Administrer StorageGRID

StorageGRID 11.5

NetApp
April 11, 2024

Sommaire

Administrer StorageGRID

Découvrez comment configurer le système StorageGRID.

- "Administration d'un système StorageGRID"
- "Contrôle de l'accès administrateur à StorageGRID"
- "Configuration des serveurs de gestion des clés"
- "Gestion des locataires"
- "Configuration des connexions des clients S3 et Swift"
- "Gestion des réseaux et des connexions StorageGRID"
- "Configuration d'AutoSupport en cours"
- "Gestion des nœuds de stockage"
- "Gestion des nœuds d'administration"
- "Gestion des nœuds d'archivage"
- "Migration des données vers StorageGRID"

Administration d'un système StorageGRID

Suivez ces instructions pour configurer et administrer un système StorageGRID.

Ces instructions expliquent comment utiliser Grid Manager pour configurer des groupes et des utilisateurs, créer des comptes de locataires pour permettre aux applications client S3 et Swift de stocker et récupérer des objets, configurer et gérer des réseaux StorageGRID, configurer AutoSupport, gérer des paramètres de nœud, etc.

> Il a été déplacé les instructions de gestion des objets avec des règles et des règles de gestion du cycle de vie des informations (ILM) vers"Gestion des objets avec ILM".

Ces instructions s'adresse au personnel technique qui devra configurer, administrer et prendre en charge un système StorageGRID après son installation.

Ce dont vous avez besoin

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

Navigateurs Web pris en charge

Vous devez utiliser un navigateur Web pris en charge.

Navigateur Web	Version minimale prise en charge
Google Chrome	87
Microsoft Edge	87

Navigateur Web	Version minimale prise en charge
Mozilla Firefox	84

Vous devez régler la fenêtre du navigateur sur une largeur recommandée.

Largeur du navigateur	Pixels
Minimum	1024
Optimale	1280

Connexion au Grid Manager

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

Ce dont vous avez besoin

- Vous devez disposer de vos identifiants de connexion.
- Vous devez disposer de l'URL pour Grid Manager.
- Vous devez utiliser un navigateur Web pris en charge.
- Les cookies doivent être activés dans votre navigateur Web.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Chaque système StorageGRID comprend un nœud d'administration principal et un nombre quelconque de nœuds d'administration non primaires. Vous pouvez vous connecter au Gestionnaire de grille sur n'importe quel noeud d'administration pour gérer le système StorageGRID. Cependant, les nœuds d'administration ne sont pas exactement les mêmes :

- Les accusés de réception d'alarme (système hérité) effectués sur un noeud d'administration ne sont pas copiés sur d'autres noeuds d'administration. Pour cette raison, les informations affichées pour les alarmes peuvent ne pas être identiques sur chaque nœud d'administration.
- Certaines procédures de maintenance peuvent uniquement être effectuées depuis le nœud d'administration principal.

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

Étapes

1. Lancez un navigateur Web pris en charge.
2. Dans la barre d'adresse du navigateur, entrez l'URL du Grid Manager :

   `https://FQDN_or_Admin_Node_IP/`

où *FQDN_or_Admin_Node_IP* Est un nom de domaine complet ou l'adresse IP d'un nœud d'administration ou l'adresse IP virtuelle d'un groupe de nœuds d'administration haute disponibilité.

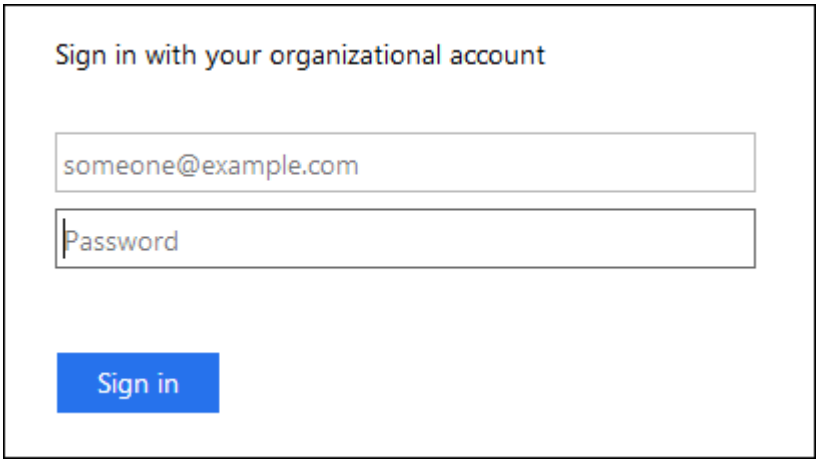
Si vous devez accéder à Grid Manager sur un port autre que le port standard pour HTTPS (443), entrez les informations suivantes, où *FQDN_or_Admin_Node_IP* Est un nom de domaine complet ou une adresse IP et le port est le numéro de port :

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

3. Si vous êtes invité à recevoir une alerte de sécurité, installez le certificat à l'aide de l'assistant d'installation du navigateur.
4. Connectez-vous au Grid Manager :
   - Si l'authentification unique (SSO) n'est pas utilisée pour votre système StorageGRID :
     i. Saisissez votre nom d'utilisateur et votre mot de passe pour le Grid Manager.
     ii. Cliquez sur **connexion**.

   - Si l'authentification SSO est activée pour votre système StorageGRID et qu'il s'agit de la première fois que vous avez accédé à l'URL sur ce navigateur :
     i. Cliquez sur **connexion**. Vous pouvez laisser le champ ID compte vide.

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

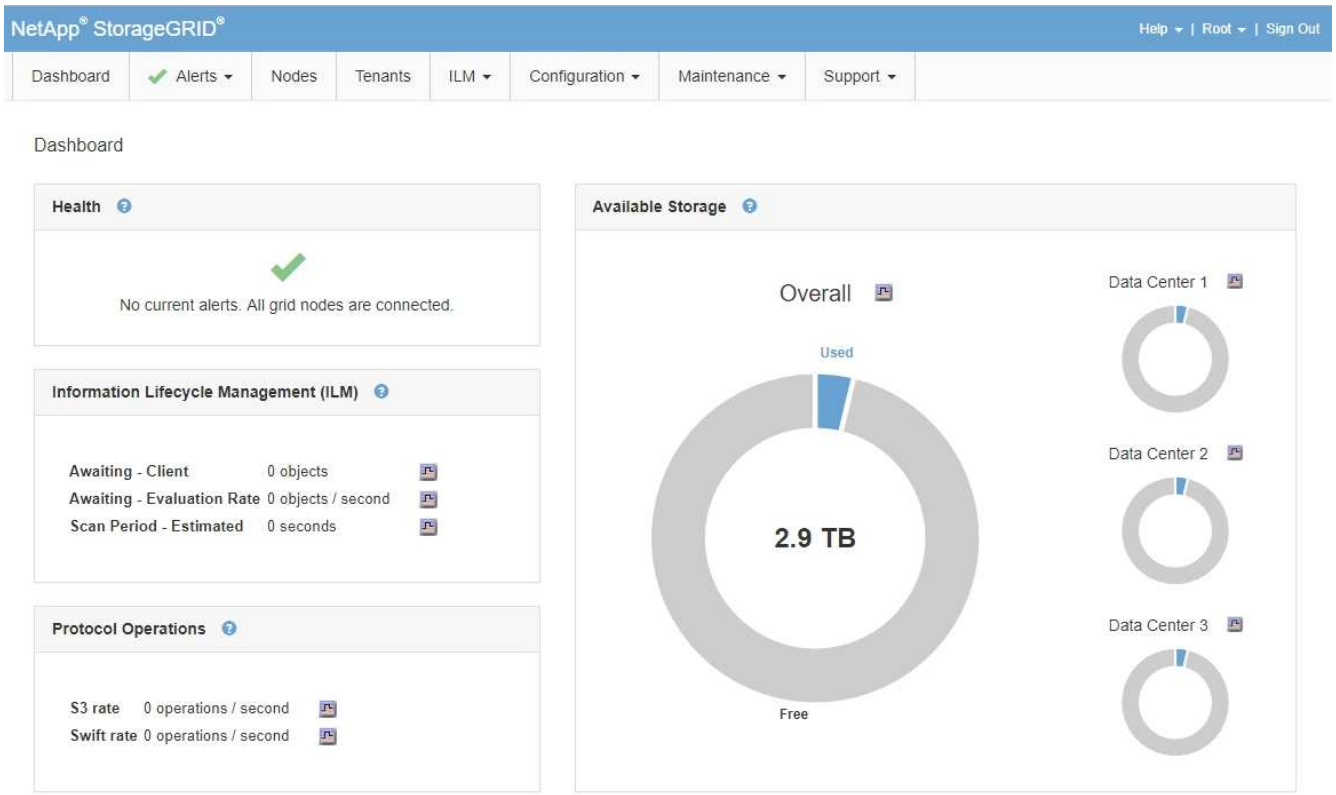


- Si l'authentification SSO est activée pour votre système StorageGRID et que vous avez déjà accédé au Grid Manager ou à un compte de locataire :

  i. Effectuez l'une des opérations suivantes :

  - Saisissez **0** (l'ID de compte du gestionnaire de grille), puis cliquez sur **connexion**.
  - Sélectionnez **Grid Manager** s'il apparaît dans la liste des comptes récents, puis cliquez sur **connexion**.

  ii. Connectez-vous à l'aide de vos identifiants SSO standard sur la page de connexion SSO de votre entreprise. Lorsque vous êtes connecté, la page d'accueil de Grid Manager s'affiche, qui inclut le tableau de bord. Pour connaître les informations fournies, consultez la section « Affichage du tableau de bord » dans les instructions de surveillance et de dépannage de StorageGRID.



5. Pour vous connecter à un autre nœud d'administration :

Option	Étapes
SSO non activé	a. Dans la barre d'adresse du navigateur, entrez le nom de domaine complet ou l'adresse IP de l'autre noeud d'administration. Indiquez le numéro de port requis. b. Saisissez votre nom d'utilisateur et votre mot de passe pour le Grid Manager. c. Cliquez sur **connexion**.
SSO activé	Dans la barre d'adresse du navigateur, entrez le nom de domaine complet ou l'adresse IP de l'autre noeud d'administration. Si vous vous êtes connecté à un nœud d'administration, vous pouvez accéder aux autres nœuds d'administration sans avoir à vous reconnecter. Toutefois, si votre session SSO expire, vous êtes invité à saisir à nouveau vos informations d'identification. **Remarque :** SSO n'est pas disponible sur le port restreint Grid Manager. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec une connexion unique.

Informations associées

"Navigateurs Web pris en charge"

"Contrôle de l'accès par pare-feu"

"Configuration des certificats de serveur"

"Configuration de l'authentification unique"

"Gestion des groupes d'administration"

"Gestion des groupes haute disponibilité"

"Utilisez un compte de locataire"

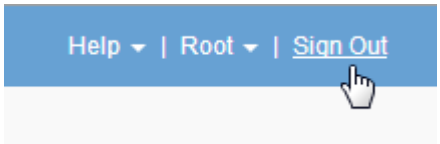
"Moniteur et amp ; dépannage"

Déconnexion du gestionnaire de grille

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

Étapes

1. Repérez le lien **Déconnexion** dans le coin supérieur droit de l'interface utilisateur.



2. Cliquez sur **Déconnexion**.

Option	Description
SSO non utilisé	Vous êtes déconnecté du nœud d'administration. La page de connexion de Grid Manager s'affiche. **Remarque :** si vous vous êtes connecté à plusieurs nœuds d'administration, vous devez vous déconnecter de chaque nœud.

Option	Description
SSO activé	Vous êtes déconnecté de tous les nœuds d'administration auxquels vous accédiez. La page de connexion StorageGRID s'affiche. **Grid Manager** est répertorié comme valeur par défaut dans la liste déroulante **comptes récents** et le champ **ID compte** affiche 0. **Remarque :** si SSO est activé et que vous êtes également connecté au Gestionnaire de tenant, vous devez également vous déconnecter du compte de tenant pour vous déconnecter de SSO.

Informations associées

"Configuration de l'authentification unique"

"Utilisez un compte de locataire"

Modification de votre mot de passe

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

Ce dont vous avez besoin

Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.

Description de la tâche

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

Étapes

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

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

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

Modification de la phrase secrète de provisionnement

Utilisez cette procédure pour modifier la phrase secrète du provisionnement StorageGRID. La phrase de passe est requise pour les procédures de restauration, d'extension et de maintenance. La phrase de passe est également requise pour télécharger les sauvegardes du pack de récupération qui incluent les informations de

topologie de la grille et les clés de chiffrement pour le système StorageGRID.

Ce dont vous avez besoin

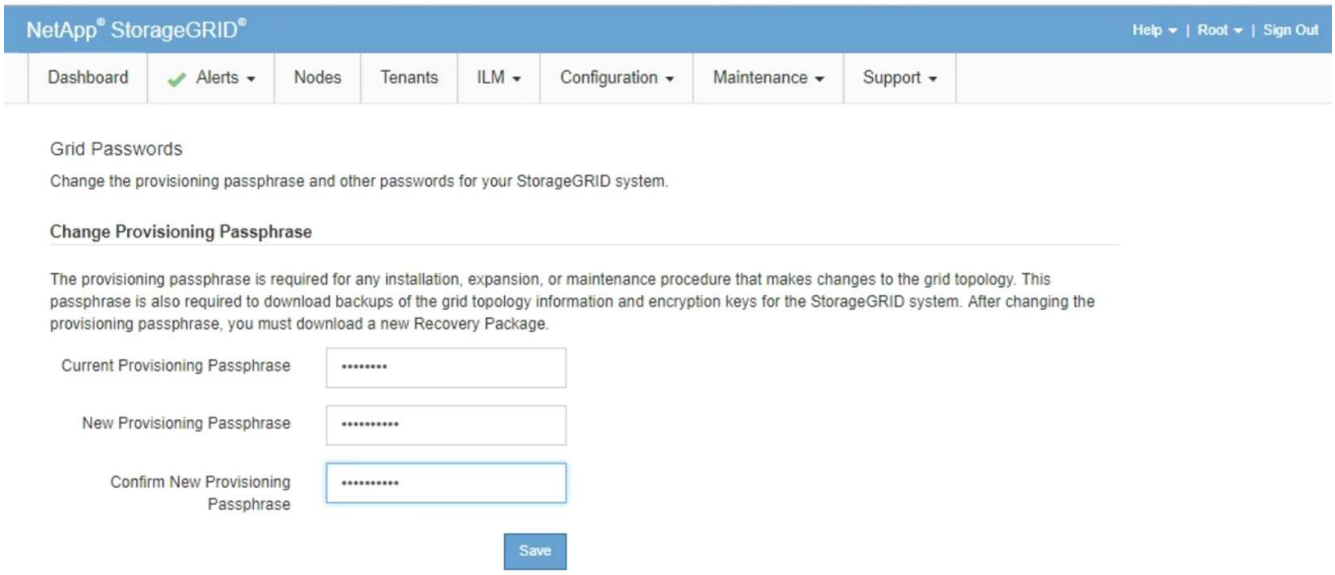
- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations Maintenance ou accès racine.
- Vous devez disposer de la phrase secrète de provisionnement actuelle.

Description de la tâche

Le mot de passe de provisionnement est requis pour de nombreuses procédures d'installation et de maintenance, ainsi que pour le téléchargement du progiciel de restauration. La phrase de passe de provisionnement n'est pas répertoriée dans le `Passwords.txt` fichier. Veillez à documenter la phrase de passe de provisionnement et à la conserver dans un emplacement sûr et sécurisé.

Étapes

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

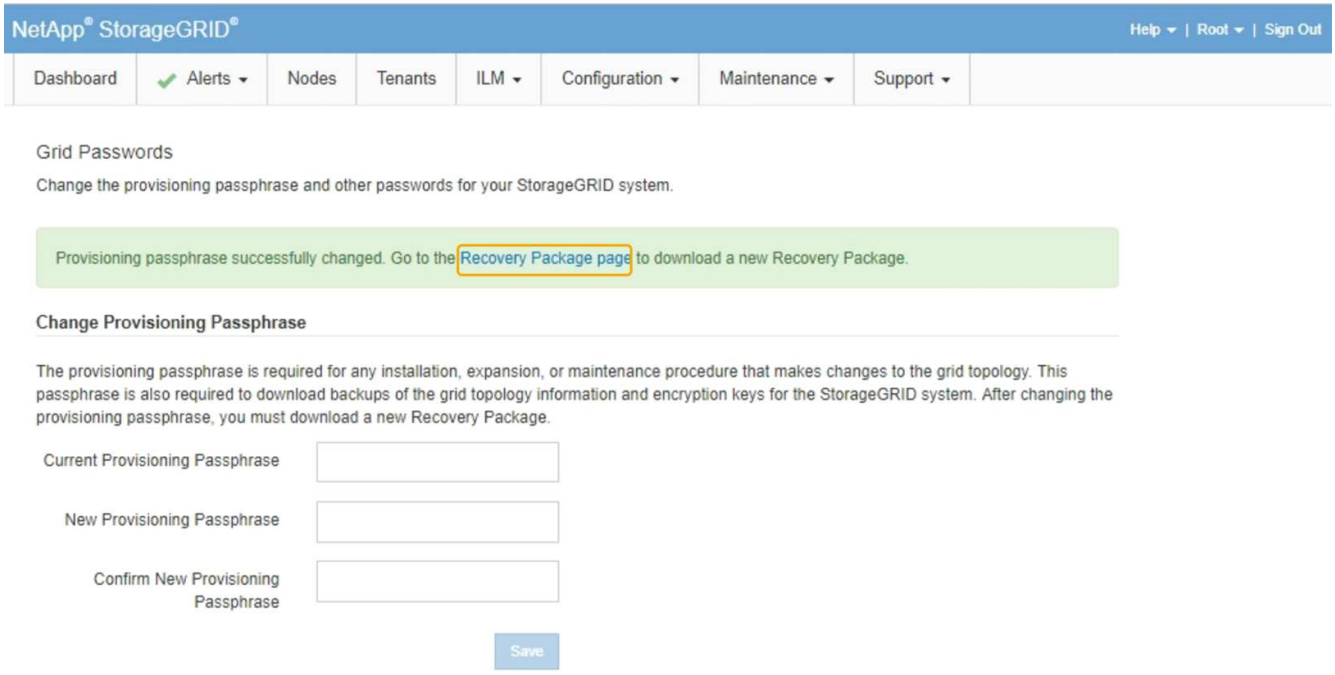


2. Saisissez votre phrase secrète pour le provisionnement.
3. Saisissez la nouvelle phrase de passe. La phrase de passe doit contenir au moins 8 caractères et 32 caractères. Les phrases passe sont sensibles à la casse.

> Stocker la nouvelle phrase secrète pour le provisionnement dans un emplacement sécurisé Elle est requise pour les procédures d'installation, d'extension et de maintenance.

4. Saisissez à nouveau la nouvelle phrase de passe, puis cliquez sur **Enregistrer**.

   Le système affiche une bannière verte de réussite lorsque la modification de la phrase de passe de provisionnement est terminée. Le changement devrait prendre moins d'une minute.



5. Sélectionnez le lien **Recovery Package page** dans la bannière de réussite.
6. Téléchargez le nouveau package de récupération depuis Grid Manager. Sélectionnez **Maintenance** > **Recovery Package** et saisissez la nouvelle phrase de passe d'approvisionnement.

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

Modification du délai d'expiration de la session du navigateur

Vous pouvez contrôler si les utilisateurs de Grid Manager et de tenant Manager sont déconnectés s'ils sont inactifs pendant plus d'un certain temps.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Le délai d'inactivité de l'interface graphique est défini par défaut sur 900 secondes (15 minutes). Si la session de navigateur d'un utilisateur n'est pas active pendant cette période, la session est expirée.

Si nécessaire, vous pouvez augmenter ou diminuer le délai d'inactivité en définissant l'option d'affichage délai d'inactivité de l'interface graphique.

Si l'authentification unique (SSO) est activée et que la session du navigateur d'un utilisateur est expirée, le système se comporte comme si l'utilisateur a cliqué sur **Déconnexion** manuellement. L'utilisateur doit saisir à nouveau ses identifiants SSO pour accéder à StorageGRID.

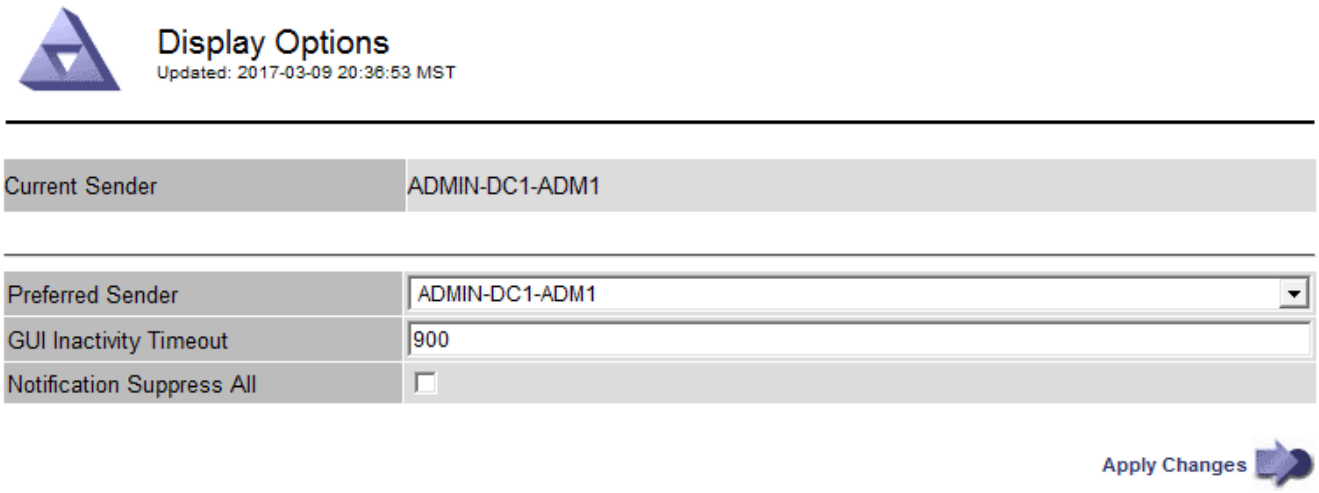
Le délai d'expiration de session utilisateur peut également être contrôlé par les éléments suivants :

- Un minuteur StorageGRID séparé non configurable, inclus pour la sécurité du système. Par défaut, le jeton d'authentification de chaque utilisateur expire 16 heures après la connexion de l'utilisateur. Lorsqu'une authentification de l'utilisateur expire, cet utilisateur est automatiquement déconnecté, même si la valeur du délai d'inactivité de l'interface graphique n'a pas été atteinte. Pour renouveler le jeton, l'utilisateur doit se reconnecter.
- Paramètres de délai pour le fournisseur d'identité, en supposant que SSO est activé pour StorageGRID.

Étapes

1. Sélectionnez **Configuration** > **Paramètres système** > **Options d'affichage**.
2. Pour **délai d'inactivité de l'interface graphique utilisateur**, entrez un délai d'expiration de 60 secondes ou plus.

   Définissez ce champ sur 0 si vous ne souhaitez pas utiliser cette fonctionnalité. Les utilisateurs sont déconnectés 16 heures après leur connexion, quand leurs jetons d'authentification expirent.



3. Cliquez sur **appliquer les modifications**.

   Le nouveau paramètre n'affecte pas les utilisateurs actuellement connectés. Les utilisateurs doivent se reconnecter ou actualiser leur navigateur pour que le nouveau paramètre de délai d'expiration prenne effet.

Informations associées

"Fonctionnement de l'authentification unique"

"Utilisez un compte de locataire"

Affichage des informations de licence StorageGRID

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

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.

Description de la tâche

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

Étape

Pour afficher la licence, effectuez l'une des opérations suivantes :

- Dans le panneau Santé du tableau de bord, cliquez sur l'icône d'état de la licence ou sur le lien **Licence**. Ce lien apparaît uniquement en cas de problème avec la licence.
- Sélectionnez **Maintenance** > **système** > **Licence**.

La page Licence s'affiche et fournit les informations suivantes en lecture seule sur la licence actuelle :

- ID du système StorageGRID, qui est le numéro d'identification unique de cette installation StorageGRID
- Numéro de série de la licence
- Capacité de stockage sous licence de la grille
- Date de fin de la licence logicielle
- Date de fin du contrat de service de support
- Contenu du fichier texte de licence

> Pour les licences émises avant StorageGRID 10.3, la capacité de stockage sous licence n'est pas incluse dans le fichier de licence et un message « Voir contrat de licence » s'affiche au lieu d'une valeur.

Mise à jour des informations de licence StorageGRID

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

Ce dont vous avez besoin

- Vous devez disposer d'un nouveau fichier de licence pour appliquer votre système StorageGRID.

- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez disposer de la phrase secrète pour le provisionnement.

Étapes

1. Sélectionnez **Maintenance** > **système** > **Licence**.
2. Saisissez le mot de passe de provisionnement de votre système StorageGRID dans la zone de texte **phrase de passe de provisionnement**.
3. Cliquez sur **Parcourir**.
4. Dans la boîte de dialogue Ouvrir, localisez et sélectionnez le nouveau fichier de licence (`.txt`), puis cliquez sur **Ouvrir**.

   Le nouveau fichier de licence est validé et affiché.

5. Cliquez sur **Enregistrer**.

Via l'API de gestion du grid

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

L'API Grid Management utilise la plateforme d'API open source swagger. Swagger fournit une interface utilisateur intuitive qui permet aux développeurs et aux non-développeurs d'effectuer des opérations en temps réel dans StorageGRID avec l'API.

Ressources générales

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

- `/grid`: L'accès est limité aux utilisateurs de Grid Manager et est basé sur les autorisations de groupe configurées.
- `/org`: L'accès est limité aux utilisateurs qui appartiennent à un groupe LDAP local ou fédéré pour un compte locataire. Pour plus de détails, reportez-vous aux informations sur l'utilisation des comptes de tenant.
- `/private`: L'accès est limité aux utilisateurs de Grid Manager et est basé sur les autorisations de groupe configurées. Ces API sont destinées à un usage interne uniquement et ne sont pas documentées publiquement. Ces API sont également susceptibles d'être modifiées sans préavis.

Informations associées

"Utilisez un compte de locataire"

"Prometheus : notions de base sur les requêtes"

Opérations de l'API de gestion du grid

L'API Grid Management organise les opérations d'API disponibles dans les sections suivantes.

- **Comptes** — opérations pour gérer les comptes de tenant du stockage, y compris la création de nouveaux comptes et la récupération de l'utilisation du stockage pour un compte donné.
- **Alarmes** — opérations pour répertorier les alarmes en cours (système hérité) et renvoyer des informations sur l'intégrité de la grille, y compris les alertes en cours et un résumé des États de connexion du nœud.
- **Alerte-historique** — opérations sur les alertes résolues.
- **Alertes-récepteurs** — opérations sur les récepteurs de notification d'alerte (e-mail).
- **Règles d'alerte** — opérations sur les règles d'alerte.
- **Seuils d'alerte** — opérations sur les silences d'alerte.
- **Alertes** — opérations sur les alertes.
- **Audit** — opérations pour répertorier et mettre à jour la configuration d'audit.
- **Auth** — opérations pour effectuer l'authentification de session utilisateur.

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

  > Si l'authentification unique est activée pour le système StorageGRID, vous devez effectuer différentes étapes pour l'authentification. Voir « authentification dans l'API si l'authentification unique est activée ».

  Voir « protection contre la contrefaçon de demandes intersites » pour des informations sur l'amélioration de la sécurité de l'authentification.

- **Certificats-client** — opérations pour configurer les certificats client afin que StorageGRID soit accessible en toute sécurité à l'aide d'outils de surveillance externes.
- **Config** — opérations liées à la version du produit et aux versions de l'API de gestion de grille. Vous pouvez répertorier la version du produit et les principales versions de l'API Grid Management prises en charge par cette version, et désactiver les versions obsolètes de l'API.
- **DESACTIVE-fonctions** — opérations pour afficher les fonctions qui pourraient avoir été désactivées.
- **dns-serveurs** — opérations pour répertorier et modifier les serveurs DNS externes configurés.
- **Endpoint-domain-names** — opérations pour lister et modifier les noms de domaine de noeud final.
- **Code d'effacement** — opérations sur les profils de code d'effacement.
- **Expansion** — opérations sur l'expansion (niveau procédure).
- **Nœuds d'extension** — opérations sur l'extension (au niveau du nœud).
- **Sites d'expansion** — opérations sur l'expansion (au niveau du site).
- **Grid-réseaux** — opérations pour lister et modifier la liste des réseaux de grille.
- **GRID-mots de passe** — opérations pour la gestion des mots de passe de grille.
- **Groupes** — opérations pour gérer les groupes d'administrateurs Grid locaux et pour extraire des groupes d'administrateurs Grid fédérés à partir d'un serveur LDAP externe.
- **Identity-source** — opérations pour configurer un référentiel d'identité externe et synchroniser manuellement les informations de groupe et d'utilisateur fédérés.
- **ilm** — opérations sur la gestion du cycle de vie de l'information (ILM).

- **Licence** — opérations pour récupérer et mettre à jour la licence StorageGRID.
- **Logs** — opérations de collecte et de téléchargement de fichiers journaux.
- **Métriques** — opérations sur les métriques StorageGRID incluant des requêtes métriques instantanées à un point unique dans les requêtes métriques de temps et de plage sur une plage de temps. L'API de gestion du grid utilise l'outil de contrôle des systèmes Prometheus comme source de données back-end. Pour plus d'informations sur la création de requêtes Prometheus, consultez le site Web Prometheus.

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

- **Node-Health** — opérations sur l'état de santé du noeud.
- **ntp-Server** — opérations pour répertorier ou mettre à jour les serveurs NTP (Network Time Protocol) externes.
- **Objets** — opérations sur les objets et les métadonnées d'objet.
- **Récupération** — opérations pour la procédure de récupération.
- **Progiciel de récupération** — opérations pour télécharger le progiciel de récupération.
- **Régions** — opérations pour afficher et créer des régions.
- **s3-Object-lock** — opérations sur les paramètres globaux de verrouillage d'objet S3.
- **Server-Certificate** — opérations pour afficher et mettre à jour les certificats de serveur Grid Manager.
- **snmp** — opérations sur la configuration SNMP actuelle.
- **Classes de trafic** — opérations pour les politiques de classification du trafic.
- **Réseau-client-non fiable** — opérations sur la configuration réseau client non fiable.
- **Utilisateurs** — opérations pour afficher et gérer les utilisateurs de Grid Manager.

Émission de requêtes API

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

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

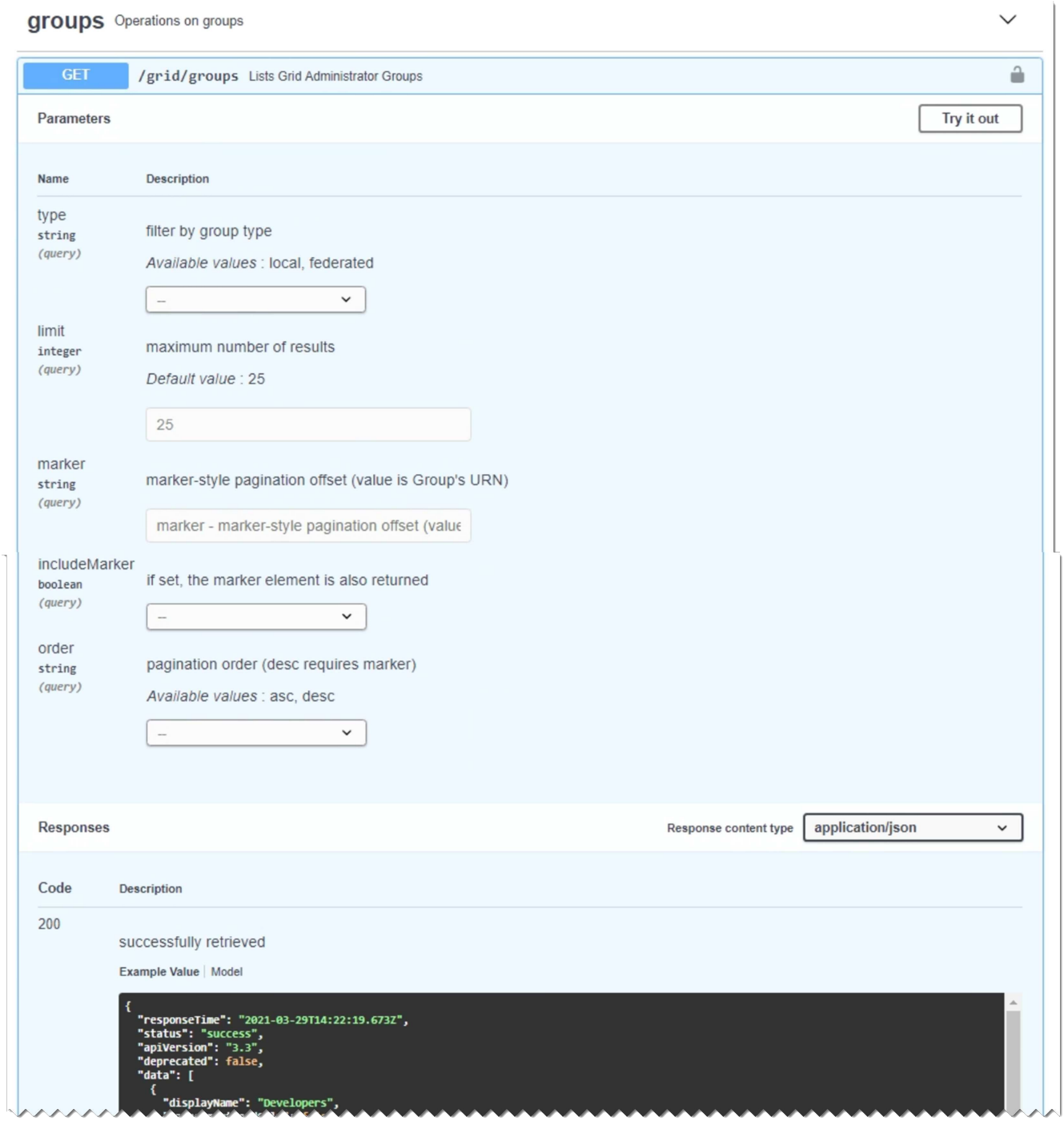
> Toutes les opérations d'API que vous effectuez à l'aide de la page Web API Docs sont des opérations en direct. Veillez à ne pas créer, mettre à jour ou supprimer des données de configuration ou d'autres données par erreur.

Étapes

1. Sélectionnez **aide** > **Documentation API** dans l'en-tête de Grid Manager.
2. Sélectionnez l'opération souhaitée.

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

3. Sélectionnez une action HTTP pour afficher les détails de la demande, notamment l'URL du noeud final, la liste de tous les paramètres obligatoires ou facultatifs, un exemple de l'organisme de demande (si nécessaire) et les réponses possibles.



4. Déterminez si la demande nécessite des paramètres supplémentaires, tels qu'un ID de groupe ou d'utilisateur. Ensuite, obtenir ces valeurs. Vous devrez peut-être d'abord lancer une autre demande d'API pour obtenir les informations dont vous avez besoin.
5. Déterminez si vous devez modifier l'exemple de corps de la demande. Si c'est le cas, vous pouvez cliquer sur **modèle** pour connaître les exigences de chaque champ.
6. Cliquez sur **essayez-le**.
7. Fournir tous les paramètres requis ou modifier le corps de la demande selon les besoins.

8. Cliquez sur **Exécuter**.
9. Vérifiez le code de réponse pour déterminer si la demande a réussi.

Gestion des versions de l'API de gestion du grid

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

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

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

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

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

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

> Vous pouvez utiliser l'API Grid Management pour configurer les versions prises en charge. Pour plus d'informations, reportez-vous à la section « config » de la documentation de l'API swagger. Vous devez désactiver la prise en charge de l'ancienne version après avoir mis à jour tous les clients de l'API Grid Management pour utiliser la version la plus récente.

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

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

```
Received call to deprecated v1 API at POST "/api/v1/authorize"
```

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

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

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

Spécification d'une version d'API pour une requête

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

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

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

Protection contre la contrefaçon de demandes intersites (CSRF)

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

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

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

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

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

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

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

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

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

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

Utilisation de l'API si l'authentification unique est activée

Si l'authentification unique (SSO) a été activée pour votre système StorageGRID, vous ne pouvez pas utiliser les requêtes standard de l'API d'authentification pour vous connecter à l'API de gestion du grid ou l'API de gestion des locataires et vous déconnecter.

Connexion à l'API si l'authentification unique est activée

Si l'authentification unique (SSO) a été activée, vous devez émettre une série de requêtes API pour obtenir un jeton d'authentification auprès d'AD FS valide pour l'API de gestion de grille ou l'API de gestion des locataires.

Ce dont vous avez besoin

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

Description de la tâche

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

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

- Un exemple de flux de travail des requêtes Curl.

  Le flux de travail de boucle risque de s'échapper si vous l'effectuez trop lentement. L'erreur peut s'afficher : aucune confirmation de soumission valide n'a été trouvée dans cette réponse.

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

Si vous avez un problème de codage d'URL, l'erreur peut s'afficher : version SAML non prise en charge.

Étapes

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

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

   - Le nom d'utilisateur SSO
   - Domaine dans lequel StorageGRID est installé
   - L'adresse de StorageGRID
   - Pour accéder à l'API de gestion des locataires, entrez l'ID de compte de locataire.

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

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

   +

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

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

   a. Déclarez les variables nécessaires pour la connexion.

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

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

b. Pour recevoir une URL d'authentification signée, lancez une demande POST à `/api/v3/authorize-saml`, Et supprimez le codage JSON supplémentaire de la réponse.

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

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

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

```
{
    "apiVersion": "3.0",
    "data":
"https://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` à partir de la réponse pour une utilisation dans les commandes suivantes.

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

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

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

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

   La réponse inclut l'ID de demande client :

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

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

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

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

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

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

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

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

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

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

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

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

Les en-têtes de réponse contiennent des informations sur la session AD FS pour une utilisation de déconnexion ultérieure et le corps de réponse contient SAMLResponse dans un champ de formulaire masqué.

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

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

i. Enregistrez le `SAMLResponse` dans le champ masqué :

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

j. À l'aide de la sauvegarde `SAMLResponse`, Faire un StorageGRID`/api/saml-response` Demande de génération d'un jeton d'authentification StorageGRID.

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

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

La réponse inclut le jeton d'authentification.

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

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

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

Vous pouvez maintenant utiliser `MYTOKEN` Pour les autres demandes, comme le ferait l'utilisation de l'API si SSO n'était pas utilisé.

Déconnexion de l'API si l'authentification unique est activée

Si l'authentification unique (SSO) a été activée, vous devez émettre une série de requêtes API pour vous déconnecter de l'API de gestion Grid ou de l'API de gestion des locataires.

Description de la tâche

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

Étapes

1. Pour générer une demande de déconnexion signée, passez `cookie "sso=true"` Pour 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=fZDNboMwEI
RfhZ...HcQ%3D%3D'
```

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

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

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

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

4. Supprimez le jeton de support StorageGRID.

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

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

A `204 No Content` reponse indique que l'utilisateur est déconnecté.

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

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

Lorsqu'un client se connecte au serveur via HTTPS, le serveur répond avec le certificat du serveur, qui contient une clé publique. Le client vérifie ce certificat en comparant la signature du serveur à la signature figurant sur sa copie du certificat. Si les signatures correspondent, le client démarre une session avec le serveur en utilisant la même clé publique.

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

Une autorité de certification externe peut émettre des certificats personnalisés qui sont entièrement conformes aux politiques de sécurité des informations de votre entreprise. StorageGRID inclut également une autorité de certification intégrée qui génère des certificats CA internes lors de l'installation du système. Ces certificats d'autorité de certification internes sont utilisés par défaut pour sécuriser le trafic StorageGRID interne. Bien que vous puissiez utiliser les certificats d'autorité de certification internes pour un environnement non productif, la meilleure pratique pour un environnement de production consiste à utiliser des certificats personnalisés signés par une autorité de certification externe. Les connexions non sécurisées sans certificat sont également prises en charge mais ne sont pas recommandées.

- Les certificats d'autorité de certification personnalisés ne suppriment pas les certificats internes ; cependant, les certificats personnalisés doivent être ceux spécifiés pour vérifier les connexions du serveur.
- Tous les certificats personnalisés doivent respecter les directives de renforcement du système pour les certificats de serveur.

  "Durcissement du système"

- StorageGRID prend en charge le regroupement de certificats d'une autorité de certification dans un seul fichier (appelé bundle de certificats d'autorité de certification).

> StorageGRID inclut également des certificats CA du système d'exploitation identiques sur toutes les grilles. Dans les environnements de production, assurez-vous de spécifier un certificat personnalisé signé par une autorité de certification externe à la place du certificat d'autorité de certification du système d'exploitation.

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

Certificat	Type de certificat	Description	Emplacement de navigation	Détails
Certificat du client administrateur	Client	Installé sur chaque client, permettant à StorageGRID d'authentifier l'accès client externe. • Permet aux clients externes autorisés d'accéder à la base de données StorageGRID Prometheus. • Contrôle sécurisé de StorageGRID à l'aide d'outils externes.	**Configuration** > **contrôle d'accès** > **certificats client**	"Configuration des certificats client administrateur"
Certificat de fédération des identités	Serveur	Authentifie la connexion entre StorageGRID et un Active Directory externe, OpenLDAP ou Oracle Directory Server.utilisé pour la fédération des identités, ce qui permet aux groupes d'administration et aux utilisateurs d'être gérés par un système externe.	**Configuration** > **contrôle d'accès** > **Fédération d'identité**	"Utilisation de la fédération des identités"
Certificat SSO (Single Sign-on)	Serveur	Authentifie la connexion entre Active Directory Federation Services (AD FS) et StorageGRID utilisée pour les demandes SSO (Single Sign-on).	**Configuration** > **contrôle d'accès** > **connexion unique**	"Configuration de l'authentification unique"

Certificat	Type de certificat	Description	Emplacement de navigation	Détails
Certificat de serveur de gestion des clés (KMS)	Serveur et client	Authentifie la connexion entre StorageGRID et un serveur de gestion des clés (KMS) externe qui fournit les clés de chiffrement aux nœuds d'appliance StorageGRID.	**Configuration** > **Paramètres système** > **serveur de gestion des clés**	"Ajout d'un serveur de gestion des clés (KMS)"
Certificat de notification d'alerte par e-mail	Serveur et client	Authentifie la connexion entre un serveur de messagerie SMTP et StorageGRID utilisé pour les notifications d'alerte. • Si les communications avec le serveur SMTP nécessitent TLS (transport Layer Security), vous devez spécifier le certificat AC du serveur de messagerie. • Spécifiez un certificat client uniquement si le serveur de messagerie SMTP nécessite des certificats client pour l'authentification.	**Alertes** > **Configuration email**	"Moniteur et amp ; dépannage"

Certificat	Type de certificat	Description	Emplacement de navigation	Détails
Certificat de terminal de l'équilibreur de charge	Serveur	Authentifie la connexion entre les clients S3 ou Swift et le service StorageGRID Load Balancer sur les nœuds de passerelle ou les nœuds d'administration. Vous téléchargez ou générez un certificat d'équilibreur de charge lorsque vous configurez un noeud final d'équilibreur de charge.les applications client utilisent le certificat d'équilibreur de charge lors de la connexion à StorageGRID pour enregistrer et récupérer les données d'objet. **Remarque :** le certificat d'équilibreur de charge est le certificat le plus utilisé pendant le fonctionnement normal de StorageGRID.	**Configuration** > **Paramètres réseau** > **points d'extrémité Load Balancer**	• "Configuration des terminaux d'équilibrage de charge" • Création d'un noeud final d'équilibrage de charge pour FabricPool "Configuration de StorageGRID pour FabricPool"

Certificat	Type de certificat	Description	Emplacement de navigation	Détails
Certificat de serveur de l'interface de gestion	Serveur	Authentifie la connexion entre les navigateurs Web client et l'interface de gestion StorageGRID, permettant aux utilisateurs d'accéder à Grid Manager et au gestionnaire de locataires sans avertissement de sécurité. Ce certificat authentifie également les connexions de l'API de gestion du grid et de l'API de gestion des locataires. Vous pouvez utiliser le certificat de l'autorité de certification interne ou télécharger un certificat personnalisé.	**Configuration** > **Paramètres réseau** > **certificats serveur**	• "Configuration des certificats de serveur" • "Configuration d'un certificat de serveur personnalisé pour le Grid Manager et le tenant Manager"
Certificat de terminal Cloud Storage Pool	Serveur	Authentifie la connexion entre le pool de stockage cloud StorageGRID et un emplacement de stockage externe (tel que le stockage Glacier S3 ou Microsoft Azure Blob). Un certificat différent est requis pour chaque type de fournisseur cloud.	**ILM** > **pools de stockage**	"Gestion des objets avec ILM"

Certificat	Type de certificat	Description	Emplacement de navigation	Détails
Certificat de terminal des services de plate-forme	Serveur	Authentification de la connexion depuis le service de la plateforme StorageGRID vers une ressource de stockage S3	**Tenant Manager** > **STORAGE (S3)** > **Platform services Endpoints**	"Utilisez un compte de locataire"
Certificat de serveur de point final de service d'API de stockage d'objet	Serveur	Authentifie les connexions client S3 ou Swift sécurisées vers le service LDR (local distribution Router) sur un nœud de stockage ou vers le service CLB (Connection Load Balancer) obsolète sur un nœud de passerelle.	**Configuration** > **Paramètres réseau** > **points d'extrémité Load Balancer**	"Configuration d'un certificat de serveur personnalisé pour les connexions au nœud de stockage ou au service CLB"

Exemple 1 : service Load Balancer

Dans cet exemple, StorageGRID sert de serveur.

