouvez utiliser des politiques de classification du trafic conjointement avec des limites de capacité et la protection des données pour faire respecter des accords de niveau de service (SLA) qui précisent la capacité, la protection des données et les performances.

L'exemple suivant illustre trois niveaux d'un SLA. Vous pouvez créer des politiques de classification du trafic pour atteindre les objectifs de performance de chaque niveau de SLA.

Niveau de service	Capacité	Protection des données	Performances maximales autorisées	Coût
Or	1 PB de stockage autorisé	Règle ILM 3 copies	25 K requêtes/seconde Bande passante de 5 Go/s (40 Gbit/s)	$$$ par mois
Argent	250 To de stockage autorisé	Règle ILM à 2 copies	10 000 requêtes/seconde 1,25 Go/s (10 Gbit/s) de bande passante	$$ par mois
Bronze	100 To de stockage autorisé	Règle ILM à 2 copies	5 K requêtes/seconde Bande passante de 1 Go/s (8 Gbit/s)	$ par mois

Créer des politiques de classification du trafic StorageGRID

Vous pouvez créer des politiques de classification du trafic si vous souhaitez surveiller et, éventuellement, limiter le trafic réseau par compartiment, expression régulière de compartiment, CIDR, point de terminaison d'équilibreur de charge ou locataire. Vous pouvez également définir des limites pour une politique en fonction de la bande passante, du nombre de requêtes simultanées ou du débit de requêtes.

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 root".
- Vous avez créé tous les points de terminaison de load balancer que vous souhaitez faire correspondre.
- Vous avez créé tous les locataires que vous souhaitez associer.

Étapes

1. Sélectionnez **Configuration** > **Réseau** > **Classification du trafic**.
2. Sélectionnez **Create**.
3. Saisissez un nom et une description (facultatif) pour la règle, puis sélectionnez **Continuer**.

   Par exemple, décrivez à quoi s'applique cette politique de classification du trafic et ce qu'elle limitera.

4. Sélectionnez **Ajouter une règle** et indiquez les détails suivants pour créer une ou plusieurs règles correspondant à 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 de correspondance. Les types de trafic sont : bucket, expression régulière de bucket, CIDR, point de terminaison de load balancer et tenant.

Champ	Description
Valeur de correspondance	Saisissez la valeur correspondant au type sélectionné. • Compartiment : Saisissez un ou plusieurs noms de compartiment. • Expression régulière pour les compartiments : saisissez une ou plusieurs expressions régulières utilisées pour faire correspondre un ensemble de noms de compartiments. L'expression régulière n'est pas ancrée. Utilisez l'ancre ^ pour effectuer une correspondance au début du nom du compartiment, et l'ancre $ pour effectuer une correspondance à la fin du nom. La correspondance par expression régulière prend en charge un sous-ensemble de la syntaxe PCRE (Perl compatible regular expression). • CIDR : Entrez un ou plusieurs sous-réseaux IPv4, en notation CIDR, qui correspondent au sous-réseau souhaité. • Point de terminaison de l'équilibreur de charge : sélectionnez un nom de point de terminaison. Voici les points de terminaison de l'équilibreur de charge que vous avez définis sur le "Configurer les points de terminaison de l'équilibreur de charge". • Locataire : L'identification du locataire repose sur l'identifiant de clé d'accès. Si la requête ne contient pas d'identifiant de clé d'accès (par exemple, accès anonyme), alors la propriété du compartiment consulté est utilisée pour déterminer le locataire.
Correspondance inverse	Si vous souhaitez faire correspondre tout le trafic réseau *à l'exception* du trafic conforme au Type et à la valeur de correspondance que vous venez de définir, cochez la case **Correspondance inverse**. Sinon, laissez la case décochée. Par exemple, si vous souhaitez que cette politique s'applique à tous les points de terminaison de l'équilibreur de charge sauf un, spécifiez le point de terminaison de l'équilibreur de charge à exclure et sélectionnez **Correspondance inverse**. Pour une politique contenant plusieurs critères de correspondance, dont au moins un est un critère de correspondance inverse, veillez à ne pas créer une politique qui correspond à toutes les requêtes.

5. Vous pouvez également sélectionner **Ajouter une limite** et sélectionner les détails suivants pour ajouter une ou plusieurs limites afin de contrôler le trafic réseau correspondant à une règle.

> StorageGRID collecte des métriques même si vous n'ajoutez aucune limite, afin que vous puissiez comprendre les tendances du trafic.

Champ	Description
Type	Le type de limite que vous souhaitez appliquer au trafic réseau correspondant à la règle. Par exemple, vous pouvez limiter la bande passante ou le débit de requêtes. **Remarque** : Vous pouvez créer des règles pour limiter la bande passante de l'agrégat ou la bande passante par requête. 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 requête est indisponible. Inversement, lorsque la bande passante par requête est utilisée, la bande passante de l'agrégat est indisponible. Les limites de la bande passante de l'agrégat peuvent avoir un impact mineur supplémentaire sur les performances du trafic non limité. Pour les limites de bande passante, StorageGRID applique la règle la plus adaptée au type de limite défini. Par exemple, si vous avez une règle qui limite le trafic dans un seul sens, alors le trafic dans le sens opposé sera illimité, même s'il existe du trafic correspondant à d'autres règles imposant des limites de bande passante. StorageGRID applique les « meilleures » correspondances pour les limites de bande passante dans l'ordre suivant : • Adresse IP exacte (masque /32) • Nom exact du compartiment • Expression régulière de compartiment • Locataire • Point de terminaison • Correspondances CIDR non exactes (pas /32) • Correspondances inverses
S'applique à	Que cette limite s'applique aux requêtes de lecture du client (GET ou HEAD) ou aux requêtes d'écriture (PUT, POST ou DELETE).
Valeur	La valeur à laquelle le trafic réseau sera limité, en fonction de l'unité que vous sélectionnez. Par exemple, saisissez 10 et sélectionnez Mio/s pour empêcher le trafic réseau correspondant à cette règle de dépasser 10 Mio/s. **Remarque** : Selon le paramètre d'unités, les unités disponibles seront binaires (par exemple, GiB) ou décimales (par exemple, GB). Pour modifier le paramètre d'unités, sélectionnez le menu déroulant utilisateur en haut à droite du Grid Manager, puis sélectionnez **User Preferences**.
Unité	L'unité qui décrit la valeur que vous avez saisie.

Par exemple, si vous souhaitez créer une limite de bande passante de l'agrégat de 4 Go/s pour un niveau SLA, créez deux limites de bande passante de l'agrégat : GET/HEAD à 4 Go/s et PUT/POST/DELETE à 4 Go/s.

6. Sélectionnez **Continue**.

7. Veuillez lire et examiner la politique de classification du trafic. Utilisez le bouton **Précédent** pour revenir en arrière et apporter les modifications nécessaires. Lorsque vous êtes satisfait de la politique, sélectionnez **Enregistrer et continuer**.

   Le trafic client S3 est désormais géré conformément à la politique de classification du trafic.

Après avoir terminé

"Afficher les indicateurs de trafic réseau"pour vérifier que les règles appliquent les limites de trafic que vous attendez.

Modifier une politique de classification du trafic StorageGRID

Vous pouvez modifier une politique de classification du trafic pour en changer le nom ou la description, ou pour créer, modifier ou supprimer des règles ou des limites pour cette politique.

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 root".

Étapes

1. Sélectionnez **Configuration** > **Réseau** > **Classification du trafic**.

   La page des politiques de classification du trafic s'affiche et les politiques existantes sont répertoriées dans un tableau.

2. Modifiez la politique via le menu Actions ou la page de détails. Consultez "créer des politiques de classification du trafic" pour savoir quoi saisir.

   Menu Actions

   a. Cochez la case correspondant à la politique.

   b. Sélectionnez **Actions** > **Modifier**.

   Page de détails

   a. Sélectionnez le nom de la règle.

   b. Sélectionnez le bouton **Modifier** situé à côté du nom de la stratégie.

3. À l'étape « Saisir le nom de la politique », vous pouvez éventuellement modifier le nom ou la description de la politique, puis sélectionner **Continue**.
4. Pour l'étape Ajouter des règles de correspondance, vous pouvez éventuellement ajouter une règle ou modifier le **Type** et la **valeur de correspondance** de la règle existante, puis sélectionner **Continuer**.
5. À l'étape Définir les limites, vous pouvez éventuellement ajouter, modifier ou supprimer une limite, puis sélectionner **Continuer**.
6. Examinez la politique mise à jour, puis sélectionnez **Enregistrer et continuer**.

   Les modifications apportées à la politique ont été enregistrées et le trafic réseau est désormais géré conformément aux politiques de classification du trafic. Vous pouvez consulter les graphiques de trafic et vérifier que les politiques appliquent les limites de trafic que vous attendez.

Supprimer une politique de classification du trafic StorageGRID

Vous pouvez supprimer une règle de classification du trafic si vous n'en avez plus besoin. Assurez-vous de supprimer la bonne règle, car une règle ne peut pas être récupérée une fois 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 root".

Étapes

1. Sélectionnez **Configuration** > **Réseau** > **Classification du trafic**.

   La page des politiques de classification du trafic affiche les politiques existantes répertoriées dans un tableau.

2. Supprimez la politique à l'aide du menu Actions ou de la page de détails.

   Menu Actions

   a. Cochez la case correspondant à la politique.

   b. Sélectionnez **Actions** > **Supprimer**.

   Page de détails de la politique

   a. Sélectionnez le nom de la règle.

   b. Sélectionnez le bouton **Supprimer** situé à côté du nom de la stratégie.

3. Sélectionnez **Oui** pour confirmer que vous souhaitez supprimer la politique.

   La politique a été supprimée.

Afficher les indicateurs de trafic réseau dans StorageGRID

Vous pouvez surveiller le trafic réseau en consultant les graphiques disponibles sur la page des politiques 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 root ou autorisation de comptes locataires".

À propos de cette tâche

Pour toute politique de classification du trafic existante, vous pouvez consulter les indicateurs du service de load balancer afin de déterminer si la politique limite efficacement le trafic sur le réseau. Les données des graphiques peuvent vous aider à déterminer si vous devez ajuster la politique.

Même si aucune limite n'est fixée pour une politique de classification du trafic, des indicateurs sont collectés et les graphiques fournissent des informations utiles pour comprendre les tendances du trafic.

Étapes

1. Sélectionnez **Configuration** > **Réseau** > **Classification du trafic**.

   La page des politiques de classification du trafic s'affiche et les politiques existantes sont répertoriées dans le tableau.

2. Sélectionnez le nom de la politique de classification du trafic pour laquelle vous souhaitez consulter les indicateurs.
3. Sélectionnez l'onglet **Métriques**.

   Les graphiques de la politique de classification du trafic s'affichent. Les graphiques présentent des indicateurs uniquement pour le trafic correspondant à la politique sélectionnée.

   Les graphiques suivants figurent sur la page.

   - Débit des requêtes : ce graphique indique la quantité de bande passante correspondant à cette politique, gérée par l'ensemble des équilibreurs de charge. Les données reçues comprennent les en-têtes de toutes les requêtes et la taille du corps des réponses qui contiennent des données de corps. Les données envoyées comprennent les en-têtes de réponse pour toutes les requêtes et la taille du corps de la réponse pour les requêtes qui incluent des données de corps dans la réponse.

     > ⓘ Une fois les requêtes terminées, ce graphique affiche uniquement l'utilisation de la bande passante. Pour les requêtes lentes ou portant sur des objets volumineux, la bande passante instantanée réelle peut différer des valeurs indiquées dans ce graphique.

   - Taux de réponse en cas d'erreur : ce graphique fournit un taux approximatif auquel les requêtes correspondant à cette politique renvoient des erreurs (code d'état HTTP >= 400) aux clients.
   - Durée moyenne des requêtes (sans erreur) : ce graphique présente la durée moyenne des requêtes réussies correspondant à cette politique.
   - Utilisation de la bande passante de la politique : ce graphique indique la quantité de bande passante correspondant à cette politique, gérée par l'ensemble des équilibreurs de charge. Les données reçues comprennent les en-têtes de requête pour toutes les requêtes et la taille des données du corps pour les réponses qui en contiennent. Les données envoyées comprennent les en-têtes de réponse pour toutes les requêtes et la taille des données du corps de la réponse pour les requêtes dont la réponse contient des données de corps.
4. Placez le curseur sur un graphique linéaire pour afficher une fenêtre contextuelle des valeurs sur une partie spécifique du graphique.
5. Sélectionnez **Grafana dashboard** juste en dessous du titre **Metrics** pour afficher tous les graphiques d'une policy. En plus des quatre graphiques de l'onglet **Metrics**, vous pouvez en consulter deux autres :
   - Taux de requêtes d'écriture par taille d'objet : Ce taux correspond aux requêtes PUT/POST/DELETE conformes à cette politique. Le positionnement sur une cellule indique le taux par seconde. Les taux affichés au survol sont tronqués à un nombre entier et peuvent indiquer 0 même lorsqu'il y a des requêtes non nulles dans le compartiment.
   - Taux de requêtes de lecture par taille d'objet : le taux des requêtes GET/HEAD correspondant à cette politique. Le positionnement sur une cellule individuelle indique les taux par seconde. Les taux affichés au survol sont tronqués à des nombres entiers et peuvent indiquer 0 même s'il y a des requêtes non nulles dans le compartiment.
6. Vous pouvez également accéder aux graphiques depuis le menu **Support**.
   a. Sélectionnez **Support** > **Tools** > **Metrics**.

b. Sélectionnez **Politique de classification du trafic** dans la section **Grafana**.

c. Sélectionnez la règle dans le menu situé 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 des objets agrégées dans le décompte et le nombre de requêtes par seconde pendant cette période.

   Les politiques de classification du trafic sont identifiées par leur identifiant. Les identifiants des politiques sont répertoriés sur la page des politiques de classification du trafic.

7. Analysez les graphiques pour déterminer la fréquence à laquelle la politique limite le trafic et si vous devez ajuster la politique.

Chiffrements pris en charge pour les connexions TLS sortantes dans StorageGRID

Le système StorageGRID prend en charge un ensemble limité de suites de chiffrement pour les connexions TLS (Transport Layer Security) aux systèmes externes utilisés pour la fédération d'identité et les Cloud Storage Pools.