1. Vous configurez un noeud final de l'équilibreur de charge et téléchargez ou générez un certificat de serveur dans StorageGRID.
2. Vous configurez une connexion client S3 ou Swift au point de terminaison de l'équilibreur de charge et téléchargez le même certificat au client.
3. Lorsque le client souhaite enregistrer ou récupérer des données, il se connecte au point de terminaison de l'équilibreur de charge à l'aide de HTTPS.
4. StorageGRID répond avec le certificat du serveur, qui contient une clé publique, et une signature basée sur la clé privée.
5. Le client vérifie ce certificat en comparant la signature du serveur à la signature figurant sur sa copie du certificat. Si les signatures correspondent, le client lance une session à l'aide de la même clé publique.
6. Le client envoie des données d'objet à StorageGRID.

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

Dans cet exemple, StorageGRID agit comme client.

1. À l'aide du logiciel serveur de gestion de clés externe, vous configurez StorageGRID en tant que client KMS et obtenez un certificat de serveur signé par l'autorité de certification, un certificat de client public et la clé privée pour le certificat client.
2. À l'aide de Grid Manager, vous configurez un serveur KMS et téléchargez les certificats du serveur et du client ainsi que la clé privée du client.
3. Lorsqu'un nœud StorageGRID a besoin d'une clé de chiffrement, il envoie une requête au serveur KMS qui

inclut les données du certificat et une signature basée sur la clé privée.

4. Le serveur KMS valide la signature du certificat et décide qu'il peut faire confiance à StorageGRID.
5. Le serveur KMS répond à l'aide de la connexion validée.

Contrôle de l'accès administrateur à StorageGRID

Vous pouvez contrôler l'accès des administrateurs au système StorageGRID en ouvrant ou en fermant des ports de pare-feu, en gérant les groupes et les utilisateurs d'administration, en configurant l'authentification unique (SSO) et en fournissant des certificats client pour autoriser un accès externe sécurisé aux mesures StorageGRID.

- "Contrôle de l'accès par pare-feu"
- "Utilisation de la fédération des identités"
- "Gestion des groupes d'administration"
- "Gestion des utilisateurs locaux"
- "Utilisation de l'authentification unique (SSO) pour StorageGRID"
- "Configuration des certificats client administrateur"

Contrôle de l'accès par pare-feu

Lorsque vous souhaitez contrôler l'accès par le biais de pare-feu, vous ouvrez ou fermez des ports spécifiques au niveau du pare-feu externe.

Contrôle de l'accès au pare-feu externe

Vous pouvez contrôler l'accès aux interfaces utilisateur et aux API des nœuds d'administration StorageGRID en ouvrant ou en fermant des ports spécifiques au pare-feu externe. Par exemple, vous pouvez empêcher les locataires de se connecter à Grid Manager au niveau du pare-feu, en plus d'utiliser d'autres méthodes pour contrôler l'accès au système.

Port	Description	Si le port est ouvert…
443	Port HTTPS par défaut pour les nœuds d'administration	Les navigateurs Web et les clients d'API de gestion peuvent accéder à Grid Manager, à l'API de gestion du grid, au gestionnaire des locataires et à l'API de gestion des locataires. **Remarque :** le port 443 est également utilisé pour un trafic interne.

Port	Description	Si le port est ouvert…
8443	Port restreint de Grid Manager sur les nœuds d'administration	• Les navigateurs Web et les clients d'API de gestion peuvent accéder à Grid Manager et à l'API de gestion Grid via HTTPS. • Les navigateurs Web et les clients de l'API de gestion ne peuvent pas accéder au Gestionnaire de locataires ou à l'API de gestion des locataires. • Les demandes de contenu interne seront rejetées.
9443	Port de gestionnaire de locataires restreint sur les nœuds d'administration	• Les navigateurs Web et les clients d'API de gestion peuvent accéder au Gestionnaire de locataires et à l'API de gestion des locataires via HTTPS. • Les navigateurs Web et les clients de l'API de gestion ne peuvent pas accéder à Grid Manager ou à l'API de gestion Grid. • Les demandes de contenu interne seront rejetées.

L'authentification unique (SSO) n'est pas disponible sur les ports du gestionnaire de grille restreinte ou du gestionnaire de locataires. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec une connexion unique.

Informations associées

"Connexion au Grid Manager"

"Création d'un compte de locataire si StorageGRID n'utilise pas SSO"

"Résumé : adresses IP et ports pour les connexions client"

"Gestion des réseaux clients non fiables"

"Installez Ubuntu ou Debian"

"Installez VMware"

"Installez Red Hat Enterprise Linux ou CentOS"

Utilisation de la fédération des identités

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

Configuration de la fédération des identités

Vous pouvez configurer la fédération des identités si vous souhaitez que les groupes et utilisateurs d'administration soient gérés dans un autre système, tel qu'Active Directory, OpenLDAP ou Oracle Directory

Server.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.
- Si vous prévoyez d'activer l'authentification unique (SSO), vous devez utiliser Active Directory comme source d'identité fédérée et AD FS comme fournisseur d'identité. Voir « exigences relatives à l'utilisation d'un seul signe ».
- Vous devez utiliser Active Directory, OpenLDAP ou Oracle Directory Server comme fournisseur d'identité.

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

- Si vous prévoyez d'utiliser TLS (transport Layer Security) pour les communications avec le serveur LDAP, le fournisseur d'identité doit utiliser TLS 1.2 ou 1.3.

Description de la tâche

Vous devez configurer un référentiel d'identité pour le Grid Manager si vous souhaitez importer les types de groupes fédérés suivants :

- Groupes d'administration. Les utilisateurs des groupes admin peuvent se connecter au gestionnaire de grille et effectuer des tâches en fonction des autorisations de gestion attribuées au groupe.
- Groupes d'utilisateurs locataires pour les locataires qui n'utilisent pas leur propre référentiel d'identité. Les utilisateurs des groupes de locataires peuvent se connecter au Gestionnaire de locataires et effectuer des tâches en fonction des autorisations attribuées au groupe dans le Gestionnaire de locataires.

Étapes

1. Sélectionnez **Configuration** > **contrôle d'accès** > **fédération d'identités**.
2. Sélectionnez **Activer la fédération d'identités**.

   Les champs de configuration du serveur LDAP s'affichent.

3. Dans la section Type de service LDAP, sélectionnez le type de service LDAP que vous souhaitez configurer.

   Vous pouvez sélectionner **Active Directory**, **OpenLDAP** ou **autre**.

   > Si vous sélectionnez **OpenLDAP**, vous devez configurer le serveur OpenLDAP. Reportez-vous aux instructions de configuration d'un serveur OpenLDAP.

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

4. Si vous avez sélectionné **autre**, renseignez les champs de la section attributs LDAP.
   - **Nom unique utilisateur** : nom de l'attribut qui contient l'identifiant unique d'un utilisateur LDAP. Cet attribut est équivalent à `sAMAccountName` Pour Active Directory et `uid` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `uid`.
   - **UUID d'utilisateur** : nom de l'attribut qui contient l'identifiant unique permanent d'un utilisateur LDAP. Cet attribut est équivalent à `objectGUID` Pour Active Directory et `entryUUID` Pour OpenLDAP. Si

vous configurez Oracle Directory Server, entrez `nsuniqueid`. La valeur de chaque utilisateur pour l'attribut spécifié doit être un nombre hexadécimal à 32 chiffres au format 16 octets ou chaîne, où les tirets sont ignorés.

- **Nom unique de groupe** : nom de l'attribut qui contient l'identifiant unique d'un groupe LDAP. Cet attribut est équivalent à `sAMAccountName` Pour Active Directory et `cn` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `cn`.
- **UUID de groupe** : nom de l'attribut qui contient l'identificateur unique permanent d'un groupe LDAP. Cet attribut est équivalent à `objectGUID` Pour Active Directory et `entryUUID` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `nsuniqueid`. La valeur de chaque groupe pour l'attribut spécifié doit être un nombre hexadécimal à 32 chiffres au format 16 octets ou chaîne, où les tirets sont ignorés.

5. Dans la section configurer le serveur LDAP, entrez les informations de serveur LDAP et de connexion réseau requises.
   - **Nom d'hôte** : le nom d'hôte du serveur ou l'adresse IP du serveur LDAP.
   - **Port** : port utilisé pour se connecter au serveur LDAP.

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

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

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

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

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

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

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

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

6. Dans la section **transport Layer Security (TLS)**, sélectionnez un paramètre de sécurité.
   - **Utilisez STARTTLS (recommandé)** : utilisez STARTTLS pour sécuriser les communications avec le serveur LDAP. Il s'agit de l'option recommandée.
   - **Utilisez LDAPS** : l'option LDAPS (LDAP sur SSL) utilise TLS pour établir une connexion au serveur LDAP. Cette option est prise en charge pour des raisons de compatibilité.
   - **N'utilisez pas TLS** : le trafic réseau entre le système StorageGRID et le serveur LDAP ne sera pas sécurisé.

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

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

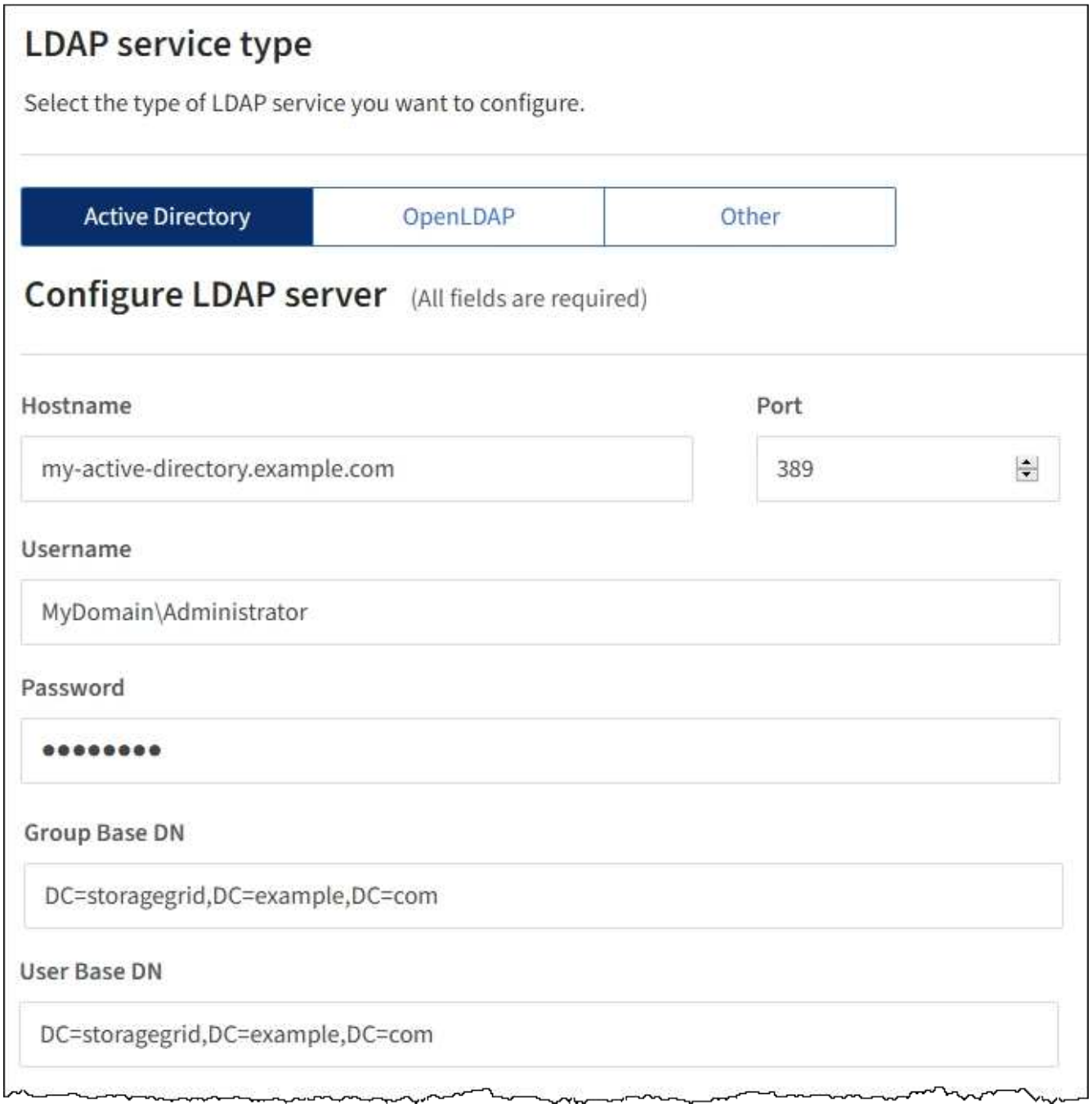
     Si vous sélectionnez ce paramètre, copiez et collez le certificat de sécurité personnalisé dans la zone de texte certificat de l'autorité de certification.

8. Vous pouvez également sélectionner **Tester la connexion** pour valider vos paramètres de connexion pour le serveur LDAP.

   Un message de confirmation s'affiche dans le coin supérieur droit de la page si la connexion est valide.

9. Si la connexion est valide, sélectionnez **Enregistrer**.

   La capture d'écran suivante montre des exemples de valeurs de configuration pour un serveur LDAP qui utilise Active Directory.



Informations associées

"Chiffrement pris en charge pour les connexions TLS sortantes"

"Conditions requises pour l'utilisation de l'authentification unique"

"Création d'un compte de locataire"

"Utilisez un compte de locataire"

Instructions de configuration d'un serveur OpenLDAP

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

Recouvrements de memberOf et de raffint

Les recouvrements de membre et de raffinage doivent être activés. Pour plus d'informations, reportez-vous aux instructions relatives à la maintenance de l'adhésion inverse au groupe dans le Guide de l'administrateur pour OpenLDAP.

Indexation

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

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

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

Reportez-vous aux informations sur la maintenance de l'adhésion au groupe inverse dans le Guide de l'administrateur pour OpenLDAP.

Informations associées

"Documentation OpenLDAP : version 2.4 - Guide de l'administrateur"

Forcer la synchronisation avec le référentiel d'identité

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

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.
- Le référentiel d'identité doit être activé.

Étapes

1. Sélectionnez **Configuration** > **contrôle d'accès** > **fédération d'identités**.

   La page Fédération des identités s'affiche. Le bouton **Synchroniser** se trouve en bas de la page.

2. Cliquez sur **Synchroniser**.

   Un message de confirmation indique que la synchronisation a démarré correctement. Le processus de synchronisation peut prendre un certain temps en fonction de votre environnement.

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

Désactivation de la fédération des identités

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

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

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

- Les utilisateurs fédérés ne pourront pas se connecter.
- Les utilisateurs fédérés qui sont actuellement connectés conservent l'accès au système StorageGRID jusqu'à l'expiration de leur session, mais ils ne pourront pas se connecter après l'expiration de leur session.
- La synchronisation entre le système StorageGRID et le référentiel d'identité ne se produira pas et des alertes ou des alarmes ne seront pas émises pour les comptes qui n'ont pas été synchronisés.
- La case à cocher **Activer la fédération d'identités** est désactivée si l'authentification unique (SSO) est définie sur **Enabled** ou **Sandbox mode**. Le statut SSO sur la page connexion unique doit être **désactivé** avant de pouvoir désactiver la fédération d'identités.

Étapes

1. Sélectionnez **Configuration** > **contrôle d'accès** > **fédération d'identités**.
2. Décochez la case **Activer la fédération d'identités**.
3. Cliquez sur **Enregistrer**.

Informations associées

"Désactivation de la connexion unique"

Gestion des groupes d'administration

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

Création de groupes d'administration

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

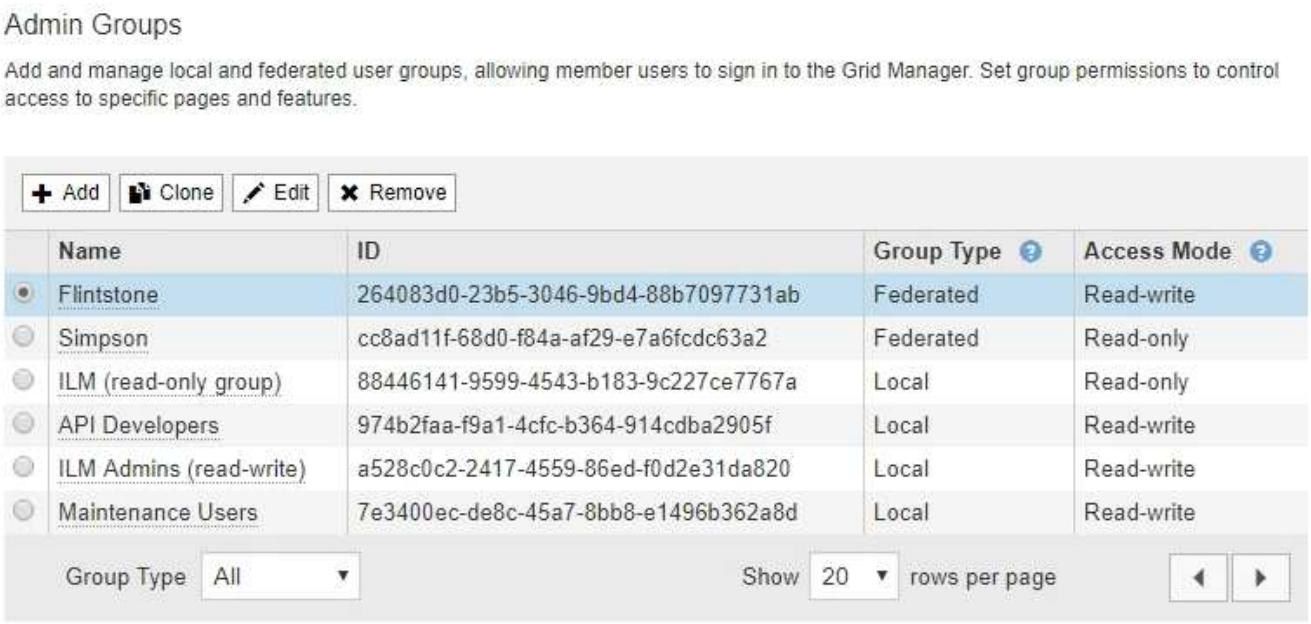
Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.
- Si vous envisagez d'importer un groupe fédéré, vous devez avoir configuré la fédération des identités et le groupe fédéré doit déjà exister dans le référentiel d'identité configuré.

Étapes

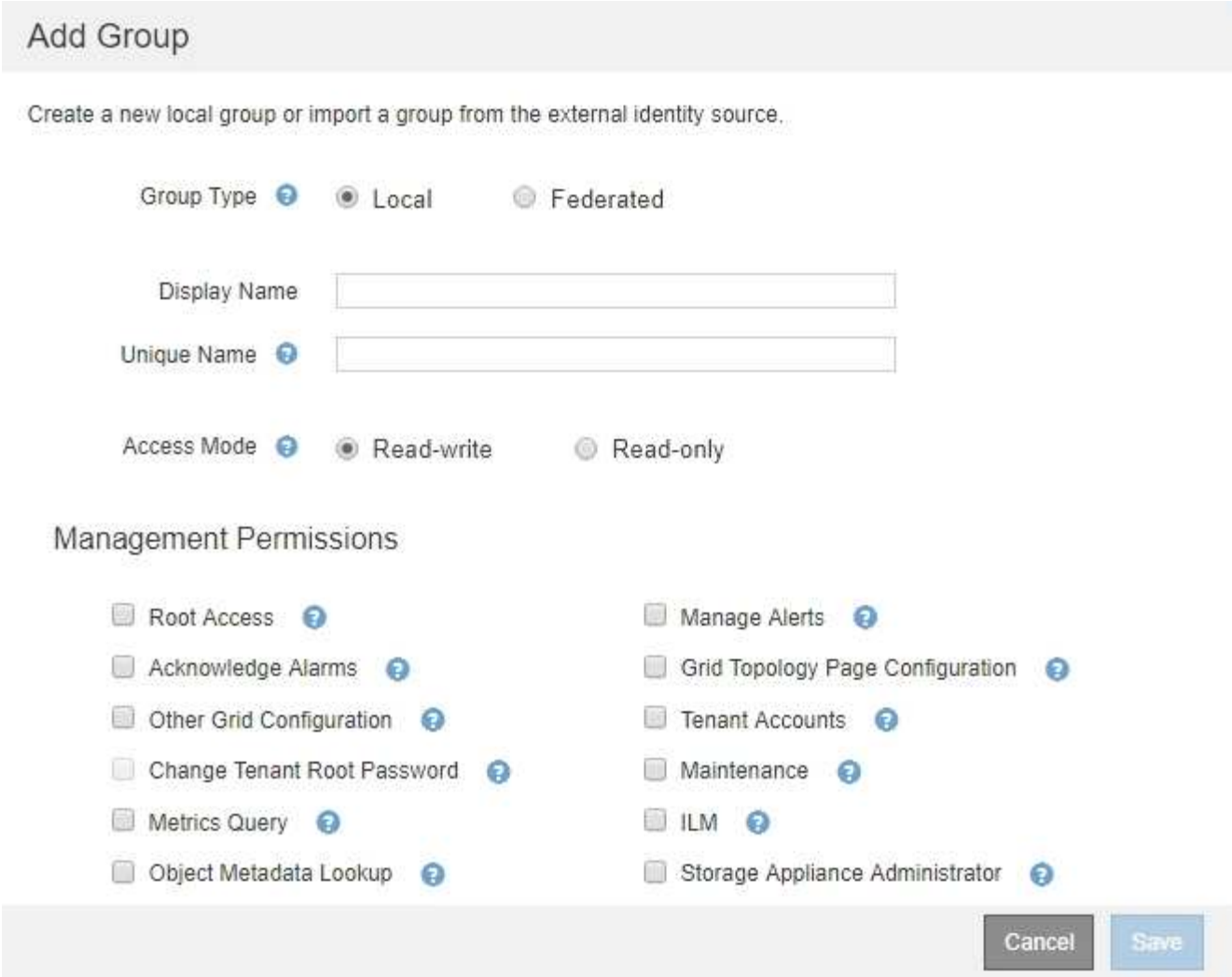
1. Sélectionnez **Configuration** > **contrôle d'accès** > **groupes d'administration**.

   La page groupes d'administration s'affiche et répertorie tous les groupes d'administration existants.



2. Sélectionnez **Ajouter**.

   La boîte de dialogue Ajouter un groupe s'affiche.



3. Pour Type de groupe, sélectionnez **local** si vous souhaitez créer un groupe qui sera utilisé uniquement dans StorageGRID, ou sélectionnez **fédéré** si vous souhaitez importer un groupe à partir du référentiel d'identité.
4. Si vous avez sélectionné **local**, entrez un nom d'affichage pour le groupe. Le nom affiché est le nom qui apparaît dans le gestionnaire de grille. Par exemple, « Maintenance Users » ou « ILM Administrators ».
5. Entrez un nom unique pour le groupe.
   - **Local** : saisissez le nom unique de votre choix. Par exemple, « administrateurs ILM ».
   - **Fédéré** : saisissez le nom du groupe exactement tel qu'il apparaît dans le référentiel d'identité configuré.
6. Dans **Access mode**, sélectionnez si les utilisateurs du groupe peuvent modifier les paramètres et effectuer des opérations dans le gestionnaire de grille et l'API de gestion de grille ou s'ils ne peuvent afficher que les paramètres et les fonctionnalités.
   - **Lecture-écriture** (par défaut) : les utilisateurs peuvent modifier les paramètres et effectuer les opérations autorisées par leurs autorisations de gestion.
   - **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent pas apporter de modifications ni effectuer d'opérations dans Grid Manager ou Grid Management API. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.

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

7. Sélectionnez une ou plusieurs autorisations de gestion.

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

8. Sélectionnez **Enregistrer**.

   Le nouveau groupe est créé. S'il s'agit d'un groupe local, vous pouvez à présent ajouter un ou plusieurs utilisateurs. S'il s'agit d'un groupe fédéré, le référentiel d'identité gère quels utilisateurs appartiennent au groupe.

Informations associées

"Gestion des utilisateurs locaux"

Autorisations de groupe d'administration

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

Vous devez affecter au moins une autorisation à chaque groupe ; sinon, les utilisateurs appartenant à ce groupe ne pourront pas se connecter au gestionnaire de grille.

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

- Connectez-vous au Grid Manager
- Afficher le tableau de bord
- Affichez les pages nœuds
- Surveiller la topologie de la grille
- Afficher les alertes actuelles et résolues
- Afficher les alarmes actuelles et historiques (système hérité)
- Modifier son propre mot de passe (utilisateurs locaux uniquement)
- Afficher certaines informations sur les pages Configuration et maintenance

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

Accès racine

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

Gérer les alertes

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

Accuser réception d'alarmes (système hérité)

Cette autorisation permet d'accuser réception et de répondre aux alarmes (système hérité). Tous les utilisateurs connectés peuvent afficher les alarmes actuelles et historiques.

Si vous souhaitez qu'un utilisateur surveille la topologie de la grille et accuse réception des alarmes uniquement, vous devez attribuer cette autorisation.

Configuration de la page topologie de la grille

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

- Onglets de configuration disponibles dans les pages **support** > **Outils** > **topologie de grille**.
- **Réinitialiser le nombre d'événements** sur l'onglet **noeuds** > **Evénements**.

Autre configuration de grille

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

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

- **Alarmes** (système hérité) :
  - Alarmes globales
  - Configuration de l'ancien e-mail
- **ILM** :
  - Pools de stockage
  - Notes de stockage
- **Configuration** > **Paramètres réseau**
  - Coût des liens
- **Configuration** > **Paramètres système** :
  - Options d'affichage
  - Options de grid
  - Options de stockage
- **Configuration** > **surveillance** :
  - Événements
- **Support**:
  - AutoSupport

Comptes de locataires

Cette autorisation permet d'accéder à la page **locataires** > **tenant Accounts**.

> La version 1 de l'API de gestion du grid (obsolète) utilise cette autorisation pour gérer les règles de groupe de locataires, réinitialiser les mots de passe d'administration Swift et gérer les clés d'accès S3 des utilisateurs root.

Modifier le mot de passe racine du locataire

Cette autorisation donne accès à l'option **changer mot de passe racine** de la page comptes de tenant, ce qui vous permet de contrôler qui peut modifier le mot de passe de l'utilisateur racine local du locataire. Les utilisateurs qui ne disposent pas de cette autorisation ne peuvent pas voir l'option **Modifier le mot de passe racine**.

> Vous devez attribuer l'autorisation comptes de tenant au groupe avant de pouvoir attribuer cette autorisation.

Maintenance

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

- **Configuration** > **Paramètres système** :
  - Noms de domaine*
  - Certificats de serveur*
- **Configuration** > **surveillance** :
  - Vérification*
- **Configuration** > **contrôle d'accès** :
  - Mots de passe de grille
- **Maintenance** > **tâches de maintenance**
  - Désaffectation
  - De développement
  - Reprise après incident
- **Maintenance** > **réseau** :
  - Serveurs DNS*
  - Réseau de grille*
  - Serveurs NTP*
- **Maintenance** > **système** :
  - Licence*
  - Package de restauration
  - Mise à jour logicielle
- **Support** > **Outils** :
  - Journaux
- Les utilisateurs qui ne disposent pas de l'autorisation Maintenance peuvent afficher, mais pas modifier, les pages marquées d'un astérisque.

Requête de metrics

Cette autorisation permet d'accéder à la page **support** > **Outils** > **métriques**. Cette autorisation permet également d'accéder à des requêtes de metrics Prometheus personnalisées à l'aide de la section **Metrics** de l'API Grid Management.

ILM

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

- **Codage d'effacement**
- **Règles**
- **Politiques**
- * Régions*

> L'accès aux options de menu **ILM** > **Storage pools** et **ILM** > **Storage Grapes** est contrôlé par les autres autorisations de configuration de la page de configuration de la grille et de la topologie de la grille.

Recherche des métadonnées d'objet

Cette autorisation permet d'accéder à l'option de menu **ILM** > **Object Metadata Lookup**.

Administrateur de l'appliance de stockage

Cette autorisation permet d'accéder à la gamme E-Series SANtricity System Manager sur les appliances de stockage via Grid Manager.

Interaction entre les autorisations et le mode d'accès

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

Désactivation des fonctions à partir de l'API Grid Management

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

Description de la tâche

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

Pour comprendre l'utilité de cette fonctionnalité, prenez en compte le scénario suivant :

La Société A est un fournisseur de services qui loue la capacité de stockage de son système StorageGRID en créant des comptes de tenant. Pour protéger la sécurité des objets de leurs détenteurs de bail, la Société A veut s'assurer que ses employés ne peuvent jamais accéder à un compte de locataire après le déploiement du compte.

*Société A peut atteindre cet objectif en utilisant le système Désactiver les fonctions dans l'API de gestion de grille. En désactivant complètement la fonction **Modifier le mot de passe racine du locataire** dans le gestionnaire de grille (à la fois l'interface utilisateur et l'API), la société A peut s'assurer qu'aucun utilisateur Admin, y compris l'utilisateur racine et les utilisateurs appartenant à des groupes avec l'autorisation accès racine, ne peut modifier le mot de passe de l'utilisateur racine d'un compte locataire.*

Réactivation des fonctions désactivées

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

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

Pour plus de détails, consultez les instructions d'implémentation des applications client S3 ou Swift.

Étapes

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

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

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

4. Pour réactiver toutes les fonctions, envoyez un corps à l'API comme suit :

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

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

   > L'exemple précédent provoque la réactivation des fonctions *All* DESACTIVE. Si d'autres fonctions doivent rester désactivées, vous devez les spécifier explicitement dans la demande PUT. Par exemple, pour réactiver la fonction Modifier le mot de passe racine du locataire et continuer à désactiver la fonction accusé de réception d'alarme, envoyez cette demande PUT :

   ```
   { "grid": { "alarmAcknowledgment": true } }
   ```

Informations associées

"Via l'API de gestion du grid"

Modification d’un groupe d’administration

Vous pouvez modifier un groupe d’administration pour modifier les autorisations associées au groupe. Pour les groupes d’administration locaux, vous pouvez également mettre à jour le nom d’affichage.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l’aide d’un navigateur pris en charge.
- Vous devez disposer d’autorisations d’accès spécifiques.

Étapes

1. Sélectionnez **Configuration** > **contrôle d’accès** > **groupes d’administration**.
2. Sélectionnez le groupe.

   Si votre système comprend plus de 20 éléments, vous pouvez spécifier le nombre de lignes affichées simultanément sur chaque page. Vous pouvez ensuite utiliser la fonction Rechercher de votre navigateur pour rechercher un élément spécifique dans les lignes affichées.

3. Cliquez sur **Modifier**.
4. Éventuellement, pour les groupes locaux, entrez le nom du groupe qui apparaîtra aux utilisateurs, par exemple "utilisateurs de maintenance".

   Vous ne pouvez pas modifier le nom unique, qui est le nom du groupe interne.

5. Vous pouvez également modifier le mode d’accès du groupe.
   - **Lecture-écriture** (par défaut) : les utilisateurs peuvent modifier les paramètres et effectuer les opérations autorisées par leurs autorisations de gestion.
   - **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent pas apporter de modifications ni effectuer d’opérations dans Grid Manager ou Grid Management API. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.

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

6. Vous pouvez éventuellement ajouter ou supprimer des autorisations de groupe.

   Reportez-vous à la section informations sur les autorisations de groupe d’administration.

7. Sélectionnez **Enregistrer**.

Informations associées

Autorisations de groupe d’administration

Suppression d’un groupe d’administration

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

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Lorsque vous supprimez un groupe, les utilisateurs affectés à ce groupe perdront tous les privilèges d'accès au gestionnaire de grille, à moins qu'ils ne soient accordés par un autre groupe.

Étapes

1. Sélectionnez **Configuration** > **contrôle d'accès** > **groupes d'administration**.
2. Sélectionnez le nom du groupe.

   Si votre système comprend plus de 20 éléments, vous pouvez spécifier le nombre de lignes affichées simultanément sur chaque page. Vous pouvez ensuite utiliser la fonction Rechercher de votre navigateur pour rechercher un élément spécifique dans les lignes affichées.

3. Sélectionnez **Supprimer**.
4. Sélectionnez **OK**.

Gestion des utilisateurs locaux

Vous pouvez créer des utilisateurs locaux et les affecter à des groupes d'administration locaux pour déterminer les fonctions de Grid Manager auxquelles ces utilisateurs peuvent accéder.

Le gestionnaire de grille inclut un utilisateur local prédéfini, nommé « root ». Bien que vous puissiez ajouter et supprimer des utilisateurs locaux, vous ne pouvez pas supprimer l'utilisateur racine.

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

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Création d'un utilisateur local

Si vous avez créé des groupes d'administration locaux, vous pouvez créer un ou plusieurs utilisateurs locaux et attribuer chaque utilisateur à un ou plusieurs groupes. Les autorisations du groupe contrôlent les fonctions de Grid Manager auxquelles l'utilisateur peut accéder.

Description de la tâche

Vous ne pouvez créer que des utilisateurs locaux, et vous pouvez uniquement attribuer ces utilisateurs à des groupes d'administration locaux. Les utilisateurs fédérés et les groupes fédérés sont gérés à l'aide du référentiel d'identité externe.

Étapes

1. Sélectionnez **Configuration** > **contrôle d'accès** > **utilisateurs Admin**.
2. Cliquez sur **Créer**.
3. Entrez le nom d'affichage, le nom unique et le mot de passe de l'utilisateur.
4. Attribuez l'utilisateur à un ou plusieurs groupes qui régissent les autorisations d'accès.

La liste des noms de groupes est générée à partir de la table Groups.

5. Cliquez sur **Enregistrer**.

Informations associées

"Gestion des groupes d'administration"

Modification du compte d'un utilisateur local

Vous pouvez modifier le compte d'un administrateur local pour mettre à jour le nom d'affichage de l'utilisateur ou l'appartenance à un groupe. Vous pouvez également empêcher temporairement un utilisateur d'accéder au système.

Description de la tâche

Vous ne pouvez modifier que les utilisateurs locaux. Les détails de l'utilisateur fédéré sont automatiquement synchronisés avec le référentiel d'identité externe.

Étapes

1. Sélectionnez **Configuration** > **contrôle d'accès** > **utilisateurs Admin**.
2. Sélectionnez l'utilisateur que vous souhaitez modifier.

   Si votre système comprend plus de 20 éléments, vous pouvez spécifier le nombre de lignes affichées simultanément sur chaque page. Vous pouvez ensuite utiliser la fonction Rechercher de votre navigateur pour rechercher un élément spécifique dans les lignes affichées.

3. Cliquez sur **Modifier**.
4. Vous pouvez éventuellement modifier le nom ou l'appartenance à un groupe.
5. Si vous le souhaitez, pour empêcher l'utilisateur d'accéder temporairement au système, cochez la case **refuser l'accès**.
6. Cliquez sur **Enregistrer**.

   Les nouveaux paramètres sont appliqués à la prochaine ouverture de session de l'utilisateur, puis se reconnecte au Gestionnaire de grille.

Suppression du compte d'un utilisateur local

Vous pouvez supprimer des comptes pour les utilisateurs locaux qui n'ont plus besoin d'accéder à Grid Manager.

Étapes

1. Sélectionnez **Configuration** > **contrôle d'accès** > **utilisateurs Admin**.
2. Sélectionnez l'utilisateur local que vous souhaitez supprimer.

   Vous ne pouvez pas supprimer l'utilisateur local racine prédéfini.

   Si votre système comprend plus de 20 éléments, vous pouvez spécifier le nombre de lignes affichées simultanément sur chaque page. Vous pouvez ensuite utiliser la fonction Rechercher de votre navigateur pour rechercher un élément spécifique dans les lignes affichées.

3. Cliquez sur **Supprimer**.

4. Cliquez sur **OK**.

Modification du mot de passe d'un utilisateur local

Les utilisateurs locaux peuvent modifier leurs propres mots de passe à l'aide de l'option **changer mot de passe** de la bannière du gestionnaire de grille. En outre, les utilisateurs qui ont accès à la page Admin Users peuvent modifier les mots de passe d'autres utilisateurs locaux.

Description de la tâche

Vous ne pouvez modifier les mots de passe que pour les utilisateurs locaux. Les utilisateurs fédérés doivent modifier leurs propres mots de passe dans le référentiel d'identité externe.

Étapes

1. Sélectionnez **Configuration** > **contrôle d'accès** > **utilisateurs Admin**.
2. Sur la page utilisateurs, sélectionnez l'utilisateur.

   Si votre système comprend plus de 20 éléments, vous pouvez spécifier le nombre de lignes affichées simultanément sur chaque page. Vous pouvez ensuite utiliser la fonction Rechercher de votre navigateur pour rechercher un élément spécifique dans les lignes affichées.

3. Cliquez sur **Modifier le mot de passe**.
4. Saisissez et confirmez le mot de passe, puis cliquez sur **Enregistrer**.

Utilisation de l'authentification unique (SSO) pour StorageGRID

Le système StorageGRID prend en charge la fonctionnalité SSO (Single Sign-on) en utilisant la 2.0 norme SAML 2.0 (Security assertion Markup Language). Lorsque l'authentification SSO est activée, tous les utilisateurs doivent être authentifiés par un fournisseur d'identités externe avant d'accéder au Grid Manager, au tenant Manager, à l'API Grid Management ou à l'API de gestion des locataires. Les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

- "Fonctionnement de l'authentification unique"
- "Conditions requises pour l'utilisation de l'authentification unique"
- "Configuration de l'authentification unique"

Fonctionnement de l'authentification unique

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

Connexion lorsque SSO est activé

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

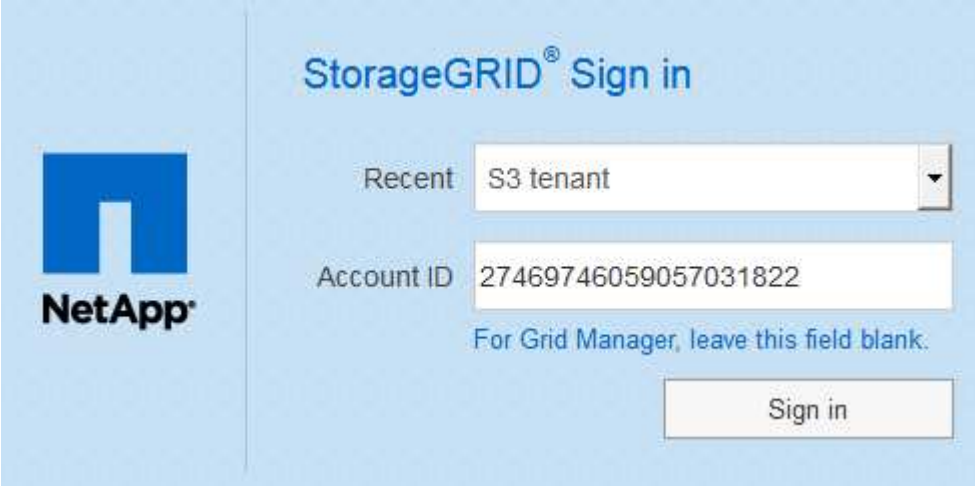
Étapes

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

La page de connexion StorageGRID s'affiche.

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

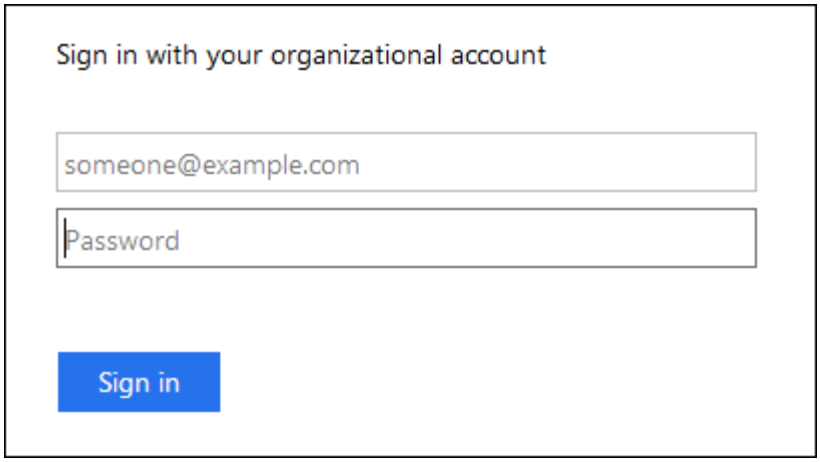
- Si vous avez déjà accédé au Grid Manager ou au tenant Manager, vous êtes invité à sélectionner un compte récent ou à saisir un ID de compte :



> La page de connexion StorageGRID n'apparaît pas lorsque vous saisissez l'URL complète d'un compte de locataire (c'est-à-dire un nom de domaine complet ou une adresse IP suivi de `/?accountId=20-digit-account-id`). Au lieu de cela, vous êtes immédiatement redirigé vers la page de connexion SSO de votre entreprise, où vous pouvez Connectez-vous à l'aide de vos identifiants SSO.

2. Indiquez si vous souhaitez accéder au Grid Manager ou au tenant Manager :
   - Pour accéder au Grid Manager, laissez le champ Identifiant de compte** vide, saisissez **0** comme ID de compte ou sélectionnez **Grid Manager** si celui-ci apparaît dans la liste des comptes récents.
   - Pour accéder au Gestionnaire de locataires, entrez l'ID de compte de tenant à 20 chiffres ou sélectionnez un locataire par nom s'il apparaît dans la liste des comptes récents.
3. Cliquez sur **connexion**

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



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

   Si vos informations d'identification SSO sont correctes :

   a. Le fournisseur d'identités fournit une réponse d'authentification à StorageGRID.
   b. StorageGRID valide la réponse d'authentification.
   c. Si la réponse est valide et que vous appartenez à un groupe fédéré disposant d'une autorisation d'accès adéquate, vous êtes connecté au Grid Manager ou au tenant Manager, selon le compte que vous avez sélectionné.

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

   Il n'est pas nécessaire de saisir à nouveau vos identifiants SSO.

Déconnexion lorsque SSO est activé

Lorsque l'authentification SSO est activée pour StorageGRID, le processus de déconnexion dépend de ce que vous êtes connecté et de l'endroit où vous vous déconnectez.

Étapes

1. Repérez le lien **Déconnexion** dans le coin supérieur droit de l'interface utilisateur.
2. Cliquez sur **Déconnexion**.

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

Si vous êtes connecté à…	Et vous vous déconnectez de…	Vous êtes déconnecté de…
Grid Manager sur un ou plusieurs nœuds d'administration	Grid Manager sur n'importe quel nœud d'administration	Grid Manager sur tous les nœuds d'administration
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

Si vous êtes connecté à…	Et vous vous déconnectez de…	Vous êtes déconnecté de…
Grid Manager et tenant Manager	Gestionnaire de grille	Le Grid Manager uniquement. Vous devez également vous déconnecter du tenant Manager pour vous déconnecter de SSO.

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

Conditions requises pour l'utilisation de l'authentification unique

Avant d'activer la signature unique (SSO) pour un système StorageGRID, consultez les conditions requises dans cette section.

> L'authentification unique (SSO) n'est pas disponible sur les ports du gestionnaire de grille restreinte ou du gestionnaire de locataires. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec une connexion unique.

Exigences du fournisseur d'identités

Le fournisseur d'identités (IDP) pour SSO doit satisfaire aux exigences suivantes :

- L'une des versions suivantes d'Active Directory Federation Service (AD FS) :
  - AD FS 4.0, inclus dans Windows Server 2016

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

  - AD FS 3.0, inclus avec la mise à jour Windows Server 2012 R2, ou une version ultérieure.
- TLS (transport Layer Security) 1.2 ou 1.3
- Microsoft .NET Framework, version 3.5.1 ou supérieure

Configuration requise pour le certificat de serveur

StorageGRID utilise un certificat de serveur d'interface de gestion sur chaque nœud d'administration pour sécuriser l'accès à Grid Manager, au gestionnaire de locataires, à l'API de gestion du grid et à l'API de gestion des locataires. Lorsque vous configurez les approbations de tiers basés SSO pour StorageGRID dans AD FS, vous utilisez le certificat de serveur comme certificat de signature pour les requêtes StorageGRID à AD FS.

Si vous n'avez pas encore installé de certificat de serveur personnalisé pour l'interface de gestion, vous devriez le faire maintenant. Lorsque vous installez un certificat de serveur personnalisé, il est utilisé pour tous les nœuds d'administration et vous pouvez l'utiliser dans toutes les approbations de tiers StorageGRID.

> Il n'est pas recommandé d'utiliser le certificat de serveur par défaut d'un nœud d'administration dans la confiance de l'intervenant de confiance AD FS. Si le nœud échoue et que vous le récupérez, un nouveau certificat de serveur par défaut est généré. Avant de pouvoir vous connecter au nœud restauré, vous devez mettre à jour la confiance de la partie utilisatrice dans AD FS avec le nouveau certificat.