Versions de TLS prises en charge

StorageGRID prend en charge TLS 1.2 et TLS 1.3 pour les connexions aux systèmes externes utilisés pour la fédération d'identité et les Cloud Storage Pools.

Les suites de chiffrement TLS prises en charge pour les systèmes externes ont été sélectionnées afin de garantir la compatibilité avec un large éventail de systèmes externes. La liste est plus longue que la liste des suites de chiffrement prises en charge pour les applications clientes S3. Pour configurer les suites de chiffrement, allez dans **Configuration** > **Sécurité** > **Paramètres de sécurité** et sélectionnez **Stratégies TLS et SSH**.

> Les options de configuration TLS, telles que les versions de protocole, les algorithmes de chiffrement, les algorithmes d'échange de clés et les algorithmes MAC, ne sont pas configurables dans StorageGRID. Contactez votre représentant de compte NetApp si vous avez des demandes spécifiques concernant ces paramètres.

Avantages des connexions HTTP actives, inactives et simultanées dans StorageGRID

La façon dont vous configurez les connexions HTTP peut avoir un impact sur les performances du système StorageGRID. Les configurations diffèrent selon que la connexion HTTP est active, inactive ou si vous avez plusieurs connexions simultanées.

Vous pouvez identifier les gains de performance pour les types de connexions HTTP suivants :

- Connexions HTTP inactives
- Connexions HTTP actives
- Connexions HTTP simultanées

Avantages du maintien des connexions HTTP inactives ouvertes

Maintenez les connexions HTTP ouvertes lorsque les applications clientes sont inactives afin de permettre des

transactions ultérieures. Maintenez une connexion HTTP inactive ouverte pendant un maximum de 10 minutes. 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 :

- Latence réduite entre le moment où le système StorageGRID détermine qu'il doit effectuer une transaction HTTP et le moment où le système StorageGRID peut l'exécuter

  La réduction de la latence est le principal avantage, notamment en ce qui concerne le temps nécessaire à l'établissement des connexions TCP/IP et TLS.

- Augmentation du débit de transfert des données grâce à l'amorçage de l'algorithme de démarrage lent TCP/IP avec des transferts précédemment effectués
- Notification instantanée de plusieurs types de pannes interrompant la connectivité entre l'application cliente et le système StorageGRID

Déterminez la durée de maintien d'une connexion inactive en équilibrant les avantages d'un démarrage lent et l'allocation des ressources.

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.

Déterminer la durée maximale pendant laquelle une connexion doit être maintenue ouverte implique un compromis entre les avantages de la persistance de la connexion et l'allocation idéale de la connexion aux ressources internes du système.

Pour les connexions client aux nœuds de stockage, la limitation des connexions HTTP actives offre les avantages suivants :

- Permet un équilibrage de charge optimal sur l'ensemble du système StorageGRID.

  Avec le temps, une connexion HTTP peut ne plus être optimale à mesure que les exigences en matière d'équilibrage de charge évoluent. Le système offre son meilleur équilibrage de charge lorsque les applications clientes établissent une connexion HTTP distincte pour chaque transaction, mais cette méthode annule les gains précieux associés aux connexions persistantes.

- Permet aux applications clientes de diriger les transactions HTTP vers les services LDR disposant d'espace disponible.
- Permet de lancer 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 de Load Balancer, limiter la durée des connexions ouvertes peut être utile pour permettre à certaines procédures de maintenance de démarrer rapidement. Si la durée des connexions client n'est pas limitée, il peut s'écouler plusieurs minutes avant que les connexions actives ne soient automatiquement fermées.

Avantages des connexions HTTP simultanées

Il est conseillé de maintenir plusieurs connexions TCP/IP ouvertes vers le système StorageGRID afin de

permettre le traitement parallèle, ce qui améliore les performances. Le nombre optimal de connexions parallèles dépend de plusieurs facteurs.

Les connexions HTTP simultanées offrent les avantages suivants :

- Latence réduite

  Les transactions peuvent démarrer immédiatement au lieu d'attendre que d'autres transactions soient terminées.

- Débit accru

  Le système StorageGRID peut effectuer des transactions parallèles et augmenter le débit de transactions agrégé.

Les applications clientes doivent établir plusieurs connexions HTTP. Lorsqu'une application cliente doit effectuer une transaction, elle peut sélectionner et utiliser immédiatement toute connexion établie qui n'est pas en train de traiter une transaction.

La topologie de chaque système StorageGRID présente un débit de pointe différent pour les transactions et connexions simultanées. Le débit de pointe dépend des ressources de calcul, de réseau, de stockage, des liaisons WAN, ainsi que du nombre de serveurs, de services et d'applications que le système StorageGRID prend en charge.

Les systèmes StorageGRID prennent souvent en charge plusieurs applications clientes. Tenez-en compte lorsque vous déterminez le nombre maximal de connexions simultanées. Si l'application cliente est composée de plusieurs entités logicielles qui établissent chacune des connexions au système StorageGRID, additionnez toutes les connexions de ces entités. Vous devrez peut-être ajuster le nombre maximal de connexions simultanées dans les situations suivantes :

- La topologie du système StorageGRID influe sur le nombre maximal de transactions et de connexions simultanées que le système peut prendre en charge.
- Les applications clientes qui interagissent avec le système StorageGRID sur un réseau à bande passante limitée peuvent devoir réduire leur niveau de concurrence afin de garantir que chaque transaction soit effectuée dans un délai raisonnable.
- Lorsque de nombreuses applications clientes partagent le système StorageGRID, vous devrez peut-être réduire le degré de concurrence afin d'éviter de dépasser les limites du système.

Séparation des pools de connexions HTTP pour les opérations de lecture et d'écriture

Vous pouvez utiliser des pools distincts de connexions HTTP pour les opérations de lecture et d'écriture et contrôler la part de chaque pool à utiliser pour chacune. Des pools distincts de connexions HTTP vous permettent de mieux contrôler les transactions et d'équilibrer les charges.

Les applications clientes peuvent générer des charges à dominante récupération (lecture) ou à dominante stockage (écriture). Avec des pools distincts de connexions HTTP pour les transactions de lecture et d'écriture, vous pouvez ajuster la part de chaque pool à consacrer aux transactions de lecture ou d'écriture.

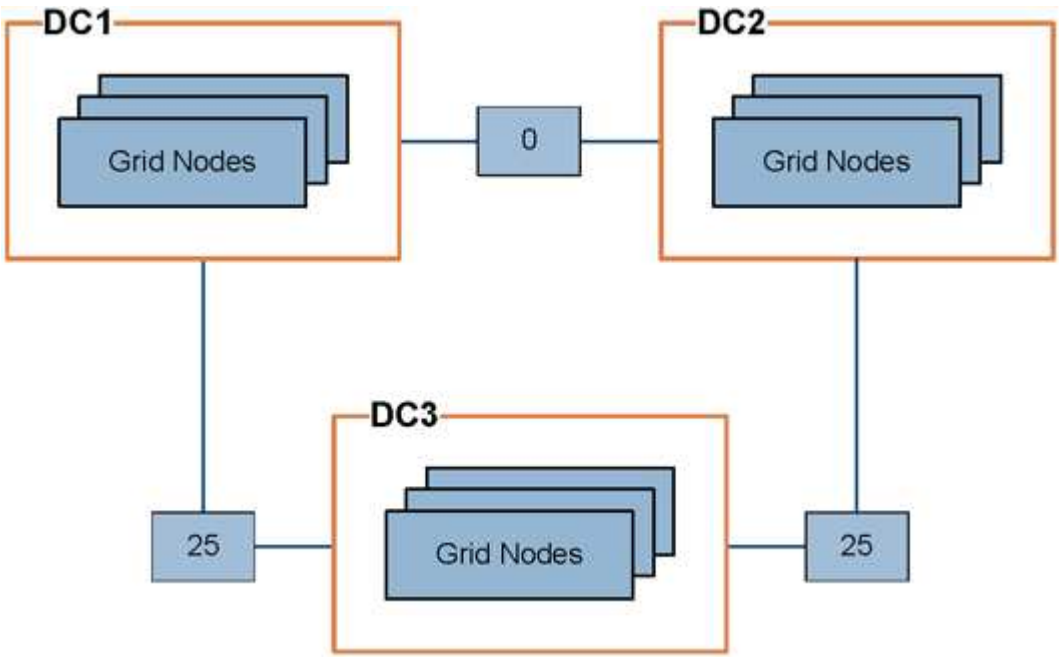
Gérer les coûts de liaison dans StorageGRID

Les coûts des liens vous permettent de prioriser le site de centre de données qui fournit un service demandé lorsque deux sites de centre de données ou plus existent. Vous pouvez ajuster les coûts des liens pour refléter la latence entre les sites.

Quels sont les coûts de liaison ?

- Les coûts des liens servent à déterminer quelle copie d'objet est utilisée pour effectuer les récupérations d'objet.
- Les coûts de liaison sont utilisés par l'API de gestion de la grille et l'API de gestion des locataires pour déterminer quels services internes StorageGRID utiliser.
- Le service d'équilibrage de charge utilise les coûts de liaison sur les nœuds d'administration et les nœuds de passerelle pour diriger les connexions client. Voir "Considérations relatives à l'équilibrage de charge".

Le diagramme montre une grille à trois sites avec des coûts de liaison configurés entre les sites :



- Le service d'équilibrage de charge sur les nœuds d'administration et les nœuds de passerelle répartit équitablement les connexions clientes entre tous les nœuds de stockage du même site de centre de données et tous les sites de centre de données dont le coût de liaison est de 0.

  Dans cet exemple, un nœud de passerelle du site de centre de données 1 (DC1) répartit équitablement les connexions client entre les nœuds de stockage de DC1 et les nœuds de stockage de DC2. Un nœud de passerelle de DC3 envoie les connexions client uniquement aux nœuds de stockage de DC3.

- Lors de la récupération d'un objet existant sous forme de plusieurs copies répliquées, StorageGRID récupère la copie située dans le centre de données dont le coût de liaison est le plus faible.

  Dans l'exemple, si une application cliente à DC2 récupère un objet qui est stocké à la fois à DC1 et à DC3, l'objet est récupéré depuis DC1, car le coût de liaison de DC1 à DC2 est de 0, ce qui est inférieur au coût de liaison de DC3 à DC2 (25).

Les coûts de liaison sont des valeurs relatives arbitraires sans unité de mesure spécifique. Par exemple, un coût de liaison de 50 est utilisé moins préférentiellement qu'un coût de 25. Le tableau présente les coûts de liaison les plus couramment utilisés.

Lien	Coût de liaison	Remarques
Entre les sites physiques des centres de données	25 (par défaut)	Centres de données connectés par une liaison WAN.
Entre sites de centres de données logiques situés au même emplacement physique	0	Centres de données logiques dans le même bâtiment ou campus physique connectés par un LAN.

Mettre à jour les coûts des liens

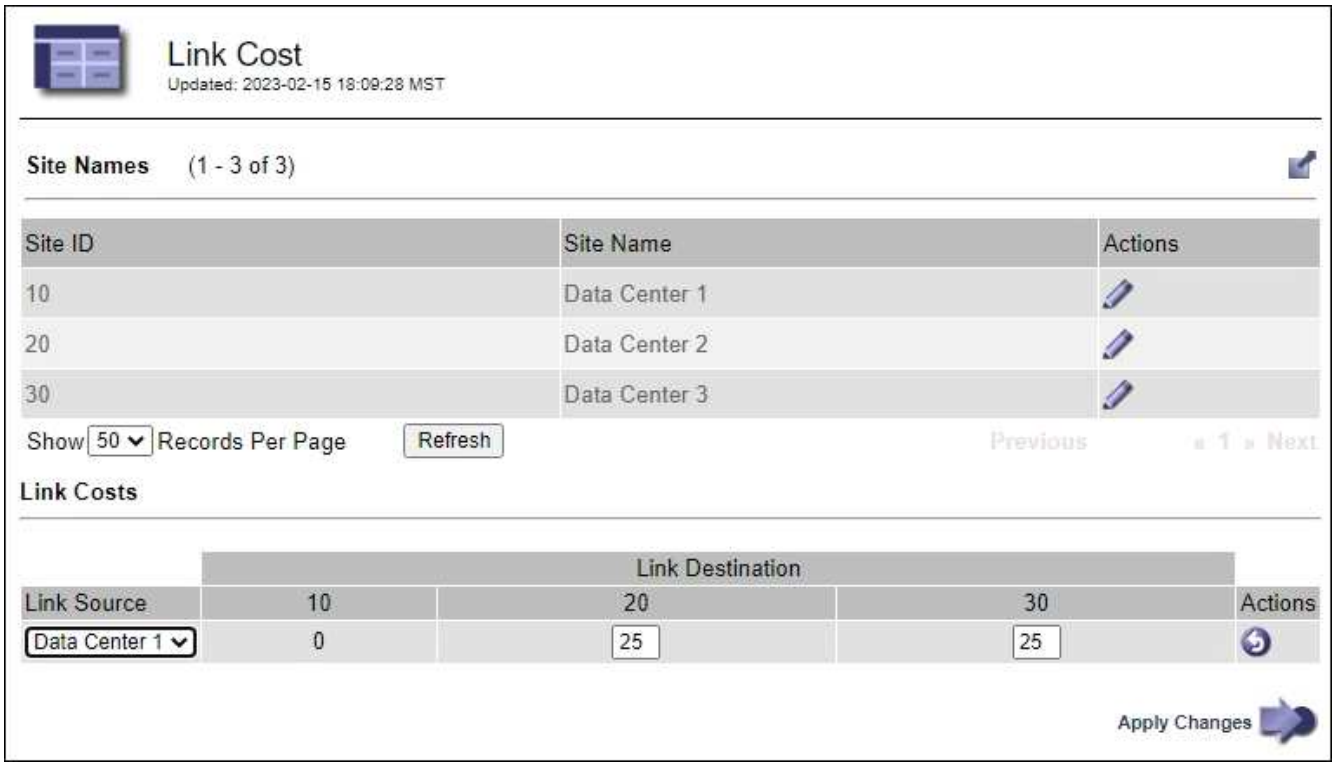
Vous pouvez mettre à jour les coûts de liaison entre les sites de centres de données pour refléter la latence entre les sites.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur Web pris en charge".
- Vous avez le "Autre autorisation de configuration de grille".

Étapes

1. Sélectionnez **Support** > **Other** > **Link cost**.



2. Sélectionnez un site sous **Source du lien** et saisissez une valeur de coût entre 0 et 100 sous **Destination du lien**.

   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**.

Utilisez AutoSupport

Découvrez AutoSupport dans StorageGRID

La fonctionnalité AutoSupport permet à StorageGRID d'envoyer des rapports d'état et de santé à l'assistance technique NetApp.

L'utilisation de AutoSupport aide à résoudre les problèmes plus rapidement. L'assistance technique peut surveiller les besoins de stockage de votre système et vous aider à déterminer si vous devez ajouter de nouveaux nœuds ou sites. En option, AutoSupport peut envoyer des paquets vers une destination supplémentaire.

StorageGRID propose deux types de AutoSupport :

- **StorageGRID AutoSupport** signale les problèmes logiciels de StorageGRID. Activé par défaut lors de la première installation de StorageGRID. Vous pouvez "modifiez la configuration AutoSupport par défaut" si nécessaire.

> Si StorageGRID AutoSupport n'est pas activé, un message s'affiche sur le tableau de bord du Grid Manager. Le message inclut un lien vers la page de configuration AutoSupport. Si vous fermez le message, il ne s'affichera plus tant que le cache de votre navigateur n'aura pas été vidé, même si AutoSupport reste désactivé.

- **Le matériel de l'appliance AutoSupport** signale des problèmes avec l'appliance StorageGRID. Vous devez "configurer le matériel AutoSupport sur chaque appareil".

Qu'est-ce que Active IQ ?

Active IQ est un conseiller numérique basé sur le cloud qui exploite l'analyse prédictive et l'expertise de la base installée de NetApp. Ses évaluations continues des risques, ses alertes prédictives, ses recommandations prescriptives et ses actions automatisées vous aident à prévenir les problèmes avant qu'ils ne surviennent, ce qui améliore la santé du système et augmente la disponibilité du système.

Si vous souhaitez utiliser les tableaux de bord et la fonctionnalité Active IQ sur le site d'assistance NetApp, vous devez activer AutoSupport.

"Documentation Active IQ Digital Advisor"

Informations incluses dans le package AutoSupport

Un paquet AutoSupport contient les fichiers et détails suivants.

Nom des fichiers	Champs	Description
AUTOSUPPORT-HISTORY.XML	AutoSupport Sequence Number + Destination for this AutoSupport + Statut de la livraison + Tentatives de livraison + AutoSupport Sujet + URI de livraison + Dernière erreur + AutoSupport PUT Nom du fichier + Heure de génération + Taille compressée Autosupport + Taille décompressée Autosupport + Durée totale de collecte (ms)	AutoSupport fichier historique.
AUTOSUPPORT.XML	Nœud + Protocole pour contacter le support + URL de support pour HTTP/HTTPS + Adresse de support + AutoSupport OnDemand État + AutoSupport OnDemand Server URL + AutoSupport OnDemand Polling Interval	Fichier d'état AutoSupport. Fournit des détails sur le protocole utilisé, l'URL et l'adresse du support technique, l'intervalle d'interrogation, et si OnDemand AutoSupport est activé ou désactivé.
BUCKETS.XML	ID du compartiment + ID du compte + Version de la build + Configuration des contraintes d'emplacement + Conformité activée + Configuration de la conformité + Verrouillage des objets S3 activé + Configuration du verrouillage des objets S3 + Configuration de la cohérence + CORS activé + Configuration CORS + Heure du dernier accès activée + Stratégie activée + Configuration de la stratégie + Notifications activées + Configuration des notifications + Cloud Mirror activé + Configuration de Cloud Mirror + Recherche activée + Configuration de la recherche + Étiquetage des compartiments activé + Configuration de l'étiquetage des compartiments + Configuration du versionnage	Fournit des détails de configuration et des statistiques au niveau du compartiment. Les configurations de compartiment incluent par exemple les services de plateforme, la conformité et la cohérence du compartiment.

Nom des fichiers	Champs	Description
GRID-CONFIGURATIONS.XML	ID de l'attribut + Nom de l'attribut + Valeur + Index + ID de la table + Nom de la table	Fichier d'informations de configuration à l'échelle de la grille. Contient des informations sur les certificats de la grille, l'espace réservé aux métadonnées, les paramètres de configuration à l'échelle de la grille (conformité, S3 Object Lock, compression d'objets, alertes, syslog et configuration ILM), les détails du profil de codage d'effacement, le nom DNS et "Nom NMS".
GRID-SPEC.XML	Spécifications de la grille, XML brut	Utilisé pour configurer et déployer StorageGRID. Contient les spécifications de la grille, l'adresse IP du serveur NTP, l'adresse IP du serveur DNS, la topologie du réseau et les profils matériels des nœuds.
GRID-TASKS.XML	Nœud + Chemin de service + ID d'attribut + Nom de l'attribut + Valeur + Index + ID de la table + Nom de la table	Fichier d'état des tâches de la grille (procédures de maintenance). Fournit des détails sur les tâches actives, terminées, achevées, ayant échoué et en attente de la grille.
GRID.JSON	Grille + Révision + Version du logiciel + Description + Licence + Mots de passe + DNS + NTP + Sites + Nœuds	Informations sur la grille.
ILM-CONFIGURATION.XML	ID de l'attribut + Nom de l'attribut + Valeur + Index + ID de la table + Nom de la table	Liste des attributs des configurations ILM.
ILM-STATUS.XML	Nœud + Chemin de service + ID d'attribut + Nom de l'attribut + Valeur + Index + ID de la table + Nom de la table	Fichier d'informations sur les métriques ILM. Contient les taux d'évaluation ILM pour chaque nœud et les métriques à l'échelle de la grille.
ILM.XML	XML brut ILM	Fichier de stratégie ILM active. Contient des informations détaillées sur les stratégies ILM actives, telles que l'ID du pool de stockage, le comportement d'ingestion, les filtres, les règles et la description.
LOG.TGZ	*n/a*	Fichier journal téléchargeable. Contient `bycast-err.log` et `servermanager.log` de chaque nœud.

Nom des fichiers	Champs	Description
MANIFEST.XML	Ordre de collecte + AutoSupport nom de fichier de contenu 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 + AutoSupport type de contenu pour ces données	Contient les métadonnées AutoSupport et de brèves descriptions de tous les fichiers AutoSupport.
NMS-ENTITIES.XML	Index d'attribut + OID d'entité + ID de nœud + ID de modèle de périphérique + Version de modèle de périphérique + Nom de l'entité	Les entités de groupe et de service dans le "Arbre NMS". Fournit des détails sur la topologie de la grille. Le nœud peut être déterminé en fonction des services exécutés sur le nœud.
OBJECTS-STATUS.XML	Nœud + Chemin de service + ID d'attribut + Nom de l'attribut + Valeur + Index + ID de la table + Nom de la table	État des objets, y compris l'état de l'analyse en arrière-plan, le transfert actif, le taux de transfert, le nombre total de transferts, le taux de suppression, les fragments corrompus, les objets perdus, les objets manquants, la réparation tentée, le taux d'analyse, la période d'analyse estimée et l'état d'achèvement de la réparation.
SERVER-STATUS.XML	Nœud + Chemin de service + ID d'attribut + Nom de l'attribut + Valeur + Index + ID de la table + Nom de la table	Configurations du serveur. Contient les détails suivants pour chaque nœud : type de plateforme, système d'exploitation, mémoire installée, mémoire disponible, connectivité de 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 électrique, taille du disque et type de disque.
SERVICE-STATUS.XML	Nœud + Chemin de service + ID d'attribut + Nom de l'attribut + Valeur + Index + ID de la table + Nom de la table	Fichier d'informations du nœud de service. Contient des détails tels que l'espace de table alloué, l'espace de table libre, les métriques Reaper de la base de données, la durée de réparation des segments, la durée des tâches de réparation, les redémarrages automatiques des tâches et l'arrêt automatique des tâches.

Nom des fichiers	Champs	Description
STORAGE-GRADES.XML	ID de niveau de stockage + Nom de niveau de stockage + ID du nœud de stockage + Chemin du nœud de stockage	Fichier de définitions de qualité de stockage pour chaque nœud de stockage.
SUMMARY-ATTRIBUTES.XML	OID du groupe + Chemin du groupe + ID de l'attribut de synthèse + Nom de l'attribut de synthèse + Valeur + Index + ID de la table + Nom de la table	Données d'état système de haut niveau récapitulant les informations d'utilisation de StorageGRID. Fournit des détails tels que le nom de la grille, les noms des sites, le nombre de nœuds de stockage par grille et par site, le type de licence, la capacité et l'utilisation de la licence, les conditions de support logiciel et les détails des opérations S3.
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 + Désactivé + Autres annotations + Autres étiquettes	Alertes système actuelles indiquant des problèmes potentiels dans le système StorageGRID.
USERAGENTS.XML	Agent utilisateur + Nombre de jours + Nombre total de requêtes HTTP + Nombre total d'octets ingérés + Nombre total d'octets récupérés + Requêtes PUT + Requêtes GET + Requêtes DELETE + Requêtes HEAD + Requêtes POST + Requêtes OPTIONS + Temps moyen de requête (ms) + Temps moyen de requête PUT (ms) + Temps moyen de requête GET (ms) + Temps moyen de requête DELETE (ms) + Temps moyen de requête HEAD (ms) + Temps moyen de requête POST (ms) + Temps moyen de requête OPTIONS (ms)	Statistiques basées sur les agents utilisateurs de l'application. Par exemple, le nombre d'opérations PUT/GET/DELETE/HEAD par agent utilisateur et la taille totale en octets de chaque opération.

Nom des fichiers	Champs	Description
X-HEADER-DATA	X-Netapp-asup-generated-on + X-Netapp-asup-hostname + X-Netapp-asup-os-version + X-Netapp-asup-serial-num + X-Netapp-asup-subject + X-Netapp-asup-system-id + X-Netapp-asup-model-name	AutoSupport Données d'en-tête.

Configurer AutoSupport dans StorageGRID

Par défaut, la fonctionnalité AutoSupport de StorageGRID est activée lors de la première installation de StorageGRID. Cependant, vous devez configurer le AutoSupport matériel sur chaque appliance. Au besoin, vous pouvez modifier la configuration AutoSupport.

Si vous souhaitez modifier la configuration de StorageGRID AutoSupport, effectuez vos modifications uniquement sur le nœud d'administration principal. Vous devez configurer le matériel AutoSupport sur chaque appliance.

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 root".
- Si vous utilisez HTTPS pour l'envoi de colis 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 "configuré un serveur proxy" pour transférer les packages AutoSupport en HTTPS. Les serveurs AutoSupport de NetApp rejetteront les packages envoyés via HTTP.
- Si vous utilisez SMTP comme protocole pour les paquets AutoSupport, vous avez configuré un serveur de messagerie SMTP.

À propos de cette tâche

Vous pouvez utiliser n'importe quelle combinaison des options suivantes pour envoyer des packages AutoSupport au support technique :

- **Hebdomadaire** : Envoyez automatiquement les packages AutoSupport une fois par semaine. Paramètre par défaut : Activé.
- **Déclenchement par événement** : Envoyez automatiquement des paquets AutoSupport toutes les heures ou lors d'événements système importants. Paramètre par défaut : Activé.
- **À la demande** : Autorise le support technique à demander à votre système StorageGRID d'envoyer automatiquement des packages AutoSupport, ce qui est utile lorsqu'ils traitent activement un problème (nécessite le protocole de transmission AutoSupport en HTTPS). Paramètre par défaut : Désactivé.
- **Déclenché par l'utilisateur** : Envoyez manuellement des packages AutoSupport à tout moment.
- **Collecte des journaux** : "Collecter manuellement les fichiers journaux et les données système et envoyer un colis AutoSupport".

Spécifiez le protocole pour les paquets 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 souhaitez activer la fonction AutoSupport on Demand, vous devez utiliser HTTPS.
- **HTTP** : si vous sélectionnez HTTP, vous devez configurer un serveur proxy pour transférer les packages AutoSupport en HTTPS. Les serveurs AutoSupport de NetApp rejettent les packages envoyés via HTTP. Ce protocole utilise le port 80.
- **SMTP** : Utilisez cette option si vous souhaitez que les packages AutoSupport soient envoyés par e-mail.

Le protocole que vous avez défini est utilisé pour l'envoi de tous les types de packages AutoSupport.

Étapes

1. Sélectionnez **Support** > **Outils** > **AutoSupport** > **Paramètres**.
2. Sélectionnez le protocole que vous souhaitez utiliser pour envoyer des paquets AutoSupport.
3. Si vous avez sélectionné **HTTPS**, indiquez si vous souhaitez utiliser un certificat de support NetApp (certificat TLS) pour sécuriser la connexion au serveur de support technique.
   - **Vérifier le certificat** (par défaut) : Garantit que la transmission des 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 du certificat, par exemple en cas de problème temporaire avec un certificat.
4. Sélectionnez **Enregistrer**. Tous les paquets hebdomadaires, déclenchés par l'utilisateur et déclenchés par un événement, sont envoyés en utilisant le protocole sélectionné.

Désactiver l'envoi hebdomadaire AutoSupport

Par défaut, le système StorageGRID est configuré pour envoyer un AutoSupport package au support technique une fois par semaine.

Pour déterminer quand le package hebdomadaire AutoSupport sera envoyé, allez dans l'onglet **AutoSupport** > **Results**. Dans la section **Weekly AutoSupport**, regardez la valeur de **Next Scheduled Time**.

Vous pouvez désactiver l'envoi automatique des packages hebdomadaires AutoSupport à tout moment.

Étapes

1. Sélectionnez **Support** > **Outils** > **AutoSupport** > **Paramètres**.
2. Décochez la case **Activer l'AutoSupport hebdomadaire**.
3. Sélectionnez **Enregistrer**.

Désactiver le déclenchement par événement AutoSupport

Par défaut, le système StorageGRID est configuré pour envoyer un paquet AutoSupport au support technique toutes les heures.