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

Informations associées

"Contrôle de l'accès par pare-feu"

"Configuration d'un certificat de serveur personnalisé pour le Grid Manager et le tenant Manager"

Configuration de l'authentification unique

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

- "Confirmer que les utilisateurs fédérés peuvent se connecter"
- "Utilisation du mode sandbox"
- "Création de fiducies de tiers de confiance dans AD FS"
- "Confiance de la partie qui fait confiance aux essais"
- "Activation de l'authentification unique"
- "Désactivation de la connexion unique"
- "Désactivation et réactivation temporaire de l'authentification unique pour un nœud d'administration"

Confirmer que les utilisateurs fédérés peuvent se connecter

Avant d'activer l'authentification unique (SSO), vous devez confirmer qu'au moins un utilisateur fédéré peut se connecter au Grid Manager et au tenant Manager pour tout compte de tenant existant.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous utilisez Active Directory en tant que source d'identité fédérée et AD FS en tant que fournisseur d'identité.

  "Conditions requises pour l'utilisation de l'authentification unique"

Étapes

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

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

a. Connectez-vous au Gestionnaire de locataires pour chaque compte de locataire.

b. Sélectionnez **contrôle d'accès** > **fédération d'identités**.

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

d. Si c'est le cas, vérifiez que les groupes fédérés qui pourraient être utilisés pour ce compte de locataire ne sont plus nécessaires, désélectionnez la case à cocher et cliquez sur **Enregistrer**.

2. Vérifiez qu'un utilisateur fédéré peut accéder au Grid Manager :

   a. Dans Grid Manager, sélectionnez **Configuration** > **contrôle d'accès** > **groupes d'administration**.

   b. Assurez-vous qu'au moins un groupe fédéré a été importé du référentiel d'identité Active Directory et qu'il a reçu l'autorisation accès racine.

   c. Se déconnecter.

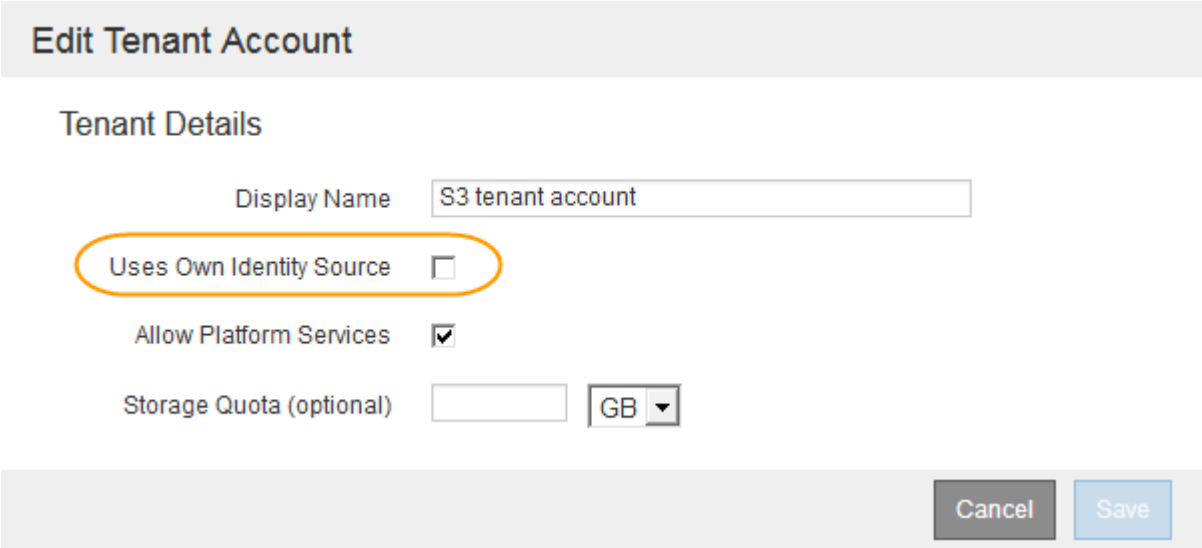
   d. Confirmez que vous pouvez vous reconnecter au Grid Manager en tant qu'utilisateur dans le groupe fédéré.

3. S'il existe déjà des comptes de tenant, confirmez qu'un utilisateur fédéré disposant d'une autorisation accès racine peut se connecter :

   a. Dans Grid Manager, sélectionnez **tenants**.

   b. Sélectionnez le compte de tenant, puis cliquez sur **Modifier le compte**.

   c. Si la case **utilise son propre référentiel d'identité** est cochée, décochez la case et cliquez sur **Enregistrer**.



   La page comptes de tenant s'affiche.

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

   b. Dans le Gestionnaire de locataires, cliquez sur **contrôle d'accès** > **groupes**.

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

   d. Se déconnecter.

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

Informations associées

"Conditions requises pour l'utilisation de l'authentification unique"

"Gestion des groupes d'administration"

"Utilisez un compte de locataire"

Utilisation du mode sandbox

Vous pouvez utiliser le mode sandbox pour configurer et tester les approbations de parties utilisatrices Active Directory Federation Services (AD FS) avant d'appliquer l'authentification unique (SSO) pour les utilisateurs StorageGRID. Une fois l'authentification SSO activée, vous pouvez réactiver le mode sandbox pour configurer ou tester les approbations nouvelles et existantes. La réactivation du mode sandbox désactive temporairement l'authentification SSO pour les utilisateurs StorageGRID.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Lorsque SSO est activé et qu'un utilisateur tente de se connecter à un nœud d'administration, StorageGRID envoie une demande d'authentification à AD FS. À son tour, AD FS renvoie une réponse d'authentification à StorageGRID, indiquant si la demande d'autorisation a réussi. Pour les requêtes réussies, la réponse inclut un identificateur unique universel (UUID) pour l'utilisateur.

Pour permettre à StorageGRID (le fournisseur de services) et à AD FS (le fournisseur d'identité) de communiquer en toute sécurité au sujet des demandes d'authentification des utilisateurs, vous devez configurer certains paramètres dans StorageGRID. Ensuite, vous devez utiliser AD FS pour créer une confiance de partie de confiance pour chaque nœud d'administration. Enfin, vous devez revenir à StorageGRID pour activer le SSO.

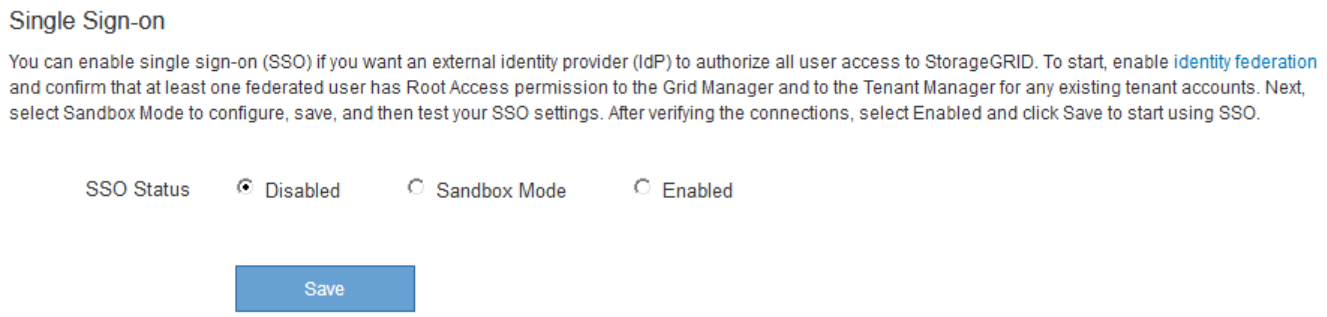
Le mode sandbox facilite l'exécution de cette configuration et le test de tous vos paramètres avant l'activation de SSO.

> L'utilisation du mode sandbox est fortement recommandée, mais pas strictement nécessaire. Si vous êtes prêt à créer des approbations de tiers AD FS immédiatement après avoir configuré SSO dans StorageGRID, Vous n'avez pas besoin de tester les processus SSO et SLO (Single logout) pour chaque noeud d'administration, cliquez sur **Enabled**, saisissez les paramètres StorageGRID, créez une confiance de partie de confiance pour chaque noeud d'administration dans AD FS, puis cliquez sur **Save** pour activer SSO.

Étapes

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

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



> Si les options d'état SSO ne s'affichent pas, confirmez que vous avez configuré Active Directory en tant que référentiel d'identité fédéré. Voir « exigences relatives à l'utilisation d'un seul signe ».

2. Sélectionnez l'option **Sandbox mode**.

   Les paramètres fournisseur d'identité et partie de confiance s'affichent. Dans la section Identity Provider, le champ **Service Type** est en lecture seule. Elle indique le type de service de fédération d'identités que vous utilisez (par exemple, Active Directory).

3. Dans la section Identity Provider :

   a. Entrez le nom du service de fédération, exactement tel qu'il apparaît dans AD FS.

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

   b. Indiquez si vous souhaitez utiliser TLS (transport Layer Security) pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux requêtes StorageGRID.

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

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

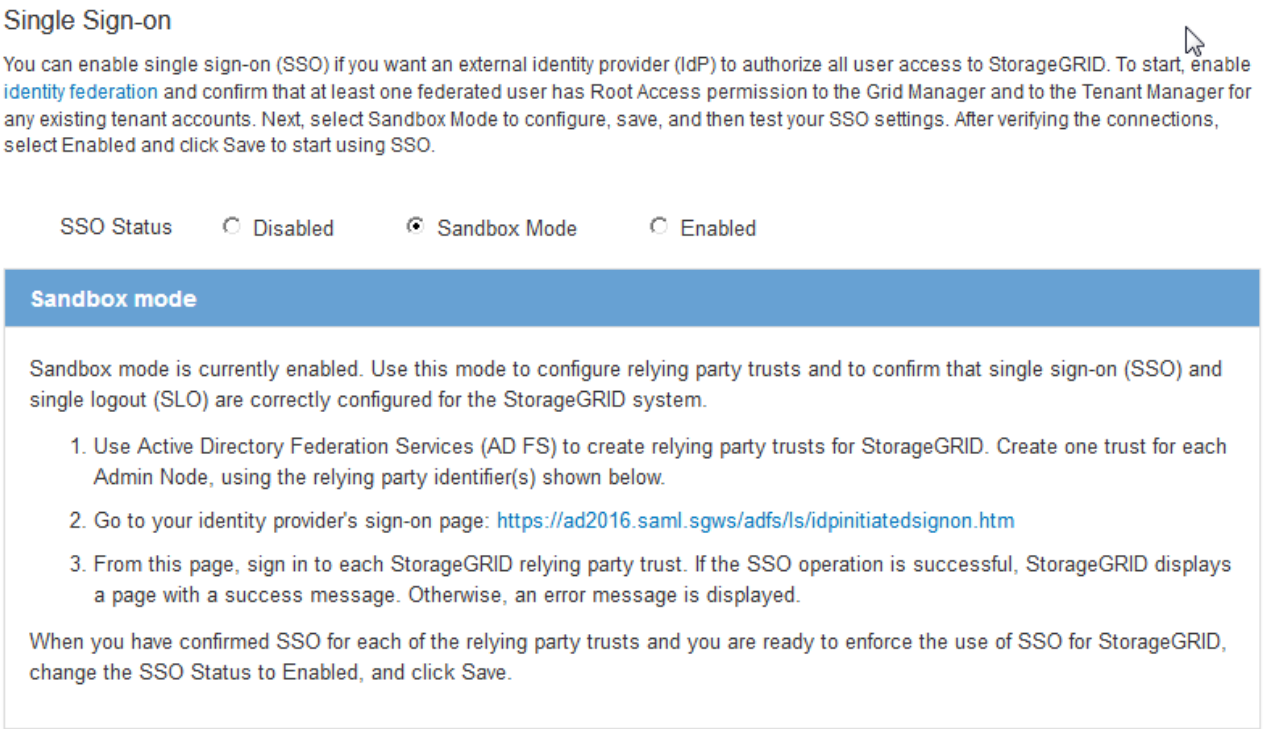
      - **N'utilisez pas TLS**: N'utilisez pas de certificat TLS pour sécuriser la connexion.

4. Dans la section partie utilisatrice, spécifiez l'identifiant de partie utilisatrice que vous utiliserez pour les nœuds Admin StorageGRID lorsque vous configurez des approbations de partie utilisatrice.

   - Par exemple, si votre grid ne comporte qu'un seul nœud d'administration et que vous n'prévoyez pas d'ajouter de nœuds d'administration à l'avenir, entrez `SG` ou `StorageGRID`.
   - Si votre grid inclut plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identificateur. Par exemple : `SG-[HOSTNAME]`. Cela génère une table qui inclut un identifiant de partie de confiance pour chaque nœud d'administration, en fonction du nom d'hôte du nœud. + REMARQUE : vous devez créer une confiance en tiers pour chaque nœud d'administration de votre système StorageGRID. Le fait d'avoir une confiance de partie de confiance pour chaque nœud d'administration permet aux utilisateurs de se connecter et de se déconnecter en toute sécurité à n'importe quel nœud d'administration.

5. Cliquez sur **Enregistrer**.
   - Une coche verte apparaît sur le bouton **Save** pendant quelques secondes.

   - L'avis de confirmation du mode Sandbox s'affiche, confirmant que le mode sandbox est à présent activé. Vous pouvez utiliser ce mode pendant que vous utilisez AD FS pour configurer une confiance de tiers de confiance pour chaque nœud d'administration et tester les processus d'ouverture de session unique (SSO) et de déconnexion unique (SLO).



Informations associées

"Conditions requises pour l'utilisation de l'authentification unique"

Création de fiducies de tiers de confiance dans AD FS

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

Création d'une confiance de confiance avec Windows PowerShell

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

Ce dont vous avez besoin

- Vous avez configuré l'authentification unique dans StorageGRID et vous connaissez le nom de domaine complet (ou l'adresse IP) et l'identifiant de partie utilisatrice pour chaque noeud d'administration de votre

système.

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

- Vous avez l'expérience de créer des approbations de tiers de confiance dans AD FS, ou vous avez accès à la documentation Microsoft AD FS.
- Vous utilisez le composant logiciel enfichable AD FS Management et vous appartenez au groupe administrateurs.

Description de la tâche

Ces instructions s'appliquent à AD FS 4.0, qui est inclus dans Windows Server 2016. Si vous utilisez AD FS 3.0, qui est inclus dans Windows 2012 R2, vous remarquerez de légères différences dans la procédure. Pour toute question, consultez la documentation Microsoft AD FS.

Étapes

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

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

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

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

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

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

c. Cliquez sur **Ajouter règle**.

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

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

   Par exemple, **objectGUID to Name ID**.

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

g. Dans la colonne attribut LDAP de la table mappage, saisissez **objectGUID**.

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

i. Cliquez sur **Terminer**, puis sur **OK**.

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

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

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

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

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

9. Lorsque vous avez terminé, revenez à StorageGRID et "tester toutes les fiducies de la partie qui repose" pour confirmer qu'ils sont correctement configurés.

Création d'une confiance de tiers de confiance en important des métadonnées de fédération

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

Ce dont vous avez besoin

- Vous avez configuré l'authentification unique dans StorageGRID et vous connaissez le nom de domaine complet (ou l'adresse IP) et l'identifiant de partie utilisatrice pour chaque noeud d'administration de votre système.

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

- Vous avez l'expérience de créer des approbations de tiers de confiance dans AD FS, ou vous avez accès à la documentation Microsoft AD FS.
- Vous utilisez le composant logiciel enfichable AD FS Management et vous appartenez au groupe administrateurs.

Description de la tâche

Ces instructions s'appliquent à AD FS 4.0, qui est inclus dans Windows Server 2016. Si vous utilisez AD FS

3.0, qui est inclus dans Windows 2012 R2, vous remarquerez de légères différences dans la procédure. Pour toute question, consultez la documentation Microsoft AD FS.

Étapes

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

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

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

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

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

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

      Par exemple, **objectGUID to Name ID**.

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

      Si les métadonnées sont manquantes, confirmez que l'adresse des métadonnées de la fédération est

correcte ou entrez simplement les valeurs manuellement.

9. Répétez ces étapes pour configurer une confiance de tiers pour tous les nœuds d'administration de votre système StorageGRID.
10. Lorsque vous avez terminé, revenez à StorageGRID et "tester toutes les fiducies de la partie qui repose" pour confirmer qu'ils sont correctement configurés.

Création manuelle d'une confiance de partie de confiance

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

Ce dont vous avez besoin

- Vous avez configuré l'authentification unique dans StorageGRID et vous connaissez le nom de domaine complet (ou l'adresse IP) et l'identifiant de partie utilisatrice pour chaque noeud d'administration de votre système.

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

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

Description de la tâche

Ces instructions s'appliquent à AD FS 4.0, qui est inclus dans Windows Server 2016. Si vous utilisez AD FS 3.0, qui est inclus dans Windows 2012 R2, vous remarquerez de légères différences dans la procédure. Pour toute question, consultez la documentation Microsoft AD FS.

Étapes

1. Dans le Gestionnaire de serveur Windows, cliquez sur **Outils**, puis sélectionnez **AD FS Management**.
2. Sous actions, cliquez sur **Ajouter la confiance de la partie de confiance**.
3. Sur la page de bienvenue, choisissez **revendications Aware**, puis cliquez sur **Démarrer**.
4. Sélectionnez **Entrez les données relatives à la partie de confiance manuellement**, puis cliquez sur **Suivant**.
5. Suivez l'assistant confiance de la partie de confiance :

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

      Pour plus de cohérence, utilisez l'identifiant de partie utilisatrices du nœud d'administration, exactement comme il apparaît sur la page Single Sign-On du Grid Manager. Par exemple : `SG-DC1-ADM1`.

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

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

WebSSO.

d. Saisissez l'URL du noeud final du service SAML pour le noeud d'administration :

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

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

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

```
Admin_Node_Identifier
```

Pour *`Admin_Node_Identifier`*, Entrez l'identifiant de partie de confiance du noeud d'administration, exactement comme il apparaît sur la page Single Sign-On. Par exemple : `SG-DC1-ADM1`.

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

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

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

6. Pour démarrer l'assistant règle de sinistre, cliquez sur **Ajouter règle** :
   a. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer attributs LDAP en tant que revendications** dans la liste, puis cliquez sur **Suivant**.
   b. Sur la page configurer la règle, entrez un nom d'affichage pour cette règle.

      Par exemple, **objectGUID to Name ID**.

   c. Pour le magasin d'attributs, sélectionnez **Active Directory**.
   d. Dans la colonne attribut LDAP de la table mappage, saisissez **objectGUID**.
   e. Dans la colonne Type de demande sortante de la table mappage, sélectionnez **Nom ID** dans la liste déroulante.
   f. Cliquez sur **Terminer**, puis sur **OK**.
7. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrices pour ouvrir ses propriétés.
8. Dans l'onglet **Endpoints**, configurez le noeud final pour une déconnexion unique (SLO) :
   a. Cliquez sur **Ajouter SAML**.
   b. Sélectionnez **Endpoint Type** > **SAML Logout**.
   c. Sélectionnez **Redirect** > **Redirect**.
   d. Dans le champ **URL de confiance**, entrez l'URL utilisée pour la déconnexion unique (SLO) à partir de ce noeud d'administration :

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

Pour *`Admin_Node_FQDN`*, Entrez le nom de domaine complet du nœud d'administration. (Si nécessaire,

vous pouvez utiliser l'adresse IP du nœud à la place. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)

a. Cliquez sur **OK**.

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

   a. Ajouter le certificat personnalisé :

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

        Remarque : utilisation du certificat par défaut du noeud d'administration (`server.crt`) n'est pas recommandé. Si le nœud d'administration échoue, le certificat par défaut sera régénéré lorsque vous restaurez le nœud et vous devrez mettre à jour la confiance de l'organisme de confiance.

   b. Cliquez sur **appliquer**, puis sur **OK**.

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

10. Répétez ces étapes pour configurer une confiance de tiers pour tous les nœuds d'administration de votre système StorageGRID.
11. Lorsque vous avez terminé, revenez à StorageGRID et "tester toutes les fiducies de la partie qui repose" pour confirmer qu'ils sont correctement configurés.

Confiance de la partie qui fait confiance aux essais

Avant d'appliquer l'utilisation de l'authentification unique (SSO) pour StorageGRID, vérifiez que l'authentification unique et la déconnexion unique (SLO) sont correctement configurées. Si vous avez créé une confiance en tiers pour chaque nœud d'administration, confirmez que vous pouvez utiliser SSO et SLO pour chaque nœud d'administration.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous avez configuré une ou plusieurs fiducies de tiers de confiance dans AD FS.

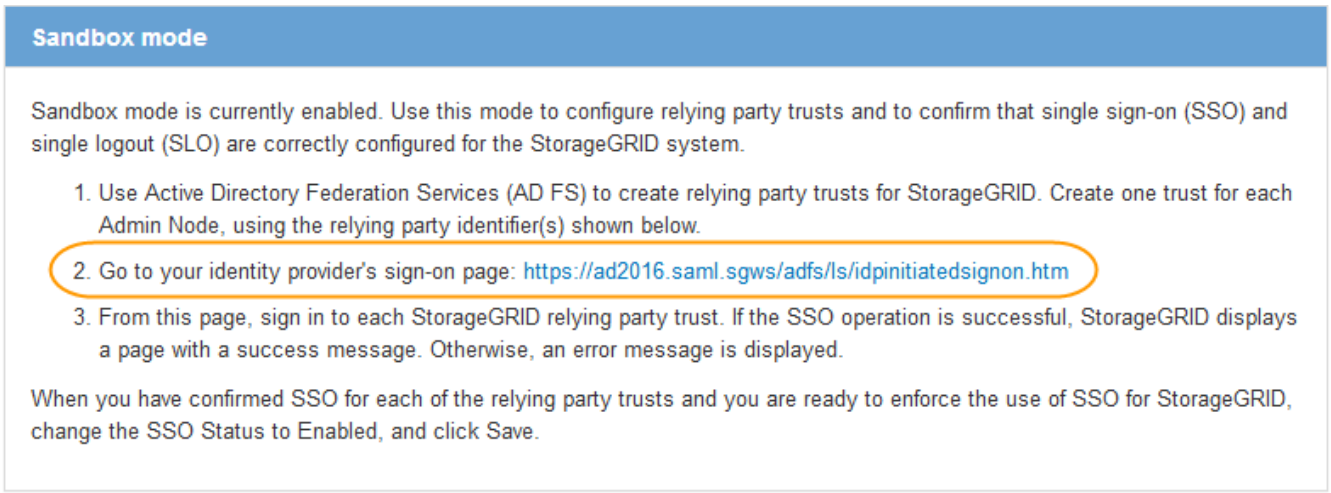
Étapes

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

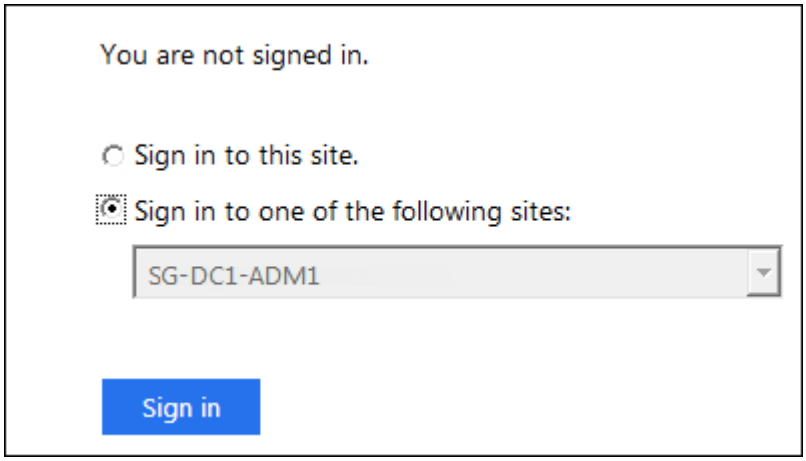
   La page connexion unique s'affiche, avec l'option **Sandbox mode** sélectionnée.

2. Dans les instructions pour le mode sandbox, recherchez le lien vers la page de connexion de votre fournisseur d'identités.

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

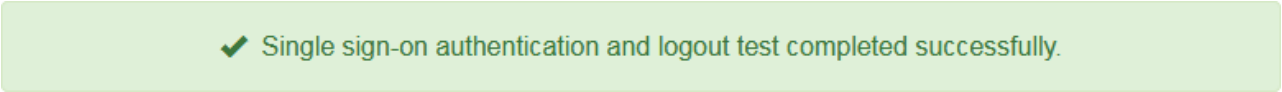


3. Cliquez sur le lien ou copiez et collez l'URL dans un navigateur pour accéder à la page de connexion de votre fournisseur d'identités.
4. Pour confirmer que vous pouvez utiliser l'authentification SSO pour vous connecter à StorageGRID, sélectionnez **connexion à l'un des sites suivants**, sélectionnez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



Vous devez entrer votre nom d'utilisateur et votre mot de passe.

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



   - Si l'opération SSO échoue, un message d'erreur s'affiche. Corrigez le problème, effacez les cookies du navigateur et réessayez.
6. Répétez les étapes précédentes pour confirmer que vous pouvez vous connecter à n'importe quel autre nœud d'administration.

   Si toutes les opérations de connexion SSO et de déconnexion ont réussi, vous êtes prêt à activer SSO.

Activation de l'authentification unique

Après avoir utilisé le mode sandbox pour tester toutes vos approbations StorageGRID, vous êtes prêt à activer l'authentification unique (SSO).

Ce dont vous avez besoin

- Vous devez avoir importé au moins un groupe fédéré du référentiel d'identité et affecté des autorisations de gestion de l'accès racine au groupe. Vous devez confirmer qu'au moins un utilisateur fédéré dispose d'une autorisation d'accès racine au gestionnaire de grille et au gestionnaire de locataires pour tout compte de locataire existant.
- Vous devez avoir testé toutes les approbations de parties utilisatrices à l'aide du mode sandbox.

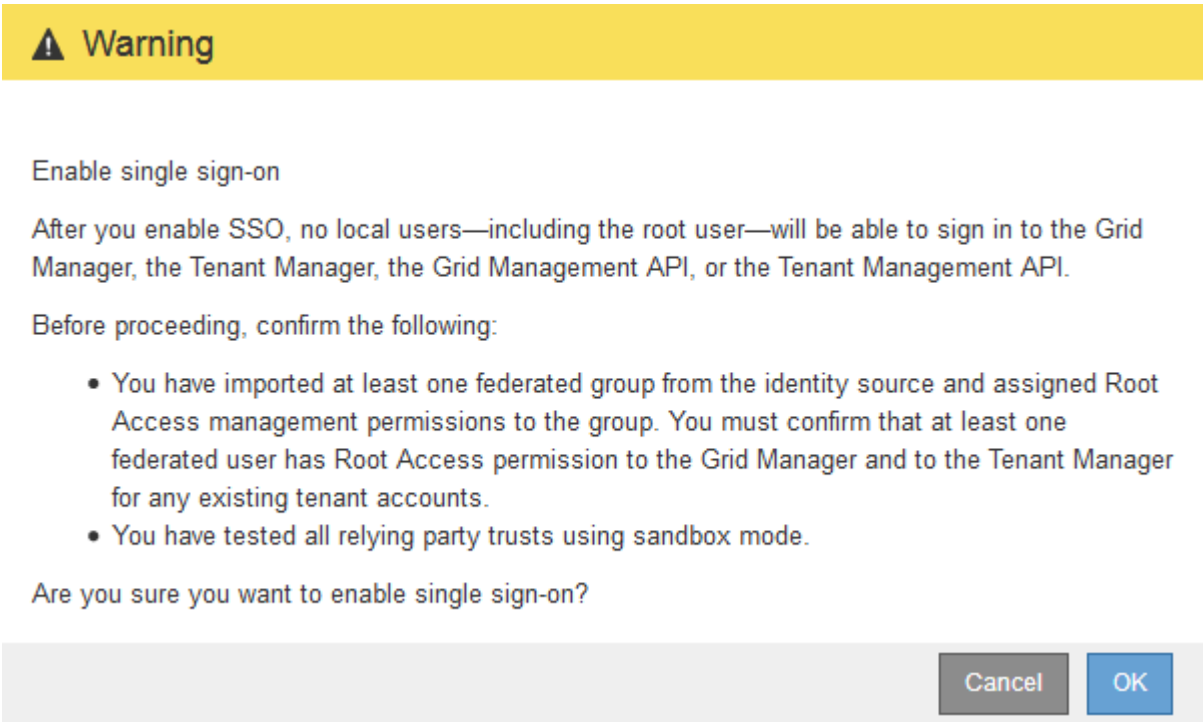
Étapes

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

   La page Single Sign-On s'affiche avec **Sandbox mode** sélectionné.

2. Définissez l'état SSO sur **activé**.
3. Cliquez sur **Enregistrer**.

   Un message d'avertissement s'affiche.



4. Vérifiez l'avertissement et cliquez sur **OK**.

   L'authentification unique est désormais activée.

> Tous les utilisateurs doivent utiliser l'authentification SSO pour accéder au Grid Manager, au Gestionnaire de locataires, à l'API de gestion Grid et à l'API de gestion des locataires. Les utilisateurs locaux ne peuvent plus accéder à StorageGRID.

Désactivation de la connexion unique

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

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

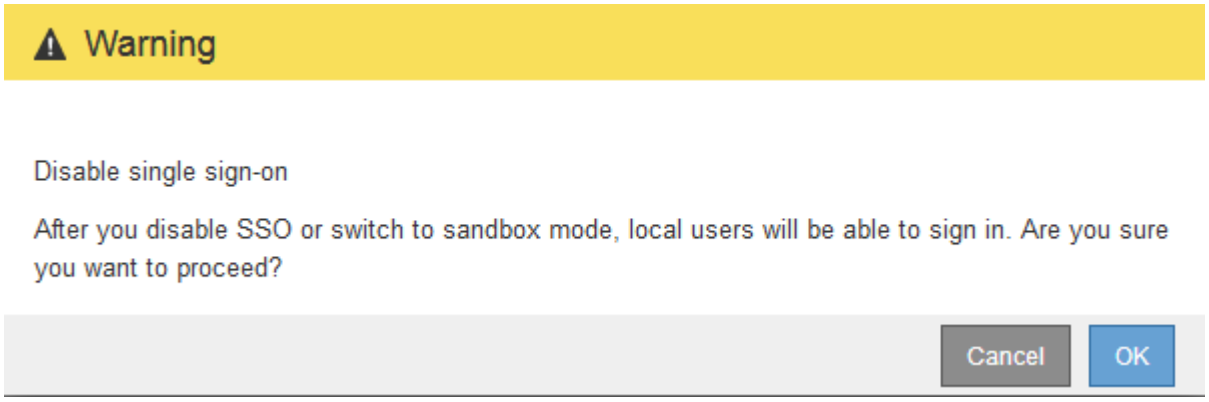
Étapes

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

   La page authentification unique s'affiche.

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

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



4. Cliquez sur **OK**.

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

Désactivation et réactivation temporaire de l'authentification unique pour un nœud d'administration

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

Ce dont vous avez besoin

- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir le `Passwords.txt` fichier.
- Vous devez connaître le mot de passe de l'utilisateur root local.

Description de la tâche

Après avoir désactivé SSO pour un noeud d'administration, vous pouvez vous connecter à Grid Manager en tant qu'utilisateur racine local. Pour sécuriser votre système StorageGRID, vous devez utiliser le shell de commande du nœud pour réactiver SSO sur le nœud d'administration dès que vous vous déconnectez.

> La désactivation de SSO pour un nœud d'administration n'affecte pas les paramètres SSO pour les autres nœuds d'administration de la grille. La case à cocher **Activer SSO** sur la page d'ouverture de session unique dans Grid Manager reste sélectionnée et tous les paramètres SSO existants sont conservés à moins que vous ne les mettrez à jour.

Étapes

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

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
2. Exécutez la commande suivante :`disable-saml`

   Un message indique que la commande s'applique uniquement à ce nœud d'administration.
3. Confirmez que vous souhaitez désactiver l'authentification SSO.

   Un message indique que l'authentification unique est désactivée sur le nœud.
4. À partir d'un navigateur Web, accédez à Grid Manager sur le même nœud d'administration.

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

      Si vous cliquez sur **Enregistrer** à partir de la page connexion unique, l'option SSO est automatiquement réactivée pour l'ensemble de la grille.
7. Si vous avez désactivé l'authentification SSO temporairement car vous devez accéder au Grid Manager pour une autre raison :
   a. Effectuez les tâches que vous souhaitez effectuer.
   b. Cliquez sur **Déconnexion** et fermez le gestionnaire de grille.
   c. Réactivez SSO sur le nœud d'administration. Vous pouvez effectuer l'une des opérations suivantes :
      - Exécutez la commande suivante : `enable-saml`

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

Confirmez que vous souhaitez activer le SSO.

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

- Redémarrez le nœud grid : `reboot`

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

Informations associées

"Configuration de l'authentification unique"

Configuration des certificats client administrateur

Vous pouvez utiliser les certificats client pour permettre aux clients externes autorisés d'accéder à la base de données StorageGRID Prometheus. Les certificats client constituent un moyen sécurisé d'utiliser des outils externes pour 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 de certificat dans l'outil externe.

Ajout de certificats client administrateur

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

Ce dont vous avez besoin

- Vous devez disposer de l'autorisation accès racine.
- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez connaître l'adresse IP ou le nom de domaine du nœud d'administration.
- Vous devez avoir configuré le certificat de serveur de l'interface de gestion StorageGRID et avoir le bundle CA correspondant
- Si vous souhaitez télécharger votre propre certificat, la clé publique et la clé privée du certificat doivent être disponibles sur votre ordinateur local.

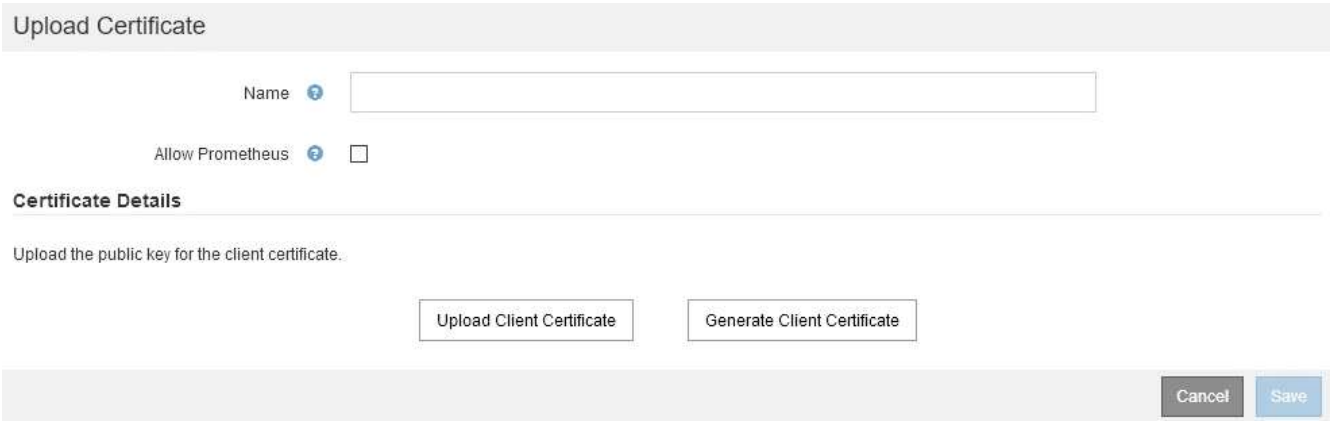
Étapes

1. Dans Grid Manager, sélectionnez **Configuration** > **contrôle d'accès** > **certificats client**.

   La page certificats client s'affiche.

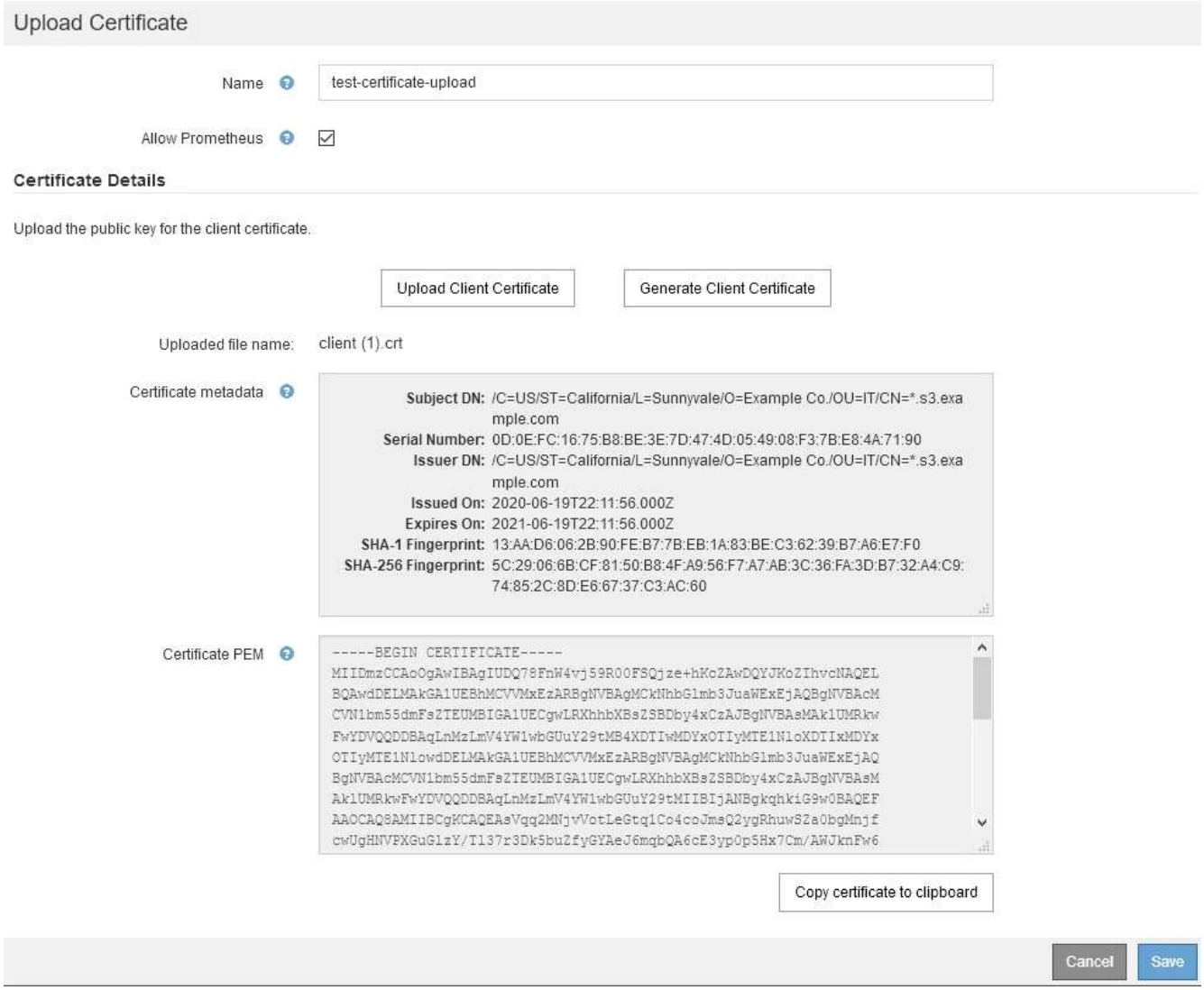
2. Sélectionnez **Ajouter**.

   La page Télécharger le certificat s'affiche.



3. Saisissez un nom entre 1 et 32 caractères pour le certificat.
4. Pour accéder aux metrics Prometheus à l'aide de votre outil de surveillance externe, cochez la case **Autoriser Prometheus**.
5. Télécharger ou générer un certificat :
   a. Pour télécharger un certificat, accédez à ici.
   b. Pour générer un certificat, accédez à ici.
6. pour télécharger un certificat :
   a. Sélectionnez **Télécharger le certificat client**.
   b. Recherchez la clé publique du certificat.

      Une fois la clé publique chargée pour le certificat, les champs **métadonnées de certificat** et **PEM de certificat** sont renseignés.



a. Sélectionnez **Copier le certificat dans le presse-papiers** et collez le certificat dans votre outil de surveillance externe.

b. Utilisez un outil d'édition pour copier et coller la clé privée dans votre outil de surveillance externe.

c. Sélectionnez **Enregistrer** pour enregistrer le certificat dans Grid Manager.

7. pour générer un certificat :

a. Sélectionnez **générer certificat client**.

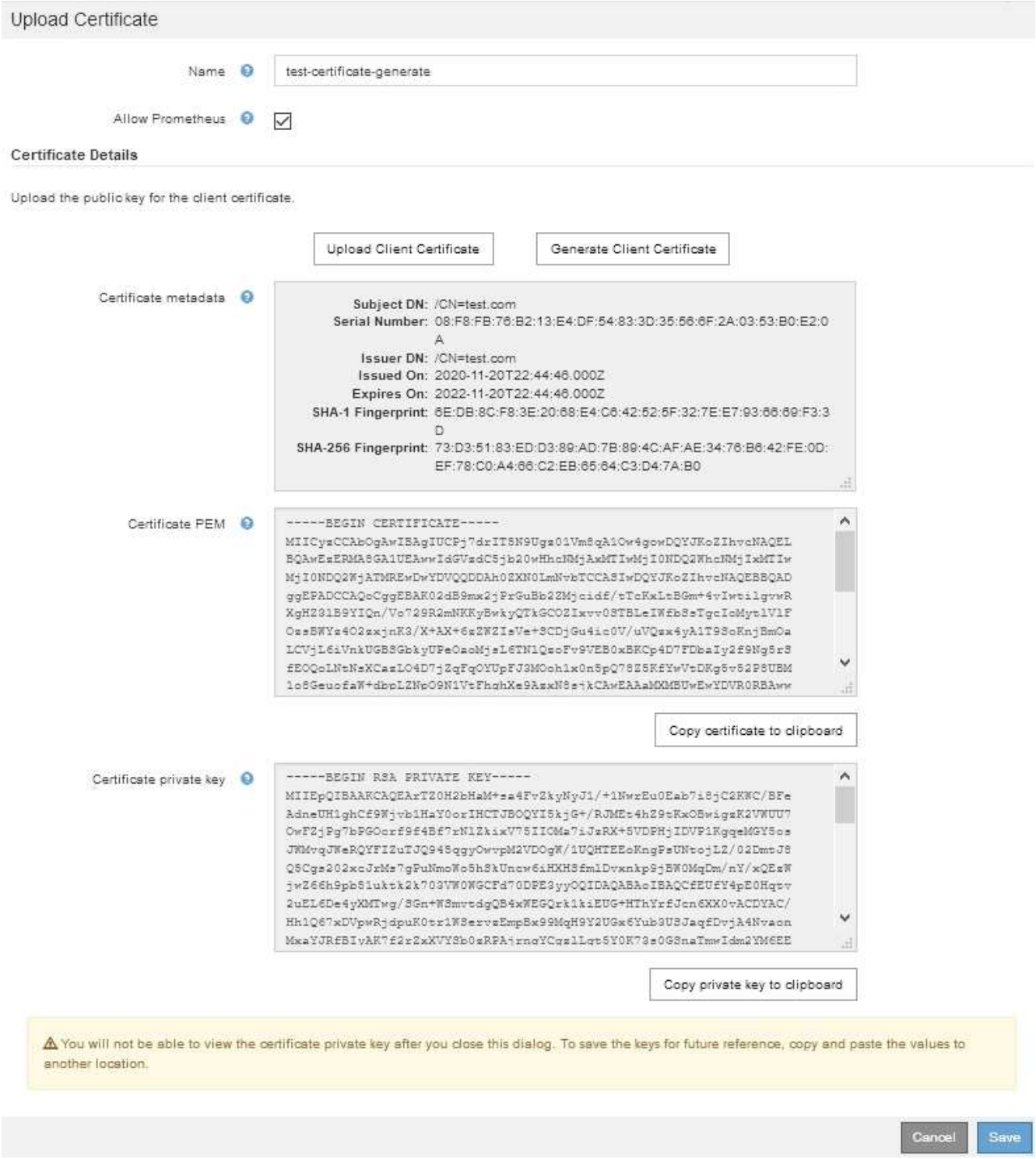
b. Entrez le nom de domaine ou l'adresse IP du nœud d'administration.

c. Vous pouvez également saisir un sujet X.509, également appelé Nom unique (DN), pour identifier l'administrateur qui possède le certificat.

d. Vous pouvez également sélectionner le nombre de jours pendant lesquels le certificat est valide. La valeur par défaut est 730 jours.

e. Sélectionnez **generate**.

Les champs **Certificate Metadata**, **Certificate PEM** et **Certificate Private Key** sont renseignés.



a. Sélectionnez **Copier le certificat dans le presse-papiers** et collez le certificat dans votre outil de surveillance externe.