Vous pouvez désactiver le déclenchement par événement AutoSupport à tout moment.

Étapes

1. Sélectionnez **Support** > **Outils** > **AutoSupport** > **Paramètres**.

2. Décochez la case **Activer le déclenchement par événement AutoSupport**.
3. Sélectionnez **Enregistrer**.

Activez AutoSupport à la demande

AutoSupport on Demand peut aider à résoudre les problèmes sur lesquels le support technique travaille activement.

Par défaut, AutoSupport on Demand est désactivé. L'activation de cette fonctionnalité permet au support technique de demander à votre système StorageGRID d'envoyer automatiquement des packages AutoSupport. Le support technique peut également définir l'intervalle de temps d'interrogation pour les requêtes AutoSupport on Demand.

L'assistance technique ne peut pas activer ou désactiver AutoSupport on Demand.

Étapes

1. Sélectionnez **Support** > **Outils** > **AutoSupport** > **Paramètres**.
2. Sélectionnez **HTTPS** pour le protocole.
3. Cochez la case **Activer l'hebdomadaire AutoSupport**.
4. Cochez la case **Activer AutoSupport à la demande**.
5. Sélectionnez **Enregistrer**.

   AutoSupport on Demand est activé, et le support technique peut envoyer des requêtes AutoSupport on Demand à StorageGRID.

Désactiver la vérification 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 de mise à niveau StorageGRID.

Si nécessaire, vous pouvez désactiver la vérification des mises à jour logicielles. Par exemple, si votre système n'a pas d'accès WAN, vous devez désactiver la vérification afin d'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 paquets de santé et d'état sont envoyés au support technique. Vous pouvez spécifier une destination supplémentaire pour tous les paquets AutoSupport.

Pour vérifier ou modifier le protocole utilisé pour envoyer des paquets AutoSupport, consultez les instructions à spécifier le protocole pour les paquets AutoSupport.

> Vous ne pouvez pas utiliser le protocole SMTP pour envoyer des paquets AutoSupport vers une destination supplémentaire.

Étapes

1. Sélectionnez **Support** > **Outils** > **AutoSupport** > **Paramètres**.
2. Sélectionnez **Activer une destination AutoSupport supplémentaire**.
3. Spécifiez les éléments suivants :

   Nom d'hôte
   Le nom d'hôte ou l'adresse IP d'un serveur de destination AutoSupport supplémentaire.

   > Vous ne pouvez saisir qu'une seule destination supplémentaire.

   Port
   Le port utilisé pour se connecter à un serveur de destination AutoSupport supplémentaire. La valeur par défaut est le port 80 pour HTTP ou le port 443 pour HTTPS.

   Validation du certificat
   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 AutoSupport packages sans validation de certificat.

     Ne choisissez cette option que si vous avez une bonne raison de ne pas utiliser la validation des certificats, par exemple en cas de problème temporaire avec un certificat.

4. Si vous avez sélectionné **Vérifier le certificat**, procédez comme suit :
   a. Accédez à l'emplacement du certificat CA.
   b. Téléversez le fichier de certificat de l'autorité de certification.

   Les métadonnées du certificat d'autorité de certification apparaissent.

5. Sélectionnez **Enregistrer**.

   Tous les futurs colis AutoSupport hebdomadaires, déclenchés par des événements ou par l'utilisateur, seront envoyés à la destination supplémentaire.

Configurer AutoSupport pour les appareils

AutoSupport pour les appliances signale les problèmes matériels StorageGRID, et StorageGRID AutoSupport signale les problèmes logiciels StorageGRID, à une exception près : pour le SGF6112, StorageGRID AutoSupport signale à la fois les problèmes matériels et logiciels. Vous devez configurer AutoSupport sur chaque appliance, sauf le SGF6112 qui ne nécessite aucune configuration supplémentaire. AutoSupport est mis en œuvre différemment pour les appliances de services et les appliances de stockage.

Vous utilisez SANtricity pour activer AutoSupport pour chaque appliance de stockage. Vous pouvez configurer SANtricity AutoSupport lors de la configuration initiale de l'appliance ou après l'installation d'une appliance :

- Pour les appareils SG6000 et SG5700, "configurer AutoSupport dans SANtricity System Manager"

AutoSupport packages 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 les problèmes matériels, tels que les défaillances des modules DIMM ou des cartes d'interface d'hôte (HIC). Cependant, certaines pannes de composants peuvent déclencher "alertes matérielles". Pour les appliances StorageGRID équipées d'un contrôleur de gestion de carte mère (BMC), vous pouvez configurer l'envoi d'e-mails et de traps SNMP pour signaler les pannes matérielles.

- "Configurer les notifications par e-mail pour les alertes BMC"
- "Configurer les paramètres SNMP pour BMC"

Informations connexes

"Support NetApp"

Déclencher manuellement un AutoSupport package dans StorageGRID

Pour aider le support technique à résoudre les problèmes liés à votre système StorageGRID, vous pouvez déclencher manuellement l'envoi d'un package AutoSupport.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur Web pris en charge".
- Vous disposez de l'accès racine ou de l'autorisation de configuration de grille.

Étapes

1. Sélectionnez **Support** > **Tools** > **AutoSupport**.
2. Dans l'onglet **Actions**, sélectionnez **Envoyer AutoSupport déclenché par l'utilisateur**.

   StorageGRID tente d'envoyer un paquet AutoSupport au site de support NetApp. En cas de succès, les valeurs **Résultat le plus récent** et **Dernière tentative réussie** de l'onglet **Résultats** sont mises à jour. En cas de problème, la valeur **Résultat le plus récent** passe à « Échec », et StorageGRID n'essaie pas de renvoyer le paquet AutoSupport.

3. Au bout d'une minute, actualisez la page AutoSupport dans votre navigateur pour accéder aux résultats les plus récents.

> De plus, vous pouvez "collecter des fichiers journaux et des données système plus étendus" et les envoyer au site d'assistance NetApp.

Dépanner les packages AutoSupport de StorageGRID

Si une tentative d'envoi d'un package AutoSupport échoue, le système StorageGRID prend différentes mesures selon le type de package AutoSupport. Vous pouvez vérifier l'état des packages AutoSupport en sélectionnant **Support** > **Outils** > **AutoSupport** > **Résultats**.

Lorsque le package AutoSupport ne parvient pas à être envoyé, « Échec » apparaît dans l'onglet **Résultats** de la page **AutoSupport**.

> Si vous avez configuré un serveur proxy pour transférer les paquets AutoSupport à NetApp, vous devriez "vérifiez que les paramètres de configuration du serveur proxy sont corrects".

Échec du package AutoSupport hebdomadaire

Si un colis hebdomadaire AutoSupport échoue à être envoyé, le système StorageGRID prend les mesures suivantes :

1. Met à jour l'attribut « Most Recent Result » sur « Retrying ».
2. Tente de renvoyer le colis AutoSupport 15 fois toutes les quatre minutes pendant une heure.
3. Après une heure d'échecs d'envoi, met à jour l'attribut « Résultat le plus récent » sur Échec.
4. Tente d'envoyer à nouveau un colis AutoSupport à l'heure prévue suivante.
5. Maintient le calendrier régulier AutoSupport si l'envoi du package échoue en raison de l'indisponibilité du service NMS, et si un package est envoyé avant que sept jours ne se soient écoulés.
6. Lorsque le service NMS sera de nouveau disponible, envoie immédiatement un package AutoSupport si aucun package n'a été envoyé depuis sept jours ou plus.

Échec du paquet AutoSupport déclenché par l'utilisateur ou par un événement

Si l'envoi d'un paquet AutoSupport déclenché par l'utilisateur ou par un événement échoue, 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 les paramètres de configuration de messagerie corrects, l'erreur suivante s'affiche : `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. N'essaie pas de renvoyer le package.
3. Consigne l'erreur dans `nms.log`.

En cas d'échec et si le protocole SMTP est 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** > **Alarms (legacy)** > **Legacy Email Setup**). 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".

Corriger une défaillance de package AutoSupport

En cas d'échec et si le protocole SMTP est 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 les packages AutoSupport E-Series SANtricity System Manager au support technique via un nœud d'administration StorageGRID plutôt que via le port de gestion de l'appliance de stockage.

Consultez "Matériel E-Series AutoSupport" pour plus d'informations sur l'utilisation de AutoSupport avec les appliances E-Series.

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 administrateur ou Root pour un périphérique de stockage".
- Vous avez configuré SANtricity AutoSupport :
  - Pour les appareils SG6000 et SG5700, "configurer AutoSupport dans SANtricity System Manager"

> Vous devez disposer du firmware SANtricity 8.70 ou supérieur pour accéder à SANtricity System Manager à l'aide de Grid Manager.

À propos de cette tâche

Les packages AutoSupport de la série E contiennent des détails sur le matériel de stockage et sont plus spécifiques que les autres packages AutoSupport envoyés par le système StorageGRID.

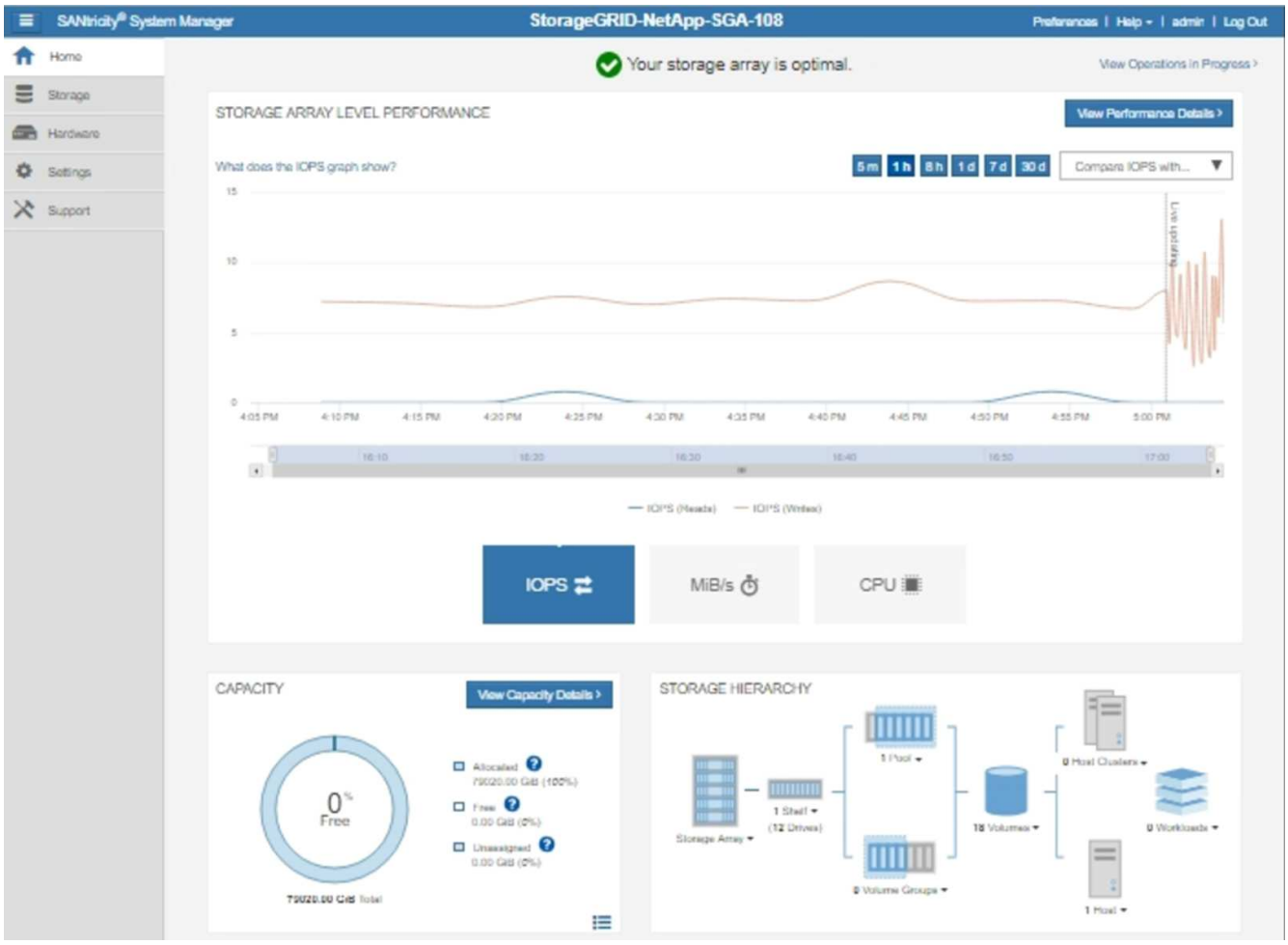
Vous pouvez configurer une adresse de serveur proxy spéciale dans SANtricity System Manager pour transmettre des paquets AutoSupport via un nœud d'administration StorageGRID sans utiliser le port de gestion de l'appliance. Les paquets AutoSupport transmis de cette manière sont envoyés par le "Nœud d'administration de l'expéditeur préféré" et utilisent tous les "paramètres proxy d'administration" qui ont été configurés dans Grid Manager.

> 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 "NetApp Documentation E-Series et SANtricity".

Étapes

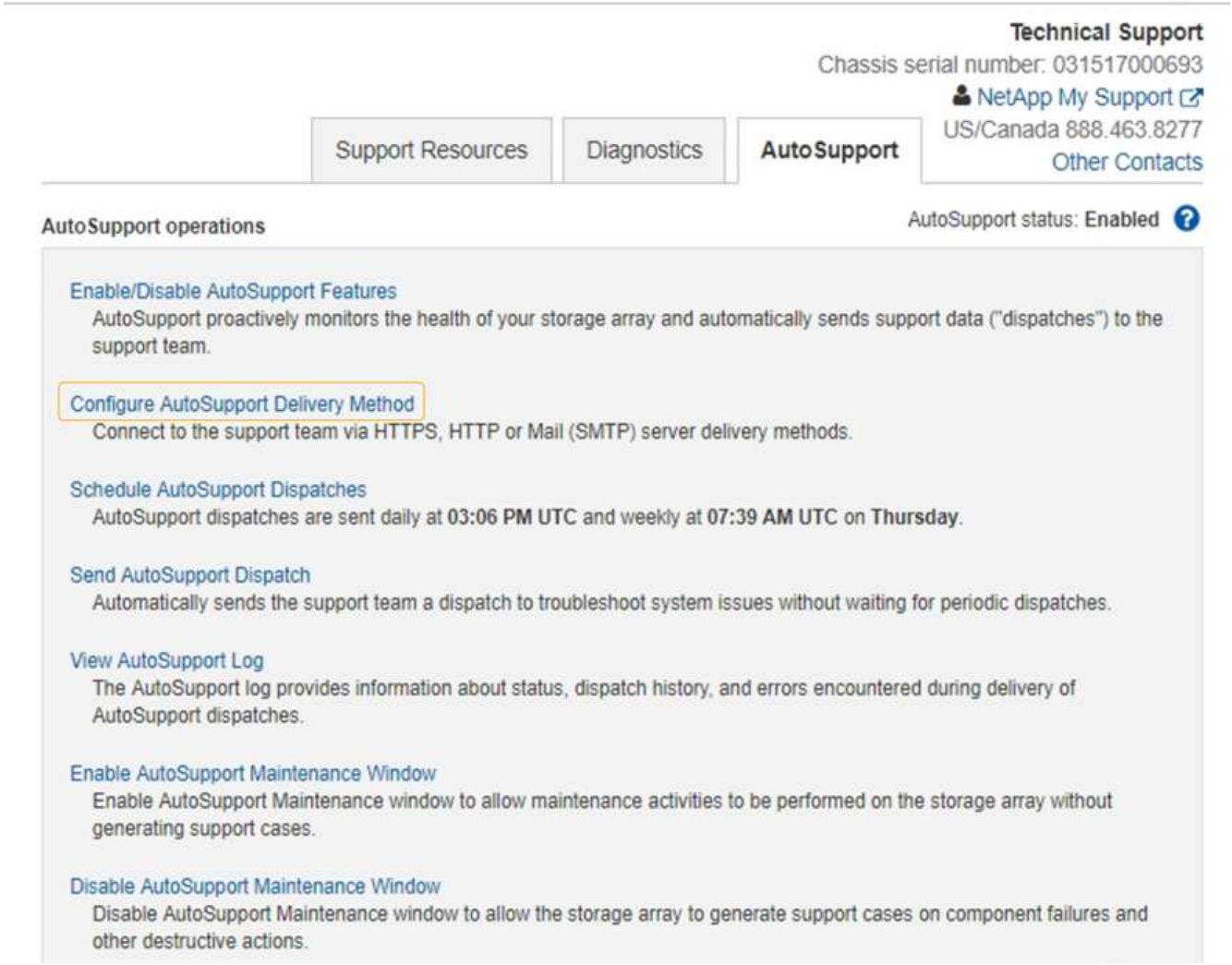
1. Dans le Gestionnaire de grille, sélectionnez **Nœuds**.
2. Dans la liste des nœuds à gauche, sélectionnez le nœud de l'appliance de stockage que vous souhaitez configurer.
3. Sélectionnez **SANtricity System Manager**.

   La page d'accueil de SANtricity System Manager s'affiche.



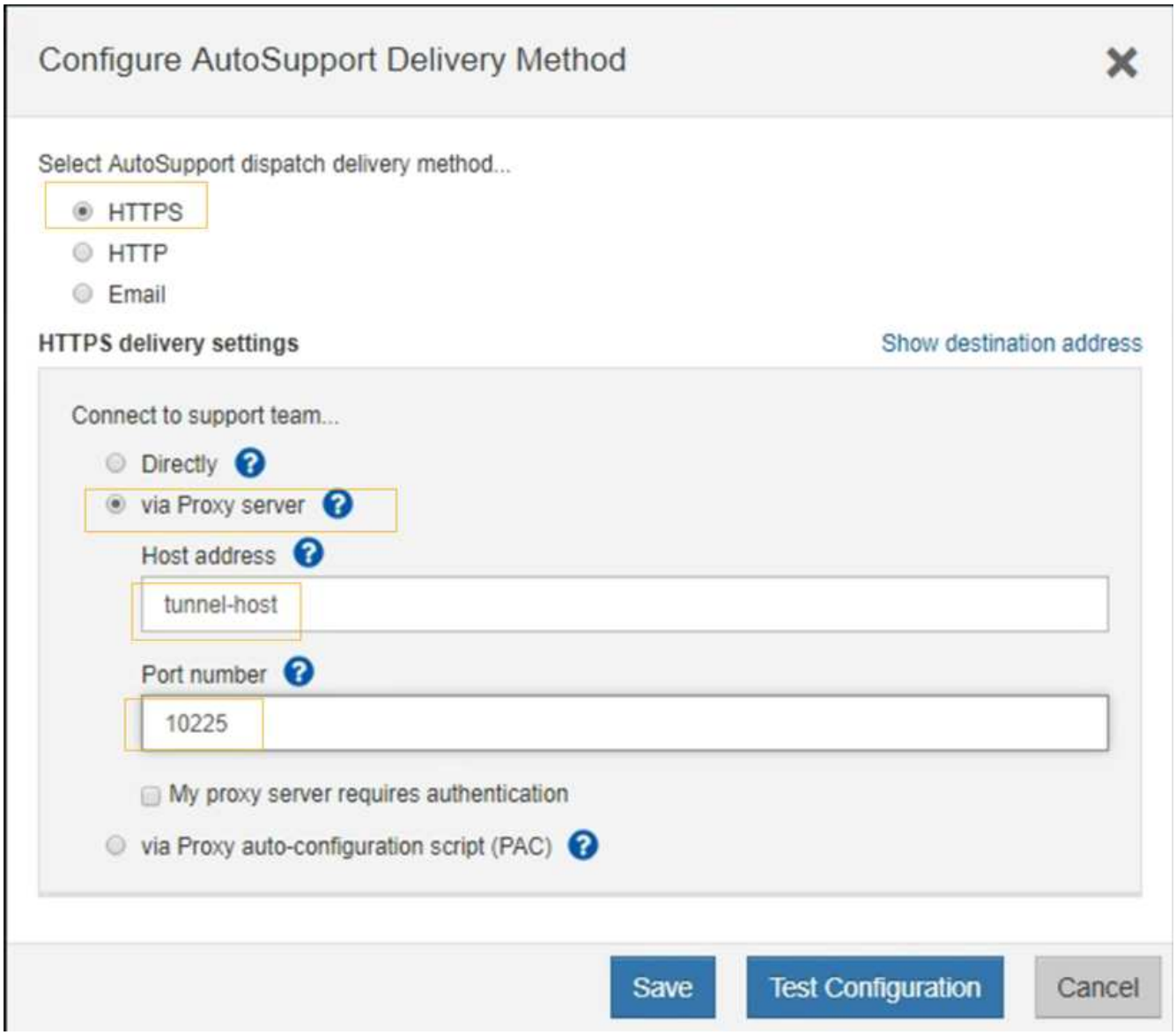
4. Sélectionnez **Support** > **Support center** > **AutoSupport**.

   La page des opérations AutoSupport s’affiche.



5. Sélectionnez **Configurer AutoSupport Delivery Method**.

   La page Configurer la méthode de livraison AutoSupport s'affiche.



6. Sélectionnez **HTTPS** comme méthode de livraison.

   Le certificat qui active le protocole HTTPS est préinstallé.

7. Sélectionnez **via Proxy server**.
8. Saisissez `tunnel-host` pour l'adresse de l'hôte.

   `tunnel-host` est l'adresse spéciale à utiliser avec un nœud d'administration pour envoyer des packages AutoSupport E-Series.

9. Saisissez `10225` pour le **numéro de port**.

   `10225` correspond au numéro de port sur le serveur proxy StorageGRID qui reçoit les paquets AutoSupport du contrôleur E-Series dans l'appliance.

10. Sélectionnez **Tester la configuration** pour tester le routage et la configuration de votre serveur proxy AutoSupport.

Si la configuration est correcte, un message apparaît dans une bannière verte : « Votre AutoSupport configuration a été vérifiée. »

Si le test échoue, un message d'erreur s'affiche dans une bannière rouge. Vérifiez vos paramètres DNS et réseau StorageGRID, assurez-vous que "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 apparaît : « AutoSupport delivery method a été configuré. »

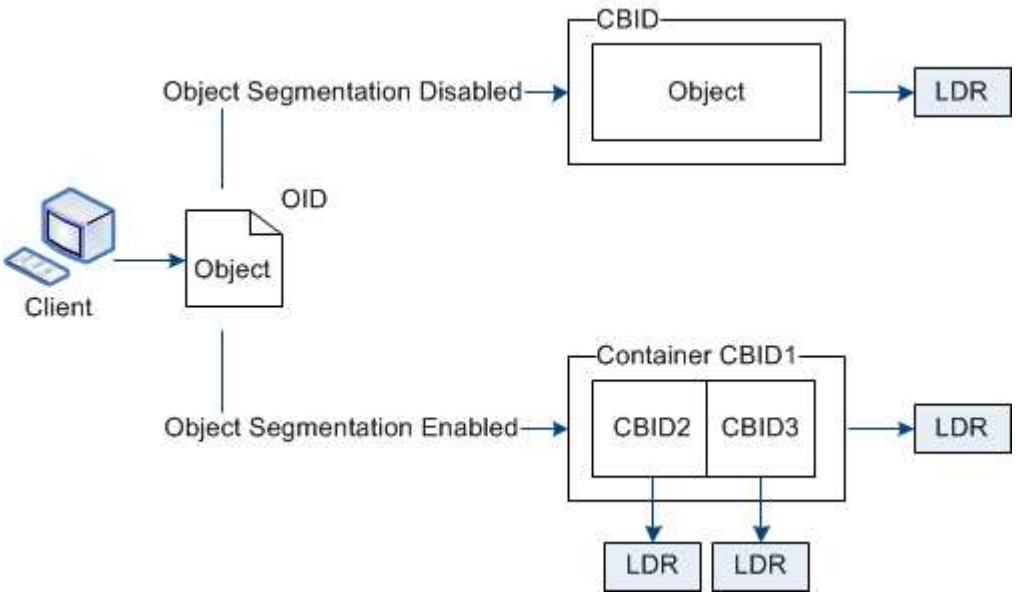
Gérer les nœuds de stockage

Utilisez les options de stockage

Découvrez la segmentation des objets dans StorageGRID

La segmentation d'objets consiste à diviser un objet en une collection d'objets plus petits et de taille fixe afin d'optimiser le stockage et l'utilisation des ressources pour les objets volumineux. Le chargement multipartie S3 crée également des objets segmentés, chaque partie étant représentée par un objet.

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 comme contenu.



Lors de la récupération d'un conteneur de segment, le service LDR assemble l'objet d'origine à partir de ses segments et renvoie l'objet au client.

Le conteneur et les segments ne sont pas nécessairement stockés sur le même nœud de stockage. Le conteneur et les segments peuvent être stockés sur n'importe quel nœud de stockage du pool de stockage spécifié dans la règle ILM.

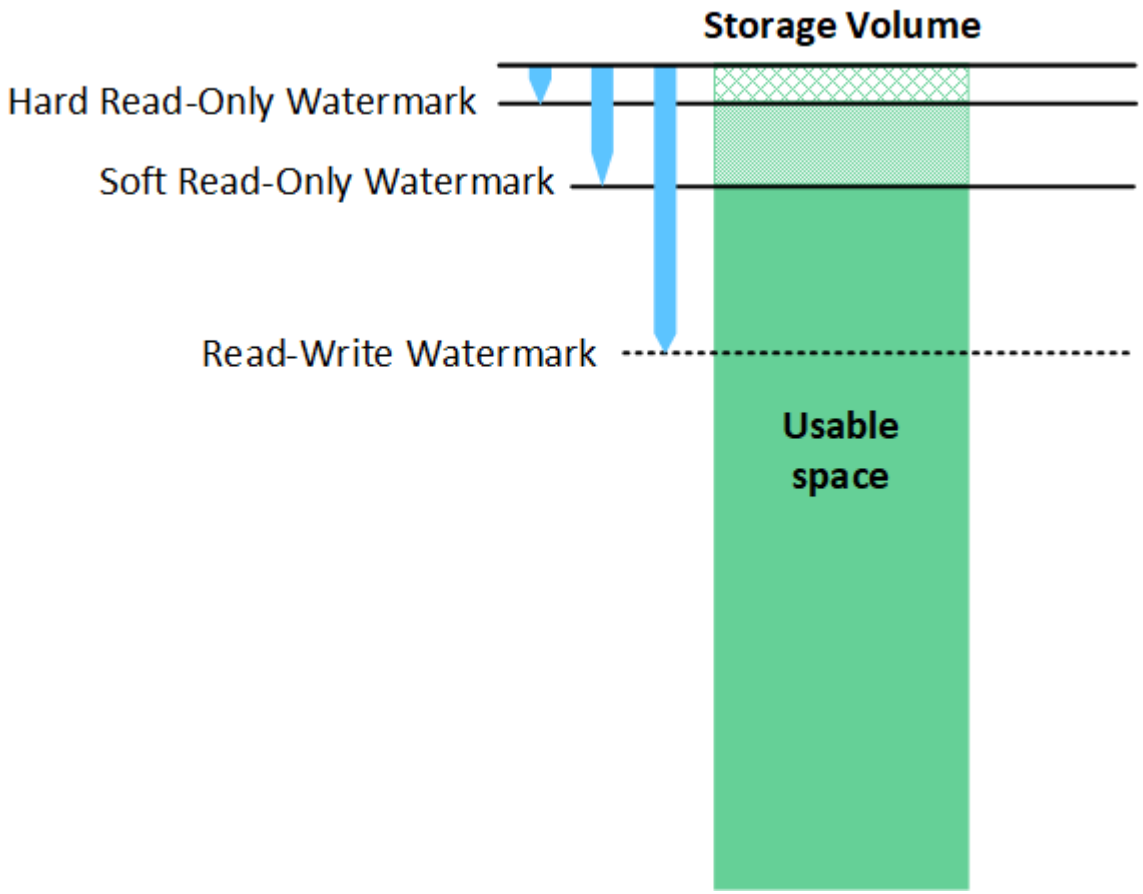
Chaque segment est traité indépendamment par le système StorageGRID et contribue au décompte d'attributs

tels que les objets gérés et les objets stockés. Par exemple, si un objet stocké dans le système StorageGRID est divisé en deux segments, la valeur des objets gérés augmente de trois une fois l'ingestion terminée, comme suit :

```
segment container + segment 1 + segment 2 = three stored objects
```

Découvrez les seuils de volume de stockage dans StorageGRID

StorageGRID utilise trois marques de volume de stockage pour garantir que les nœuds de stockage passent en toute sécurité en état de lecture seule avant qu'ils n'atteignent un niveau d'espace critique et pour permettre aux nœuds de stockage qui ont été transférés en état de lecture seule de redevenir en lecture-écriture.