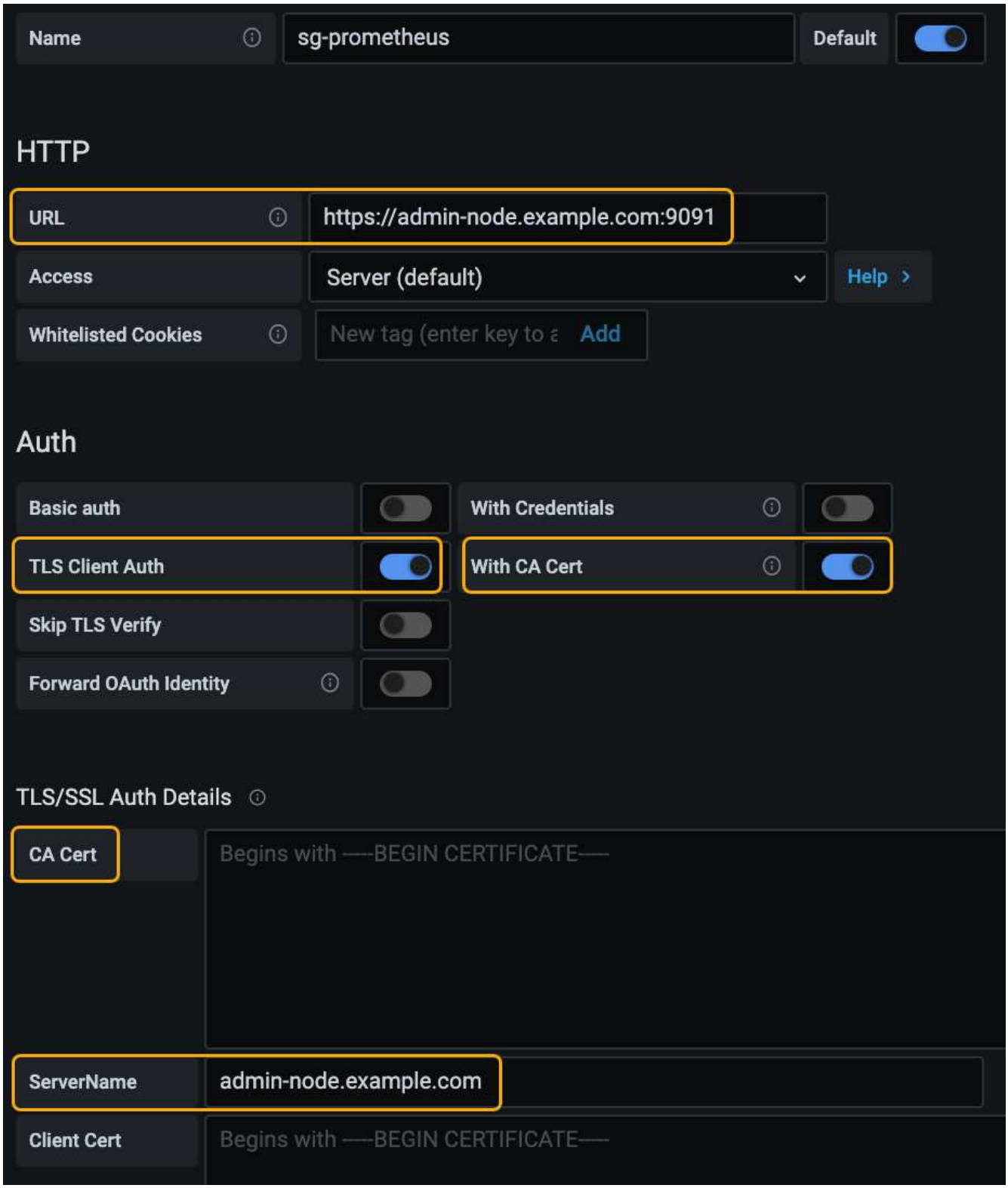
b. Sélectionnez **Copier la clé privée dans le presse-papiers** et collez la clé dans votre outil de surveillance externe.

> Vous ne pourrez pas afficher la clé privée après avoir fermé la boîte de dialogue. Copiez la clé dans un endroit sûr.

c. Sélectionnez **Enregistrer** pour enregistrer le certificat dans Grid Manager.

8. Configurez les paramètres suivants sur votre outil de surveillance externe, tels que Grafana.

   L'exemple de Grafana est présenté dans la capture d'écran suivante :



   a. **Nom** : saisissez un nom pour la connexion.

      StorageGRID ne requiert pas ces informations, mais vous devez fournir un nom pour tester la connexion.

b. **URL** : saisissez le nom de domaine ou l'adresse IP du noeud d'administration. Spécifiez HTTPS et le port 9091.

   Par exemple : `https://admin-node.example.com:9091`

c. Activez **TLS client Authorization** et **avec CA Cert**.

d. Copiez et collez le certificat de serveur d'interface de gestion ou le paquet CA dans le fichier **CA Cert** sous TLS/SSL Auth Details.

e. **NomServeur** : saisissez le nom de domaine du noeud d'administration.

   Le nom de serveur doit correspondre au nom de domaine tel qu'il apparaît dans le certificat de serveur de l'interface de gestion.

f. Enregistrez et testez le certificat et la clé privée que vous avez copiés à partir de StorageGRID ou d'un fichier local.

   Vous avez désormais accès aux metrics Prometheus à partir de StorageGRID grâce à votre outil de surveillance externe.

Pour plus d'informations sur les mesures, reportez-vous aux instructions de contrôle et de dépannage de StorageGRID.

Informations associées

"Utilisation des certificats de sécurité StorageGRID"

"Configuration d'un certificat de serveur personnalisé pour le Grid Manager et le tenant Manager"

"Moniteur et amp ; dépannage"

Modification des certificats du client administrateur

Vous pouvez modifier un certificat pour en changer le nom, activer ou désactiver l'accès Prometheus, ou télécharger un nouveau certificat lorsque celui actuel a expiré.

Ce dont vous avez besoin

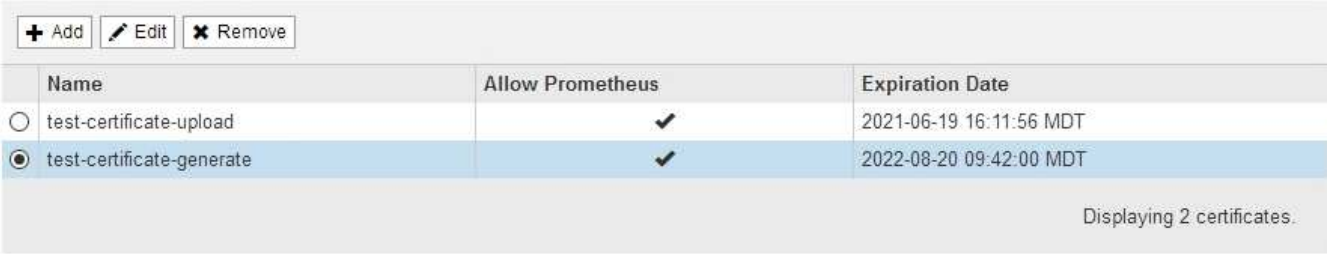
- Vous devez disposer de l'autorisation accès racine.
- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez connaître l'adresse IP ou le nom de domaine du nœud d'administration.
- Si vous souhaitez télécharger un nouveau certificat et une nouvelle clé privée, ils doivent être disponibles sur votre ordinateur local.

Étapes

1. Sélectionnez **Configuration** > **contrôle d'accès** > **certificats client**.

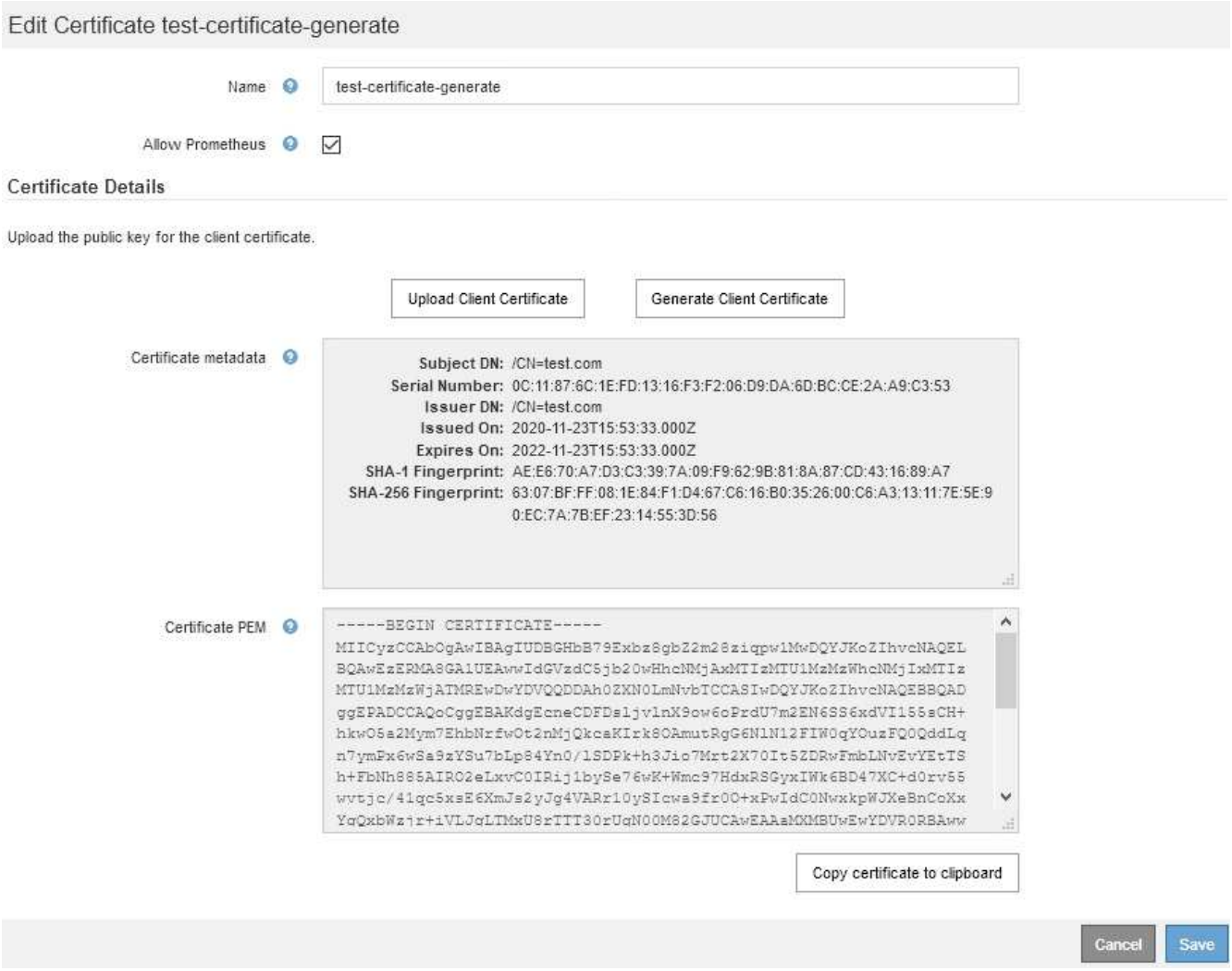
   La page certificats client s'affiche. Les certificats existants sont répertoriés.

   Les dates d'expiration du certificat sont répertoriées dans le tableau. Si un certificat expire bientôt ou est déjà expiré, un message apparaît dans le tableau et une alerte est déclenchée.



2. Sélectionnez le bouton radio à gauche du certificat que vous souhaitez modifier.
3. Sélectionnez **Modifier**.

   La boîte de dialogue Modifier le certificat s'affiche.



4. Apportez les modifications souhaitées au certificat.
5. Sélectionnez **Enregistrer** pour enregistrer le certificat dans Grid Manager.
6. Si vous avez téléchargé un nouveau certificat :
   a. Sélectionnez **Copier le certificat dans le presse-papiers** pour coller le certificat dans votre outil de surveillance externe.
   b. Utilisez un outil de modification pour copier et coller la nouvelle clé privée dans votre outil de surveillance externe.

c. Enregistrez et testez le certificat et la clé privée dans votre outil de surveillance externe.

7. Si vous avez généré un nouveau certificat :
   a. Sélectionnez **Copier le certificat dans le presse-papiers** pour coller le certificat dans votre outil de surveillance externe.
   b. Sélectionnez **Copier la clé privée dans le presse-papiers** pour coller le certificat dans votre outil de surveillance externe.

   > Vous ne pourrez pas afficher ou copier la clé privée après avoir fermé la boîte de dialogue. Copiez la clé dans un endroit sûr.

   c. Enregistrez et testez le certificat et la clé privée dans votre outil de surveillance externe.

Suppression des certificats client administrateur

Si vous n'avez plus besoin d'un certificat, vous pouvez le supprimer.

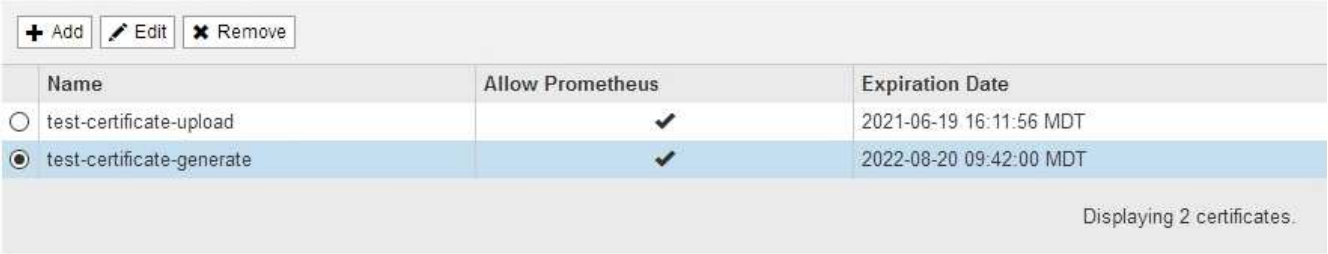
Ce dont vous avez besoin

- Vous devez disposer de l'autorisation accès racine.
- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.

Étapes

1. Sélectionnez **Configuration** > **contrôle d'accès** > **certificats client**.

   La page certificats client s'affiche. Les certificats existants sont répertoriés.

2. Sélectionnez le bouton radio à gauche du certificat que vous souhaitez supprimer.
3. Sélectionnez **Supprimer**.

   Une boîte de dialogue de confirmation s'affiche.

4. Sélectionnez **OK**.

Le certificat a été supprimé.

Configuration des serveurs de gestion des clés

Vous pouvez configurer un ou plusieurs serveurs de gestion externe des clés (KMS) afin de protéger les données sur les nœuds d'appliance spécialement configurés.

Qu'est-ce qu'un serveur de gestion des clés (KMS) ?

Un serveur de gestion des clés (KMS) est un système externe tiers qui fournit des clés de chiffrement aux nœuds d'appliance StorageGRID sur le site StorageGRID associé à l'aide du protocole KMIP (Key Management Interoperability Protocol).

Vous pouvez utiliser un ou plusieurs serveurs de gestion des clés pour gérer les clés de cryptage de nœud pour tous les nœuds d'appliance StorageGRID dont le paramètre **Node Encryption** est activé pendant l'installation. L'utilisation de serveurs de gestion des clés avec ces nœuds de dispositif permet de protéger vos données même en cas de retrait d'une appliance du data Center. Une fois les volumes de l'appliance chiffrés, vous ne pouvez accéder à aucune donnée sur l'appliance à moins que le nœud ne puisse communiquer avec le KMS.

> StorageGRID ne crée ni ne gère pas les clés externes utilisées pour chiffrer et décrypter les nœuds des systèmes. Si vous prévoyez d'utiliser un serveur de gestion externe des clés pour protéger les données StorageGRID, vous devez comprendre comment configurer ce serveur et savoir comment gérer les clés de cryptage. Ces instructions ne sont pas uniquement destinées à effectuer des tâches de gestion clés. Si vous avez besoin d'aide, consultez la documentation de votre serveur de gestion des clés ou contactez le support technique.

Passer en revue les méthodes de cryptage StorageGRID

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

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

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

Option de chiffrement	Comment cela fonctionne	S'applique à
Sécurité des disques dans SANtricity System Manager	Si la fonction sécurité des disques est activée pour une appliance de stockage, vous pouvez utiliser SANtricity System Manager pour créer et gérer la clé de sécurité. La clé est requise pour accéder aux données sur les disques sécurisés.	Appliances de stockage dotées de disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard). Toutes les données des disques sécurisés sont protégées contre les pertes ou suppressions physiques du data Center. Ne peut pas être utilisé avec certains dispositifs de stockage ni avec des appliances de service. "Dispositifs de stockage SG6000" "Appliances de stockage SG5700" "Appliances de stockage SG5600"
Option de grille de chiffrement d'objet stocké	L'option **Inenregistré Object Encryption** peut être activée dans Grid Manager (**Configuration** > **Paramètres système** > **Options de grille**). Lorsqu'il est activé, tout nouvel objet qui n'est pas chiffré au niveau du compartiment ou au niveau de l'objet est chiffré lors de l'ingestion.	Les données d'objet S3 et Swift récemment ingérées.les objets stockés existants ne sont pas chiffrés. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées. "Configuration du chiffrement des objets stockés"
Chiffrement de compartiment S3	Vous émettez une demande de chiffrement Put bucket pour activer le chiffrement du compartiment. Tout nouvel objet non chiffré au niveau de l'objet est chiffré lors de l'ingestion.	Données d'objet S3 récemment ingérées uniquement.le chiffrement doit être spécifié pour le compartiment. Les objets de compartiment existants ne sont pas chiffrés. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées. "Utilisation de S3"
Chiffrement côté serveur d'objets S3 (SSE)	Vous émettez une demande S3 pour stocker un objet et inclure le `x-amz-server-side-encryption` en-tête de demande.	Données d'objet S3 récemment ingérées uniquement.le chiffrement doit être spécifié pour l'objet. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées. StorageGRID gère les clés. "Utilisation de S3"

Option de chiffrement	Comment cela fonctionne	S'applique à
Chiffrement côté serveur objet S3 avec clés fournies par le client (SSE-C)	Vous émettez une demande S3 pour stocker un objet et incluez trois en-têtes de requête. • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	Données d'objet S3 récemment ingérées uniquement.le chiffrement doit être spécifié pour l'objet. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées. Les clés sont gérées en dehors du StorageGRID. "Utilisation de S3"
Chiffrement de volume ou de datastore externe	Vous utilisez une méthode de chiffrement autres que StorageGRID pour chiffrer un volume ou un datastore entier, si votre plateforme de déploiement le prend en charge.	Toutes les données d'objet, de métadonnées et de configuration du système, en supposant que chaque volume ou datastore est chiffré. Une méthode de chiffrement externe permet un contrôle plus précis des clés et des algorithmes de chiffrement. Peut être combiné avec les autres méthodes répertoriées.
Chiffrement d'objet en dehors de StorageGRID	Vous utilisez une méthode de chiffrement à l'extérieur de StorageGRID pour chiffrer les données d'objet et les métadonnées avant leur ingestion dans StorageGRID.	Données et métadonnées d'objet uniquement (les données de configuration du système ne sont pas chiffrées). Une méthode de chiffrement externe permet un contrôle plus précis des clés et des algorithmes de chiffrement. Peut être combiné avec les autres méthodes répertoriées. "Amazon simple Storage Service - Guide des développeurs : protection des données à l'aide du chiffrement côté client"

Utilisation de plusieurs méthodes de chiffrement

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

- Vous pouvez utiliser un KMS pour protéger les nœuds d'appliance et utiliser également la fonctionnalité de sécurité des disques de SANtricity System Manager pour « déchiffrer » les données présentes sur les

disques à autocryptage des mêmes dispositifs.

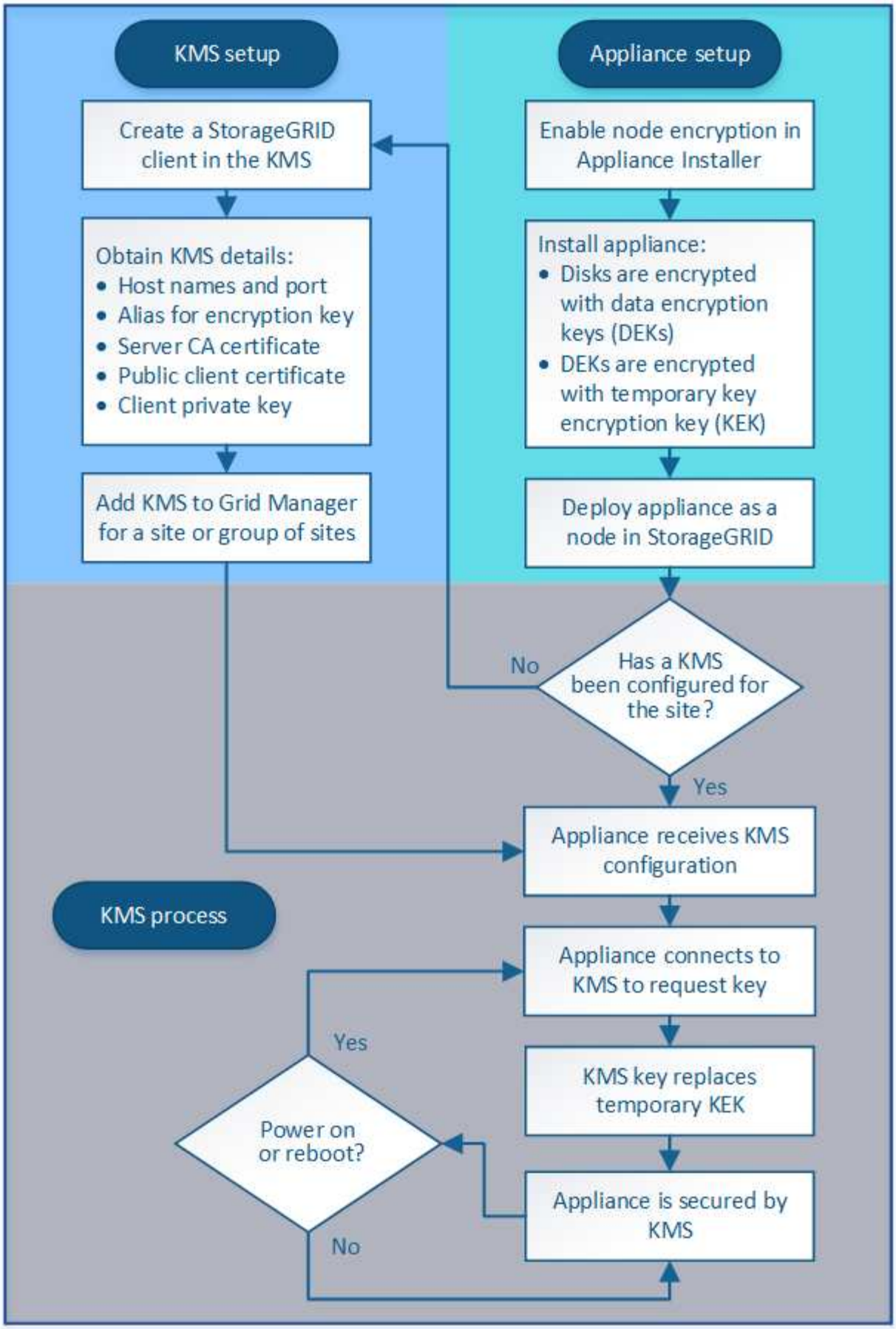
- Vous pouvez utiliser un KMS pour sécuriser les données sur les nœuds d'appliance et utiliser l'option GRID de chiffrement d'objet stocké pour chiffrer tous les objets à l'ingestion.

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

Présentation de la configuration des appliances et KMS

Avant d'utiliser un serveur de gestion des clés (KMS) afin de sécuriser les données StorageGRID sur les nœuds de l'appliance, vous devez effectuer deux tâches de configuration : configurer un ou plusieurs serveurs KMS et activer le chiffrement des nœuds pour les nœuds de l'appliance. Une fois ces deux tâches de configuration terminées, le processus de gestion des clés est automatique.

L'organigramme présente les étapes générales permettant d'utiliser un KMS pour sécuriser les données StorageGRID sur les nœuds du dispositif.



L'organigramme présente la configuration du KMS et l'appliance en parallèle. Toutefois, vous pouvez

configurer les serveurs de gestion des clés avant ou après avoir activé le chiffrement des nœuds pour les nouveaux nœuds d'appliance, selon vos besoins.

Configuration du serveur de gestion des clés (KMS)

La configuration d'un serveur de gestion des clés comprend les étapes générales suivantes.

Étape	Reportez-vous à la section
Accédez au logiciel KMS et ajoutez un client pour StorageGRID à chaque cluster KMS ou KMS.	"Configuration de StorageGRID en tant que client dans le KMS"
Obtenir les informations requises pour le client StorageGRID sur le KMS.	"Configuration de StorageGRID en tant que client dans le KMS"
Ajoutez le KMS à Grid Manager, attribuez-le à un seul site ou à un groupe de sites par défaut, téléchargez les certificats requis et enregistrez la configuration KMS.	"Ajout d'un serveur de gestion des clés (KMS)"

Configuration de l'appareil

La configuration d'un nœud d'appliance pour l'utilisation de KMS comprend les étapes générales suivantes.

1. Pendant l'étape de configuration matérielle de l'installation de l'appliance, utilisez le programme d'installation de l'appliance StorageGRID pour activer le paramètre **Node Encryption** pour l'appliance.

   > Vous ne pouvez pas activer le paramètre **Node Encryption** après l'ajout d'une appliance à la grille et vous ne pouvez pas utiliser la gestion externe des clés pour les appliances dont le cryptage de nœud n'est pas activé.

2. Exécutez le programme d'installation de l'appliance StorageGRID. Lors de l'installation, une clé de chiffrement aléatoire des données (DEK) est attribuée à chaque volume de dispositif, comme suit :
   - Les clés de licence sont utilisées pour chiffrer les données sur chaque volume. Ces clés sont générées à l'aide du chiffrement de disque 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 cryptage principale (KEK). La KEK initiale est une clé temporaire qui chiffre les clés de fin de séjour jusqu'à ce que l'appareil puisse se connecter au KMS.
3. Ajoutez le nœud d'appliance à StorageGRID.

Pour plus de détails, reportez-vous aux sections suivantes :

- "SG100 etamp ; appareils de services SG1000"
- "Dispositifs de stockage SG6000"
- "Appliances de stockage SG5700"
- "Appliances de stockage SG5600"

Processus de chiffrement de la gestion des clés (automatique)

Le chiffrement de la gestion des clés inclut les étapes générales suivantes qui sont automatiquement effectuées.

1. Lorsque vous installez une appliance sur laquelle le chiffrement de nœud est activé dans le grid, StorageGRID détermine si une configuration KMS existe pour le site qui contient le nouveau nœud.
   - Si un KMS a déjà été configuré pour le site, l'appliance reçoit la configuration KMS.
   - Si un KMS n'a pas encore été configuré pour le site, les données de l'appliance continuent d'être cryptées par le KEK temporaire jusqu'à ce que vous configuriez un KMS pour le site et que l'appliance reçoive la configuration KMS.
2. L'appliance utilise la configuration KMS pour vous connecter au KMS et demander une clé de chiffrement.
3. Le KMS envoie une clé de chiffrement à l'appliance. La nouvelle clé du KMS remplace la KEK temporaire et est maintenant utilisée pour crypter et décrypter les clés de fin de séjour des volumes d'appliance.

   > Toutes les données qui existent avant que le nœud d'appliance chiffré ne se connecte au KMS configuré sont chiffrées à l'aide d'une clé temporaire. Cependant, les volumes de l'appliance ne doivent pas être considérés comme protégés de leur retrait du data Center tant que la clé temporaire n'est pas remplacée par la clé de cryptage KMS.

4. Si l'appliance est sous tension ou redémarrée, elle se reconnecte au KMS pour demander la clé. La clé, qui est enregistrée dans la mémoire volatile, ne peut pas survivre à une perte de puissance ou à un redémarrage.

Considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés

Avant de configurer un serveur de gestion des clés externe (KMS), vous devez connaître les considérations et les exigences requises.

Quelles sont les exigences du protocole KMIP ?

StorageGRID prend en charge KMIP version 1.4.

"Spécification du protocole d'interopérabilité de gestion des clés version 1.4"

Les communications entre les nœuds d'appliance et le KMS configuré utilisent des connexions TLS sécurisées. StorageGRID prend en charge le chiffrement TLS v1.2 suivant pour KMIP :

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Vous devez vous assurer que chaque nœud d'appliance qui utilise le chiffrement de nœud dispose d'un accès réseau au cluster KMS ou KMS que vous avez configuré pour le site.

Les paramètres de pare-feu réseau doivent permettre à chaque nœud de l'appliance de communiquer via le port utilisé pour les communications KMIP (Key Management Interoperability Protocol). Le port KMIP par défaut est 5696.

Quels dispositifs sont pris en charge ?

Vous pouvez utiliser un serveur de gestion des clés (KMS) pour gérer les clés de cryptage de n'importe quelle appliance StorageGRID de la grille dont le paramètre **Node Encryption** est activé. Ce paramètre ne peut être activé que lors de l'étape de configuration matérielle de l'installation de l'appliance à l'aide du programme d'installation de l'appliance StorageGRID.

> Vous ne pouvez pas activer le chiffrement de nœud après l'ajout d'une appliance à la grille et ne pouvez pas utiliser la gestion externe des clés pour les appliances pour lesquelles le chiffrement de nœud n'est pas activé.

Vous pouvez utiliser le KMS configuré pour les nœuds d'appliance et les appliances StorageGRID suivants :

Appliance	Type de nœud
Appareil de services SG1000	Nœud d'administration ou nœud de passerelle
Appareil de services SG100	Nœud d'administration ou nœud de passerelle
Dispositif de stockage SG6000	Nœud de stockage
Appliance de stockage SG5700	Nœud de stockage
Appliance de stockage SG5600	Nœud de stockage

Vous ne pouvez pas utiliser le KMS configuré pour les nœuds Software-based (non appliance), notamment :

- Nœuds déployés en tant que machines virtuelles
- Nœuds déployés dans des conteneurs Docker sur des hôtes Linux

Les nœuds déployés sur ces autres plateformes peuvent utiliser le cryptage en dehors de StorageGRID au niveau du datastore ou du disque.

Quand dois-je configurer les serveurs de gestion des clés ?

Dans le cadre d'une nouvelle installation, vous devez généralement configurer un ou plusieurs serveurs de gestion des clés dans Grid Manager avant de créer des locataires. Cette commande garantit que les nœuds sont protégés avant que des données d'objet ne soient stockées sur ces nœuds.

Vous pouvez configurer les serveurs de gestion des clés dans Grid Manager avant ou après l'installation des nœuds de l'appliance.

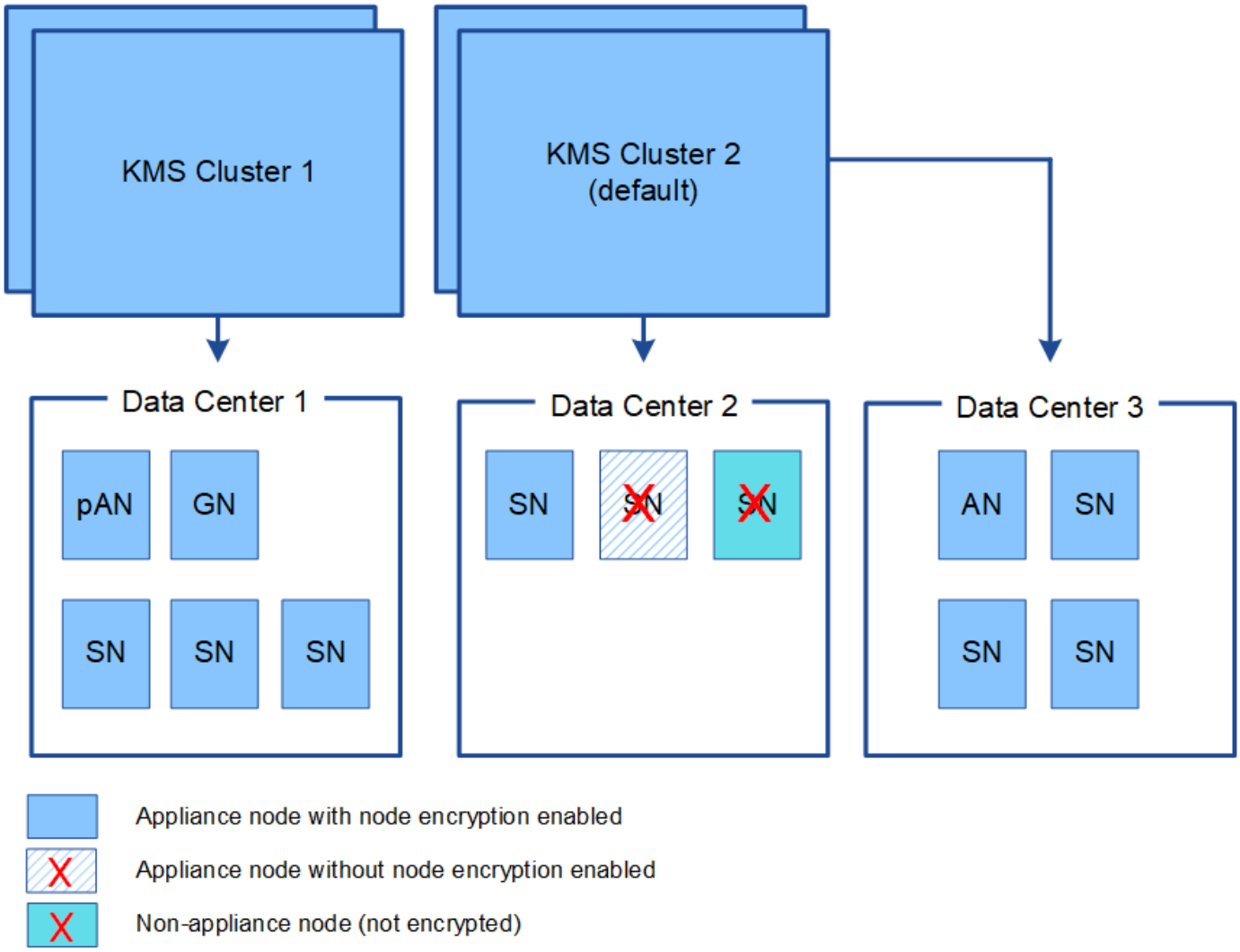
Combien de serveurs de gestion des clés ai-je besoin ?

Vous pouvez configurer un ou plusieurs serveurs de gestion externe des clés de chiffrement pour les nœuds d'appliance de votre système StorageGRID. Chaque KMS fournit une clé de chiffrement unique aux nœuds d'appliance StorageGRID sur un seul site ou dans un groupe de sites.

StorageGRID prend en charge l'utilisation des clusters KMS. Chaque cluster KMS contient plusieurs serveurs de gestion des clés répliqués qui partagent les paramètres de configuration et les clés de chiffrement. L'utilisation de clusters KMS pour la gestion des clés est recommandée, car il améliore les fonctionnalités de basculement d'une configuration haute disponibilité.

Supposons par exemple que votre système StorageGRID possède trois sites de data Center. Vous pouvez configurer un cluster KMS pour que tous les nœuds d'appliance soient essentiels dans le Data Center 1 et un second cluster KMS pour que ces derniers soient essentiels pour que tous les nœuds d'appliance soient disponibles sur les autres sites. Lorsque vous ajoutez le second cluster KMS, vous pouvez configurer un KMS par défaut pour Data Center 2 et Data Center 3.

Notez que vous ne pouvez pas utiliser de KMS pour les nœuds non-appliance ou pour les nœuds d'appliance dont le paramètre **Node Encryption** n'est pas activé au cours de l'installation.



Que se passe-t-il lorsqu'une clé est tournée ?

Dans le cadre de nos meilleures pratiques en matière de sécurité, vous devez régulièrement faire tourner la clé de chiffrement utilisée par chaque KMS configuré.

Lors de la rotation de la clé de chiffrement, utilisez le logiciel KMS pour faire pivoter la dernière version utilisée de la clé vers une nouvelle version de la même clé. Ne pas tourner sur une clé totalement différente.

> Ne tentez jamais de faire pivoter une clé en modifiant le nom de clé (alias) du KMS dans Grid Manager. Faites plutôt pivoter la clé en mettant à jour la version de clé dans le logiciel KMS. Utilisez le même alias de clé pour les nouvelles clés que celles utilisées pour les touches précédentes. Si vous modifiez l'alias de clé pour un KMS configuré, StorageGRID risque de ne pas être en mesure de décrypter vos données.

Lorsque la nouvelle version de clé est disponible :

- Elle est automatiquement distribuée aux nœuds d'appliance chiffrés sur le site ou les sites associés au KMS. La distribution doit se produire dans une heure après la rotation de la clé.
- Si le nœud d'appliance chiffré est hors ligne lorsque la nouvelle version de clé est distribuée, le nœud reçoit la nouvelle clé dès le redémarrage.
- Si la nouvelle version de la clé ne peut pas être utilisée pour crypter les volumes de l'appliance, l'alerte **KMS échec de rotation de la clé de chiffrement** est déclenchée pour le nœud de l'appliance. Vous devrez peut-être contacter le support technique pour obtenir de l'aide afin de résoudre cette alerte.

Puis-je réutiliser un nœud d'appliance après chiffrement ?

Si vous devez installer une appliance chiffrée dans un autre système StorageGRID, vous devez d'abord désactiver le nœud de grille pour déplacer les données d'objet vers un autre nœud. Ensuite, vous pouvez utiliser le programme d'installation de l'appliance StorageGRID pour effacer la configuration KMS. L'effacement de la configuration KMS désactive le paramètre **Node Encryption** et supprime l'association entre le nœud de l'appliance et la configuration KMS pour le site StorageGRID.

> Étant donnée l'accès à la clé de chiffrement KMS, toutes les données conservées sur l'appliance ne sont plus accessibles et sont verrouillées en permanence.

"SG100 etamp ; appareils de services SG1000"

"Dispositifs de stockage SG6000"

"Appliances de stockage SG5700"

"Appliances de stockage SG5600"

Considérations relatives à la modification du KMS pour un site

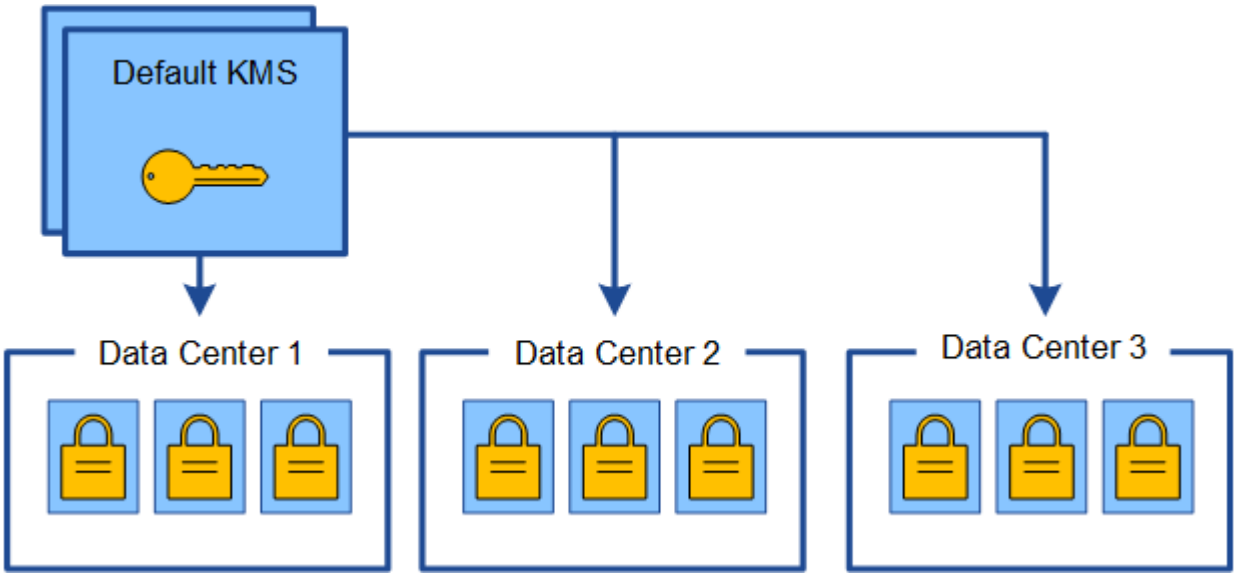
Chaque cluster de serveur de gestion des clés (KMS) ou KMS fournit une clé de chiffrement à tous les nœuds d'appliance sur un site unique ou dans un groupe de sites. Si vous devez modifier le KMS utilisé pour un site, vous devrez peut-être copier la clé de chiffrement d'un KMS vers un autre.

Si vous modifiez le KMS utilisé pour un site, vous devez vous assurer que les nœuds d'appliance précédemment cryptés de ce site peuvent être déchiffrés à l'aide de la clé stockée sur le nouveau KMS. Dans certains cas, vous devrez peut-être copier la version actuelle de la clé de chiffrement à partir du KMS d'origine vers le nouveau KMS. Vous devez vous assurer que le KMS dispose de la clé correcte pour décrypter les nœuds de l'appliance chiffrée sur le site.

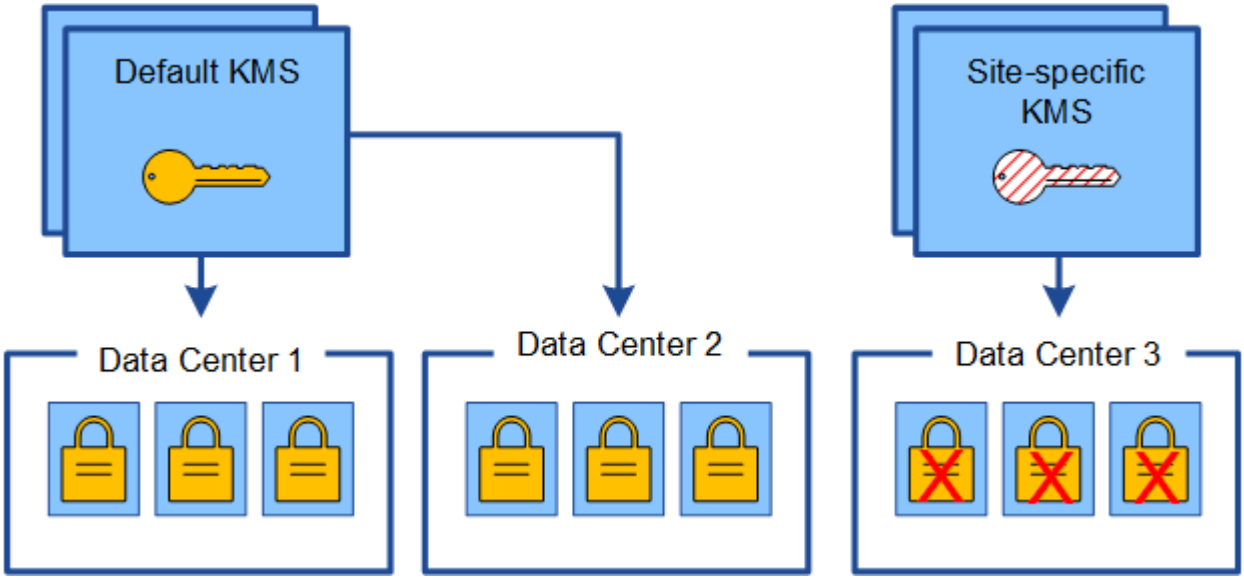
Par exemple :

1. Vous configurez au départ un KMS par défaut qui s'applique à tous les sites qui ne disposent pas d'un KMS dédié.

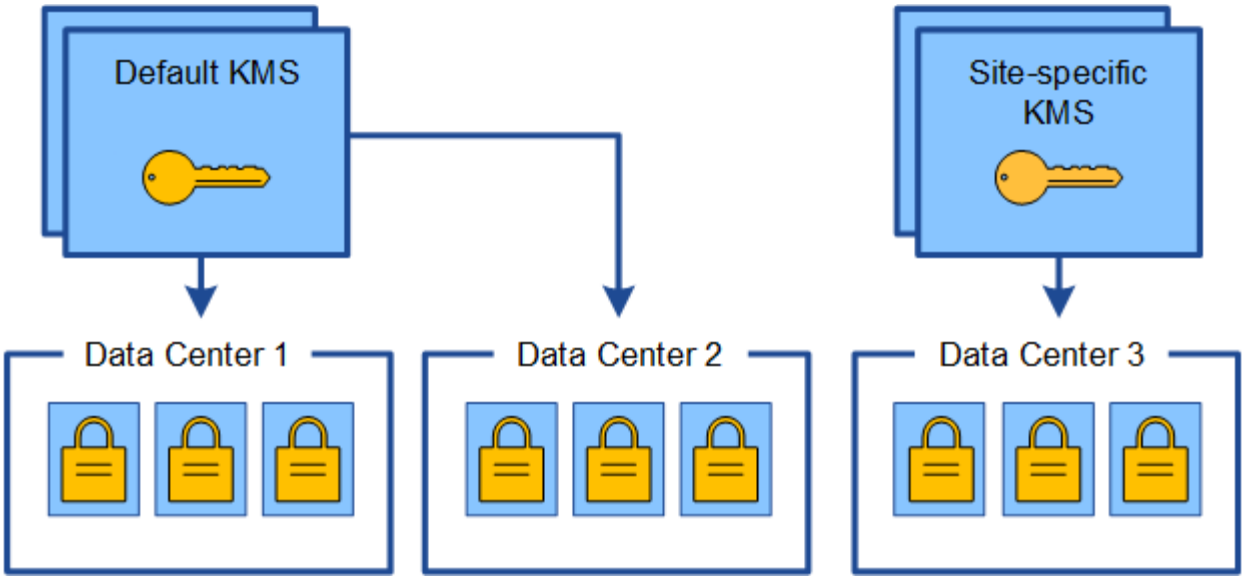
2. Lorsque le KMS est enregistré, tous les nœuds de l'appliance dont le paramètre **Node Encryption** est activé se connectent au KMS et demandent la clé de chiffrement. Cette clé est utilisée pour chiffrer les nœuds de l'appliance sur tous les sites. Cette même clé doit également être utilisée pour décrypter ces dispositifs.