> Les filigranes de volume de stockage s'appliquent uniquement à l'espace utilisé pour les données d'objets répliquées et codées par effacement. Pour en savoir plus sur l'espace réservé aux métadonnées des objets sur le volume 0, accédez à "Gérer le stockage des métadonnées des objets".

Qu'est-ce que le filigrane souple en lecture seule ?

Le **filigrane de lecture seule logicielle du volume de stockage** est le premier filigrane indiquant que l'espace utilisable d'un nœud de stockage pour les données d'objet est en train de se remplir.

Si l'espace libre de chaque volume d'un nœud de stockage est inférieur au seuil de 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 de lecture seule au reste du système StorageGRID, mais traite toutes les

requêtes d'écriture en attente.

Par exemple, supposons que chaque volume d'un Storage Node possède un seuil de lecture seule souple de 10 Go. Dès que chaque volume dispose de moins de 10 Go d'espace libre, le Storage Node passe en mode lecture seule souple.

Qu'est-ce que le seuil en lecture seule strict ?

Le **filigrane de lecture seule du volume de stockage** est le prochain filigrane indiquant que l'espace utilisable d'un nœud pour les données d'objet est en train de se remplir.

Si l'espace libre sur un volume est inférieur au seuil strict de lecture seule de ce volume, les écritures sur ce 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 leur seuil strict de lecture seule.

Par exemple, supposons que chaque volume d'un Storage Node possède une limite de lecture seule de 5 Go. Dès que l'espace libre de chaque volume descend en dessous de 5 Go, le Storage Node n'accepte plus aucune requête d'écriture.

Le filigrane en lecture seule physique est toujours inférieur au filigrane en lecture seule logicielle.

Qu'est-ce qu'un watermark de lecture-écriture ?

Le **filigrane de lecture-écriture du volume de stockage** s'applique uniquement aux nœuds de stockage qui sont passés en mode lecture seule. Il détermine à quel moment le nœud peut repasser en mode lecture-écriture. Lorsque l'espace libre sur l'un des volumes de stockage d'un nœud de stockage est supérieur au filigrane de lecture-écriture de ce volume, le nœud repasse automatiquement à l'état de lecture-écriture.

Par exemple, supposons que le nœud de stockage soit passé en mode lecture seule. Supposons également que chaque volume ait une limite de lecture/écriture de 30 Go. Dès que l'espace libre d'un volume atteint 30 Go, le nœud repasse en mode lecture/écriture.

Le filigrane de lecture-écriture est toujours plus grand que le filigrane de lecture seule souple et que le filigrane de lecture seule rigide.

Afficher les filigranes de volume de stockage

Vous pouvez consulter les paramètres actuels du filigrane et les valeurs optimisées par le système. Si les filigranes optimisés ne sont pas utilisés, vous pouvez déterminer si vous pouvez ou devez ajuster les paramètres.

Avant de commencer

- Vous avez terminé la mise à niveau vers StorageGRID 11.6 ou une version supérieure.
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur Web pris en charge".
- Vous avez le "Autorisation d'accès root".

Afficher les paramètres de filigrane actuels

Vous pouvez consulter les paramètres actuels de filigrane de stockage dans le Grid Manager.

Étapes

1. Sélectionnez **Support** > **Other** > **Storage watermarks**.
2. Sur la page des filigranes de stockage, regardez la case à cocher Utiliser les valeurs optimisées.

- Si la 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 paramétrage par défaut et recommandé. Ne modifiez pas ces valeurs. Vous pouvez éventuellement Afficher les seuils 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. Utilisez les instructions pour "Dépannage des alertes de remplacement du seuil bas en lecture seule" déterminer si vous pouvez ou devez ajuster les paramètres.

  Lorsque vous spécifiez des paramètres de filigrane personnalisés, vous devez saisir des valeurs supérieures à 0.

Afficher les filigranes de stockage optimisés

StorageGRID utilise deux métriques Prometheus pour afficher les valeurs optimisées qu'il a calculées pour le filigrane de lecture seule logicielle du volume de stockage. Vous pouvez consulter les valeurs minimales et maximales optimisées pour chaque nœud de stockage dans votre grid.

1. Sélectionnez **Support** > **Tools** > **Metrics**.
2. Dans la section Prometheus, sélectionnez le lien pour accéder à l'interface utilisateur de Prometheus.
3. Pour afficher le filigrane minimal recommandé en lecture seule, saisissez la métrique Prometheus suivante et sélectionnez **Exécuter** :

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   La dernière colonne indique la valeur minimale optimisée du seuil de lecture seule souple pour tous les volumes de stockage sur chaque Storage Node. Si cette valeur est supérieure au paramètre personnalisé du seuil de lecture seule souple du volume de stockage, l'alerte **Low read-only watermark override** est déclenchée pour le Storage Node.

4. Pour afficher la valeur maximale recommandée du filigrane souple en lecture seule, saisissez la métrique Prometheus suivante et sélectionnez **Exécuter** :

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   La dernière colonne indique la valeur optimisée maximale du filigrane de lecture seule souple pour tous les volumes de stockage sur chaque Storage Node.

Gérez le stockage des métadonnées des objets dans StorageGRID

La capacité de métadonnées des objets d'un système StorageGRID contrôle le nombre maximal d'objets pouvant être stockés sur ce système. Pour garantir que votre système StorageGRID dispose d'un espace suffisant pour stocker de nouveaux objets, vous devez comprendre où et comment StorageGRID stocke les métadonnées des objets.

Que sont les métadonnées d'un objet ?

Les métadonnées d'objet sont toutes les informations qui décrivent un objet. StorageGRID utilise les métadonnées d'objet pour suivre l'emplacement de tous les objets sur la grille et gérer le cycle de vie de chaque objet au fil du temps.

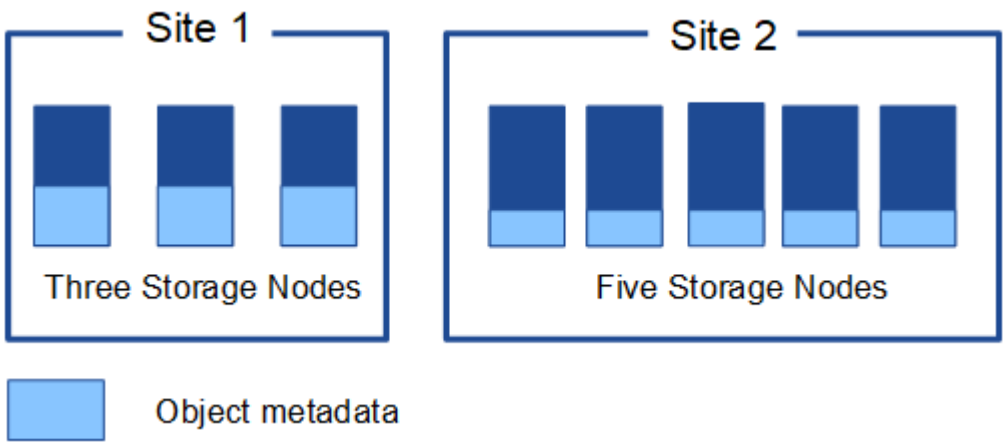
Pour un objet dans StorageGRID, les métadonnées de l'objet comprennent les types d'informations suivants :

- Métadonnées système, y compris un identifiant unique pour chaque objet (UUID), le nom de l'objet, le nom du compartiment S3, le nom ou l'identifiant du compte du locataire, la taille logique de l'objet, la date et l'heure de la première création de l'objet, et la date et l'heure de la dernière modification de l'objet.
- Toutes les paires clé-valeur de métadonnées utilisateur personnalisées associées à l'objet.
- Pour les objets S3, toutes les paires clé-valeur d'étiquette d'objet associées à l'objet.
- Pour les copies d'objets répliquées, l'emplacement de stockage actuel de chaque copie.
- Pour les copies d'objets codées par effacement, l'emplacement de stockage actuel de chaque fragment.
- Pour les copies d'objets dans un Cloud Storage Pool, l'emplacement de l'objet, y compris le nom du bucket externe et l'identifiant unique de l'objet.
- Pour les objets segmentés et les objets multipart, identifiants de segment et tailles de données.

Comment les métadonnées des objets sont-elles stockées ?

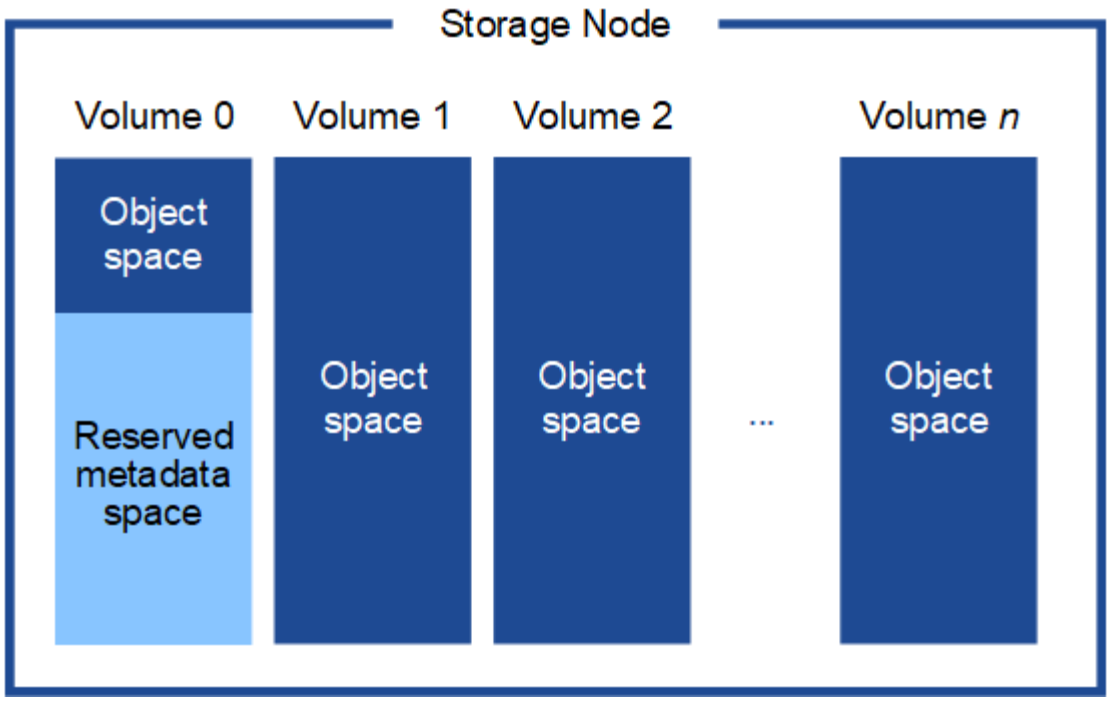
StorageGRID gère les métadonnées des objets dans une base de données Cassandra, qui est stockée indépendamment des données des objets. Afin d'assurer la redondance et de protéger les métadonnées des objets contre toute perte, StorageGRID conserve trois copies des métadonnées de tous les objets du système sur chaque site.

Cette figure représente les nœuds de stockage de deux sites. Chaque site possède la même quantité de métadonnées d'objets, et les métadonnées de chaque site sont subdivisées entre tous les nœuds de stockage de ce site.



Où sont stockées les métadonnées des objets ?

Cette figure représente les volumes de stockage d'un seul nœud de stockage.



Comme illustré dans la figure, StorageGRID réserve de l'espace pour les métadonnées des objets sur le volume de stockage 0 de chaque nœud de stockage. Il utilise cet espace réservé pour stocker les métadonnées des objets et effectuer des opérations essentielles sur la base de données. Tout espace restant sur le volume de stockage 0 ainsi que sur tous les autres volumes de stockage du nœud de stockage est utilisé exclusivement pour les données des objets (copies répliquées et fragments à codage d'effacement).

La quantité d'espace réservée aux métadonnées des objets sur un nœud de stockage particulier dépend de plusieurs facteurs, qui sont décrits ci-dessous.

Paramètre d'espace réservé aux métadonnées

L'*espace réservé aux métadonnées* est un paramètre à l'échelle du système qui représente la quantité d'espace qui sera réservée aux métadonnées sur le volume 0 de chaque Storage Node. Comme le montre le tableau, la valeur par défaut de ce paramètre est basée sur :

- La version du logiciel que vous utilisiez lors de l'installation initiale de StorageGRID.
- La quantité de RAM sur chaque nœud de stockage.

Version utilisée pour l'installation initiale de StorageGRID	Quantité de RAM sur les nœuds de stockage	Paramètre d'espace réservé aux métadonnées par défaut
11,5 à 12,0	128 Go ou plus sur chaque nœud de stockage de la grille	8 To (8 000 Go)
	Moins de 128 Go sur n'importe quel nœud de stockage du grid	3 To (3 000 Go)
11,1 à 11,4	128 Go ou plus sur chaque nœud de stockage sur un même site	4 To (4 000 Go)

Version utilisée pour l'installation initiale de StorageGRID	Quantité de RAM sur les nœuds de stockage	Paramètre d'espace réservé aux métadonnées par défaut
	Moins de 128 Go sur tout nœud de stockage à chaque site	3 To (3 000 Go)
11.0 ou version antérieure	N'importe quel montant	2 To (2 000 Go)

Afficher le paramètre d'espace réservé pour les métadonnées

Suivez ces étapes pour afficher le paramètre d'espace réservé aux métadonnées de votre système StorageGRID.

Étapes

1. Sélectionnez **Configuration** > **Système** > **Paramètres de stockage**.
2. Sur la page des paramètres de stockage, développez la section **Espace réservé aux métadonnées**.