3. Vous décidez d'ajouter un KMS spécifique au site pour un site (Data Center 3 dans la figure). Toutefois, les nœuds d'appliance sont déjà chiffrés. Une erreur de validation se produit lorsque vous tentez d'enregistrer la configuration du KMS spécifique au site. L'erreur se produit car le KMS spécifique au site ne dispose pas de la clé correcte pour décrypter les nœuds de ce site.



4. Pour résoudre ce problème, vous copiez la version actuelle de la clé de chiffrement à partir du KMS par défaut vers le nouveau KMS. (Techniquement, vous copiez la clé d'origine dans une nouvelle clé avec le même alias. La clé d'origine devient une version antérieure de la nouvelle clé.) Le KMS spécifique au site dispose désormais de la clé correcte pour décrypter les nœuds d'appliance sur Data Center 3, afin qu'ils puissent être sauvegardés sur StorageGRID.



Cas d'utilisation pour changer quel KMS est utilisé pour un site

Le tableau résume les étapes requises pour les cas les plus courants de modification du KMS pour un site.

Cas d'utilisation lors de la modification du KMS d'un site	Étapes requises
Vous avez une ou plusieurs entrées KMS spécifiques au site, et vous souhaitez utiliser l'une d'entre elles comme étant le KMS par défaut.	Modifiez le KMS spécifique au site. Dans le champ **gère clés pour**, sélectionnez **sites non gérés par un autre KMS (KMS par défaut)**. Le KMS spécifique au site sera maintenant utilisé comme KMS par défaut. Il s'appliquera à tous les sites qui n'ont pas de KMS dédié. "Modification d'un serveur de gestion des clés (KMS)"
Vous avez un KMS par défaut et vous ajoutez un nouveau site dans une extension. Vous ne souhaitez pas utiliser le KMS par défaut pour le nouveau site.	1. Si les nœuds d'appliance du nouveau site ont déjà été chiffrés par le KMS par défaut, utilisez le logiciel KMS pour copier la version actuelle de la clé de chiffrement à partir du KMS par défaut vers un nouveau KMS. 2. À l'aide de Grid Manager, ajoutez le nouveau KMS et sélectionnez le site. "Ajout d'un serveur de gestion des clés (KMS)"

Cas d'utilisation lors de la modification du KMS d'un site	Étapes requises
Vous souhaitez que le KMS pour un site utilise un serveur différent.	1. Si les nœuds d'appliance du site ont déjà été chiffrés par le KMS existant, utilisez le logiciel KMS pour copier la version actuelle de la clé de chiffrement à partir du KMS existant vers le nouveau KMS. 2. À l'aide de Grid Manager, modifiez la configuration KMS existante et entrez le nouveau nom d'hôte ou l'adresse IP. "Ajout d'un serveur de gestion des clés (KMS)"

Configuration de StorageGRID en tant que client dans le KMS

Vous devez configurer StorageGRID en tant que client pour chaque serveur de gestion externe des clés ou cluster KMS avant de pouvoir ajouter le KMS à StorageGRID.

Description de la tâche

Ces instructions s'appliquent à Thales CipherTrust Manager k170v, versions 2.0, 2.1 et 2.2. Pour toute question concernant l'utilisation d'un autre serveur de gestion des clés avec StorageGRID, contactez le support technique.

"Thales CipherTrust Manager"

Étapes

1. À partir du logiciel KMS, créez un client StorageGRID pour chaque cluster KMS ou KMS que vous souhaitez utiliser.

   Chaque KMS gère une clé de chiffrement unique pour les nœuds d'appliances StorageGRID dans un seul site ou dans un groupe de sites.

2. Depuis le logiciel KMS, créez une clé de chiffrement AES pour chaque cluster KMS ou KMS.

   La clé de cryptage doit être exportable.

3. Notez les informations suivantes pour chaque cluster KMS ou KMS.

   Vous avez besoin de ces informations lorsque vous ajoutez le KMS à StorageGRID.

   - Nom d'hôte ou adresse IP pour chaque serveur.
   - Port KMIP utilisé par le KMS.
   - Alias de clé pour la clé de cryptage dans le KMS.

   > La clé de chiffrement doit déjà exister dans le KMS. StorageGRID ne crée ni ne gère pas de clés KMS.

4. Pour chaque cluster KMS ou KMS, procurez-vous un certificat de serveur signé par une autorité de certification (CA) ou un bundle de certificats contenant chacun des fichiers de certificat d'autorité de certification codés au PEM, concaténés dans l'ordre de la chaîne de certificats.

Le certificat du serveur permet au KMS externe de s'authentifier auprès de StorageGRID.

- Le certificat doit utiliser le format X.509 encodé au format PEM (Privacy Enhanced Mail) Base-64.
- Le champ Subject alternative Name (SAN) de chaque certificat de serveur doit inclure le nom de domaine complet (FQDN) ou l'adresse IP à laquelle StorageGRID se connectera.

> Lorsque vous configurez le KMS dans StorageGRID, vous devez entrer les mêmes FQDN ou adresses IP dans le champ **Hostname**.

- Le certificat du serveur doit correspondre au certificat utilisé par l'interface KMIP du KMS, qui utilise généralement le port 5696.

5. Obtenir le certificat du client public délivré à StorageGRID par le KMS externe et la clé privée du certificat du client.

   Le certificat client permet à StorageGRID de s'authentifier auprès du KMS.

Ajout d'un serveur de gestion des clés (KMS)

L'assistant de serveur de gestion des clés StorageGRID vous permet d'ajouter chaque cluster KMS ou KMS.

Ce dont vous avez besoin

- Vous devez avoir consulté le "considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés".
- Vous devez avoir "Configuration de StorageGRID en tant que client dans le KMS", Et vous devez disposer des informations requises pour chaque cluster KMS ou KMS
- Vous devez disposer de l'autorisation accès racine.
- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.

Description de la tâche

Si possible, configurez tous les serveurs de gestion de clés spécifiques au site avant de configurer un KMS par défaut qui s'applique à tous les sites non gérés par un autre KMS. Si vous créez d'abord le KMS par défaut, toutes les appliances chiffrées par nœud dans le grid seront chiffrées par le KMS par défaut. Si vous souhaitez créer ultérieurement un KMS spécifique au site, vous devez d'abord copier la version actuelle de la clé de chiffrement à partir du KMS par défaut vers le nouveau KMS.

"Considérations relatives à la modification du KMS pour un site"

Étapes

1. "Étape 1 : saisissez les détails du KMS"
2. "Étape 2 : télécharger le certificat du serveur"
3. "Étape 3 : télécharger des certificats client"

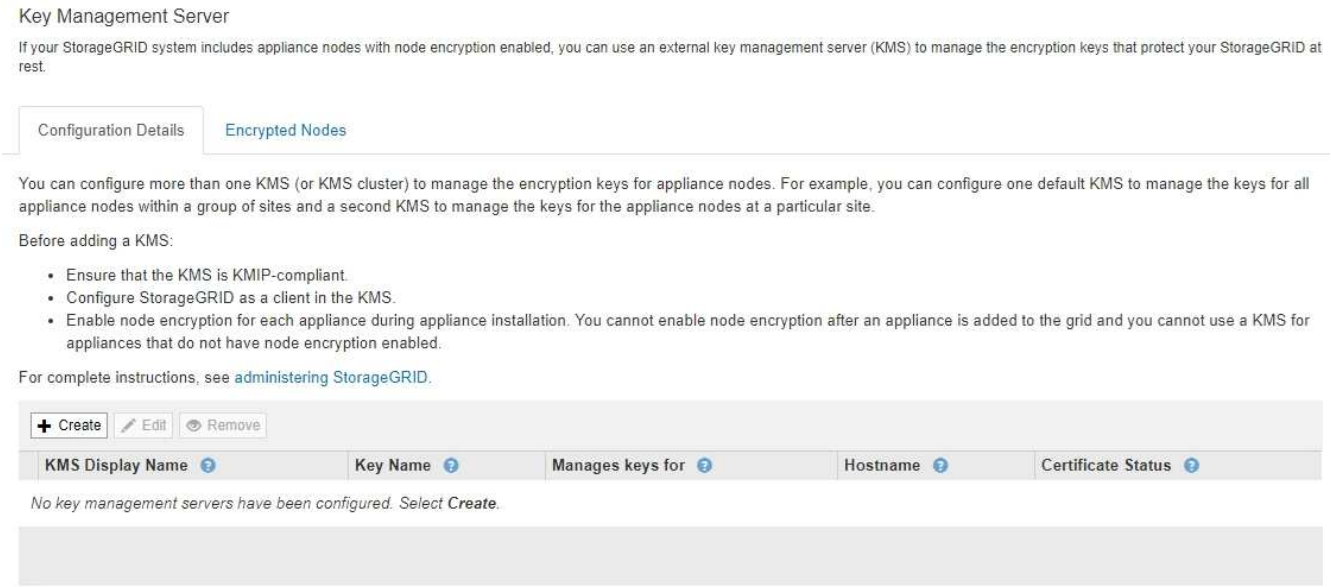
Étape 1 : saisissez les détails du KMS

À l'étape 1 (entrer les détails KMS) de l'assistant Ajout d'un serveur de gestion des clés, vous fournissez des détails sur le cluster KMS ou KMS.

Étapes

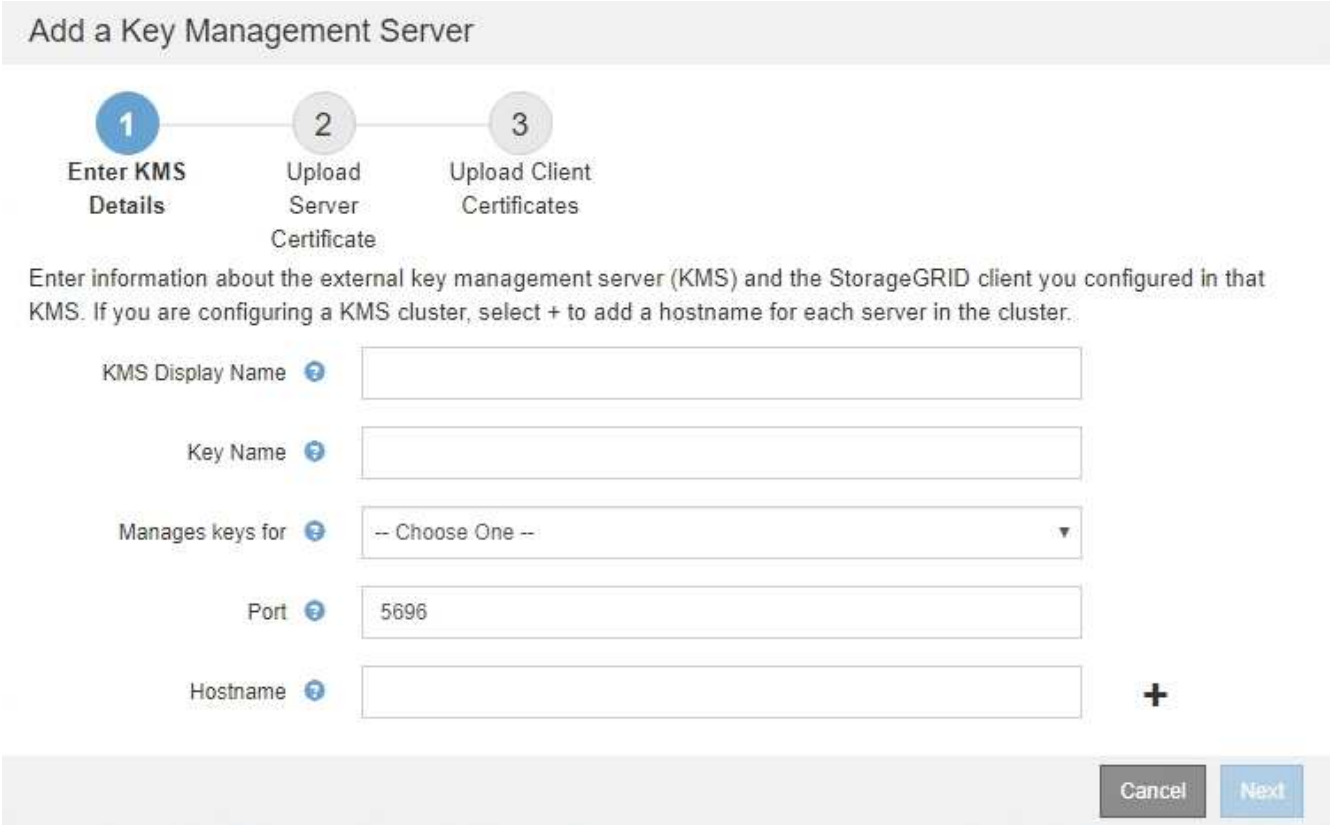
1. Sélectionnez **Configuration** > **Paramètres système** > **serveur de gestion des clés**.

   La page Key Management Server s'affiche avec l'onglet Configuration Details (Détails de la configuration) sélectionné.



2. Sélectionnez **Créer**.

   L'étape 1 (entrer les détails KMS) de l'assistant Ajout d'un serveur de gestion de clés s'affiche.



3. Entrez les informations suivantes pour le KMS et le client StorageGRID que vous avez configuré dans ce KMS.

Champ	Description
Nom d'affichage DES KMS	Un nom descriptif pour vous aider à identifier ce KMS. Doit comporter entre 1 et 64 caractères.
Nom de clé	Alias de clé exact pour le client StorageGRID dans le KMS. Doit comporter entre 1 et 255 caractères.
Gère les clés pour	Le site StorageGRID qui sera associé à ce KMS. Si possible, vous devez configurer des serveurs de gestion de clés spécifiques au site avant de configurer un KMS par défaut qui s'applique à tous les sites non gérés par un autre KMS. • Sélectionnez un site si ce KMS gère les clés de chiffrement pour les nœuds d'appliance sur un site spécifique. • Sélectionnez **sites non gérés par un autre KMS (KMS par défaut)** pour configurer un KMS par défaut qui s'appliquera à tous les sites qui ne disposent pas d'un KMS dédié et à tous les sites que vous ajoutez dans les extensions suivantes. **Remarque :** Une erreur de validation se produit lorsque vous enregistrez la configuration KMS si vous sélectionnez un site qui a été précédemment crypté par le KMS par défaut, mais que vous n'avez pas fourni la version actuelle de la clé de cryptage d'origine au nouveau KMS.
Port	Le port utilisé par le serveur KMS pour les communications KMIP (Key Management Interoperability Protocol). La valeur par défaut est 5696, qui est le port standard KMIP.
Nom d'hôte	Le nom de domaine complet ou l'adresse IP du KMS. **Remarque :** le champ SAN du certificat de serveur doit inclure le FQDN ou l'adresse IP que vous saisissez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ou à tous les serveurs d'un cluster KMS.

4. Si vous utilisez un cluster KMS, sélectionnez le signe plus ➕ pour ajouter un nom d'hôte pour chaque serveur du cluster.
5. Sélectionnez **Suivant**.

   L'étape 2 (Télécharger un certificat de serveur) de l'assistant Ajout d'un serveur de gestion de clés

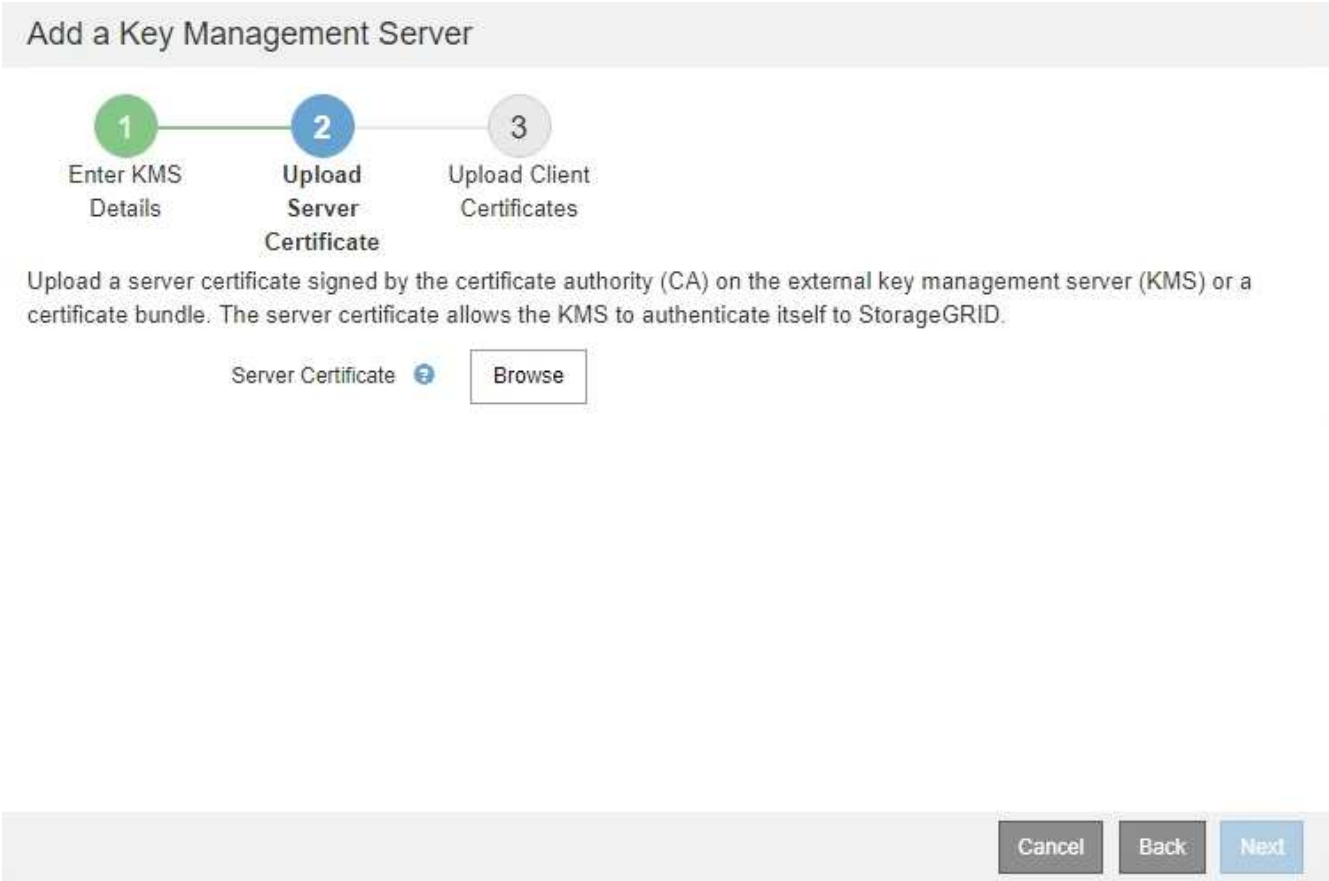
s'affiche.

Étape 2 : télécharger le certificat du serveur

À l'étape 2 (Télécharger le certificat de serveur) de l'assistant Ajout d'un serveur de gestion de clés, vous téléchargez le certificat de serveur (ou le paquet de certificats) pour le KMS. Le certificat du serveur permet au KMS externe de s'authentifier auprès de StorageGRID.

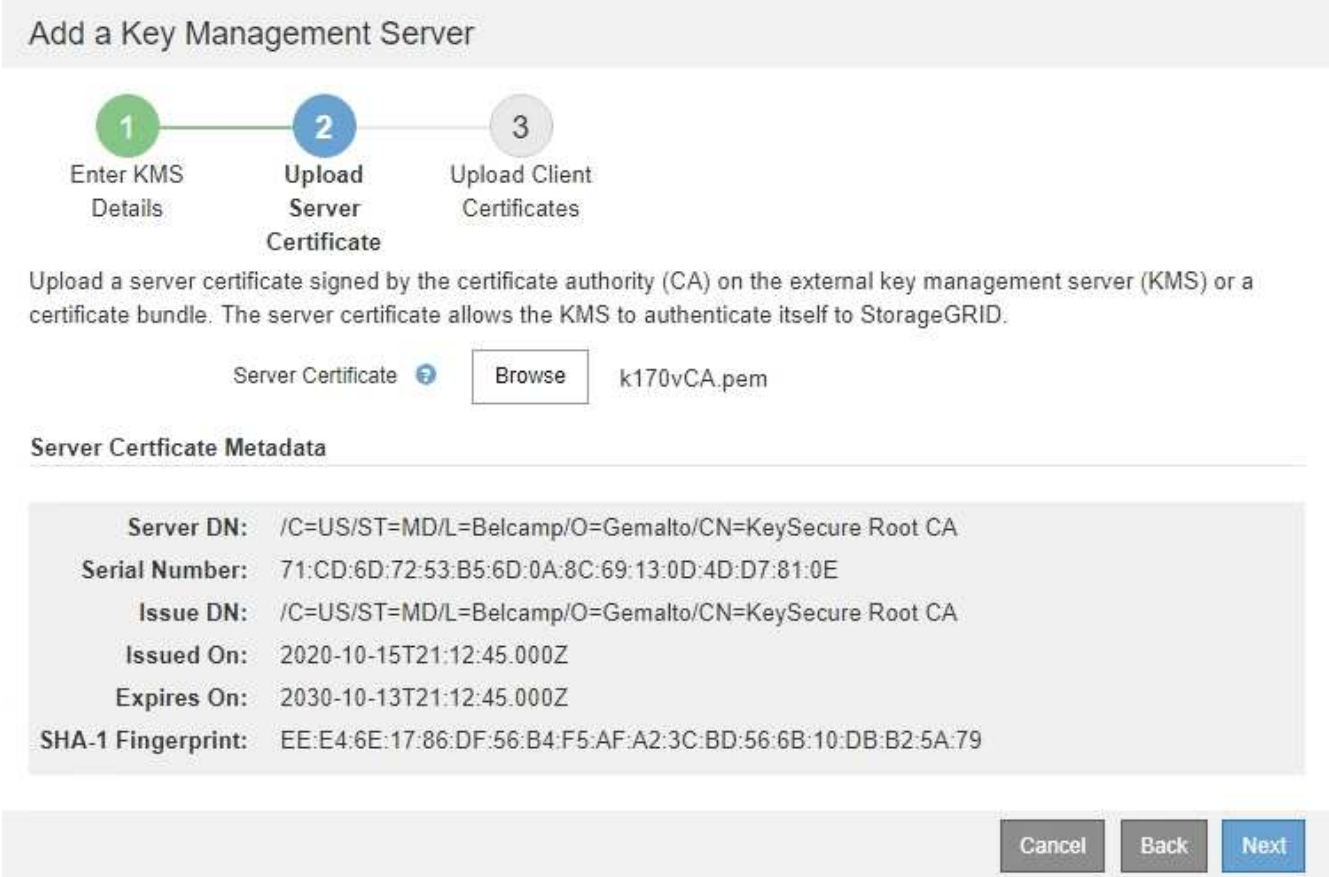
Étapes

1. À partir de **Etape 2 (Télécharger le certificat du serveur)**, accédez à l'emplacement du certificat du serveur enregistré ou du groupe de certificats.



2. Téléchargez le fichier de certificat.

   Les métadonnées du certificat de serveur s'affichent.



Si vous avez téléchargé un ensemble de certificats, les métadonnées de chaque certificat s'affichent sur son propre onglet.

3. Sélectionnez **Suivant**.

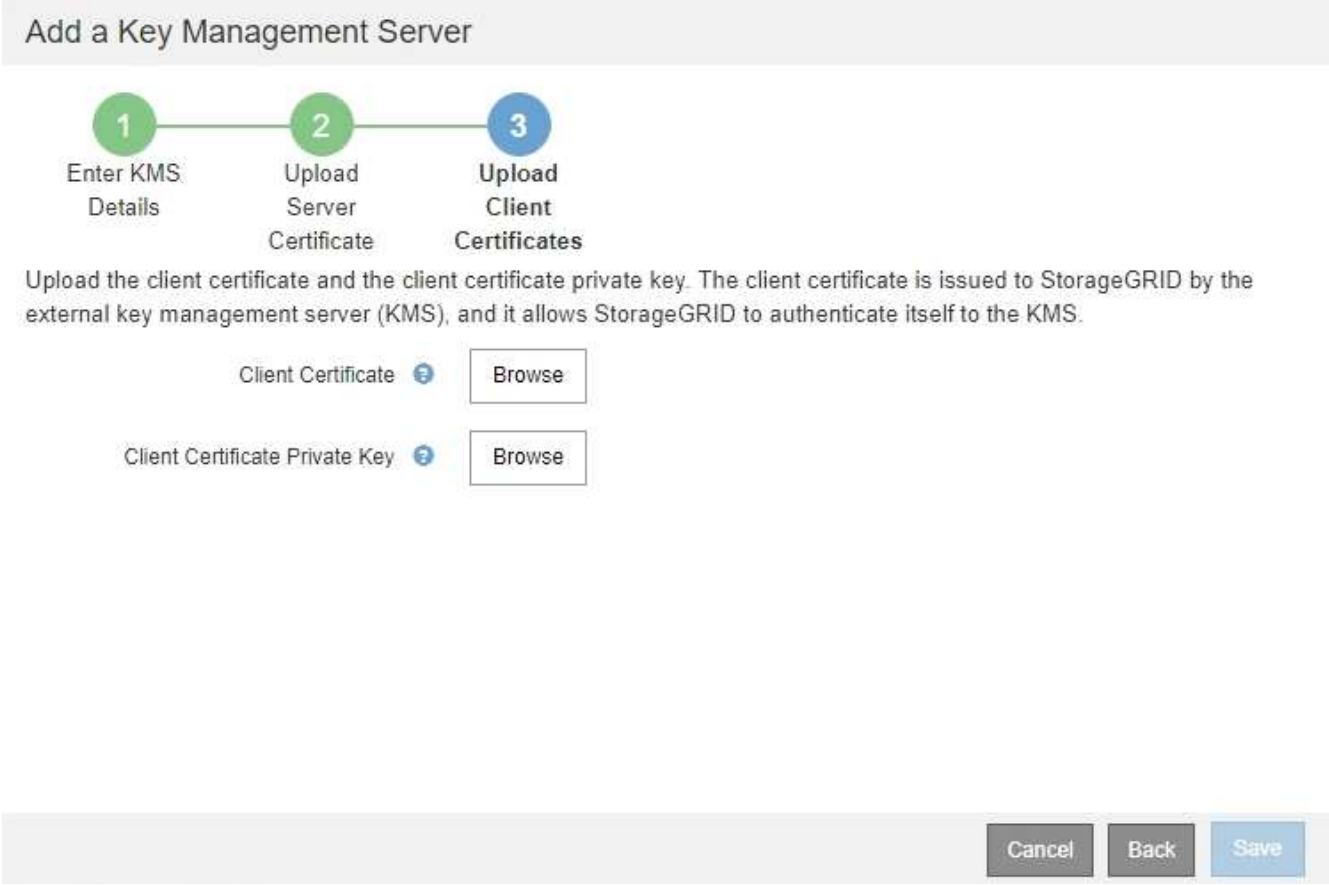
   L'étape 3 (Téléchargement de certificats client) de l'assistant Ajout d'un serveur de gestion de clés s'affiche.

Étape 3 : télécharger des certificats client

À l'étape 3 (Téléchargement de certificats client) de l'assistant Ajout d'un serveur de gestion des clés, vous téléchargez le certificat client et la clé privée du certificat client. Le certificat client permet à StorageGRID de s'authentifier auprès du KMS.

Étapes

1. À partir de **Etape 3 (Téléchargement de certificats client)**, accédez à l'emplacement du certificat client.

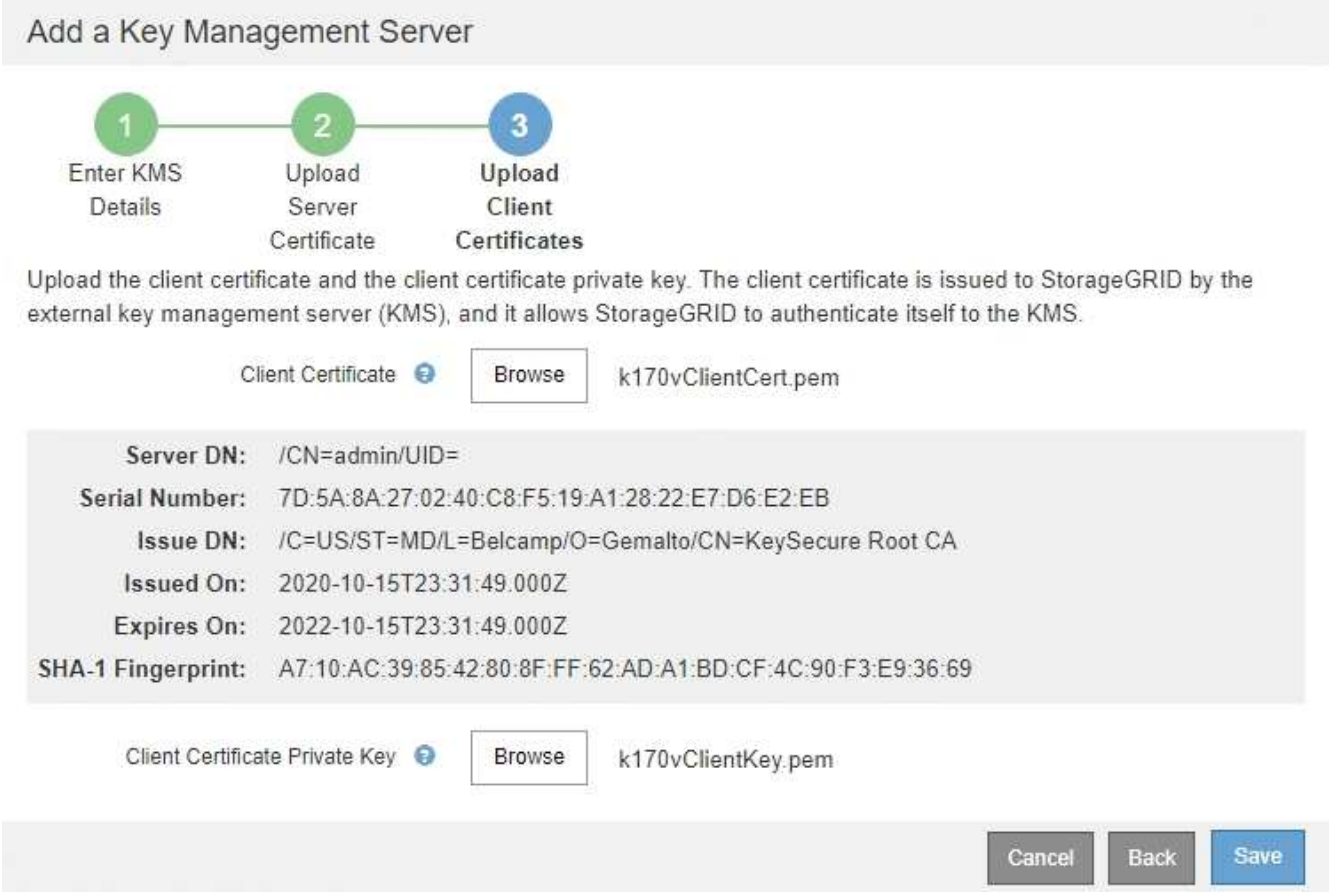


2. Téléchargez le fichier de certificat client.

   Les métadonnées du certificat client s’affichent.

3. Accédez à l’emplacement de la clé privée pour le certificat client.
4. Téléchargez le fichier de clé privée.

   Les métadonnées du certificat client et de la clé privée du certificat client s’affichent.



5. Sélectionnez **Enregistrer**.

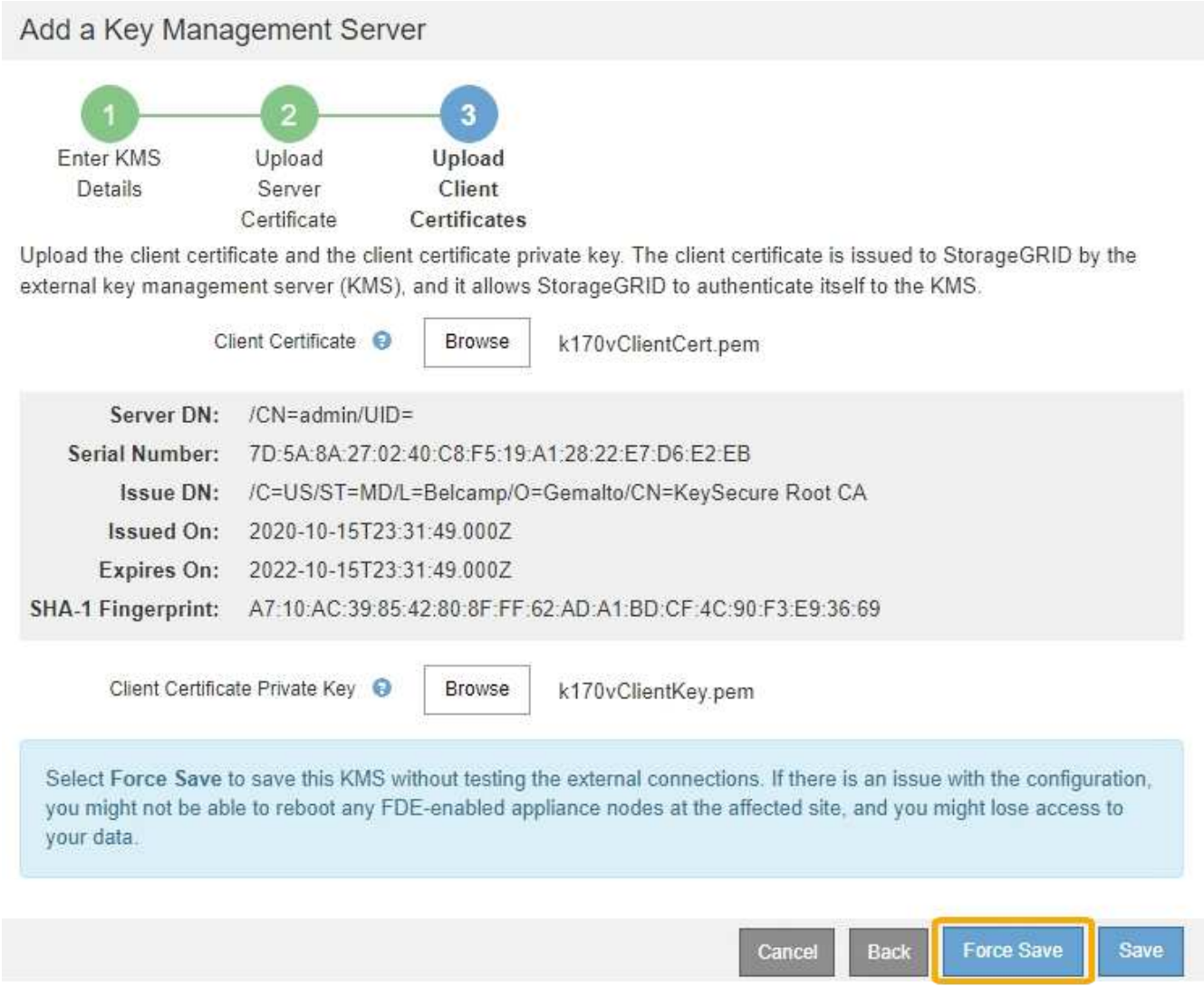
   Les connexions entre le serveur de gestion des clés et les nœuds de dispositif sont testées. Si toutes les connexions sont valides et que la clé correcte est trouvée sur le KMS, le nouveau serveur de gestion des clés est ajouté à la table de la page serveur de gestion des clés.

   > Immédiatement après l'ajout d'un KMS, l'état du certificat sur la page Key Management Server apparaît comme inconnu. Le statut réel de chaque certificat peut prendre jusqu'à 30 minutes pour StorageGRID. Vous devez actualiser votre navigateur Web pour voir l'état actuel.

6. Si un message d'erreur apparaît lorsque vous sélectionnez **Enregistrer**, vérifiez les détails du message, puis sélectionnez **OK**.

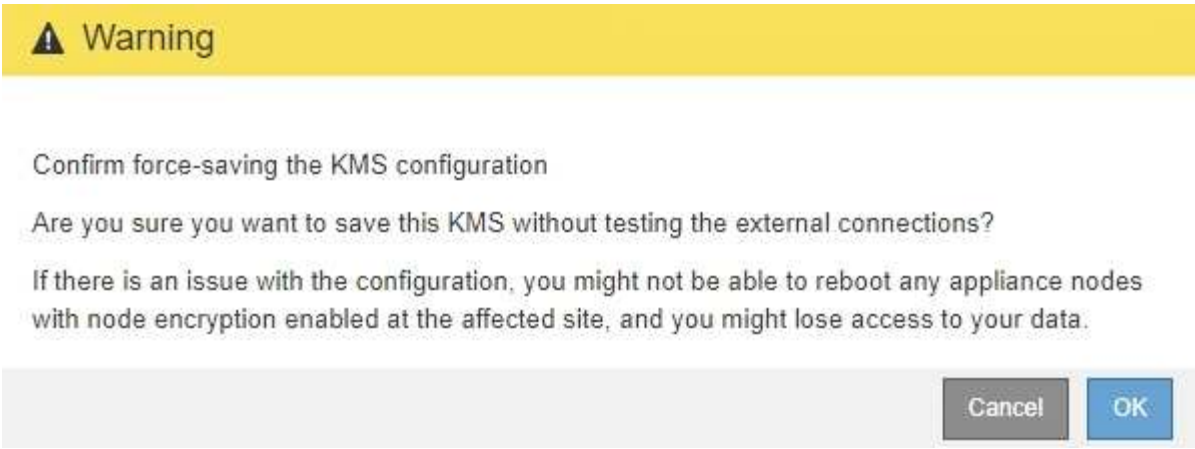
   Par exemple, vous pourriez recevoir une erreur 422 : entité impossible à traiter si un test de connexion a échoué.

7. Si vous devez enregistrer la configuration actuelle sans tester la connexion externe, sélectionnez **forcer l'enregistrement**.



Si vous sélectionnez **forcer l'enregistrement**, la configuration KMS est enregistrée, mais il ne teste pas la connexion externe de chaque appliance vers ce KMS. En cas de problème avec la configuration, vous ne pouvez pas redémarrer les nœuds d'appliance pour lesquels le chiffrement de nœud est activé sur le site affecté. L'accès à vos données risque d'être perdu jusqu'à la résolution des problèmes.

8. Vérifiez l'avertissement de confirmation et sélectionnez **OK** si vous êtes sûr de vouloir forcer l'enregistrement de la configuration.



La configuration KMS est enregistrée mais la connexion au KMS n'est pas testée.

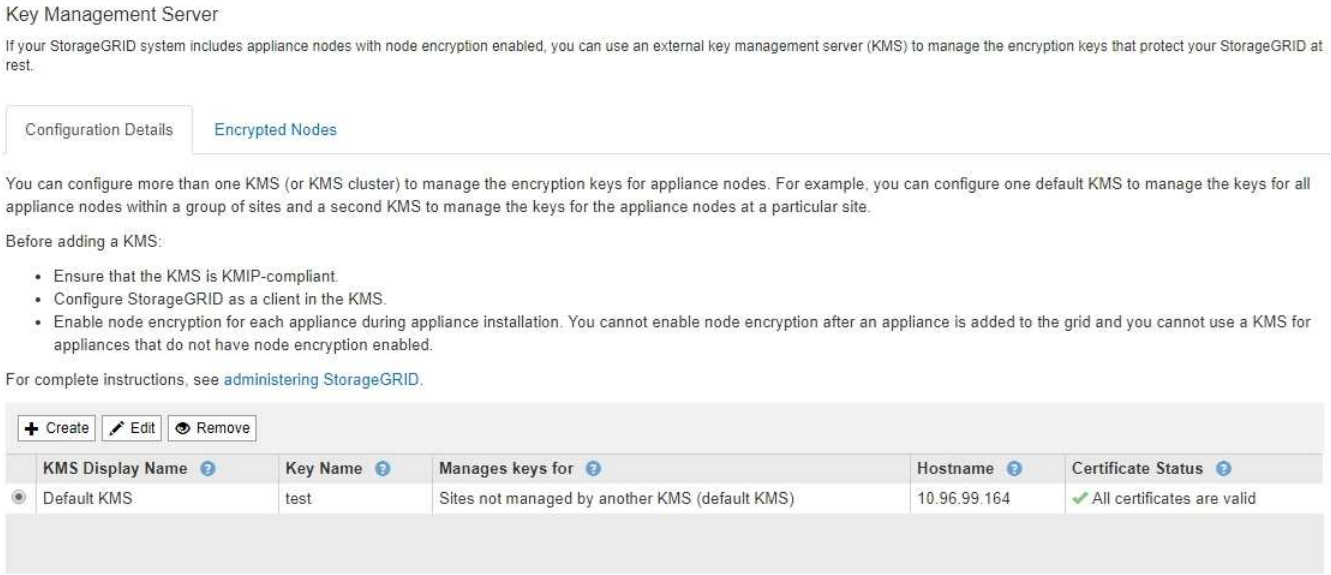
Affichage des détails KMS

Vous pouvez afficher des informations sur chaque serveur de gestion des clés (KMS) de votre système StorageGRID, notamment l'état actuel des certificats serveur et client.

Étapes

1. Sélectionnez **Configuration** > **Paramètres système** > **serveur de gestion des clés**.

   La page Key Management Server s'affiche. L'onglet Détails de la configuration affiche tous les serveurs de gestion des clés configurés.



2. Examinez les informations du tableau pour chaque KMS.

Champ	Description
Nom d'affichage DES KMS	Nom descriptif du KMS.

Champ	Description
Nom de clé	Alias de clé pour le client StorageGRID dans le KMS.
Gère les clés pour	Site StorageGRID associé au KMS Ce champ affiche le nom d'un site StorageGRID spécifique ou **sites non gérés par un autre KMS (KMS par défaut).**
Nom d'hôte	Le nom de domaine complet ou l'adresse IP du KMS. S'il existe un cluster de deux serveurs de gestion des clés, le nom de domaine complet ou l'adresse IP des deux serveurs sont répertoriés. S'il y a plus de deux serveurs de gestion des clés dans un cluster, le nom de domaine complet ou l'adresse IP du premier KMS est répertorié avec le nombre de serveurs de gestion des clés supplémentaires dans le cluster. Par exemple : `10.10.10.10 and 10.10.10.11` ou `10.10.10.10 and 2 others`. Pour afficher tous les noms d'hôte d'un cluster, sélectionnez un KMS, puis sélectionnez **Modifier**.
État du certificat	État actuel du certificat de serveur, du certificat d'autorité de certification facultatif et du certificat client : valide, expiré, proche de l'expiration ou inconnu. **Remarque :** StorageGRID peut prendre 30 minutes pour obtenir des mises à jour de l'état du certificat. Vous devez actualiser votre navigateur Web pour voir les valeurs actuelles.

3. Si l'état du certificat est inconnu, attendez jusqu'à 30 minutes, puis actualisez votre navigateur Web.

> Immédiatement après l'ajout d'un KMS, l'état du certificat sur la page Key Management Server apparaît comme inconnu. Le statut réel de chaque certificat peut prendre jusqu'à 30 minutes pour StorageGRID. Vous devez actualiser votre navigateur Web pour voir l'état réel.

4. Si la colonne État du certificat indique qu'un certificat a expiré ou qu'il arrive à expiration, traitez le problème dès que possible.

   Consultez les actions recommandées pour les alertes d'expiration du certificat CA **KMS**, **expiration du certificat client KMS** et **expiration du certificat serveur KMS** dans les instructions de surveillance et de dépannage de StorageGRID.

Vous devez corriger tout problème de certificat dès que possible pour maintenir l'accès aux données.

Informations associées

"Moniteur et amp ; dépannage"

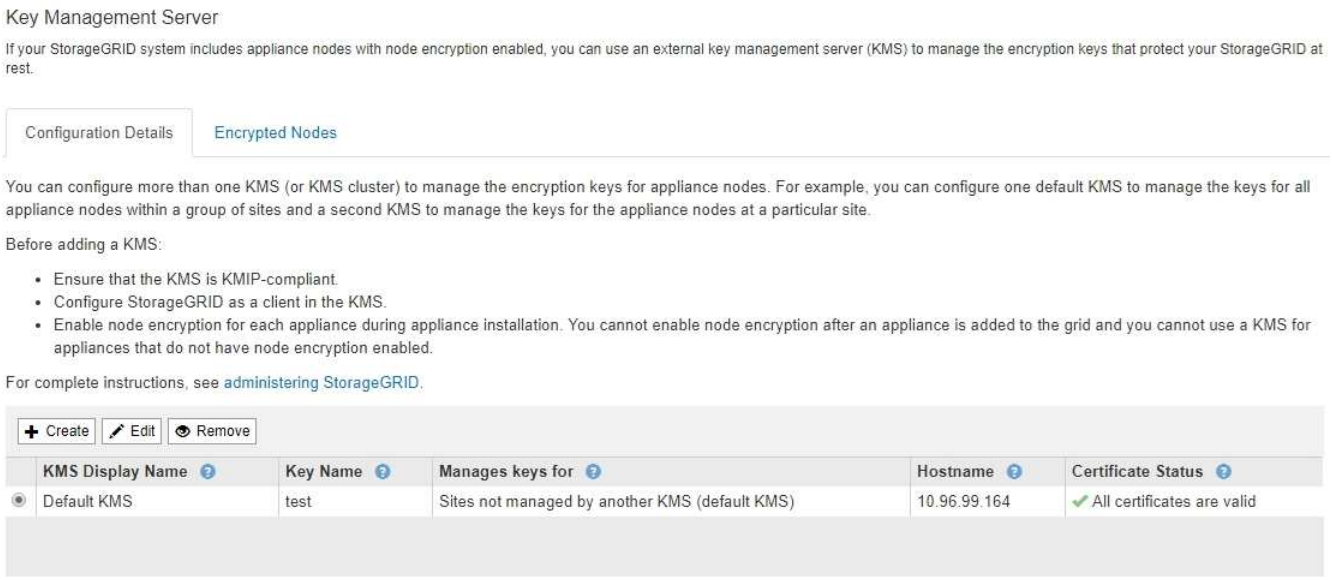
Affichage des nœuds chiffrés

Vous pouvez afficher des informations sur les nœuds d'appliance de votre système StorageGRID sur lesquels le paramètre **Node Encryption** est activé.