Pour StorageGRID 11.8 ou supérieur, la valeur de l'espace réservé aux métadonnées doit être d'au moins 100 Go et d'au plus 1 Po.

La configuration par défaut pour une nouvelle installation StorageGRID 11.6 ou supérieure dans laquelle chaque nœud de stockage dispose de 128 Go ou plus de RAM est de 8 000 Go (8 To).

Espace réellement réservé aux métadonnées

Contrairement au paramètre d'espace réservé aux métadonnées à l'échelle du système, l'espace réellement réservé aux métadonnées des objets est déterminé pour chaque nœud de stockage. Pour un nœud de stockage donné, l'espace réellement réservé aux métadonnées dépend de la taille du volume 0 de ce nœud et du paramètre d'espace réservé aux métadonnées à l'échelle du système.

Taille du volume 0 pour le nœud	Espace réellement réservé aux métadonnées
Moins de 500 Go (utilisation hors production)	10% du volume 0
500 Go ou plus + ou + Nœuds de stockage uniquement pour les métadonnées	La plus petite de ces valeurs : • Volume 0 • Paramètre d'espace réservé aux métadonnées **Remarque** : Un seul rangedb est requis pour les nœuds de stockage uniquement de métadonnées.

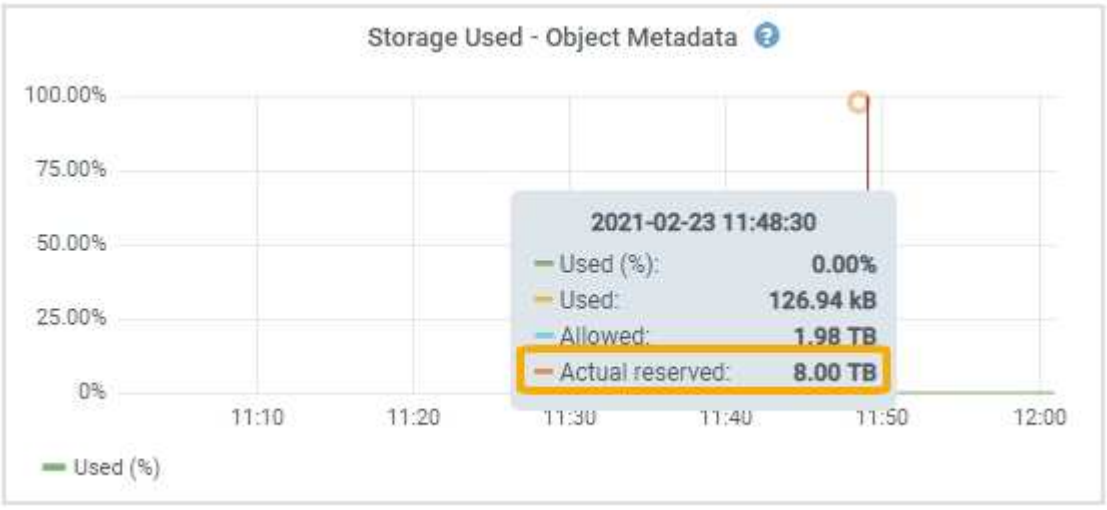
Afficher l'espace réellement réservé aux métadonnées

Suivez ces étapes pour afficher l'espace réellement réservé aux métadonnées sur un nœud de stockage particulier.

Étapes

1. Dans le Grid Manager, sélectionnez **Nœuds** > ***Storage Node***.

2. Sélectionnez l'onglet **Storage**.
3. Placez votre curseur sur le graphique « Storage Used - Object Metadata » et repérez la valeur **Actual reserved**.



Sur la capture d'écran, la valeur **Réservé réel** est de 8 To. Cette capture d'écran concerne un grand Storage Node dans une nouvelle installation StorageGRID 11.6. Parce que le paramètre d'espace réservé aux métadonnées à l'échelle du système est inférieur au volume 0 pour ce Storage Node, l'espace réellement réservé pour ce nœud est égal au paramètre d'espace réservé aux métadonnées.

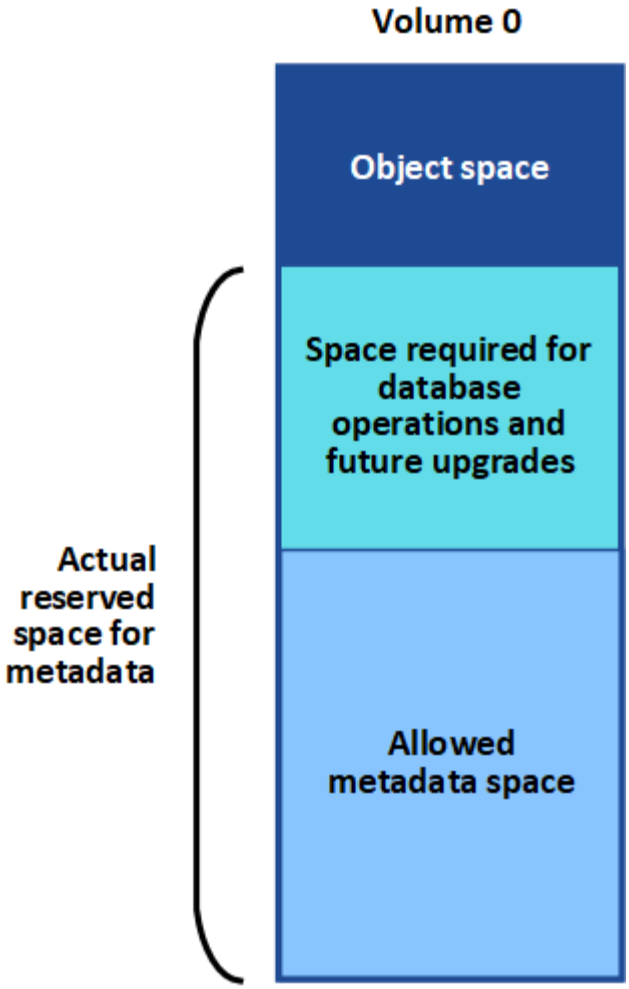
Exemple d'espace de métadonnées réellement réservé

Supposons que vous installiez un nouveau système StorageGRID en utilisant la version 11.7 ou ultérieure. Dans cet exemple, supposez que chaque nœud de stockage dispose de plus de 128 Go de RAM et que le volume 0 du nœud de stockage 1 (SN1) fait 6 To. Sur la base de ces valeurs :

- L'espace réservé aux métadonnées à l'échelle du système est fixé à 8 To. (Il s'agit de la valeur par défaut pour une nouvelle installation StorageGRID 11.6 ou supérieure si chaque nœud de stockage dispose de plus de 128 Go de RAM.)
- L'espace réellement réservé aux métadonnées pour SN1 est de 6 To. (Le volume entier est réservé car le volume 0 est plus petit que le paramètre **Espace réservé aux métadonnées**.)

Espace autorisé pour les métadonnées

L'espace réservé aux métadonnées de chaque nœud de stockage est subdivisé en l'espace disponible pour les métadonnées des objets (l'espace autorisé pour les métadonnées) et l'espace requis pour les opérations essentielles de la base de données (telles que la compaction et la réparation) ainsi que pour les futures mises à niveau matérielles et logicielles. L'espace autorisé pour les métadonnées 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 réellement réservé aux métadonnées.

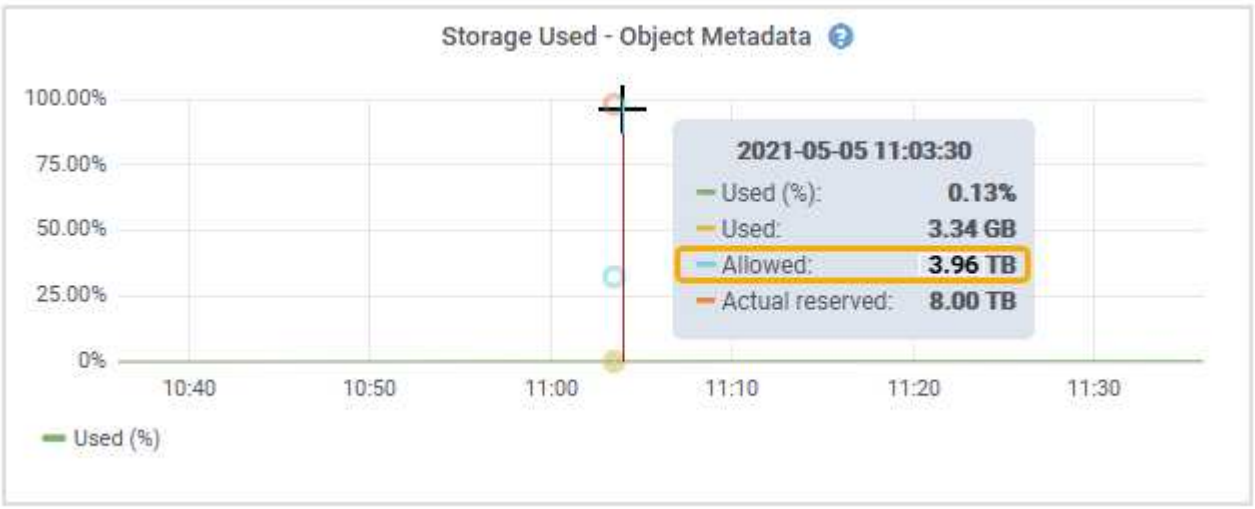
		Quantité de mémoire sur le nœud de stockage	
	< 128 Go	≥ 128 Go	**Espace réellement réservé aux métadonnées**
⇐ 4 To	60 % de l'espace réellement réservé aux métadonnées, jusqu'à un maximum de 1,32 To	60 % de l'espace réellement réservé aux métadonnées, jusqu'à un maximum de 1,98 To	4 To

Afficher l'espace de métadonnées autorisé

Suivez ces étapes pour afficher l'espace de métadonnées autorisé pour un Storage Node.

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **Nœuds**.
2. Sélectionnez le nœud de stockage.
3. Sélectionnez l'onglet **Storage**.
4. Placez votre curseur sur le graphique « Storage used - object metadata » et repérez la valeur **Allowed**.



Sur la capture d'écran, la valeur **Autorisée** est de 3,96 To, ce qui correspond à la valeur maximale pour un Storage Node dont l'espace réellement réservé aux métadonnées est supérieur à 4 To.

La valeur **Allowed** correspond à cette métrique Prometheus :

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Exemple d'espace de métadonnées autorisé

Supposons que vous installiez un système StorageGRID en version 11.6. Dans cet exemple, supposez que chaque nœud de stockage dispose de plus de 128 Go de RAM et que le volume 0 du nœud de stockage 1 (SN1) fait 6 To. Sur la base de ces valeurs :

- L'espace réservé aux métadonnées à l'échelle du système est fixé à 8 To. (Il s'agit de la valeur par défaut pour StorageGRID 11.6 ou version ultérieure lorsque chaque nœud de stockage dispose de plus de 128 Go de RAM.)
- L'espace réellement réservé aux métadonnées pour SN1 est de 6 To. (Le volume entier est réservé car le volume 0 est plus petit que le paramètre **Espace réservé aux métadonnées**.)
- L'espace autorisé pour les métadonnées sur SN1 est de 3 To, basé sur le calcul indiqué dans le tableau de l'espace autorisé pour les métadonnées : (Espace réellement réservé pour les métadonnées − 1 To) × 60 %, jusqu'à un maximum de 3,96 To.

Comment les nœuds de stockage de différentes tailles affectent la capacité des objets

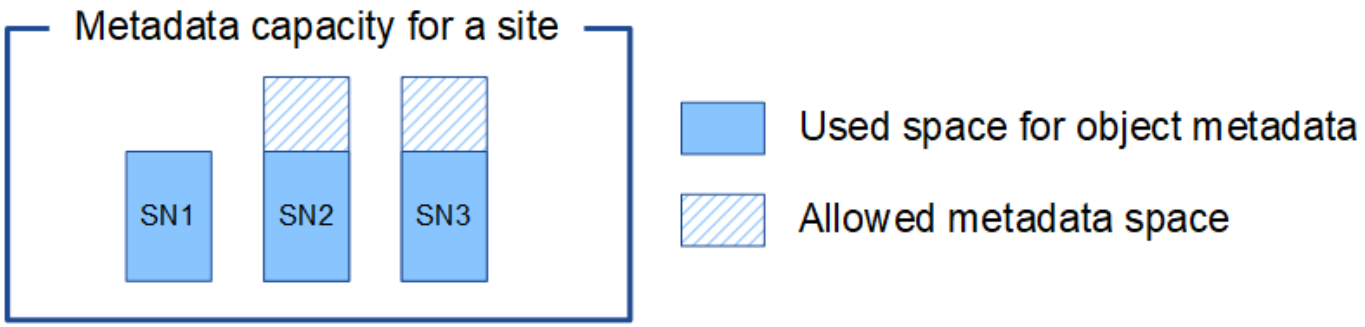
Comme indiqué précédemment, StorageGRID répartit uniformément les métadonnées des objets entre les nœuds de stockage de chaque site. Pour cette raison, si un site contient des nœuds de stockage de tailles différentes, le plus petit nœud du site détermine la capacité de métadonnées du site.

Considérez l'exemple suivant :

- Vous disposez d'une grille à site unique contenant trois nœuds de stockage de tailles différentes.
- Le paramètre **Espace réservé aux métadonnées** est de 4 To.
- Les nœuds de stockage ont les valeurs suivantes pour l'espace de métadonnées réellement réservé et l'espace de métadonnées autorisé.

Nœud de stockage	Taille du volume 0	Espace de métadonnées réellement réservé	Espace autorisé pour les métadonnées
SN1	2,2 To	2,2 To	1,32 To
SN2	5 To	4 To	1,98 To
SN3	6 To	4 To	1,98 To

Étant donné que les métadonnées des objets sont réparties uniformément entre les nœuds de stockage d'un site, 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, étant donné que StorageGRID conserve toutes les métadonnées d'objet d'un système StorageGRID sur chaque site, la capacité globale de métadonnées d'un système StorageGRID est déterminée par la capacité de métadonnées d'objet du plus petit site.

Et comme la capacité des métadonnées des objets contrôle le nombre maximal d'objets, lorsqu'un nœud n'a plus de capacité de métadonnées, la grille est effectivement pleine.

Informations connexes

- Pour savoir comment surveiller la capacité des métadonnées d'objet pour chaque nœud de stockage, consultez les instructions pour "Surveillance StorageGRID".
- Pour augmenter la capacité de métadonnées d'objets de votre système, "étendre une grille" en ajoutant de nouveaux nœuds de stockage.

Augmentez le paramètre Metadata Reserved Space dans StorageGRID

Vous pourrez peut-être augmenter le paramètre système « Espace réservé aux métadonnées » si vos nœuds de stockage répondent à des exigences spécifiques en matière de RAM et d'espace disponible.

Ce dont vous aurez besoin

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur Web pris en charge".
- Vous avez le "Autorisation d'accès racine ou autorisation de configuration de la grille Other".

À propos de cette tâche

Vous pourrez peut-être augmenter manuellement le paramètre d'espace réservé aux métadonnées à l'échelle du système jusqu'à 8 To.

Vous ne pouvez augmenter la valeur du paramètre « Espace réservé aux métadonnées » à l'échelle du système que si les deux conditions suivantes sont vraies :

- Les nœuds de stockage sur n'importe quel site de votre système disposent chacun de 128 Go de RAM ou plus.
- Chaque nœud de stockage sur n'importe quel site de votre système dispose d'un espace disponible suffisant sur le volume de stockage 0.

Notez que si vous augmentez cette valeur, vous réduirez simultanément l'espace disponible pour le stockage d'objets sur le volume de stockage 0 de tous les Storage Nodes. Pour cette raison, vous pourriez préférer définir l'espace réservé aux métadonnées sur une valeur inférieure à 8 To, en fonction de vos besoins estimés en métadonnées d'objets.

> En général, il est préférable d'utiliser une valeur élevée plutôt qu'une valeur faible. Si le paramètre « Espace réservé aux métadonnées » est trop important, vous pouvez le réduire ultérieurement. En revanche, si vous augmentez cette valeur par la suite, le système pourrait devoir déplacer des données d'objet pour libérer de l'espace.

Pour une explication détaillée de la manière dont le paramètre Espace réservé aux métadonnées affecte l'espace autorisé pour le stockage des métadonnées d'objet sur un nœud de stockage particulier, voir "Gérer le stockage des métadonnées des objets".

Étapes

1. Déterminez le paramètre actuel d'espace réservé aux métadonnées.
   a. Sélectionnez **Configuration** > **Système** > **Paramètres de stockage**.
   b. Notez la valeur de **Metadata Reserved Space**.
2. Assurez-vous de disposer de suffisamment d'espace disponible sur le volume de stockage 0 de chaque Storage Node pour augmenter cette valeur.
   a. Sélectionnez **Nœuds**.
   b. Sélectionnez le premier nœud de stockage dans la grille.
   c. Sélectionnez l'onglet Storage.
   d. Dans la section Volumes, repérez l'entrée **/var/local/rangedb/0**.
   e. Confirmez que la valeur disponible est égale ou supérieure à la différence entre la nouvelle valeur que vous souhaitez utiliser et la valeur actuelle de l'espace réservé aux métadonnées.

      Par exemple, si le paramètre Espace réservé aux métadonnées est actuellement de 4 To et que vous souhaitez l'augmenter à 6 To, la valeur Disponible doit être de 2 To ou plus.

   f. Répétez ces étapes pour tous les nœuds de stockage.
      - Si un ou plusieurs nœuds de stockage ne disposent pas d'un espace suffisant, la valeur de

l'espace réservé aux métadonnées ne peut pas être augmentée. Ne continuez pas cette procédure.

- Si chaque nœud de stockage dispose de suffisamment d'espace disponible sur le volume 0, passez à l'étape suivante.

3. Assurez-vous de disposer d'au moins 128 Go de RAM sur chaque nœud de stockage.
   a. Sélectionnez **Nœuds**.
   b. Sélectionnez le premier nœud de stockage dans la grille.
   c. Sélectionnez l'onglet **Matériel**.
   d. Placez votre curseur sur le graphique d'utilisation de la mémoire. Assurez-vous que **Total Memory** est d'au moins 128 Go.
   e. Répétez ces étapes pour tous les nœuds de stockage.
      - Si un ou plusieurs nœuds de stockage ne disposent pas d'une mémoire totale suffisante, la valeur de l'espace réservé aux métadonnées ne peut pas être augmentée. Ne continuez pas cette procédure.
      - Si chaque nœud de stockage possède au moins 128 Go de mémoire totale, passez à l'étape suivante.
4. Mettez à jour le paramètre Espace réservé aux métadonnées.
   a. Sélectionnez **Configuration** > **Système** > **Paramètres de stockage**.
   b. Sélectionnez **Espace réservé aux métadonnées**.
   c. Saisissez la nouvelle valeur.

      Par exemple, pour saisir 8 To, qui est la valeur maximale prise en charge, saisissez **8000000000000** (8 suivi de 12 zéros)

   d. Sélectionnez **Enregistrer**.

Compresser les objets stockés dans StorageGRID

Vous pouvez activer la compression des objets pour réduire la taille des objets stockés dans StorageGRID, afin que les objets consomment moins de stockage.

Avant de commencer

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

À propos de cette tâche

Par défaut, la compression des objets est désactivée. Si vous activez la compression, StorageGRID tente de compresser chaque objet lors de son enregistrement en utilisant une compression sans perte.

> Si vous modifiez ce paramètre, il faudra environ une minute pour que le nouveau paramètre soit appliqué. La valeur configurée est mise en cache pour optimiser les performances et la mise à l'échelle.

Avant d'activer la compression d'objets, veuillez prendre en compte les 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 les compresser avant l'enregistrement. Si une application cliente a déjà compressé un objet avant de l'enregistrer dans StorageGRID, la sélection de cette option ne réduira pas davantage la taille de l'objet.
- Ne sélectionnez pas **Compresser les objets stockés** si vous utilisez NetApp FabricPool avec StorageGRID.
- Si l'option **Compresser les objets stockés** est sélectionnée, les applications clientes S3 doivent éviter d'effectuer des opérations GetObject qui spécifient le retour d'une plage d'octets. Ces opérations de « lecture par plage » sont inefficaces car StorageGRID doit effectivement décompresser 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 requêtes client peuvent expirer.

> Si vous devez compresser des objets et que votre application cliente doit utiliser des lectures par plage, augmentez le délai d'expiration de lecture pour l'application.

Étapes

1. Sélectionnez **Configuration** > **Système** > **Paramètres de stockage** > **Compression des objets**.
2. Cochez la case **Compresser les objets stockés**.
3. Sélectionnez **Enregistrer**.

Gérer les nœuds de stockage complets dans StorageGRID

Lorsque les nœuds de stockage atteignent leur capacité maximale, vous devez étendre le système StorageGRID en ajoutant du stockage supplémentaire. Trois options s'offrent à vous : ajouter des volumes de stockage, ajouter des étagères d'expansion de stockage et ajouter des nœuds de stockage.

Ajouter des volumes de stockage

Chaque nœud de stockage prend en charge un nombre maximal de volumes de stockage. Le maximum défini varie selon la plateforme. Si un nœud de stockage contient moins que le nombre maximal de volumes de stockage, vous pouvez ajouter des volumes pour augmenter sa capacité. Consultez les instructions pour "extension d'un système StorageGRID".

Ajouter des étagères d'extension de stockage

Certains nœuds de stockage StorageGRID, tels que le SG6060 ou le SG6160, peuvent prendre en charge des étagères de stockage supplémentaires. Si vous disposez d'appliances StorageGRID avec des capacités d'extension qui n'ont pas encore été étendues à leur capacité maximale, vous pouvez ajouter des étagères de stockage pour augmenter la capacité. Consultez les instructions pour "extension d'un système StorageGRID".

Ajouter des nœuds de stockage

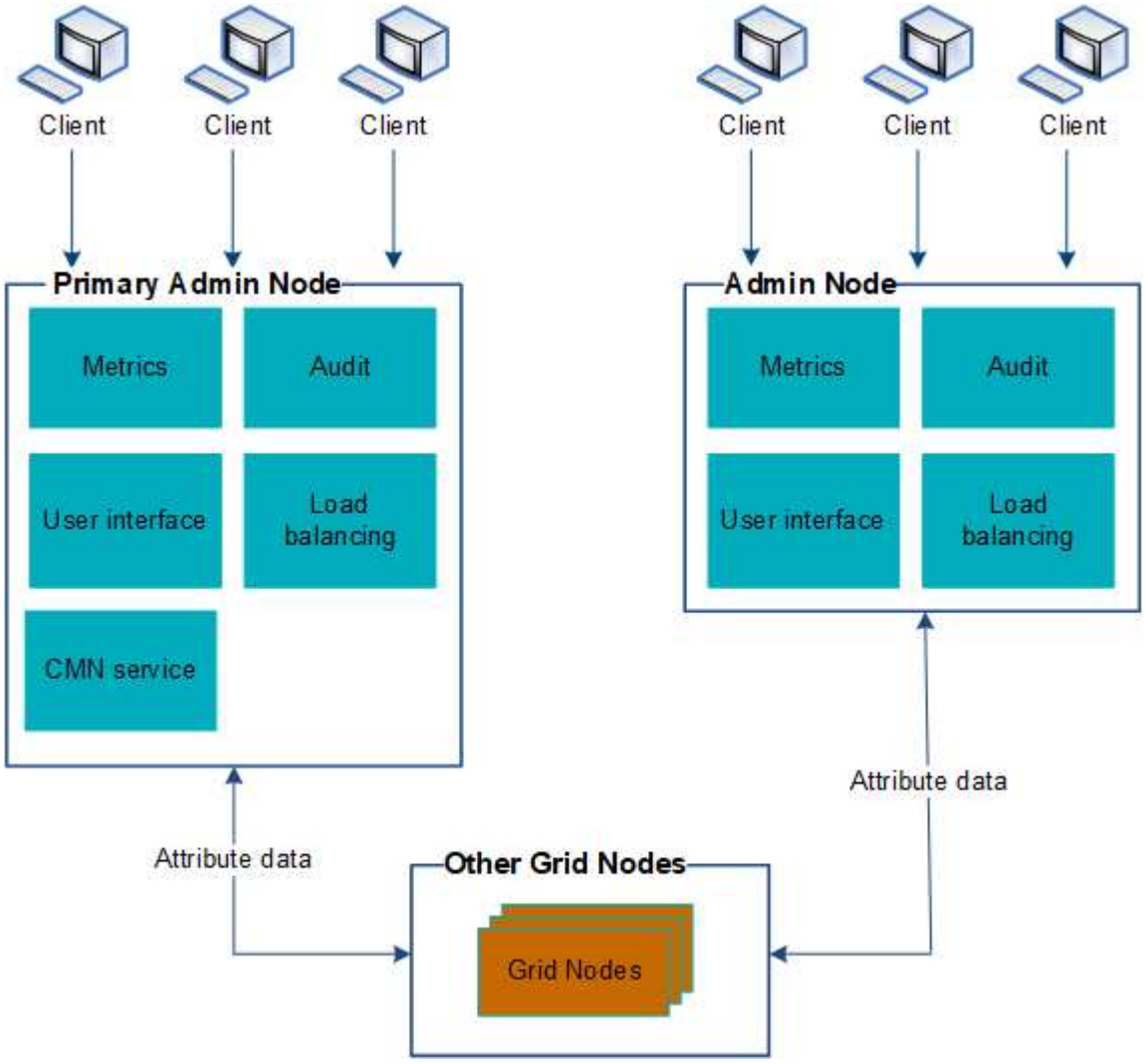
Vous pouvez augmenter la capacité de stockage en ajoutant des nœuds de stockage. Une attention particulière doit être portée aux règles ILM actuellement actives et aux exigences de capacité lors de l'ajout de stockage. Consultez les instructions pour "extension d'un système StorageGRID".

Gérer les nœuds d'administration

Utilisez plusieurs nœuds d'administration dans StorageGRID

Un système StorageGRID peut inclure plusieurs nœuds d'administration afin de vous permettre de surveiller et de configurer en continu votre système StorageGRID, même si un nœud d'administration tombe en panne.

Si un nœud d'administration devient indisponible, le traitement des attributs se poursuit, les alertes sont toujours déclenchées et les notifications par e-mail ainsi que les packages AutoSupport sont toujours envoyés. Cependant, la présence de plusieurs nœuds d'administration n'offre une protection contre les pannes que pour les notifications et les packages AutoSupport.



Deux options permettent de continuer à visualiser et à configurer le système StorageGRID en cas de défaillance d'un nœud d'administration :

- Les clients Web peuvent se reconnecter à n'importe quel autre nœud d'administration disponible.
- Si un administrateur système a configuré un groupe de nœuds d'administration à haute disponibilité, les clients web peuvent continuer à accéder au Grid Manager ou au Tenant Manager en utilisant l'adresse IP virtuelle du groupe HA. Voir "Gérer les groupes à haute disponibilité".

Lors de l'utilisation d'un groupe HA, l'accès est interrompu en cas de défaillance du nœud d'administration actif. Les utilisateurs doivent se reconnecter une fois que l'adresse IP virtuelle du groupe HA a basculé vers un autre nœud d'administration du groupe.

Certaines opérations de maintenance ne peuvent être effectuées qu'à l'aide du nœud d'administration principal. Si le nœud d'administration principal tombe en panne, il doit être restauré avant que le système StorageGRID ne soit de nouveau pleinement opérationnel.

Identifiez le nœud d'administration principal dans StorageGRID

Le nœud d'administration principal offre plus de fonctionnalité que les nœuds d'administration non principaux. Par exemple, certaines procédures de maintenance doivent être effectuées à l'aide du nœud d'administration principal.

Pour plus d'informations sur les nœuds d'administration, voir "Qu'est-ce qu'un nœud d'administration".

Avant de commencer

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

Étapes

1. Sélectionnez **Nœuds**.
2. Saisissez **primary** dans le champ de recherche.

   Dans les résultats de la recherche, identifiez le nœud dont la colonne Type affiche « Primary Admin Node ». Un seul Primary Admin Node doit être affiché.