Étapes

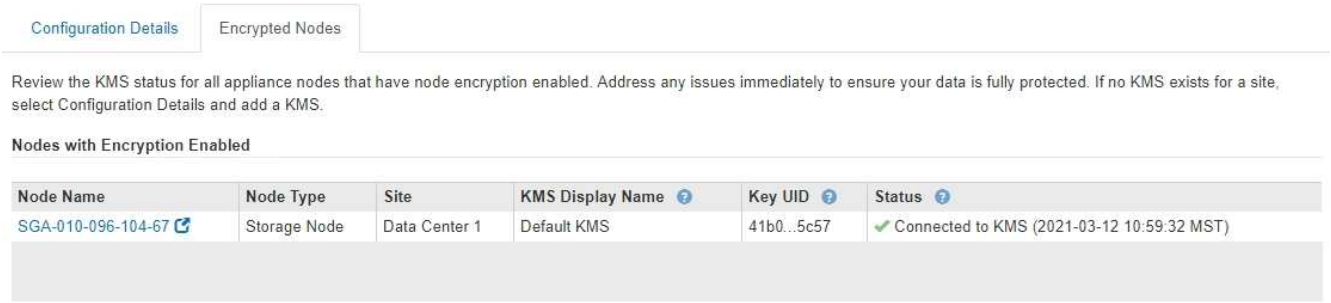
1. Sélectionnez **Configuration** > **Paramètres système** > **serveur de gestion des clés**.

   La page Key Management Server s'affiche. L'onglet Détails de la configuration affiche tous les serveurs de gestion des clés qui ont été configurés.



2. En haut de la page, sélectionnez l'onglet **Nodes cryptés**.

   L'onglet nœuds cryptés répertorie les nœuds d'appliance de votre système StorageGRID dont le paramètre **Node Encryption** est activé.



3. Vérifiez les informations du tableau pour chaque nœud d'appliance.

Colonne	Description
Nom du nœud	Nom du nœud d'appliance.
Type de nœud	Le type de nœud : stockage, Administrateur ou passerelle.
Le site	Nom du site StorageGRID sur lequel le nœud est installé.
Nom d'affichage DES KMS	Nom descriptif du KMS utilisé pour le nœud. Si aucun KMS n'est répertorié, sélectionnez l'onglet Détails de la configuration pour ajouter un KMS. "Ajout d'un serveur de gestion des clés (KMS)"
UID de clé	ID unique de la clé de cryptage utilisée pour crypter et décrypter les données sur le nœud de l'appliance. Pour afficher l'intégralité d'un UID de clé, placez le curseur sur la cellule. Un tiret (--) indique que l'UID de clé est inconnu, peut-être en raison d'un problème de connexion entre le nœud de l'appliance et le KMS.
État	L'état de la connexion entre le KMS et le nœud de l'appliance. Si le nœud est connecté, l'horodatage est mis à jour toutes les 30 minutes. La mise à jour de l'état de connexion peut prendre plusieurs minutes après la modification de la configuration KMS. **Remarque :** vous devez actualiser votre navigateur Web pour voir les nouvelles valeurs.

4. Si la colonne État indique un problème KMS, répondez immédiatement au problème.

   Pendant les opérations KMS normales, l'état sera **connecté à KMS**. Si un nœud est déconnecté de la grille, l'état de connexion du nœud est affiché (administrativement arrêté ou inconnu).

   Les autres messages d'état correspondent aux alertes StorageGRID portant le même nom :

   - Echec du chargement de la configuration DES KMS
   - Erreur de connectivité KMS

- Nom de la clé de cryptage KMS introuvable
- Echec de la rotation de la clé de chiffrement KMS
- La clé KMS n'a pas réussi à décrypter un volume d'appliance
- LES KM ne sont pas configurés Voir les actions recommandées pour ces alertes dans les instructions de surveillance et de dépannage de StorageGRID.

> Vous devez immédiatement résoudre tout problème pour assurer la protection intégrale de vos données.

Informations associées

"Moniteur et amp ; dépannage"

Modification d'un serveur de gestion des clés (KMS)

Vous devrez peut-être modifier la configuration d'un serveur de gestion des clés, par exemple si un certificat est sur le point d'expirer.

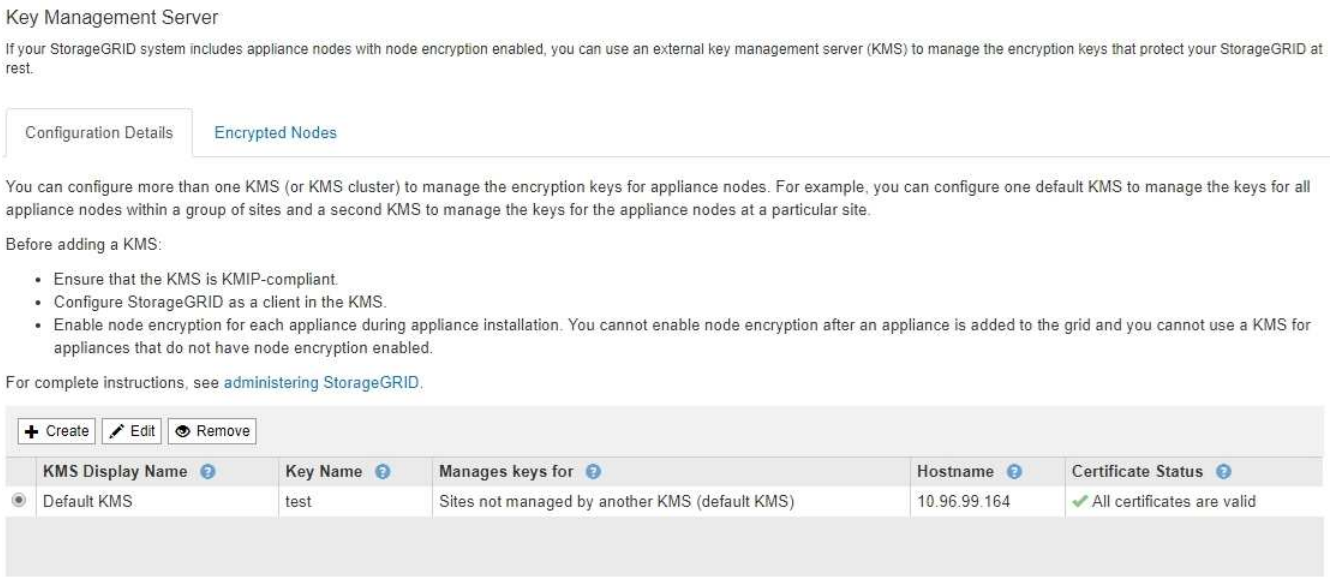
Ce dont vous avez besoin

- Vous devez avoir consulté le "considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés".
- Si vous prévoyez de mettre à jour le site sélectionné pour un KMS, vous devez avoir consulté le "Considérations relatives à la modification du KMS pour un site".
- Vous devez disposer de l'autorisation accès racine.
- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.

Étapes

1. Sélectionnez **Configuration** > **Paramètres système** > **serveur de gestion des clés**.

   La page Key Management Server s'affiche et affiche tous les serveurs de gestion des clés qui ont été configurés.



2. Sélectionnez le KMS à modifier et sélectionnez **Modifier**.

3. Vous pouvez également mettre à jour les détails dans **étape 1 (entrer les détails KMS)** de l'assistant Modifier un serveur de gestion de clés.

Champ	Description
Nom d'affichage DES KMS	Un nom descriptif pour vous aider à identifier ce KMS. Doit comporter entre 1 et 64 caractères.
Nom de clé	Alias de clé exact pour le client StorageGRID dans le KMS. Doit comporter entre 1 et 255 caractères. Il vous suffit de modifier le nom de la clé dans de rares cas. Par exemple, vous devez modifier le nom de la clé si l'alias est renommé dans le KMS ou si toutes les versions de la clé précédente ont été copiées dans l'historique des versions du nouvel alias. Ne tentez jamais de faire pivoter une clé en modifiant le nom de clé (alias) du KMS. Faites plutôt pivoter la clé en mettant à jour la version de clé dans le logiciel KMS. StorageGRID nécessite que toutes les versions de clés déjà utilisées (ainsi que toutes les versions à venir) soient accessibles depuis le KMS avec le même alias de clé. Si vous modifiez l'alias de clé pour un KMS configuré, StorageGRID risque de ne pas être en mesure de décrypter vos données. "Considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés"
Gère les clés pour	Si vous modifiez un KMS spécifique au site et que vous n'avez pas déjà un KMS par défaut, vous pouvez sélectionner **sites non gérés par un autre KMS (par défaut KMS)**. Cette sélection convertit un KMS spécifique au site en KMS par défaut, qui s'appliquera à tous les sites qui n'ont pas de KMS dédié et à tous les sites ajoutés dans une extension. **Remarque :** si vous modifiez un KMS spécifique au site, vous ne pouvez pas sélectionner un autre site. Si vous modifiez le KMS par défaut, vous ne pouvez pas sélectionner un site spécifique.
Port	Le port utilisé par le serveur KMS pour les communications KMIP (Key Management Interoperability Protocol). La valeur par défaut est 5696, qui est le port standard KMIP.
Nom d'hôte	Le nom de domaine complet ou l'adresse IP du KMS. **Remarque :** le champ SAN du certificat de serveur doit inclure le FQDN ou l'adresse IP que vous saisissez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ou à tous les serveurs d'un cluster KMS.

4. Si vous configurez un cluster KMS, sélectionnez le signe plus ➕ pour ajouter un nom d'hôte pour chaque serveur du cluster.
5. Sélectionnez **Suivant**.

   L'étape 2 (Télécharger un certificat de serveur) de l'assistant Modifier un serveur de gestion de clés s'affiche.

6. Si vous devez remplacer le certificat de serveur, sélectionnez **Parcourir** et téléchargez le nouveau fichier.
7. Sélectionnez **Suivant**.

   L'étape 3 (Téléchargement de certificats client) de l'assistant Modifier un serveur de gestion de clés s'affiche.

8. Si vous devez remplacer le certificat client et la clé privée du certificat client, sélectionnez **Parcourir** et téléchargez les nouveaux fichiers.
9. Sélectionnez **Enregistrer**.

   Les connexions entre le serveur de gestion des clés et tous les nœuds d'appliance chiffrés sur les sites affectés sont testées. Si toutes les connexions de nœud sont valides et que la clé correcte est trouvée sur le KMS, le serveur de gestion des clés est ajouté à la table de la page Key Management Server.

10. Si un message d'erreur s'affiche, vérifiez les détails du message et sélectionnez **OK**.

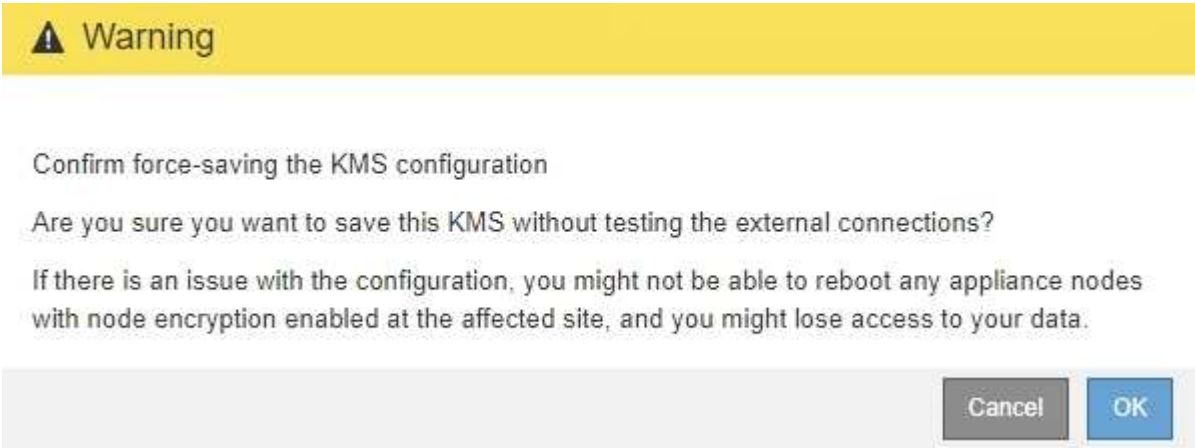
    Par exemple, vous pouvez recevoir une erreur 422 : entité impossible à traiter si le site que vous avez sélectionné pour ce KMS est déjà géré par un autre KMS, ou si un test de connexion a échoué.

11. Si vous devez enregistrer la configuration actuelle avant de résoudre les erreurs de connexion, sélectionnez **forcer l'enregistrement**.

    > Si vous sélectionnez **forcer l'enregistrement**, la configuration KMS est enregistrée, mais il ne teste pas la connexion externe de chaque appliance vers ce KMS. En cas de problème avec la configuration, vous ne pouvez pas redémarrer les nœuds d'appliance pour lesquels le chiffrement de nœud est activé sur le site affecté. L'accès à vos données risque d'être perdu jusqu'à la résolution des problèmes.

    La configuration KMS est enregistrée.

12. Vérifiez l'avertissement de confirmation et sélectionnez **OK** si vous êtes sûr de vouloir forcer l'enregistrement de la configuration.



La configuration KMS est enregistrée mais la connexion au KMS n’est pas testée.

Suppression d’un serveur de gestion des clés (KMS)

Dans certains cas, vous pouvez supprimer un serveur de gestion des clés. Par exemple, vous pouvez vouloir supprimer un KMS spécifique au site si vous avez désactivé le site.

Ce dont vous avez besoin

- Vous devez avoir consulté le "considérations et conditions requises pour l’utilisation d’un serveur de gestion des clés".
- Vous devez disposer de l’autorisation accès racine.
- Vous devez être connecté à Grid Manager à l’aide d’un navigateur pris en charge.

Description de la tâche

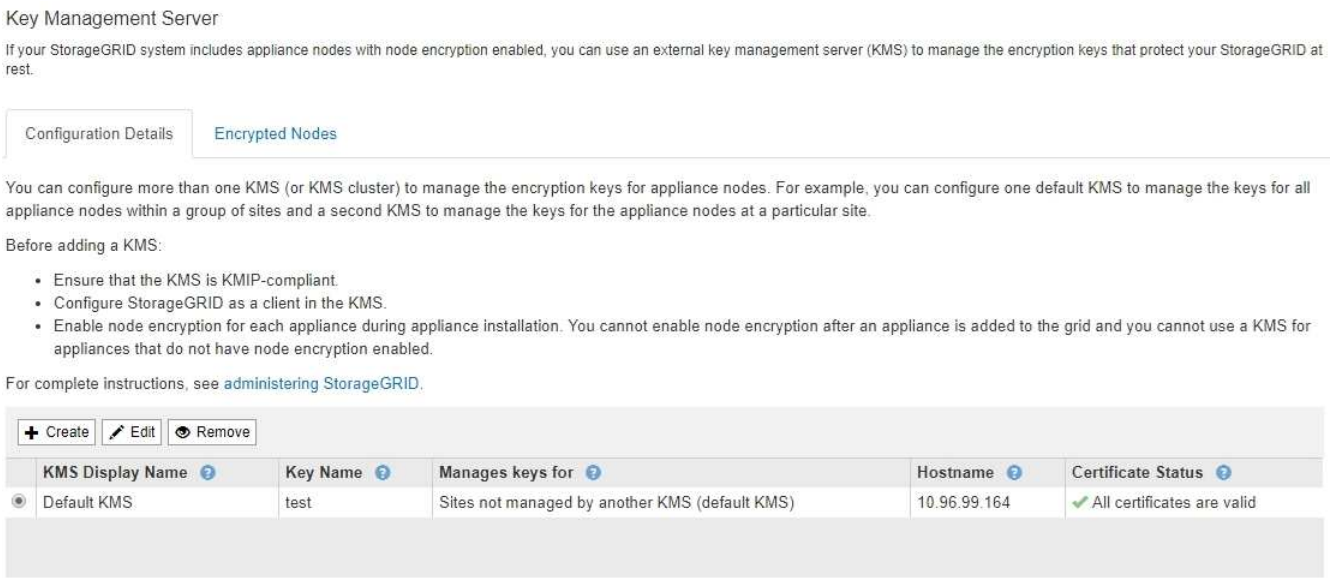
Vous pouvez supprimer un KMS dans les cas suivants :

- Vous pouvez supprimer un KMS spécifique au site si le site a été désactivé ou si le site ne contient aucun nœud d’appliance lorsque le chiffrement de nœud est activé.
- Vous pouvez supprimer le KMS par défaut si un KMS spécifique au site existe déjà pour chaque site sur lequel des nœuds d’appliance sont activés pour que le chiffrement des nœuds soit activé.

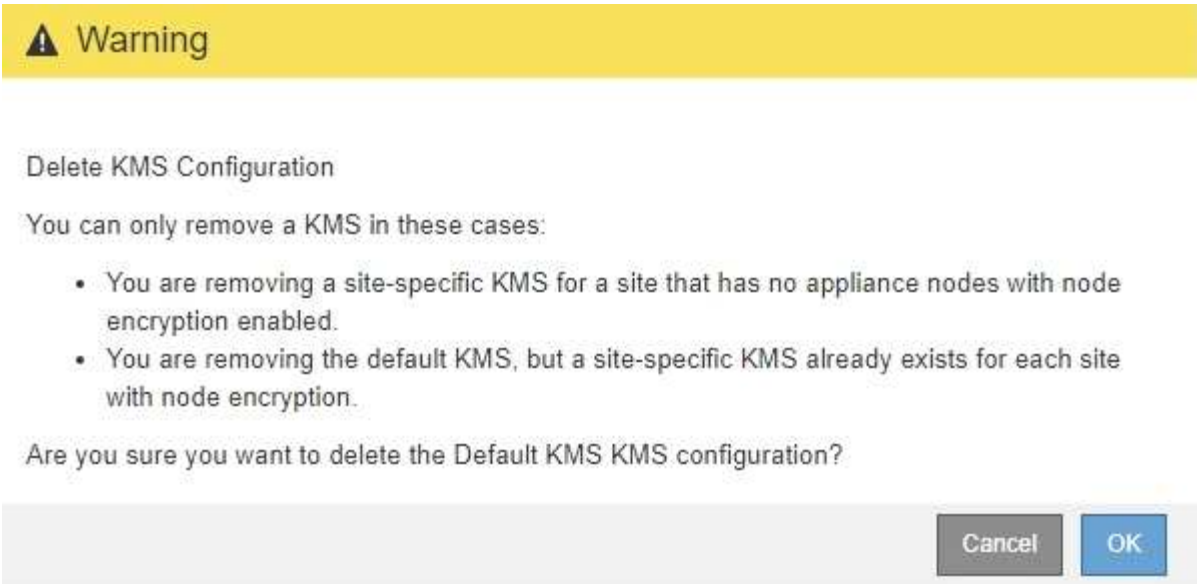
Étapes

1. Sélectionnez **Configuration** > **Paramètres système** > **serveur de gestion des clés**.

   La page Key Management Server s’affiche et affiche tous les serveurs de gestion des clés qui ont été configurés.



2. Sélectionnez le bouton radio du KMS que vous souhaitez supprimer, puis sélectionnez **Supprimer**.
3. Passez en revue les éléments à prendre en compte dans la boîte de dialogue d’avertissement.



4. Sélectionnez **OK**.

   La configuration KMS est supprimée.

Gestion des locataires

En tant qu'administrateur du grid, vous créez et gérez les comptes de locataire utilisés par les clients S3 et Swift pour stocker et récupérer des objets, surveiller l'utilisation du stockage et gérer les actions que les clients peuvent exécuter à l'aide de votre système StorageGRID.

Quels sont les comptes de locataires

Les comptes de locataires permettent aux applications client qui utilisent l'API REST S3 (simple Storage Service) ou l'API REST Swift pour stocker et récupérer des objets dans StorageGRID.

Chaque compte de locataire prend en charge l'utilisation d'un protocole unique, que vous spécifiez lors de la création du compte. Pour stocker et récupérer des objets dans un système StorageGRID avec les deux protocoles, vous devez créer deux comptes de locataire : un pour les compartiments et objets S3, et un pour les conteneurs et objets Swift. Chaque compte de locataire possède son propre ID de compte, groupes et utilisateurs autorisés, compartiments ou conteneurs, et objets.

Vous pouvez également créer des comptes de tenant supplémentaires si vous souhaitez isoler les objets stockés sur votre système par des entités différentes. Par exemple, vous pouvez définir plusieurs comptes locataires dans l'un de ces cas d'utilisation :

- **Cas d'utilisation entreprise :** si vous gérez un système StorageGRID dans une application d'entreprise, vous pourriez vouloir isoler le stockage objet de la grille par les différents départements de votre organisation. Dans ce cas, vous pouvez créer des comptes de tenant pour le département Marketing, le service Customer support, le service des ressources humaines, etc.

> Si vous utilisez le protocole client S3, il vous suffit d'utiliser des compartiments S3 et des règles de compartiment pour isoler les objets entre les différents départements d'une entreprise. Vous n'avez pas besoin d'utiliser de comptes de tenant. Pour plus d'informations, consultez les instructions d'implémentation des applications client S3.

- **Cas d'utilisation de fournisseur de services :** si vous gérez un système StorageGRID en tant que fournisseur de services, vous pouvez isoler le stockage objet de la grille par les différentes entités qui loueront le stockage sur votre grille. Dans ce cas, vous créeriez des comptes de tenant pour la société A, la société B, la société C, etc.

Création et configuration des comptes de tenant

Lorsque vous créez un compte de locataire, vous spécifiez les informations suivantes :

- Afficher le nom du compte locataire.
- Quel protocole client sera utilisé par le compte de locataire (S3 ou Swift).
- Pour les comptes de locataire S3 : si le compte du locataire est autorisé à utiliser des services de plateforme avec des compartiments S3. Si vous autorisez les comptes locataires à utiliser des services de plateforme, vous devez vous assurer que la grille est configurée pour prendre en charge leur utilisation. Voir "Manage des services de plate-forme".
- Éventuellement, un quota de stockage pour le compte du locataire, soit le nombre maximal de gigaoctets, téraoctets ou pétaoctets disponibles pour les objets du locataire. Si le quota est dépassé, le locataire ne peut pas créer de nouveaux objets.

> Le quota de stockage d'un locataire représente une quantité logique (taille d'objet), et non une quantité physique (taille sur disque).

- Si la fédération des identités est activée pour le système StorageGRID, quel groupe fédéré a l'autorisation d'accès racine pour configurer le compte de tenant.
- Si l'authentification unique (SSO) n'est pas utilisée pour le système StorageGRID, que le compte de tenant utilise son propre référentiel d'identité ou partage le référentiel d'identité de la grille et le mot de passe initial de l'utilisateur racine local du locataire.

Une fois le compte de locataire créé, vous pouvez effectuer les tâches suivantes :

- **Gérer les services de plate-forme pour le grid** : si vous activez les services de plate-forme pour les comptes de tenant, assurez-vous de comprendre comment les messages de services de plate-forme sont fournis et les exigences de mise en réseau que l'utilisation des services de plate-forme place dans votre déploiement StorageGRID.
- **Surveiller l'utilisation du stockage d'un compte locataire** : lorsque les locataires commencent à utiliser leurs comptes, vous pouvez utiliser Grid Manager pour surveiller la quantité de stockage consommée par chaque locataire.

  Si vous avez défini des quotas pour les locataires, vous pouvez activer l'alerte **usage du quota de locataires élevé** pour déterminer si les locataires consomment leurs quotas. Si elle est activée, cette alerte est déclenchée lorsqu'un locataire a utilisé 90 % de son quota. Pour plus d'informations, consultez la référence des alertes dans les instructions de surveillance et de dépannage de StorageGRID.

- **Configurer les opérations client** : vous pouvez configurer si certains types d'opérations client sont interdits.

Configuration des locataires S3

Une fois le compte de locataire S3 créé, les utilisateurs peuvent accéder au Gestionnaire des locataires pour effectuer les tâches suivantes :

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

> Les locataires S3 peuvent créer et gérer des compartiments et des clés d'accès S3 avec le gestionnaire des locataires. Cependant, ils doivent utiliser une application client S3 pour récupérer et gérer les objets.

Configuration des locataires Swift

Une fois le compte de locataire Swift créé, l'utilisateur root du locataire peut accéder au Gestionnaire de locataires pour effectuer les tâches suivantes :

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

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

Informations associées

"Utilisez un compte de locataire"

Création d'un compte de locataire

Vous devez créer au moins un compte de locataire pour contrôler l'accès au stockage dans votre système StorageGRID.

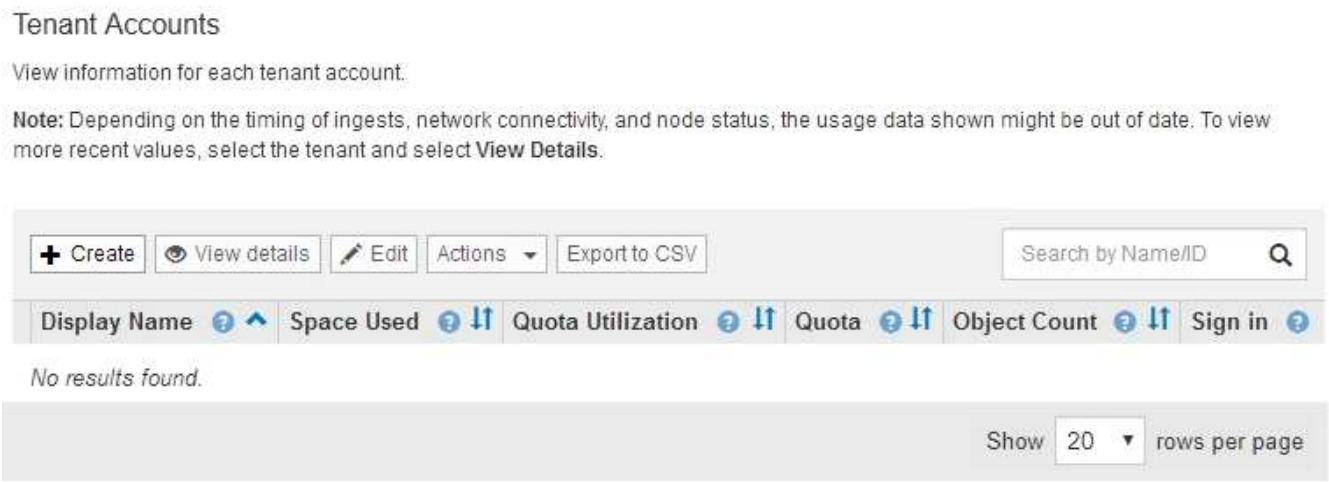
Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **locataires**.

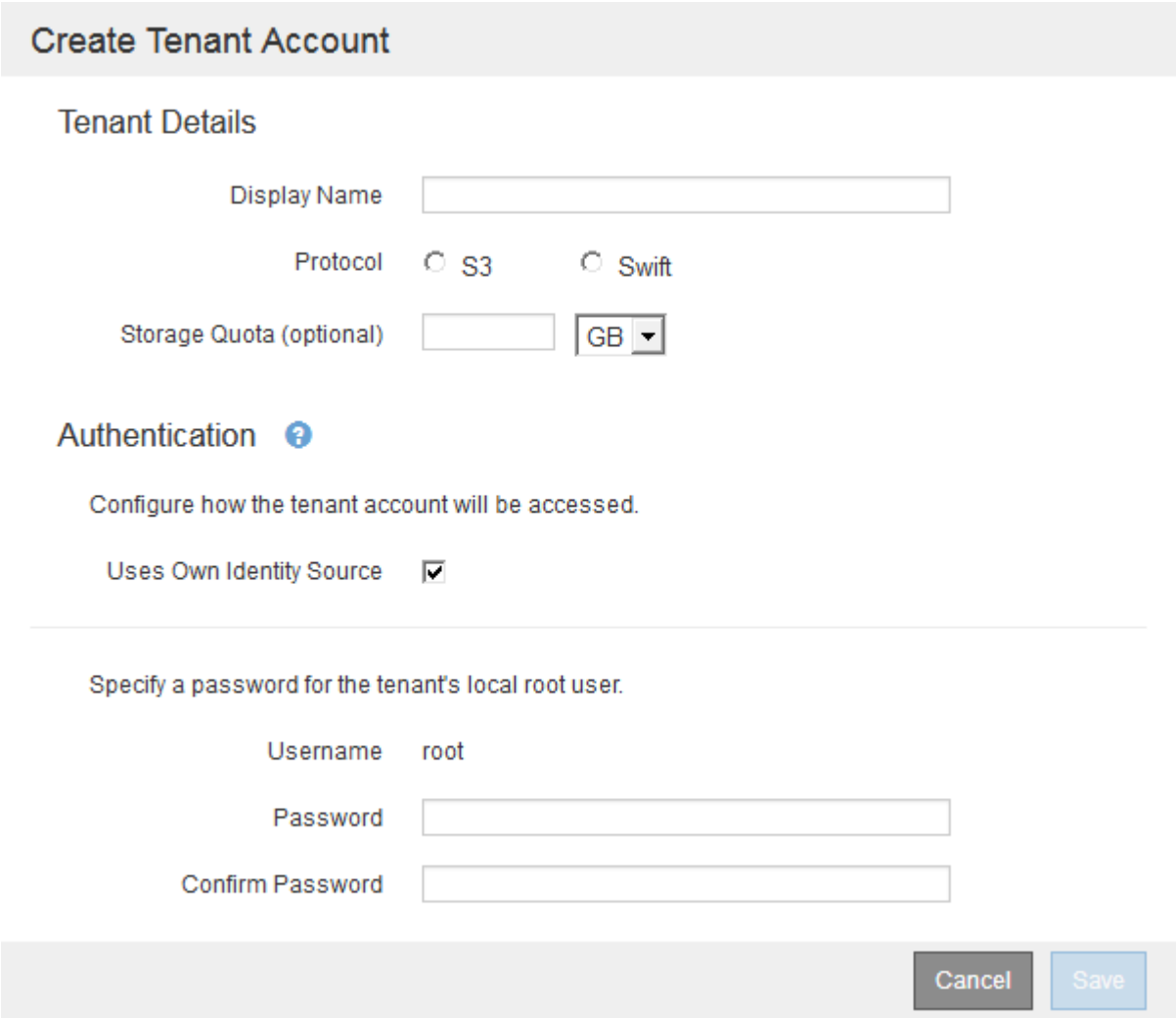
   La page comptes de tenant s'affiche et répertorie tous les comptes de tenant existants.



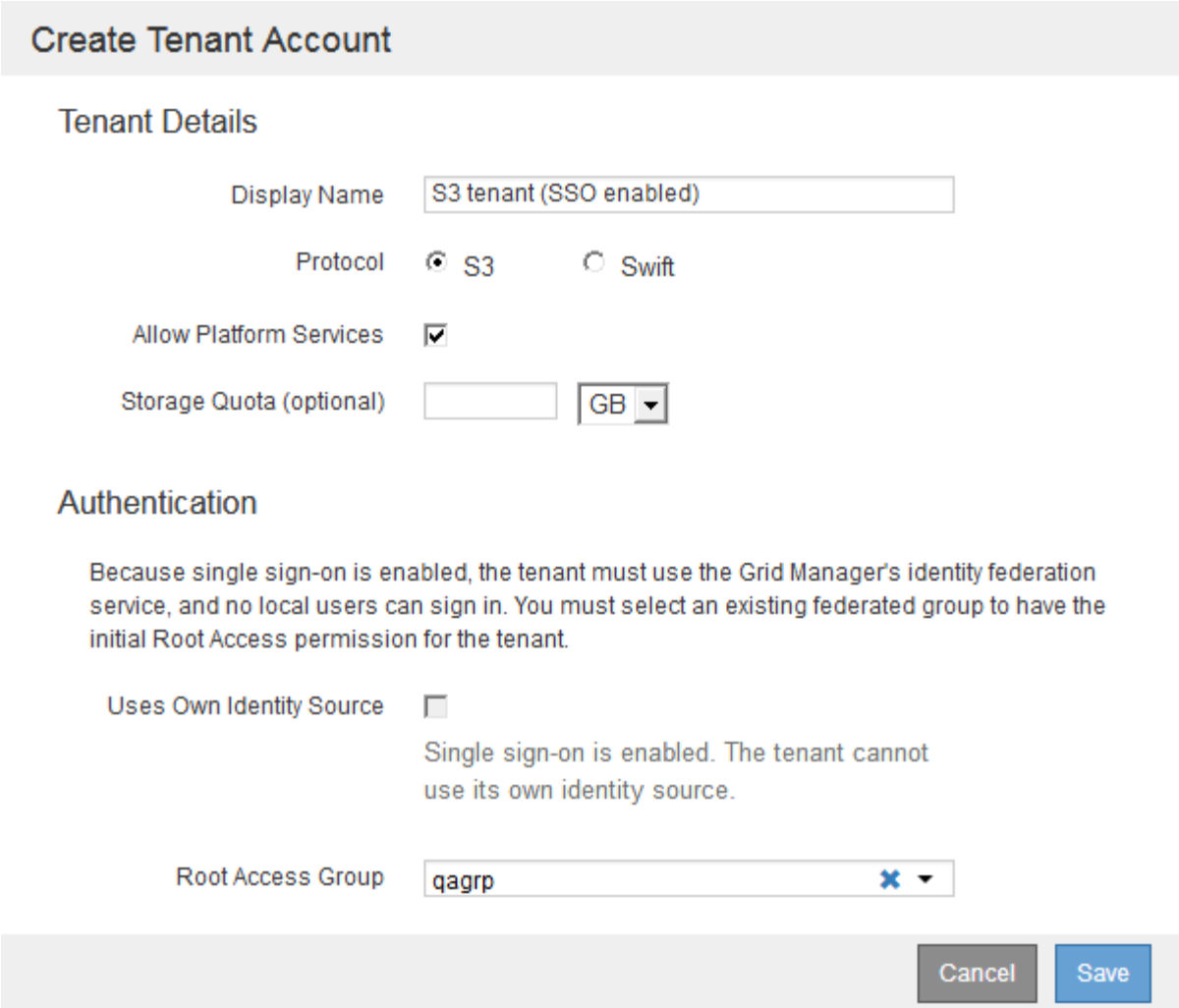
2. Sélectionnez **Créer**.

   La page Créer un compte de tenant s'affiche. Les champs de cette page dépendent de l'activation ou non de l'authentification unique (SSO) pour le système StorageGRID.

   - Si SSO n'est pas utilisé, la page Créer un compte de locataire ressemble à ceci.



   - Si SSO est activé, la page Créer un compte de tenant ressemble à ceci.



Informations associées

"Utilisation de la fédération des identités"

"Configuration de l'authentification unique"

Création d'un compte de locataire si StorageGRID n'utilise pas SSO

Lorsque vous créez un compte de locataire, vous spécifiez un nom, un protocole client et, éventuellement, un quota de stockage. Si StorageGRID n'utilise pas la connexion unique (SSO), vous devez également indiquer si le compte de tenant utilisera son propre référentiel d'identité et configurer le mot de passe initial pour l'utilisateur racine local du locataire.

Description de la tâche

Si le compte de tenant utilise le référentiel d'identité qui a été configuré pour Grid Manager et que vous souhaitez accorder l'autorisation d'accès racine au compte de tenant à un groupe fédéré, vous devez avoir importé ce groupe fédéré dans Grid Manager. Vous n'avez pas besoin d'attribuer des autorisations Grid Manager à ce groupe d'administration. Reportez-vous aux instructions pour "gestion des groupes d'administration".

Étapes

1. Dans la zone de texte **Nom d'affichage**, entrez un nom d'affichage pour ce compte locataire.

   Les noms d'affichage n'ont pas besoin d'être uniques. Lorsque le compte de tenant est créé, il reçoit un ID de compte numérique unique.

2. Sélectionnez le protocole client qui sera utilisé par ce compte locataire, soit **S3**, soit **Swift**.
3. Pour les comptes locataires S3, cochez la case **Autoriser les services de plateforme**, sauf si vous ne souhaitez pas que ce locataire utilise les services de plateforme pour les compartiments S3.

   Si les services de plateforme sont activés, un locataire peut utiliser des fonctionnalités, telles que la réplication CloudMirror, qui accèdent aux services externes. Il serait intéressant de désactiver l'utilisation de ces fonctionnalités pour limiter la quantité de bande passante du réseau ou d'autres ressources consommées par un locataire. Voir "Manage des services de plate-forme".

4. Dans la zone de texte **Storage quota**, vous pouvez éventuellement entrer le nombre maximal de gigaoctets, de téraoctets ou de pétaoctets que vous souhaitez mettre à disposition des objets de ce locataire. Sélectionnez ensuite les unités dans la liste déroulante.

   Laissez ce champ vide si vous souhaitez que ce locataire dispose d'un quota illimité.

   > Le quota de stockage d'un locataire représente une quantité logique (taille d'objet), et non une quantité physique (taille sur disque). Les copies ILM et le code d'effacement ne contribuent pas au volume de quotas utilisés. Si le quota est dépassé, le compte du locataire ne peut pas créer de nouveaux objets.

   > Pour surveiller l'utilisation du stockage de chaque compte locataire, sélectionnez **utilisation**. Les comptes des locataires peuvent également surveiller leur propre utilisation du stockage depuis le tableau de bord dans le Gestionnaire de locataires ou via l'API de gestion des locataires. Les valeurs d'utilisation du stockage d'un locataire peuvent devenir obsolètes si les nœuds sont isolés des autres nœuds de la grille. Les totaux seront mis à jour lorsque la connectivité réseau sera restaurée.

5. Si le locataire gère ses propres groupes et utilisateurs, procédez comme suit.
   a. Cochez la case **Uses own Identity Source** (par défaut).

      > Si cette case est cochée et que vous souhaitez utiliser la fédération des identités pour les groupes de locataires et les utilisateurs, le locataire doit configurer son propre référentiel d'identité. Reportez-vous aux instructions d'utilisation des comptes de tenant.

   b. Spécifiez un mot de passe pour l'utilisateur racine local du locataire.
6. Si le locataire utilise les groupes et les utilisateurs configurés pour le Grid Manager, procédez comme suit.
   a. Décochez la case **utilise son propre référentiel d'identité**.
   b. Effectuez l'une des opérations suivantes ou les deux :
      - Dans le champ Groupe d'accès racine, sélectionnez un groupe fédéré existant dans le gestionnaire de grille disposant de l'autorisation d'accès racine initiale pour le locataire.

        > Si vous disposez d'autorisations adéquates, les groupes fédérés existants dans Grid Manager sont répertoriés lorsque vous cliquez sur le champ. Sinon, entrez le nom unique du groupe.

- Spécifiez un mot de passe pour l'utilisateur racine local du locataire.

7. Cliquez sur **Enregistrer**.

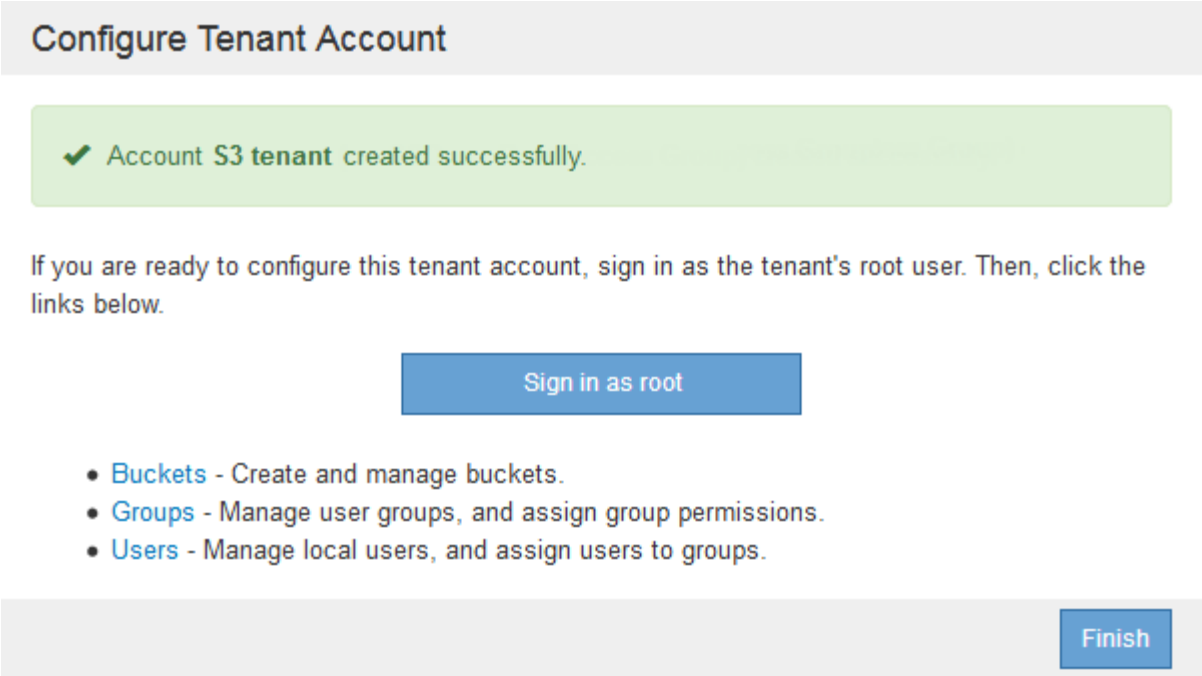
   Le compte de locataire est créé.

8. Vous pouvez également accéder au nouveau locataire. Sinon, passer à l'étape pour accès au locataire ultérieurement.

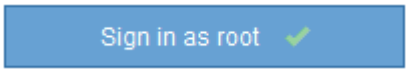
Si vous êtes…	Procédez comme ça…
Accès au Grid Manager sur un port restreint	Cliquez sur **restreint** pour en savoir plus sur l'accès à ce compte de locataire. L'URL du Gestionnaire de locataires a le format suivant : `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` • *`FQDN_or_Admin_Node_IP`* Est un nom de domaine complet ou l'adresse IP d'un nœud d'administration • *`port`* est le port locataire uniquement • *`20-digit-account-id`* Est l'ID de compte unique du locataire
Accès au gestionnaire de grille sur le port 443 mais vous n'avez pas défini de mot de passe pour l'utilisateur racine local	Cliquez sur **connexion** et entrez les informations d'identification d'un utilisateur dans le groupe fédéré d'accès racine.
Accès au gestionnaire de grille sur le port 443 et définition d'un mot de passe pour l'utilisateur racine local	Passez à l'étape suivante sur connectez-vous en tant que root.

9. se connecter au locataire en tant que root :

   a. Dans la boîte de dialogue configurer le compte de tenant, cliquez sur le bouton **se connecter en tant que root**.



Une coche verte s'affiche sur le bouton, indiquant que vous êtes maintenant connecté au compte de tenant en tant qu'utilisateur racine.



a. Cliquez sur les liens pour configurer le compte de tenant.

   Chaque lien ouvre la page correspondante dans le Gestionnaire de locataires. Pour compléter la page, reportez-vous aux instructions d'utilisation des comptes de tenant.

b. Cliquez sur **Terminer**.

10. pour accéder ultérieurement au locataire :

Si vous utilisez…	Effectuez l'une d'entre elles…
Orifice 443	• Dans Grid Manager, sélectionnez **tenants**, puis cliquez sur **connexion** à droite du nom du locataire. • Entrez l'URL du locataire dans un navigateur Web : `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ *`FQDN_or_Admin_Node_IP`* Est un nom de domaine complet ou l'adresse IP d'un nœud d'administration ◦ *`20-digit-account-id`* Est l'ID de compte unique du locataire

Si vous utilisez…	Effectuez l'une d'entre elles…
Un port restreint	• Dans Grid Manager, sélectionnez **tenants** et cliquez sur **restreint**. • Entrez l'URL du locataire dans un navigateur Web : `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ *`FQDN_or_Admin_Node_IP`* Est un nom de domaine complet ou l'adresse IP d'un nœud d'administration ◦ *`port`* est le port réservé aux locataires ◦ *`20-digit-account-id`* Est l'ID de compte unique du locataire

Informations associées

"Contrôle de l'accès par pare-feu"

"Gestion des services de plateforme pour les comptes de locataires S3"

"Utilisez un compte de locataire"

Création d'un compte de locataire si SSO est activé

Lorsque vous créez un compte de locataire, vous spécifiez un nom, un protocole client et, éventuellement, un quota de stockage. Si l'authentification unique (SSO) est activée pour StorageGRID, vous spécifiez également quel groupe fédéré a l'autorisation d'accès racine pour configurer le compte de tenant.

Étapes

1. Dans la zone de texte **Nom d'affichage**, entrez un nom d'affichage pour ce compte locataire.

   Les noms d'affichage n'ont pas besoin d'être uniques. Lorsque le compte de tenant est créé, il reçoit un ID de compte numérique unique.

2. Sélectionnez le protocole client qui sera utilisé par ce compte locataire, soit **S3**, soit **Swift**.
3. Pour les comptes locataires S3, cochez la case **Autoriser les services de plateforme**, sauf si vous ne souhaitez pas que ce locataire utilise les services de plateforme pour les compartiments S3.

   Si les services de plateforme sont activés, un locataire peut utiliser des fonctionnalités, telles que la réplication CloudMirror, qui accèdent aux services externes. Il serait intéressant de désactiver l'utilisation de ces fonctionnalités pour limiter la quantité de bande passante du réseau ou d'autres ressources consommées par un locataire. Voir "Manage des services de plate-forme".

4. Dans la zone de texte **Storage quota**, vous pouvez éventuellement entrer le nombre maximal de gigaoctets, de téraoctets ou de pétaoctets que vous souhaitez mettre à disposition des objets de ce locataire. Sélectionnez ensuite les unités dans la liste déroulante.

   Laissez ce champ vide si vous souhaitez que ce locataire dispose d'un quota illimité.

> Le quota de stockage d'un locataire représente une quantité logique (taille d'objet), et non une quantité physique (taille sur disque). Les copies ILM et le code d'effacement ne contribuent pas au volume de quotas utilisés. Si le quota est dépassé, le compte du locataire ne peut pas créer de nouveaux objets.

> Pour surveiller l'utilisation du stockage de chaque compte locataire, sélectionnez **utilisation**. Les comptes des locataires peuvent également surveiller leur propre utilisation du stockage depuis le tableau de bord dans le Gestionnaire de locataires ou via l'API de gestion des locataires. Les valeurs d'utilisation du stockage d'un locataire peuvent devenir obsolètes si les nœuds sont isolés des autres nœuds de la grille. Les totaux seront mis à jour lorsque la connectivité réseau sera restaurée.

5. Notez que la case à cocher **Uses own Identity Source** est décochée et désactivée.

   Comme SSO est activé, le locataire doit utiliser le référentiel d'identité configuré pour Grid Manager. Aucun utilisateur local ne peut se connecter.

6. Dans le champ **Root Access Group**, sélectionnez un groupe fédéré existant dans le gestionnaire de grille pour obtenir l'autorisation d'accès racine initiale pour le locataire.

   > Si vous disposez d'autorisations adéquates, les groupes fédérés existants dans Grid Manager sont répertoriés lorsque vous cliquez sur le champ. Sinon, entrez le nom unique du groupe.

7. Cliquez sur **Enregistrer**.

   Le compte de locataire est créé. La page comptes de tenant s'affiche et comprend une ligne pour le nouveau tenant.

8. Si vous êtes un utilisateur du groupe accès racine, vous pouvez également cliquer sur le lien **connexion** pour que le nouveau locataire puisse accéder immédiatement au Gestionnaire de tenant, où vous pouvez configurer le locataire. Sinon, indiquez l'URL du lien **connexion** à l'administrateur du compte de locataire. (L'URL d'un locataire correspond au nom de domaine complet ou à l'adresse IP d'un nœud d'administration, suivi de `/?accountId=`*`20-digit-account-id`*.)

   > Un message d'accès refusé s'affiche si vous cliquez sur **connexion**, mais que vous n'appartenez pas au groupe accès racine du compte de tenant.

Informations associées

"Configuration de l'authentification unique"

"Gestion des services de plateforme pour les comptes de locataires S3"

"Utilisez un compte de locataire"

Modification du mot de passe de l'utilisateur racine local d'un locataire

Vous devrez peut-être modifier le mot de passe de l'utilisateur root local d'un locataire si celui-ci est verrouillé hors du compte.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Si l'authentification unique (SSO) est activée pour votre système StorageGRID, l'utilisateur root local ne peut pas se connecter au compte du locataire. Pour effectuer des tâches utilisateur racine, les utilisateurs doivent appartenir à un groupe fédéré disposant de l'autorisation accès racine pour le locataire.

Étapes

1. Sélectionnez **locataires**.

   La page comptes de tenant s'affiche et répertorie tous les comptes de tenant existants.

   Tenant Accounts

   View information for each tenant account.

   Note: Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant and select **View Details**.

   + Create | View details | Edit | Actions | Export to CSV | Search by Name/ID

	Display Name	Space Used	Quota Utilization	Quota	Object Count	Sign in
◉	Account01	500.00 KB	0.00%	20.00 GB	100	
○	Account02	2.50 MB	0.01%	30.00 GB	500	
○	Account03	605.00 MB	4.03%	15.00 GB	31,000	
○	Account04	1.00 GB	10.00%	10.00 GB	200,000	
○	Account05	0 bytes	—	Unlimited	0	

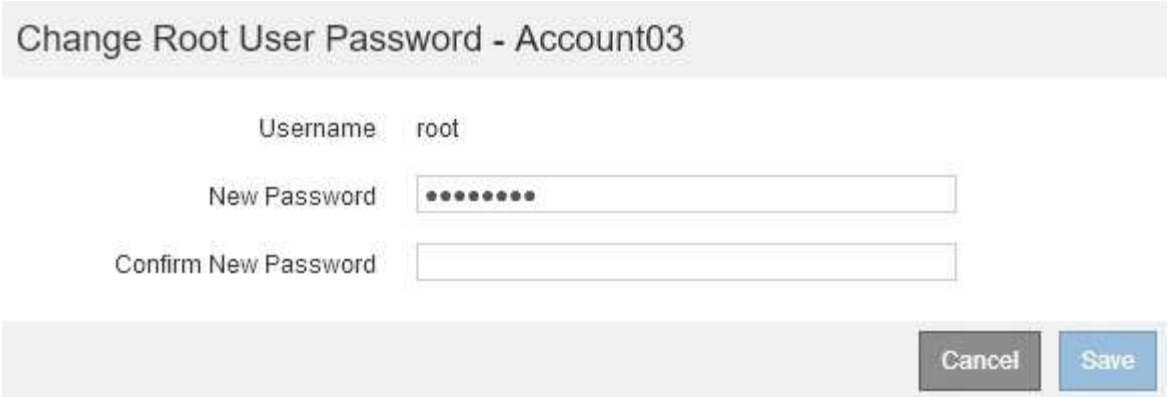
   Show 20 rows per page

2. Sélectionnez le compte de locataire à modifier.

   Si votre système comprend plus de 20 éléments, vous pouvez spécifier le nombre de lignes affichées simultanément sur chaque page. Utilisez la zone de recherche pour rechercher un compte de tenant par nom d'affichage ou ID de tenant.

   Les boutons Afficher les détails, Modifier et actions sont activés.

3. Dans la liste déroulante **actions**, sélectionnez **Modifier le mot de passe racine**.



4. Saisissez le nouveau mot de passe du compte de tenant.
5. Sélectionnez **Enregistrer**.

Informations associées

"Contrôle de l'accès administrateur à StorageGRID"

Modification d'un compte de locataire

Vous pouvez modifier un compte de tenant pour modifier le nom d'affichage, modifier le paramètre du référentiel d'identité, autoriser ou interdire les services de plate-forme, ou entrer un quota de stockage.

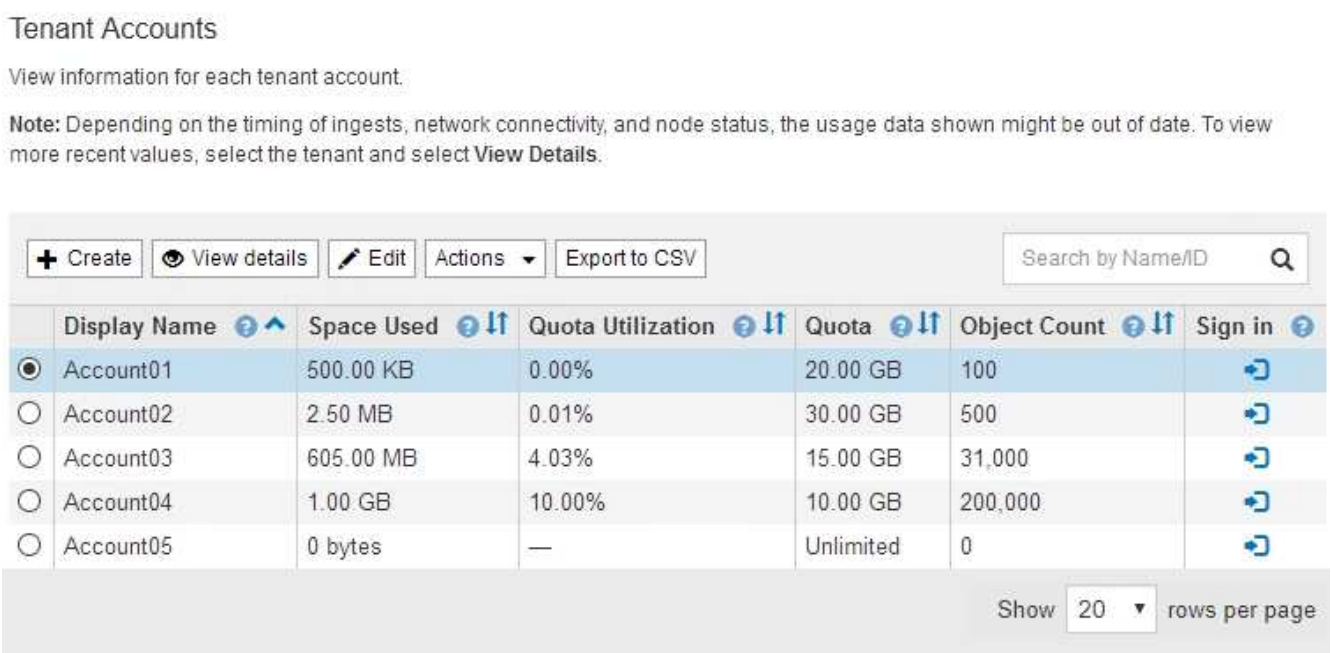
Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **locataires**.

   La page comptes de tenant s'affiche et répertorie tous les comptes de tenant existants.

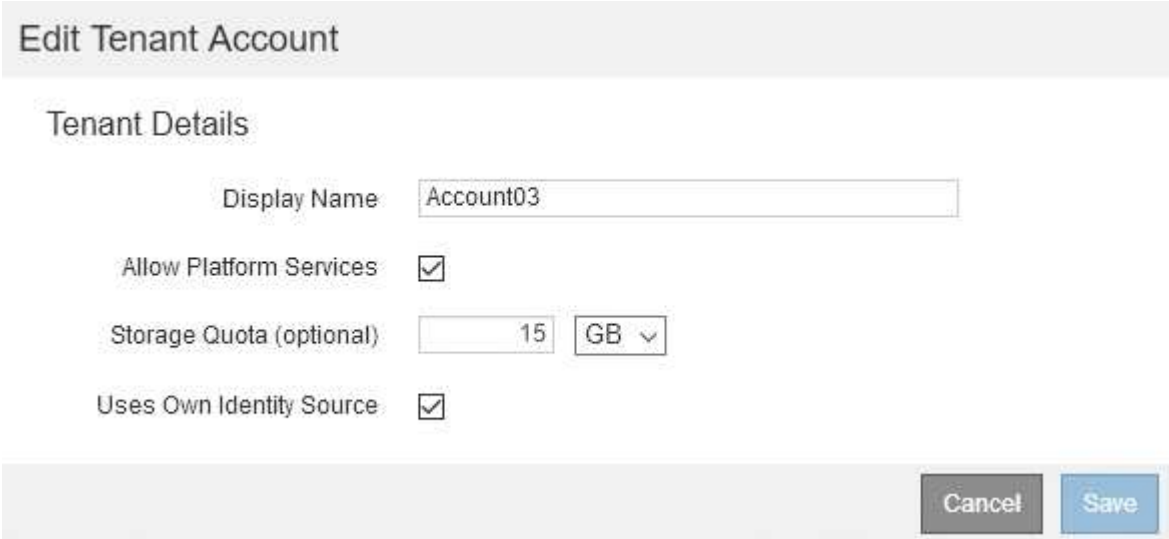


2. Sélectionnez le compte de locataire à modifier.

   Si votre système comprend plus de 20 éléments, vous pouvez spécifier le nombre de lignes affichées simultanément sur chaque page. Utilisez la zone de recherche pour rechercher un compte de tenant par nom d'affichage ou ID de tenant.

3. Sélectionnez **Modifier**.

   La page Modifier le compte de locataire s'affiche. Cet exemple concerne une grille qui n'utilise pas SSO (Single Sign-on). Ce compte de tenant n'a pas configuré son propre référentiel d'identité.



4. Modifiez les valeurs des champs selon les besoins.
   a. Modifier le nom d'affichage de ce compte de locataire.
   b. Modifiez le paramètre de la case à cocher **Autoriser les services de plate-forme** pour déterminer si le compte de tenant peut utiliser les services de plate-forme pour ses compartiments S3.

      > Si vous désactivez les services de plateforme pour un locataire qui les utilise déjà, les services qu'ils ont configurés pour leurs compartiments S3 cessent de fonctionner. Aucun message d'erreur n'est envoyé au locataire. Par exemple, si le locataire a configuré la réplication CloudMirror pour un compartiment S3, il peut toujours stocker les objets dans le compartiment, mais les copies de ces objets ne sont plus effectuées dans le compartiment S3 externe qu'ils ont configuré en tant que terminal.

   c. Pour **quota de stockage**, modifiez le nombre maximum de gigaoctets, de téraoctets ou de pétaoctets disponibles pour les objets de ce locataire, ou laissez le champ vide si vous souhaitez que ce locataire dispose d'un quota illimité.

      Le quota de stockage d'un locataire représente une quantité logique (taille d'objet), et non une quantité physique (taille sur disque). Les copies ILM et le code d'effacement ne contribuent pas au volume de quotas utilisés.

> Pour surveiller l'utilisation du stockage de chaque compte locataire, sélectionnez **utilisation**. Ils peuvent également surveiller leur propre utilisation depuis le tableau de bord dans le Gestionnaire de locataires ou à l'aide de l'API de gestion des locataires. Les valeurs d'utilisation du stockage d'un locataire peuvent devenir obsolètes si les nœuds sont isolés des autres nœuds de la grille. Les totaux seront mis à jour lorsque la connectivité réseau sera restaurée.

d. Modifiez le paramètre de la case à cocher **utilise son propre référentiel d'identité** pour déterminer si le compte de tenant utilisera son propre référentiel d'identité ou le référentiel d'identité qui a été configuré pour le gestionnaire de grille.

> Si la case à cocher **utilise son propre référentiel d'identité** est :

- Désactivé et coché, le locataire a déjà activé son propre référentiel d'identité. Un locataire doit désactiver son référentiel d'identité avant de pouvoir utiliser le référentiel d'identité configuré pour Grid Manager.
- Désactivé et décoché, la fonctionnalité SSO est activée pour le système StorageGRID. Le locataire doit utiliser le référentiel d'identité qui a été configuré pour Grid Manager.

5. Sélectionnez **Enregistrer**.

Informations associées

"Gestion des services de plateforme pour les comptes de locataires S3"

"Utilisez un compte de locataire"

Suppression d'un compte locataire

Vous pouvez supprimer un compte de tenant si vous souhaitez supprimer définitivement l'accès du tenant au système.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir supprimé tous les compartiments (S3), les conteneurs (Swift) et les objets associés au compte du locataire.

Étapes

1. Sélectionnez **locataires**.
2. Sélectionnez le compte de tenant que vous souhaitez supprimer.

   Si votre système comprend plus de 20 éléments, vous pouvez spécifier le nombre de lignes affichées simultanément sur chaque page. Utilisez la zone de recherche pour rechercher un compte de tenant par nom d'affichage ou ID de tenant.

3. Dans la liste déroulante **actions**, sélectionnez **Supprimer**.
4. Sélectionnez **OK**.

Informations associées

"Contrôle de l'accès administrateur à StorageGRID"

Gestion des services de plateforme pour les comptes de locataires S3

Si vous activez des services de plateforme pour les comptes de locataires S3, vous devez configurer votre grid de manière à ce que les locataires puissent accéder aux ressources externes nécessaires à l'utilisation de ces services.

- "Sont les services de plateforme"
- "Réseaux et ports pour les services de plate-forme"
- "Livraison par site de messages de services de plate-forme"
- "Dépannage des services de plate-forme"

Sont les services de plateforme

Les services de plateforme incluent la réplication CloudMirror, les notifications d'événement et le service d'intégration de la recherche.

Ces services permettent aux locataires d'utiliser les fonctionnalités suivantes avec leurs compartiments S3 :

- **Réplication CloudMirror** : le service de réplication StorageGRID CloudMirror permet la mise en miroir d'objets spécifiques d'un compartiment StorageGRID vers une destination externe spécifiée.

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

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

- **Notifications** : les notifications d'événements par compartiment sont utilisées pour envoyer des notifications sur des actions spécifiques effectuées sur des objets à un service externe Amazon simple notification Service™ (SNS) spécifié.

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

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

- **Service d'intégration de recherche** : le service d'intégration de recherche est utilisé pour envoyer des métadonnées d'objet S3 à un index Elasticsearch spécifié où les métadonnées peuvent être recherchées ou analysées à l'aide du service externe.

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

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

Les services de plateforme permettent aux locataires d'utiliser des ressources de stockage externes, des services de notification et des services de recherche ou d'analyse avec leurs données. Étant donné que l'emplacement cible des services de plateforme ne fait généralement pas partie de votre déploiement StorageGRID, vous devez décider si vous souhaitez autoriser les locataires à utiliser ces services. Dans ce cas, vous devez activer l'utilisation des services de plateforme lorsque vous créez ou modifiez des comptes de tenant. Vous devez également configurer votre réseau de sorte que les messages de services de plate-forme générés par les locataires puissent atteindre leurs destinations.

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

Avant d'utiliser les services de plateforme, vous devez connaître les recommandations suivantes :

- Vous ne devez pas utiliser plus de 100 locataires actifs avec les demandes S3 nécessitant la réplication CloudMirror, les notifications et l'intégration de la recherche. Avec plus de 100 locataires actifs, les performances des clients S3 sont plus lentes.
- Si le contrôle de versions et la réplication CloudMirror sont activés pour un compartiment S3 dans le système StorageGRID, vous devez également activer la gestion des versions du compartiment S3 pour le terminal de destination. Cela permet à la réplication CloudMirror de générer des versions d'objet similaires sur le noeud final.

Informations associées

"Utilisez un compte de locataire"

"Configuration des paramètres du proxy de stockage"

"Moniteur et amp ; dépannage"

Réseaux et ports pour les services de plate-forme

Si vous autorisez un locataire S3 à utiliser des services de plateforme, vous devez configurer la mise en réseau pour le grid de manière à ce que les messages des services de plateforme puissent être envoyés vers leur destination.

Lorsque vous créez ou mettez à jour le compte de locataire, vous pouvez activer des services de plateforme pour un compte de locataire S3. Si les services de plateforme sont activés, le locataire peut créer des terminaux qui servent de destination à la réplication CloudMirror, à la notification d'événement ou aux messages d'intégration de recherche à partir de ses compartiments S3. Ces messages de services de plateforme sont envoyés depuis les nœuds de stockage qui exécutent le service ADC vers les terminaux de destination.

Par exemple, les locataires peuvent configurer les types de terminaux de destination suivants :

- Un cluster Elasticsearch hébergé localement
- Application locale prenant en charge la réception de messages SNS (simple notification Service)
- Un compartiment S3 hébergé localement sur la même instance d'StorageGRID ou sur une autre instance
- Un terminal externe, tel qu'un terminal sur Amazon Web Services.

Pour vous assurer que les messages des services de plate-forme peuvent être envoyés, vous devez configurer le réseau ou les réseaux contenant les nœuds de stockage ADC. Vous devez vous assurer que les ports suivants peuvent être utilisés pour envoyer des messages de services de plate-forme aux noeuds finaux de destination.

Par défaut, les messages des services de plate-forme sont envoyés sur les ports suivants :

- **80**: Pour les URI de point final commençant par http
- **443**: Pour les URI de point final qui commencent par https

Les locataires peuvent spécifier un port différent lorsqu'ils créent ou modifient un noeud final.

> Si un déploiement StorageGRID est utilisé comme destination pour la réplication CloudMirror, des messages de réplication peuvent être reçus sur un port autre que 80 ou 443. Vérifiez que le port utilisé pour S3 par le déploiement StorageGRID de destination est spécifié dans le terminal.

Si vous utilisez un serveur proxy non transparent, vous devez également configurer les paramètres de proxy de stockage pour permettre l'envoi de messages vers des noeuds finaux externes, tels qu'un noeud final sur Internet.

Informations associées

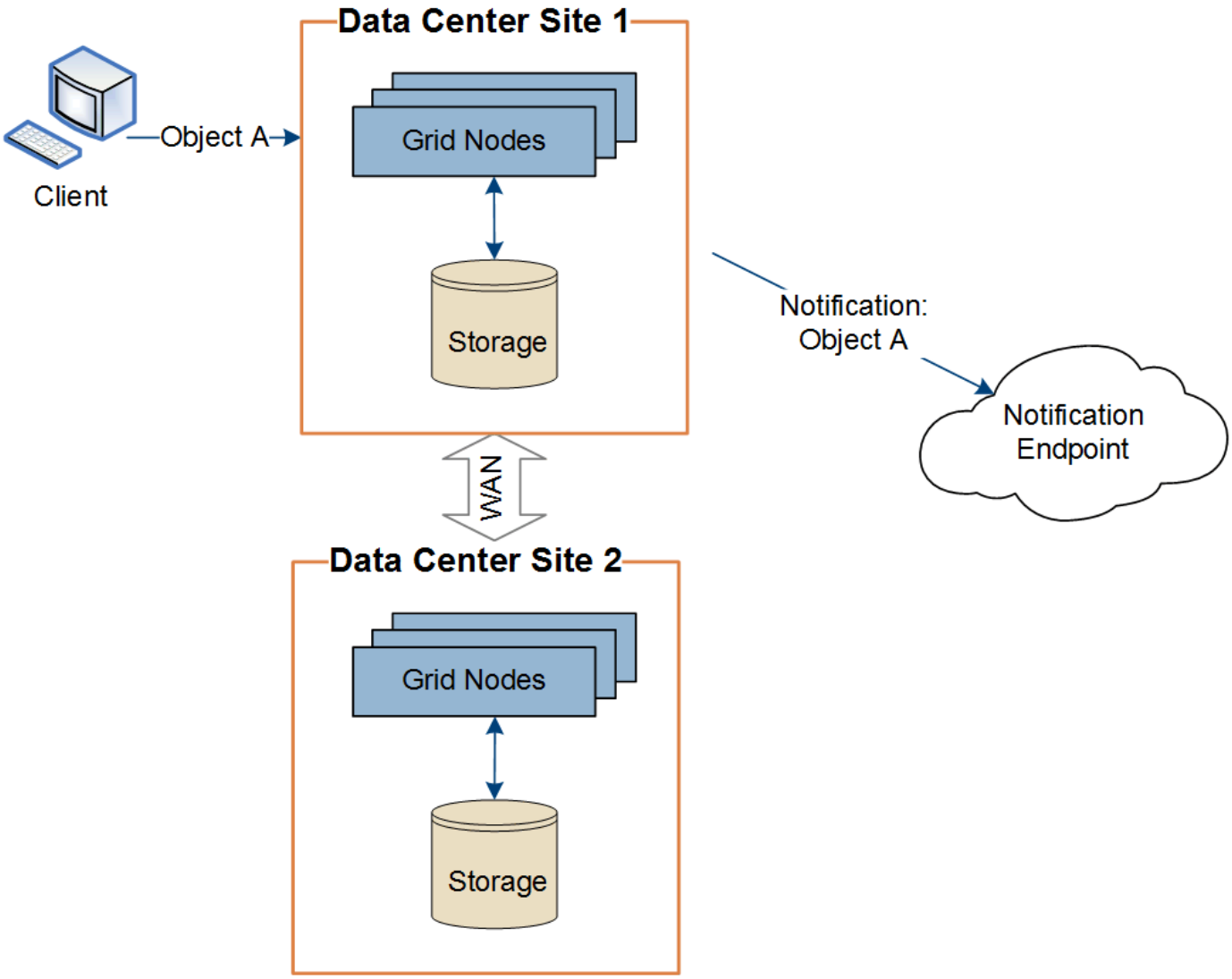
"Configuration des paramètres du proxy de stockage"

"Utilisez un compte de locataire"

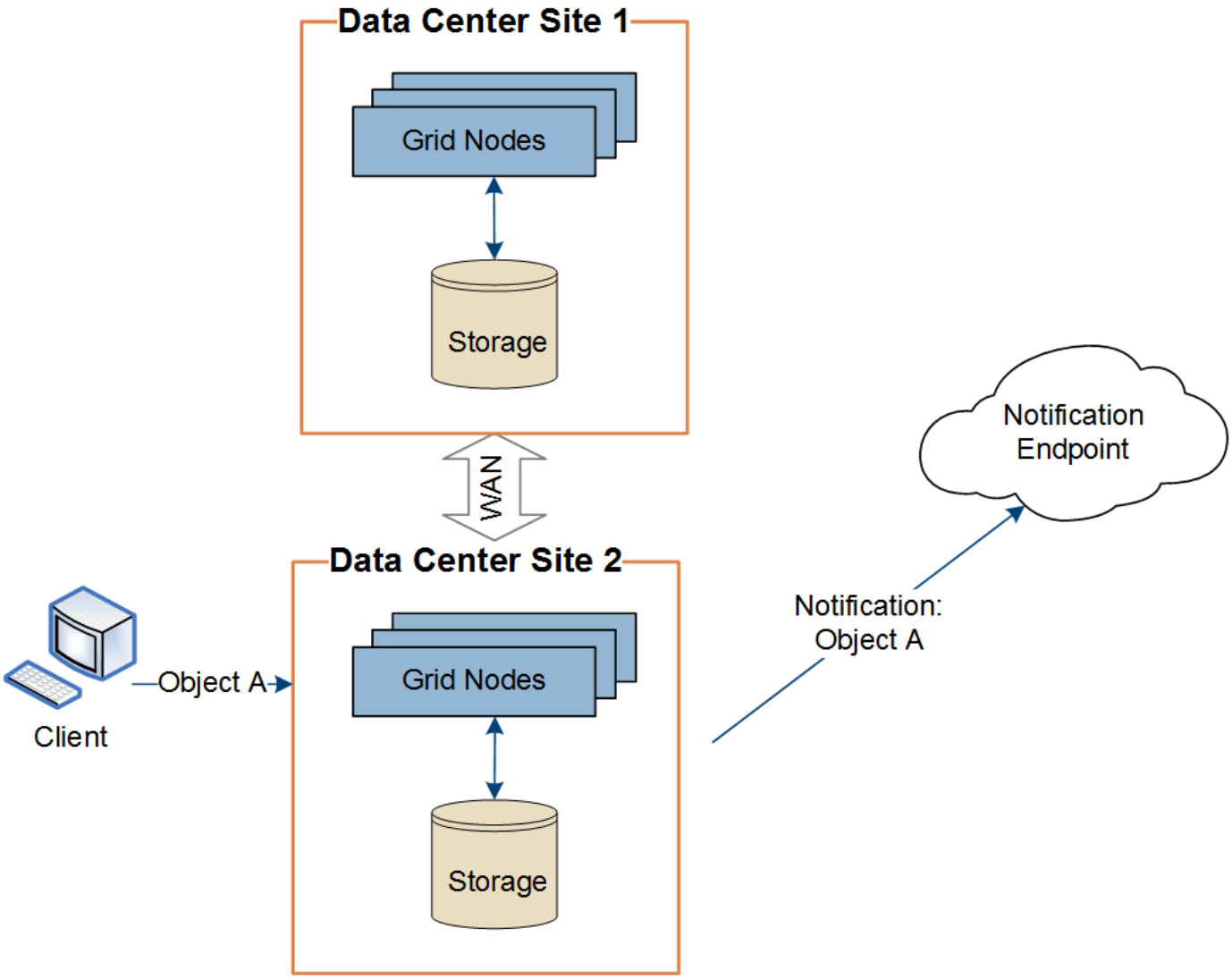
Livraison par site de messages de services de plate-forme

Toutes les opérations de services de plateforme sont réalisées sur une base par site.

C'est-à-dire que si un locataire utilise un client pour effectuer une opération de création d'API S3 sur un objet en se connectant à un nœud de passerelle sur le site de Data Center 1, la notification concernant cette action est déclenchée et envoyée depuis le site de Data Center 1.



Si le client exécute ensuite une opération de suppression d'API S3 sur ce même objet à partir du site du centre de données 2, la notification concernant l'action de suppression est déclenchée et envoyée depuis le site du centre de données 2.



Assurez-vous que le réseau de chaque site est configuré de manière à ce que les messages des services de plate-forme puissent être transmis à leurs destinations.

Dépannage des services de plate-forme

Les terminaux utilisés dans les services de plateforme sont créés et gérés par les utilisateurs locataires dans le Gestionnaire de locataires. Toutefois, si un locataire a des problèmes de configuration ou d'utilisation des services de plateforme, vous pouvez utiliser le Gestionnaire de grille pour résoudre le problème.

Problèmes liés aux nouveaux terminaux

Avant qu'un locataire ne puisse utiliser les services de plateforme, il doit créer un ou plusieurs terminaux à l'aide du Gestionnaire des locataires. Chaque terminal représente une destination externe pour un service de plateforme unique, par exemple un compartiment StorageGRID S3, un compartiment Amazon Web Services, un thème simple Service de notification ou un cluster Elasticsearch hébergé localement ou sur AWS. Chaque noeud final comprend à la fois l'emplacement de la ressource externe et les informations d'identification nécessaires pour accéder à cette ressource.

Lorsqu'un locataire crée un noeud final, le système StorageGRID valide que ce dernier existe et qu'il peut être atteint à l'aide des identifiants spécifiés. La connexion au noeud final est validée à partir d'un nœud sur chaque

site.

Si la validation du noeud final échoue, un message d'erreur explique pourquoi la validation du noeud final a échoué. L'utilisateur locataire doit résoudre le problème, puis essayer de créer à nouveau le noeud final.

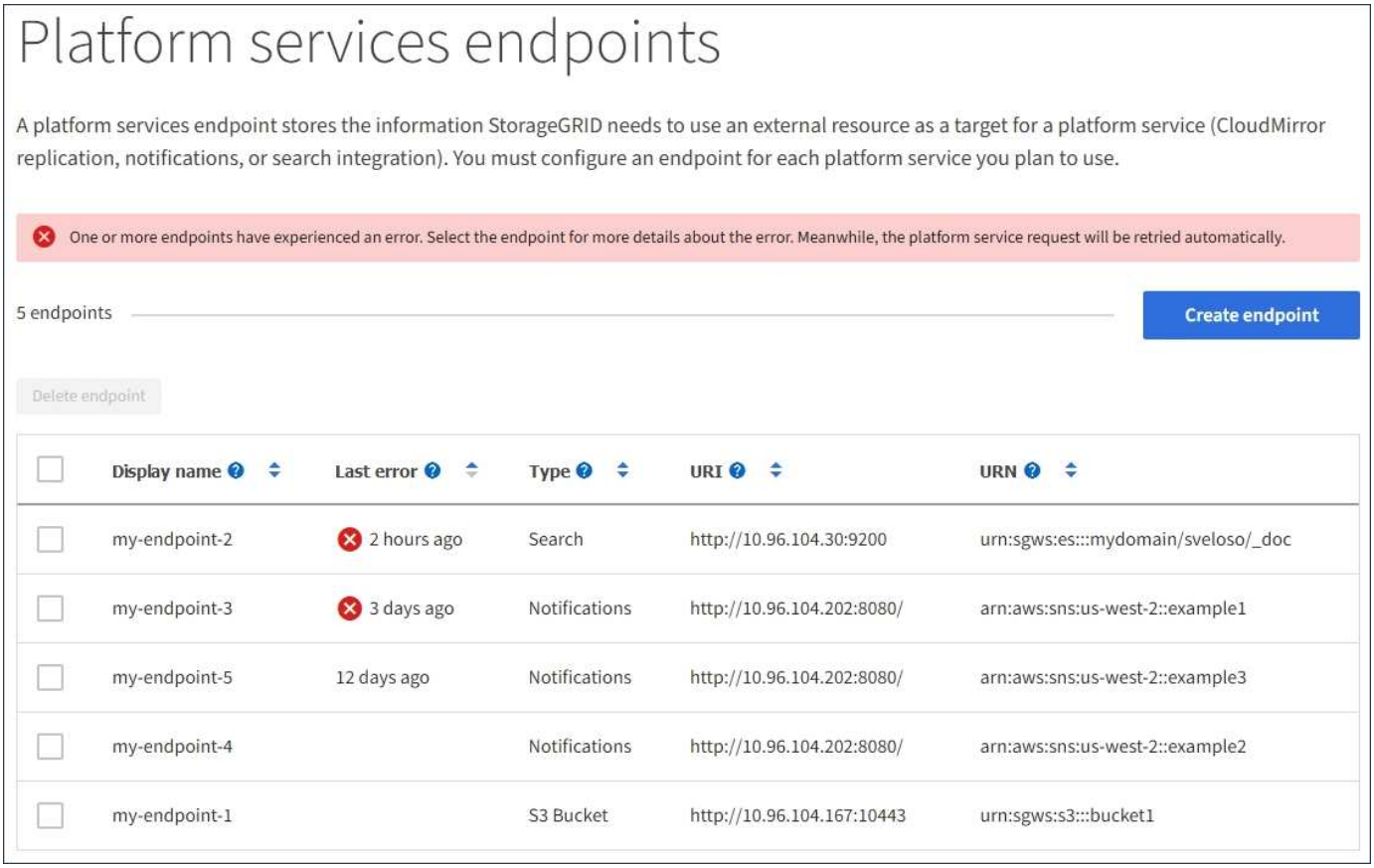
> La création de point final échoue si les services de plate-forme ne sont pas activés pour le compte de locataire.

Problèmes avec les terminaux existants

En cas d'erreur lorsqu'StorageGRID tente d'atteindre un terminal existant, un message s'affiche sur le tableau de bord dans le Gestionnaire de locataires.

> One or more endpoints have experienced an error and might not be functioning properly. Go to the Endpoints page to view the error details. The last error occurred 2 hours ago.

Les utilisateurs locataires peuvent accéder à la page noeuds finaux pour consulter le message d'erreur le plus récent pour chaque noeud final et déterminer la durée de l'erreur. La colonne **dernière erreur** affiche le message d'erreur le plus récent pour chaque noeud final et indique la durée de l'erreur. Erreurs incluant le l'icône s'est produite au cours des 7 derniers jours.



> Certains messages d'erreur dans la colonne **dernière erreur** peuvent inclure un LogId entre parenthèses. Un administrateur de grille ou le support technique peut utiliser cet ID pour trouver des informations plus détaillées sur l'erreur dans bycast.log.

Problèmes liés aux serveurs proxy

Si vous avez configuré un proxy de stockage entre des nœuds de stockage et des terminaux de service de plateforme, des erreurs peuvent se produire si votre service proxy n'autorise pas les messages de StorageGRID. Pour résoudre ces problèmes, vérifiez les paramètres de votre serveur proxy afin de vous assurer que les messages relatifs au service de la plate-forme ne sont pas bloqués.

Déterminer si une erreur s'est produite

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

Échec des opérations client

Certains problèmes de service de plateforme peuvent entraîner l'échec des opérations client dans le compartiment S3. Par exemple, les opérations client S3 échouent si le service RSM (Replicated State machine) interne s'arrête ou s'il y a trop de messages de services de plate-forme en file d'attente pour la livraison.

Pour vérifier l'état des services :

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez ***site*** > ***Storage Node*** > **SSM** > **Services**.

Erreurs récupérables et récupérables du point final

Une fois les noeuds finaux créés, des erreurs de demande de service de plate-forme peuvent se produire pour diverses raisons. Certaines erreurs peuvent être récupérées avec l'intervention de l'utilisateur. Par exemple, des erreurs récupérables peuvent se produire pour les raisons suivantes :

- Les informations d'identification de l'utilisateur ont été supprimées ou ont expiré.
- Le compartiment de destination n'existe pas.
- La notification ne peut pas être envoyée.

Si StorageGRID rencontre une erreur récupérable, la demande de service de plate-forme sera relancée jusqu'à ce qu'elle réussisse.

D'autres erreurs sont irrécupérables. Par exemple, une erreur irrécupérable se produit si le noeud final est supprimé.

Si StorageGRID rencontre une erreur de point final irrécupérable, l'alarme Total Events (SMTT) est déclenchée dans le Gestionnaire de grille. Pour afficher l'alarme Total Events :

1. Sélectionnez **noeuds**.
2. Sélectionnez ***site*** > ***grid node*** > **Events**.
3. Afficher le dernier événement en haut du tableau.

   Les messages d'événement sont également répertoriés dans le `/var/local/log/bycast-err.log`.

4. Suivez les instructions fournies dans le contenu de l'alarme SMTT pour corriger le problème.
5. Cliquez sur **Réinitialiser le nombre d'événements**.

6. Notifier le locataire des objets dont les messages de services de plate-forme n’ont pas été livrés.
7. Demandez au locataire de déclencher à nouveau la réplication ou la notification ayant échoué en mettant à jour les métadonnées ou balises de l’objet.

   Le locataire peut soumettre de nouveau les valeurs existantes afin d’éviter toute modification non souhaitée.

Les messages des services de plate-forme ne peuvent pas être transmis

Si la destination rencontre un problème qui l’empêche d’accepter des messages de services de plate-forme, l’opération client sur le compartiment réussit, mais le message des services de plate-forme n’est pas livré. Par exemple, cette erreur peut se produire si les informations d’identification sont mises à jour sur la destination de sorte que StorageGRID ne puisse plus s’authentifier auprès du service de destination.

Si les messages des services de la plate-forme ne peuvent pas être envoyés en raison d’une erreur irrécupérable, l’alarme Total Events (SMTT) est déclenchée dans Grid Manager.

Des performances plus lentes pour les demandes de services de plateforme

Le logiciel StorageGRID peut canaliser les demandes S3 entrantes pour un compartiment si le taux d’envoi des demandes dépasse le taux à partir duquel le terminal de destination peut recevoir les demandes. La restriction ne se produit que lorsqu’il existe un arriéré de demandes en attente d’envoi vers le noeud final de destination.

Le seul effet visible est que les requêtes S3 entrantes prennent plus de temps à s’exécuter. Si vous commencez à détecter les performances beaucoup plus lentes, vous devez réduire le taux d’entrée ou utiliser un terminal avec une capacité plus élevée. Si l’carnet de commandes des requêtes continue d’augmenter, les opérations S3 des clients (par EXEMPLE, LES requêtes PUT) finiront par échouer.

Les demandes CloudMirror sont plus susceptibles d’être affectées par les performances du terminal de destination, car ces demandes impliquent généralement plus de transfert de données que les demandes d’intégration de recherche ou de notification d’événements.

Les demandes de service de la plateforme échouent

Pour afficher le taux d’échec de la demande pour les services de plate-forme :

1. Sélectionnez **noeuds**.
2. Sélectionnez ***site*** > **Platform Services**.
3. Afficher le tableau des taux d’échec de la demande.

Alerte de services de plate-forme non disponibles

L'alerte **Platform services unavailable** indique qu'aucune opération de service de plate-forme ne peut être effectuée sur un site car trop de nœuds de stockage avec le service RSM sont en cours d'exécution ou disponibles.

Le service RSM garantit que les demandes de service de plate-forme sont envoyées à leurs points de terminaison respectifs.

Pour résoudre cette alerte, déterminez quels nœuds de stockage du site incluent le service RSM. (Le service RSM est présent sur les nœuds de stockage qui incluent également le service ADC.) Ensuite, assurez-vous que la plupart de ces nœuds de stockage sont exécutés et disponibles.

> Si plusieurs nœuds de stockage contenant le service RSM échouent sur un site, vous perdez toute demande de service de plateforme en attente pour ce site.

Conseils de dépannage supplémentaires pour les terminaux des services de plateforme

Pour plus d'informations sur le dépannage des terminaux de services de plateforme, reportez-vous aux instructions d'utilisation des comptes de tenant.

"Utilisez un compte de locataire"

Informations associées

"Moniteur et amp ; dépannage"

"Configuration des paramètres du proxy de stockage"

Configuration des connexions des clients S3 et Swift

En tant qu'administrateur grid, vous gérez les options de configuration qui contrôlent la manière dont les locataires S3 et Swift peuvent connecter les applications client à votre système StorageGRID pour stocker et récupérer les données. Plusieurs options sont possibles pour répondre aux différents besoins des clients et des locataires.

Les applications client peuvent stocker ou récupérer des objets en se connectant à l'un des éléments suivants :

- Le service Load Balancer sur les nœuds d'administration ou de passerelle, ou, le cas échéant, l'adresse IP virtuelle d'un groupe de nœuds d'administration ou de nœuds de passerelle haute disponibilité
- Le service CLB sur les nœuds de passerelle ou, éventuellement, l'adresse IP virtuelle d'un groupe de nœuds de passerelle haute disponibilité

  > Le service CLB est obsolète. Les clients configurés avant la version de StorageGRID 11.3 peuvent continuer à utiliser le service CLB sur les nœuds de passerelle. Toutes les autres applications client qui dépendent de StorageGRID pour fournir un équilibrage de la charge doivent se connecter à l'aide du service Load Balancer.

- Des nœuds de stockage, avec ou sans équilibreur de charge externe

Vous pouvez choisir de configurer les fonctions suivantes sur votre système StorageGRID :

- **Load Balancer service** : permet aux clients d'utiliser le service Load Balancer en créant des noeuds finaux load Balancer pour les connexions client. Lors de la création d'un noeud final d'équilibrage de charge, vous spécifiez un numéro de port, que le noeud final accepte les connexions HTTP ou HTTPS, le type de client (S3 ou Swift) qui utilisera le noeud final et le certificat à utiliser pour les connexions HTTPS (le cas échéant).
- **Réseau client non fiable** : vous pouvez sécuriser le réseau client en le configurant comme non fiable. Lorsque le réseau client n'est pas fiable, les clients peuvent uniquement se connecter à l'aide de points finaux d'équilibreur de charge.
- **Groupes haute disponibilité** : vous pouvez créer un groupe haute disponibilité de nœuds de passerelle ou de nœuds d'administration pour créer une configuration de sauvegarde active/active, ou utiliser un DNS Round-Robin ou un équilibreur de charge tiers et plusieurs groupes HA afin d'obtenir une configuration active/active. Les connexions des clients sont établies en utilisant les adresses IP virtuelles des groupes

haute disponibilité.

Vous pouvez également activer l'utilisation du protocole HTTP pour les clients qui se connectent à StorageGRID directement aux nœuds de stockage ou à l'aide du service CLB (obsolète) et vous pouvez configurer les noms de domaine de points de terminaison de l'API S3 pour les clients S3.

Résumé : adresses IP et ports pour les connexions client

Les applications client peuvent se connecter à StorageGRID en utilisant l'adresse IP d'un nœud de grid et le numéro de port d'un service sur ce nœud. Si des groupes de haute disponibilité sont configurés, les applications client peuvent se connecter en utilisant l'adresse IP virtuelle du groupe de haute disponibilité.

Description de la tâche

Ce tableau récapitule les différentes façons dont les clients peuvent se connecter à StorageGRID ainsi que les adresses IP et les ports utilisés pour chaque type de connexion. Ces instructions décrivent la recherche de ces informations dans le grid Manager si les terminaux d'équilibrage de la charge et les groupes haute disponibilité sont déjà configurés.

Là où la connexion est établie	Service auquel le client se connecte	Adresse IP	Port
Groupe HAUTE DISPONIBILITÉ	Équilibreur de charge	Adresse IP virtuelle d'un groupe haute disponibilité	• Port du terminal de l'équilibreur de charge
Groupe HAUTE DISPONIBILITÉ	CLB **Note:** le service CLB est obsolète.	Adresse IP virtuelle d'un groupe haute disponibilité	Ports S3 par défaut : • HTTPS: 8082 • HTTP : 8084 Ports Swift par défaut : • HTTPS:8083 • HTTP : 8085
Nœud d'administration	Équilibreur de charge	Adresse IP du nœud d'administration	• Port du terminal de l'équilibreur de charge
Nœud de passerelle	Équilibreur de charge	Adresse IP du nœud de passerelle	• Port du terminal de l'équilibreur de charge

Là où la connexion est établie	Service auquel le client se connecte	Adresse IP	Port
Nœud de passerelle	CLB **Note:** le service CLB est obsolète.	Adresse IP du nœud de passerelle **Remarque :** par défaut, les ports HTTP pour CLB et LDR ne sont pas activés.	Ports S3 par défaut : • HTTPS: 8082 • HTTP : 8084 Ports Swift par défaut : • HTTPS:8083 • HTTP : 8085
Nœud de stockage	LDR	Adresse IP du nœud de stockage	Ports S3 par défaut : • HTTPS: 18082 • HTTP : 18084 Ports Swift par défaut : • HTTPS: 18083 • HTTP : 18085

Exemples

Pour connecter un client S3 au terminal Load Balancer d'un groupe HA de nœuds de passerelle, utilisez une URL structurée comme illustré 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 le numéro de port d'un terminal S3 Load Balancer est 10443, un client S3 peut utiliser l'URL suivante pour vous connecter à StorageGRID :

- `https://192.0.2.5:10443`

Pour connecter un client Swift au point de terminaison Load Balancer 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 192.0.2.6 et que le numéro de port d'un noeud final Swift Load Balancer est 10444, un client Swift peut utiliser l'URL suivante pour se connecter à StorageGRID :

- `https://192.0.2.6:10444`

Il est possible de configurer un nom DNS pour l'adresse IP que les clients utilisent pour se connecter à StorageGRID. Contactez votre administrateur réseau local.

Étapes

1. Connectez-vous au Grid Manager à l'aide d'un navigateur pris en charge.
2. Pour trouver l'adresse IP d'un nœud de grille :

a. Sélectionnez **noeuds**.
b. Sélectionnez le nœud d'administration, le nœud de passerelle ou le nœud de stockage auquel vous souhaitez vous connecter.
c. Sélectionnez l'onglet **Aperçu**.
d. Dans la section informations sur le nœud, notez les adresses IP du nœud.
e. Cliquez sur **Afficher plus** pour afficher les adresses IPv6 et les mappages d'interface.

   Vous pouvez établir des connexions entre les applications client et n'importe quelle adresse IP de la liste :

   - **Eth0:** réseau de grille
   - **Eth1:** réseau d'administration (facultatif)
   - **Eth2:** réseau client (facultatif)

   > Si vous affichez un nœud d'administration ou un nœud de passerelle et qu'il s'agit du nœud actif dans un groupe haute disponibilité, l'adresse IP virtuelle du groupe haute disponibilité est affichée sur eth2.

3. Pour trouver l'adresse IP virtuelle d'un groupe haute disponibilité :
   a. Sélectionnez **Configuration** > **Paramètres réseau** > **groupes haute disponibilité**.
   b. Dans le tableau, noter l'adresse IP virtuelle du groupe haute disponibilité.
4. Pour trouver le numéro de port d'un noeud final Load Balancer :
   a. Sélectionnez **Configuration** > **Paramètres réseau** > **points d'extrémité Load Balancer**.

      La page Load Balancer Endpoints s'affiche et affiche la liste des noeuds finaux qui ont déjà été configurés.

   b. Sélectionnez un noeud final et cliquez sur **Modifier le noeud final**.

      La fenêtre Modifier le point final s'ouvre et affiche des informations supplémentaires sur le point final.

   c. Vérifiez que le noeud final que vous avez sélectionné est configuré pour une utilisation avec le protocole correct (S3 ou Swift), puis cliquez sur **Annuler**.
   d. Notez le numéro de port du noeud final que vous souhaitez utiliser pour une connexion client.

   > Si le numéro de port est 80 ou 443, le noeud final est configuré uniquement sur les noeuds de passerelle, car ces ports sont réservés sur les noeuds d'administration. Tous les autres ports sont configurés sur les nœuds de passerelle et sur les nœuds d'administration.

Gestion de l'équilibrage des charges

Vous pouvez utiliser les fonctions d'équilibrage de charge StorageGRID pour gérer les workloads d'ingestion et de récupération à partir de clients S3 et Swift. L'équilibrage de la charge optimise la vitesse et la capacité de connexion en distribuant les charges de travail et les connexions entre plusieurs nœuds de stockage.

Vous pouvez réaliser l'équilibrage de la charge dans votre système StorageGRID de plusieurs manières :

- Utilisez le service Load Balancer, qui est installé sur les nœuds d'administration et les nœuds de passerelle. Le service Load Balancer assure l'équilibrage de la charge de couche 7 et effectue la résiliation TLS des requêtes client, inspecte les requêtes et établit de nouvelles connexions sécurisées vers les nœuds de stockage. Il s'agit du mécanisme d'équilibrage de charge recommandé.
- Utilisez le service Connection Load Balancer (CLB), qui est installé uniquement sur les nœuds de passerelle. Le service CLB assure l'équilibrage de charge de couche 4 et prend en charge les coûts de liaison.

  Le service CLB est obsolète.

- Intégrez un équilibreur de charge tiers. Pour plus d'informations, contactez votre ingénieur commercial NetApp.

Fonctionnement de l'équilibrage de la charge : service Load Balancer

Le service Load Balancer distribue les connexions réseau entrantes des applications client aux nœuds de stockage. Pour activer l'équilibrage de charge, vous devez configurer les noeuds finaux de l'équilibreur de charge à l'aide de Grid Manager.

Vous pouvez configurer les noeuds finaux de l'équilibreur de charge uniquement pour les nœuds d'administration ou les nœuds de passerelle, car ces types de nœuds contiennent le service Load Balancer. Vous ne pouvez pas configurer de noeuds finaux pour les noeuds de stockage ou les noeuds d'archivage.

Chaque point final de l'équilibreur de charge spécifie un port, un protocole (HTTP ou HTTPS), un type de service (S3 ou Swift) et un mode de liaison. Les terminaux HTTPS requièrent un certificat de serveur. Les modes de liaison vous permettent de limiter l'accessibilité des ports de point final à :

- Adresses IP virtuelles (VIP) haute disponibilité (HA) spécifiques
- Interfaces réseau spécifiques de nœuds spécifiques

Considérations relatives aux ports

Les clients peuvent accéder à tous les terminaux que vous configurez sur n'importe quel nœud exécutant le service Load Balancer, à deux exceptions près : les ports 80 et 443 sont réservés aux nœuds d'administration. Les terminaux configurés sur ces ports prennent donc en charge les opérations d'équilibrage de la charge uniquement sur les nœuds de passerelle.

Si vous avez mappé de nouveau des ports, vous ne pouvez pas utiliser les mêmes ports pour configurer les points finaux de l'équilibreur de charge. Vous pouvez créer des noeuds finaux à l'aide de ports remappés, mais ces noeuds finaux seront remappés vers les ports et le service CLB d'origine, et non le service Load Balancer. Suivez les étapes des instructions de récupération et de maintenance pour supprimer les mappages de port.

Le service CLB est obsolète.

Disponibilité du processeur

Le service Load Balancer sur chaque nœud d'administration et chaque nœud de passerelle fonctionne de manière indépendante lors du transfert du trafic S3 ou Swift vers les nœuds de stockage. Par le biais d'un processus de pondération, le service Load Balancer achemine davantage de requêtes vers des nœuds de stockage avec une disponibilité de processeur supérieure. Les informations de charge de l'UC du nœud sont

mises à jour toutes les quelques minutes, mais la pondération peut être mise à jour plus fréquemment. Tous les nœuds de stockage se voient attribuer une valeur de poids de base minimale, même si un nœud indique une utilisation de 100 % ou ne parvient pas à signaler son utilisation.

Dans certains cas, les informations relatives à la disponibilité du processeur sont limitées au site où se trouve le service Load Balancer.

Informations associées

"Maintenance et récupération"

Configuration des terminaux d'équilibrage de charge

Vous pouvez créer, modifier et supprimer des noeuds finaux de l'équilibreur de charge.

Création de terminaux d'équilibrage de charge

Chaque terminal de l'équilibreur de charge spécifie un port, un protocole réseau (HTTP ou HTTPS) et un type de service (S3 ou Swift). Si vous créez un noeud final HTTPS, vous devez télécharger ou générer un certificat de serveur.

Ce dont vous avez besoin

- Vous devez disposer de l'autorisation accès racine.
- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Si vous avez précédemment mappé des ports que vous souhaitez utiliser pour le service Load Balancer, vous devez avoir supprimé les mappages.

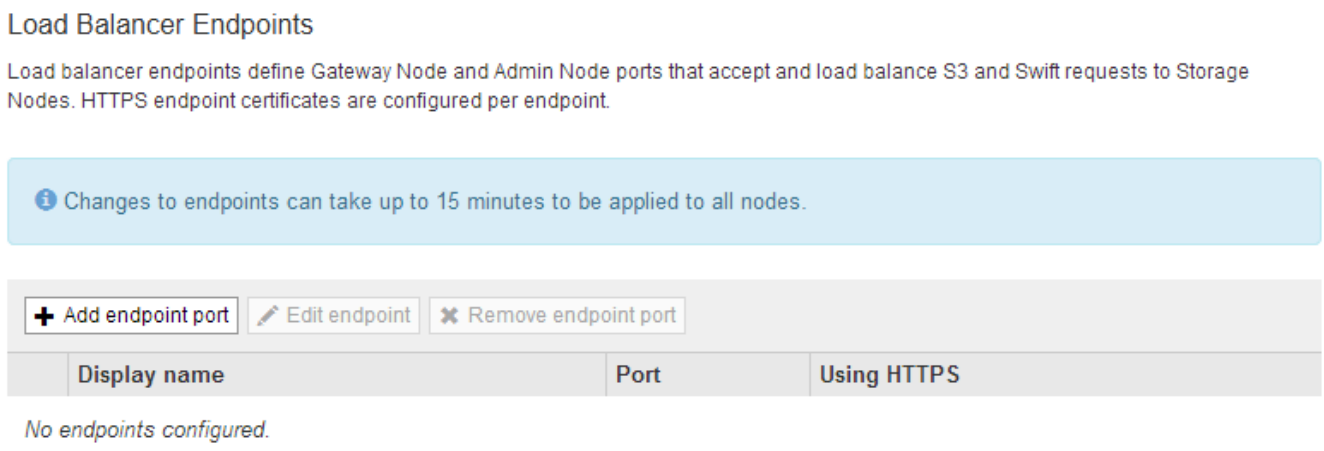
> Si vous avez mappé de nouveau des ports, vous ne pouvez pas utiliser les mêmes ports pour configurer les points finaux de l'équilibreur de charge. Vous pouvez créer des noeuds finaux à l'aide de ports remappés, mais ces noeuds finaux seront remappés vers les ports et le service CLB d'origine, et non le service Load Balancer. Suivez les étapes des instructions de récupération et de maintenance pour supprimer les mappages de port.

> Le service CLB est obsolète.

Étapes

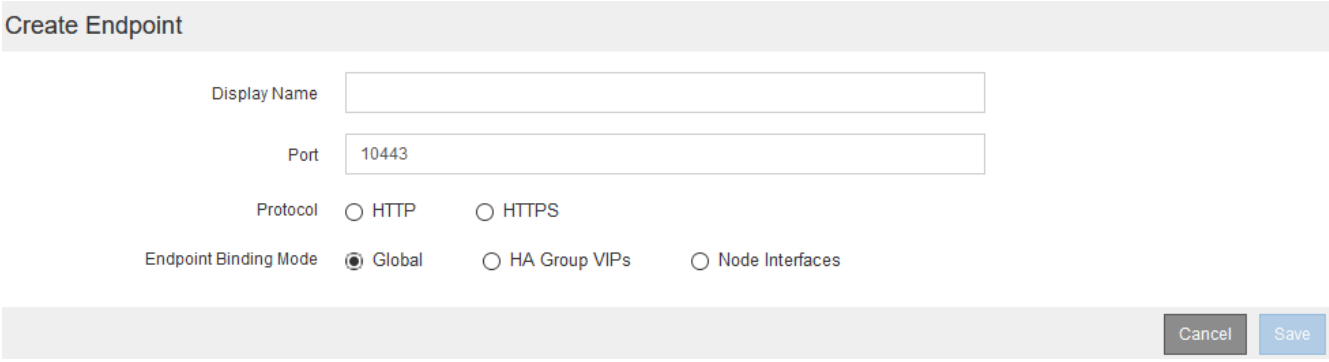
1. Sélectionnez **Configuration** > **Paramètres réseau** > **points d'extrémité Load Balancer**.

   La page Load Balancer Endpoints s'affiche.



2. Sélectionnez **Ajouter un noeud final**.

   La boîte de dialogue Créer un point final s'affiche.

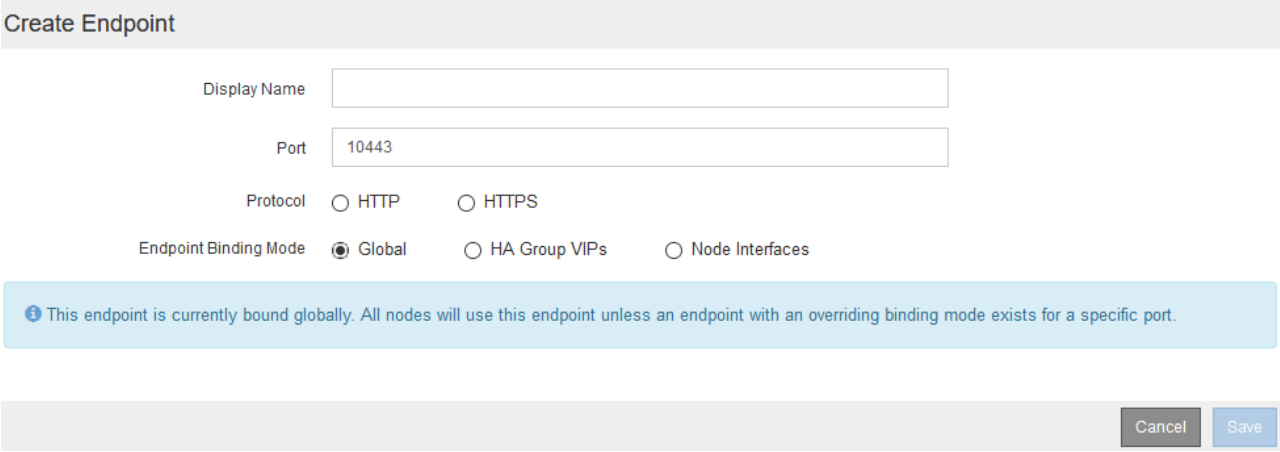


3. Entrez un nom d'affichage pour le noeud final, qui apparaîtra dans la liste de la page noeuds finaux Load Balancer.
4. Entrez un numéro de port ou laissez le numéro de port pré-rempli tel quel.

   Si vous entrez le numéro de port 80 ou 443, le noeud final est configuré uniquement sur les noeuds de passerelle, car ces ports sont réservés sur les noeuds d'administration.

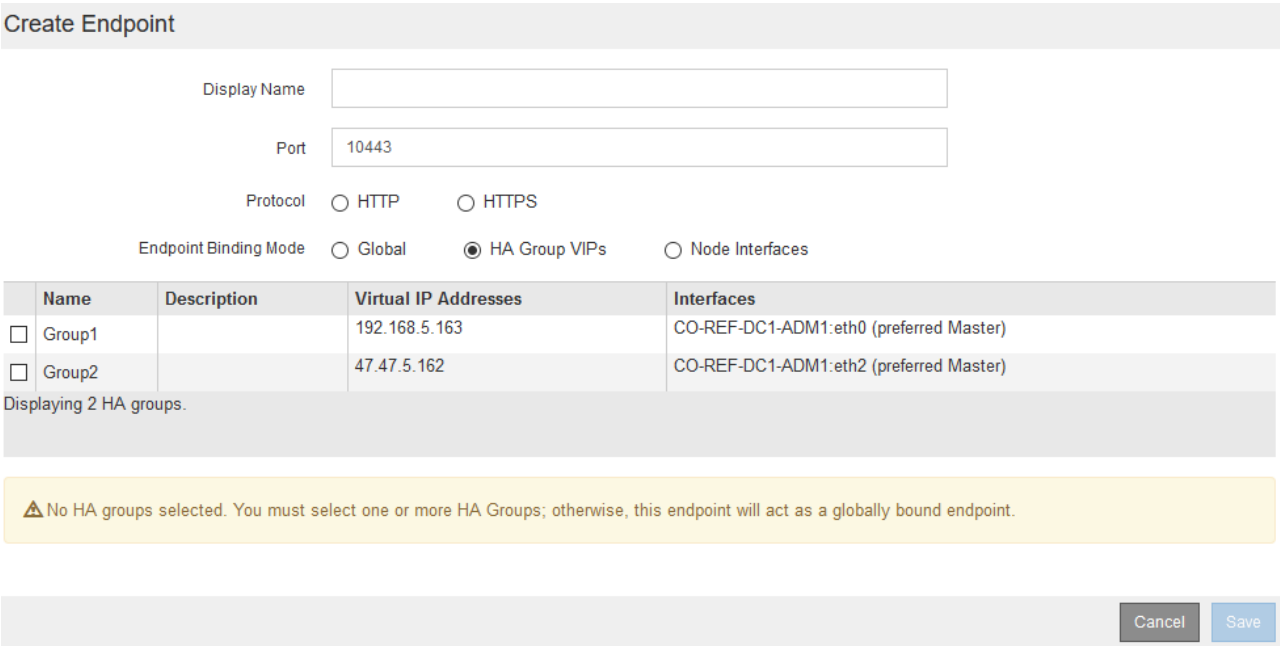
   > Les ports utilisés par d'autres services de réseau ne sont pas autorisés. Reportez-vous aux instructions de mise en réseau pour obtenir la liste des ports utilisés pour les communications internes et externes.

5. Sélectionnez **HTTP** ou **HTTPS** pour spécifier le protocole réseau pour ce noeud final.
6. Sélectionnez un mode de liaison de point final.
   - **Global** (par défaut) : le noeud final est accessible sur tous les noeuds de passerelle et les noeuds d'administration sur le numéro de port spécifié.



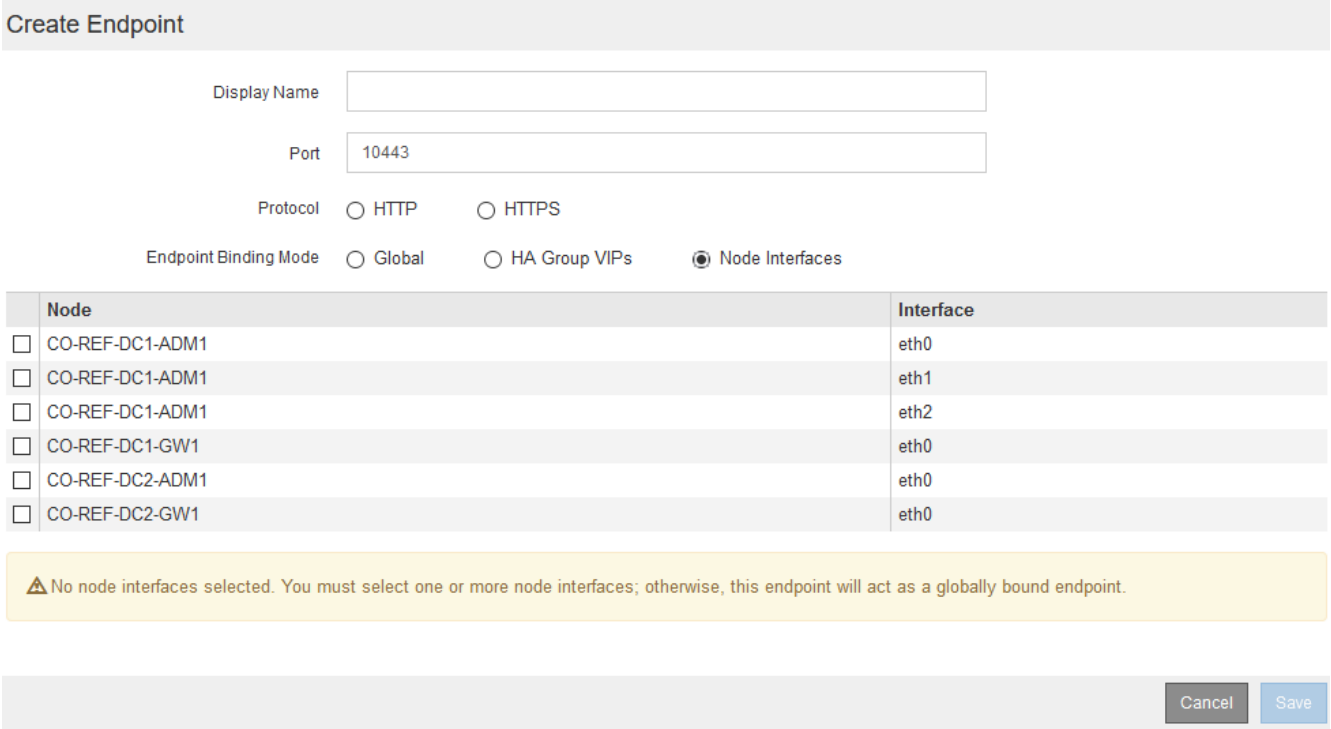
- **VIP de groupe HA** : le noeud final est accessible uniquement via les adresses IP virtuelles définies pour les groupes HA sélectionnés. Les terminaux définis dans ce mode peuvent réutiliser le même numéro de port, tant que les groupes HA définis par ces terminaux ne se chevauchent pas.

  Sélectionnez les groupes HA avec les adresses IP virtuelles où vous souhaitez que le noeud final apparaisse.



- **Node interfaces** : le noeud final est accessible uniquement sur les noeuds désignés et les interfaces réseau. Les points d'extrémité définis dans ce mode peuvent réutiliser le même numéro de port tant que ces interfaces ne se chevauchent pas.

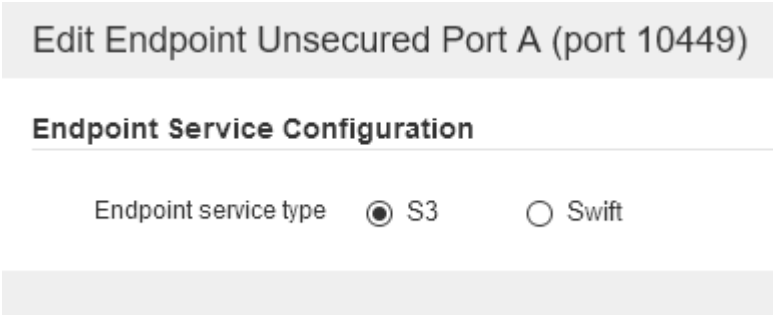
  Sélectionnez les interfaces de nœud sur lesquelles vous souhaitez que le noeud final apparaisse.



7. Sélectionnez **Enregistrer**.

   La boîte de dialogue Modifier le point final s'affiche.

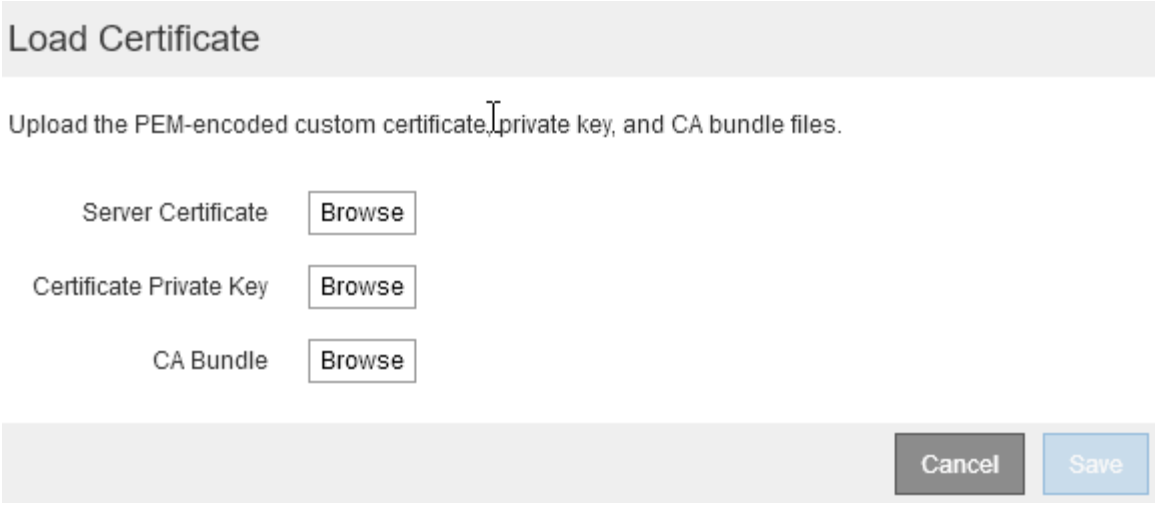
8. Sélectionnez **S3** ou **Swift** pour spécifier le type de trafic que ce noeud final servira.



9. Si vous avez sélectionné **HTTP**, sélectionnez **Enregistrer**.

   Le point final non sécurisé est créé. Le tableau de la page des noeuds finaux Load Balancer répertorie le nom d'affichage, le numéro de port, le protocole et l'ID de noeud final du noeud final.

10. Si vous avez sélectionné **HTTPS** et que vous souhaitez télécharger un certificat, sélectionnez **Télécharger le certificat**.



a. Recherchez le certificat du serveur et la clé privée du certificat.

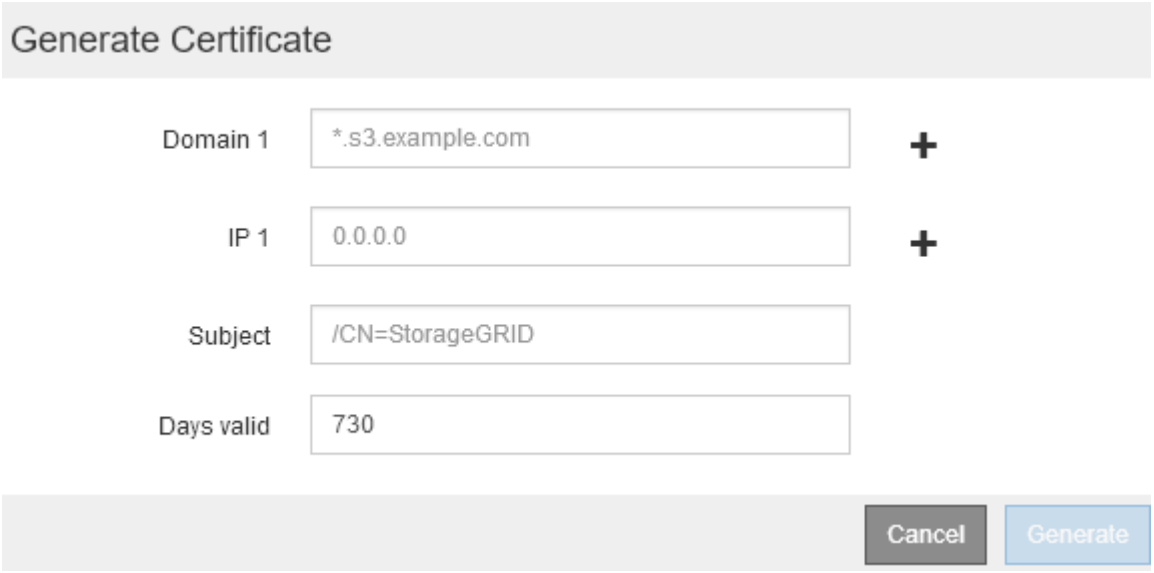
   Pour permettre aux clients S3 de se connecter à l'aide d'un nom de domaine de terminal de l'API S3, utilisez un certificat multi-domaine ou avec caractère générique correspondant à tous les noms de domaine que le client peut utiliser pour se connecter à la grille. Par exemple, le certificat de serveur peut utiliser le nom de domaine `*.example.com`.

"Configuration des noms de domaine de terminaux API S3"

a. Vous pouvez également rechercher un ensemble CA.
b. Sélectionnez **Enregistrer**.

   Les données de certificat codées PEM pour le noeud final apparaissent.

11. Si vous avez sélectionné **HTTPS** et que vous souhaitez générer un certificat, sélectionnez **générer certificat**.



a. Entrez un nom de domaine ou une adresse IP.

   Vous pouvez utiliser des caractères génériques pour représenter les noms de domaine complets de tous les nœuds d'administration et de passerelle exécutant le service Load Balancer. Par exemple :

`*.sgws.foo.com` utilise le caractère générique * pour représenter `gn1.sgws.foo.com` et `gn2.sgws.foo.com`.

"Configuration des noms de domaine de terminaux API S3"

a. Sélectionnez ➕ Pour ajouter d'autres noms de domaine ou adresses IP.

   Si vous utilisez des groupes haute disponibilité (HA), ajoutez les noms de domaine et les adresses IP des adresses IP virtuelles haute disponibilité.

b. Vous pouvez également saisir un sujet X.509, également appelé Nom unique (DN), pour identifier qui possède le certificat.

c. Vous pouvez également sélectionner le nombre de jours pendant lesquels le certificat est valide. La valeur par défaut est 730 jours.

d. Sélectionnez **generate**.

   Les métadonnées du certificat et les données du certificat codées PEM du noeud final apparaissent.

12. Cliquez sur **Enregistrer**.

    Le noeud final est créé. Le tableau de la page des noeuds finaux Load Balancer répertorie le nom d'affichage, le numéro de port, le protocole et l'ID de noeud final du noeud final.

Informations associées

"Maintenance et récupération"

"Instructions réseau"

"Gestion des groupes haute disponibilité"

"Gestion des réseaux clients non fiables"

Modification des noeuds finaux de l'équilibreur de charge

Dans le cas d'un terminal HTTP non sécurisé, vous pouvez modifier le type de service de terminal entre S3 et Swift. Pour un noeud final sécurisé (HTTPS), vous pouvez modifier le type de service de noeud final et afficher ou modifier le certificat de sécurité.

Ce dont vous avez besoin

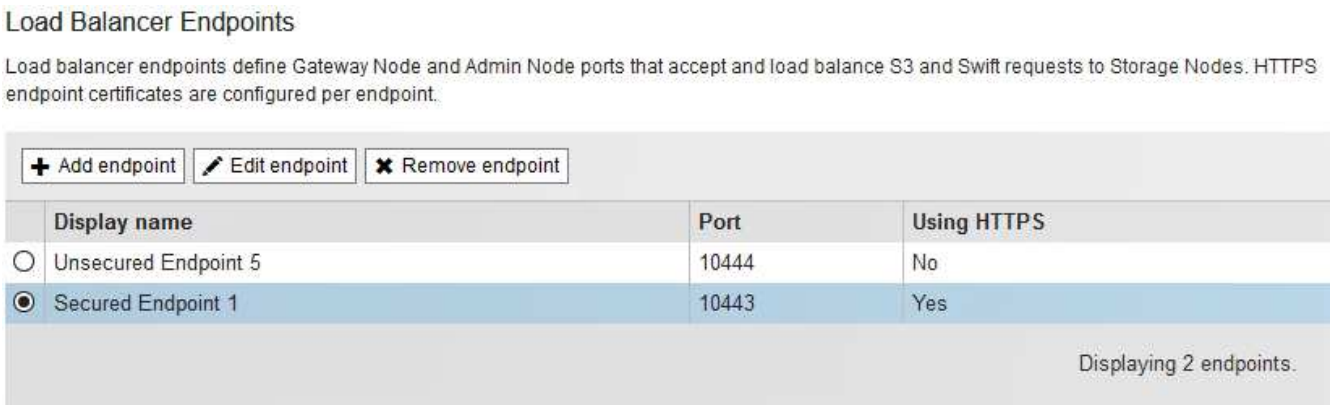
- Vous devez disposer de l'autorisation accès racine.
- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.

Étapes

1. Sélectionnez **Configuration** > **Paramètres réseau** > **points d'extrémité Load Balancer**.

   La page Load Balancer Endpoints s'affiche. Les noeuds finaux existants sont répertoriés dans le tableau.

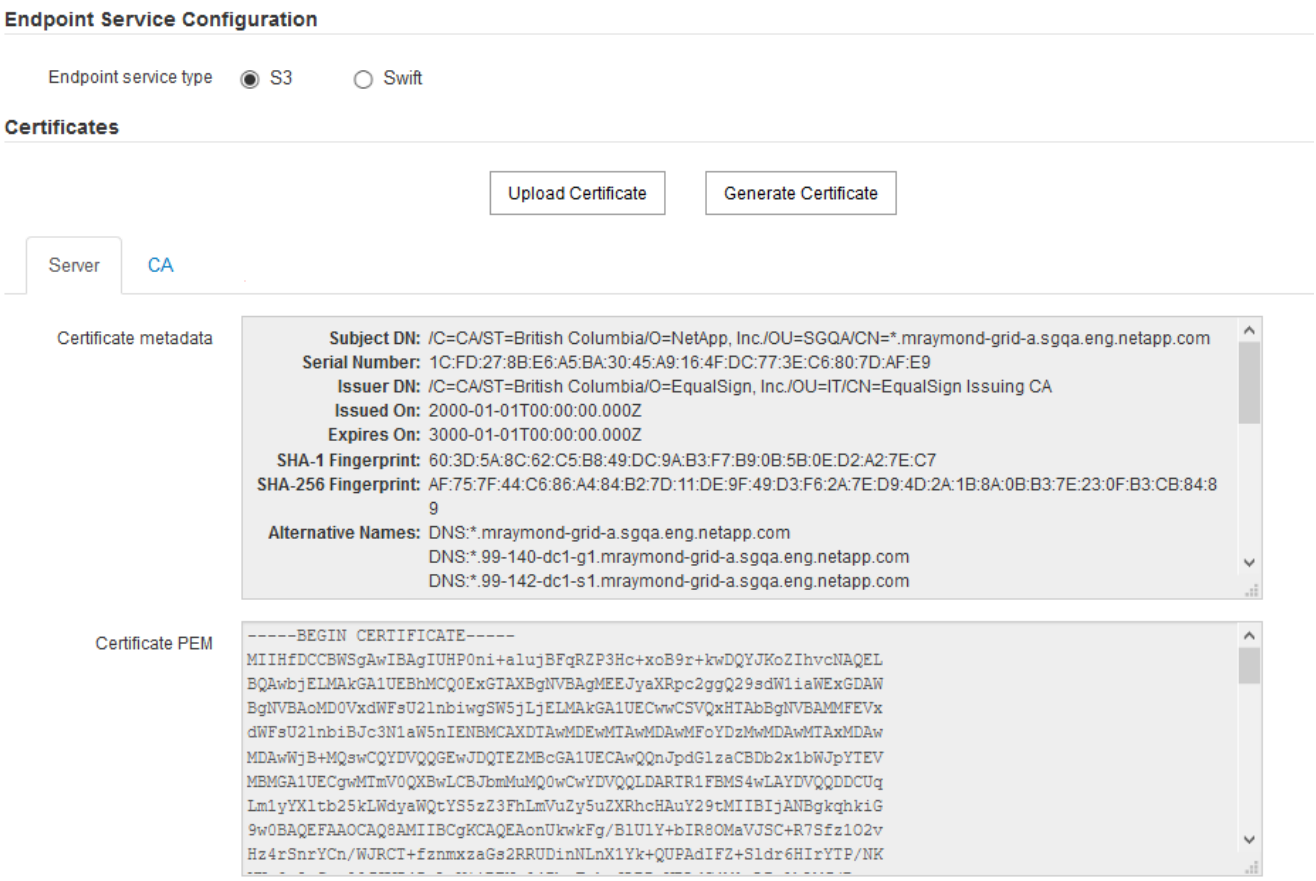
   Les noeuds finaux dont les certificats expireront bientôt sont identifiés dans le tableau.



2. Sélectionnez le point final que vous souhaitez modifier.
3. Cliquez sur **Edit Endpoint**.

   La boîte de dialogue Modifier le point final s'affiche.

   Pour un noeud final non sécurisé (HTTP), seule la section Configuration du service de point final de la boîte de dialogue s'affiche. Pour un noeud final sécurisé (HTTPS), les sections Configuration du service de point final et certificats de la boîte de dialogue s'affichent, comme illustré dans l'exemple suivant.



4. Apportez les modifications souhaitées au noeud final.

   Pour un point final non sécurisé (HTTP), vous pouvez :

   - Changez le type de service de terminal entre S3 et Swift.

- Modifiez le mode de liaison du point final. Pour un point de terminaison sécurisé (HTTPS), vous pouvez :
- Changez le type de service de terminal entre S3 et Swift.
- Modifiez le mode de liaison du point final.
- Afficher le certificat de sécurité.
- Téléchargez ou générez un nouveau certificat de sécurité lorsque le certificat actuel a expiré ou est sur le point d'expirer.

  Sélectionnez un onglet pour afficher des informations détaillées sur le certificat de serveur StorageGRID par défaut ou sur un certificat signé par l'autorité de certification qui a été téléchargé.

> Pour modifier le protocole d'un noeud final existant, par exemple de HTTP à HTTPS, vous devez créer un nouveau noeud final. Suivez les instructions de création des points d'extrémité de l'équilibreur de charge et sélectionnez le protocole souhaité.

5. Cliquez sur **Enregistrer**.

Informations associées

Création de terminaux d'équilibrage de charge

Suppression des points finaux de l'équilibreur de charge

Si vous n'avez plus besoin d'un point final d'équilibreur de charge, vous pouvez le supprimer.

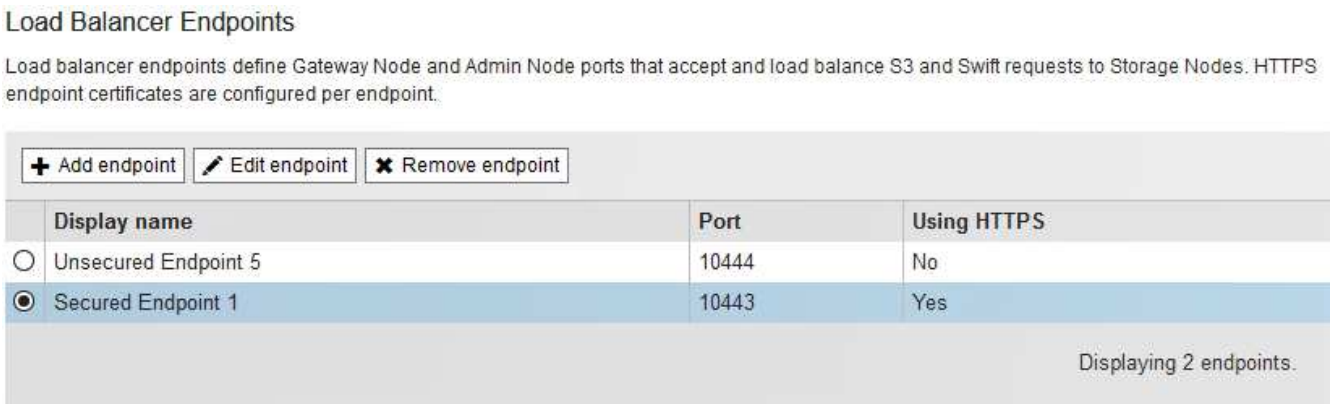
Ce dont vous avez besoin

- Vous devez disposer de l'autorisation accès racine.
- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.

Étapes

1. Sélectionnez **Configuration** > **Paramètres réseau** > **points d'extrémité Load Balancer**.

   La page Load Balancer Endpoints s'affiche. Les noeuds finaux existants sont répertoriés dans le tableau.



2. Sélectionnez le bouton radio à gauche du noeud final que vous souhaitez supprimer.
3. Cliquez sur **Supprimer le noeud final**.

   Une boîte de dialogue de confirmation s'affiche.

4. Cliquez sur **OK**.

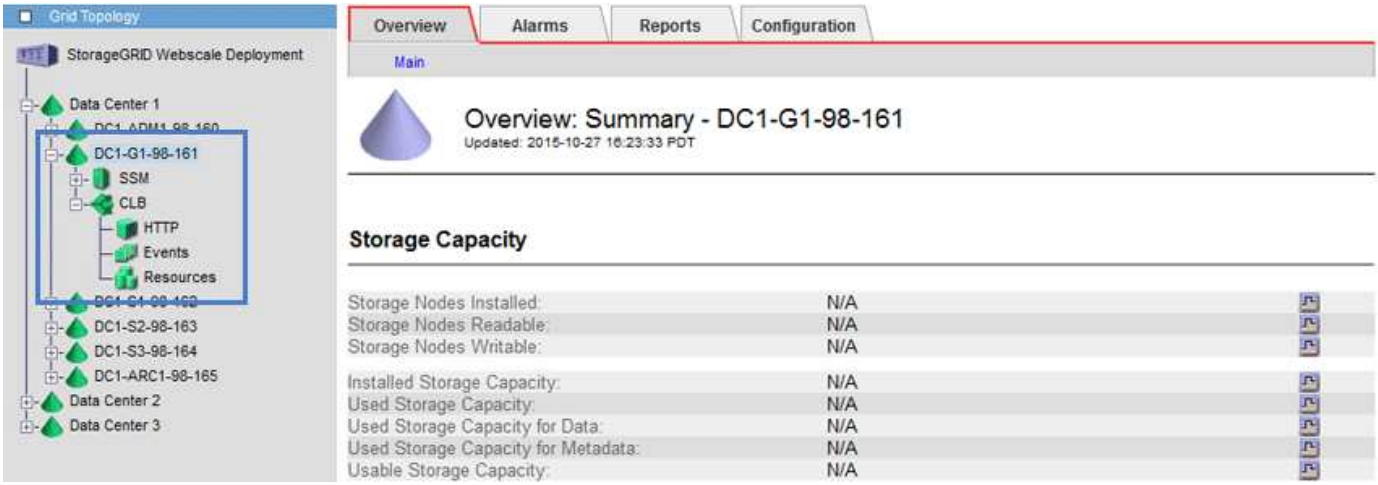
   Le noeud final est supprimé.

Fonctionnement de l'équilibrage de charge - service CLB

Le service Connection Load Balancer (CLB) sur les nœuds de passerelle est obsolète. Le service Load Balancer est désormais le mécanisme d'équilibrage de charge recommandé.

Le service CLB utilise l'équilibrage de charge de couche 4 pour distribuer les connexions réseau TCP entrantes des applications clientes vers le nœud de stockage optimal en fonction de la disponibilité, de la charge système et du coût de liaison configuré par l'administrateur. Lorsque le nœud de stockage optimal est choisi, le service CLB établit une connexion réseau bidirectionnelle et transfère le trafic vers et depuis le nœud choisi. Le CLB ne prend pas en compte la configuration du réseau Grid lors de la direction des connexions réseau entrantes.

Pour afficher des informations sur le service CLB, sélectionnez **support** > **Outils** > **topologie de grille**, puis développez un nœud de passerelle jusqu'à ce que vous puissiez sélectionner **CLB** et les options situées en dessous.



Si vous choisissez d'utiliser le service CLB, vous devriez envisager de configurer les coûts de liaison pour votre système StorageGRID.

Informations associées

"Quels sont les coûts de liaison"

"Mise à jour des coûts de lien"

Gestion des réseaux clients non fiables

Si vous utilisez un réseau client, vous pouvez protéger StorageGRID des attaques hostiles en acceptant le trafic client entrant uniquement sur les noeuds finaux configurés explicitement.

Par défaut, le réseau client sur chaque nœud de la grille est *Trusted*. Par défaut, StorageGRID approuve les connexions entrantes à chaque nœud de grid sur tous les ports externes disponibles (voir les informations sur les communications externes dans les instructions réseau).

Vous pouvez réduire la menace d'attaques hostiles sur votre système StorageGRID en spécifiant que le réseau client sur chaque nœud est *non fiable*. Si le réseau client d'un nœud n'est pas fiable, le nœud accepte uniquement les connexions entrantes sur les ports explicitement configurés en tant que points finaux d'équilibreur de charge.

Exemple 1 : le nœud de passerelle n'accepte que les requêtes HTTPS S3

Supposons que vous souhaitiez qu'un nœud de passerelle refuse tout trafic entrant sur le réseau client, à l'exception des requêtes HTTPS S3. Vous devez effectuer les étapes générales suivantes :

1. À partir de la page des noeuds finaux Load Balancer, configurez un noeud final Load Balancer pour S3 sur HTTPS sur le port 443.
2. Dans la page réseaux clients non approuvés, spécifiez que le réseau client sur le nœud de passerelle n'est pas fiable.

Après avoir enregistré votre configuration, tout le trafic entrant sur le réseau client du nœud passerelle est supprimé, sauf pour les requêtes HTTPS S3 sur le port 443 et les requêtes ICMP Echo (ping).

Exemple 2 : le nœud de stockage envoie des demandes de services de plateforme S3

Supposons que vous souhaitiez activer le trafic de service de la plateforme S3 sortant à partir d'un nœud de stockage, mais que vous voulez empêcher toute connexion entrante à ce nœud de stockage sur le réseau client. Vous devez effectuer cette étape générale :

- Dans la page réseaux clients non approuvés, indiquez que le réseau client sur le nœud de stockage n'est pas fiable.

Après avoir enregistré votre configuration, le nœud de stockage n'accepte plus de trafic entrant sur le réseau client, mais continue d'autoriser les requêtes sortantes vers Amazon Web Services.

Informations associées

"Instructions réseau"

"Configuration des terminaux d'équilibrage de charge"

La spécification du réseau client d'un nœud n'est pas fiable

Si vous utilisez un réseau client, vous pouvez spécifier si le réseau client de chaque nœud est fiable ou non fiable. Vous pouvez également spécifier le paramètre par défaut pour les nouveaux nœuds ajoutés dans une extension.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation accès racine.
- Si vous souhaitez qu'un nœud d'administration ou un nœud de passerelle accepte le trafic entrant uniquement sur des noeuds finaux configurés explicitement, vous avez défini les noeuds finaux de l'équilibreur de charge.

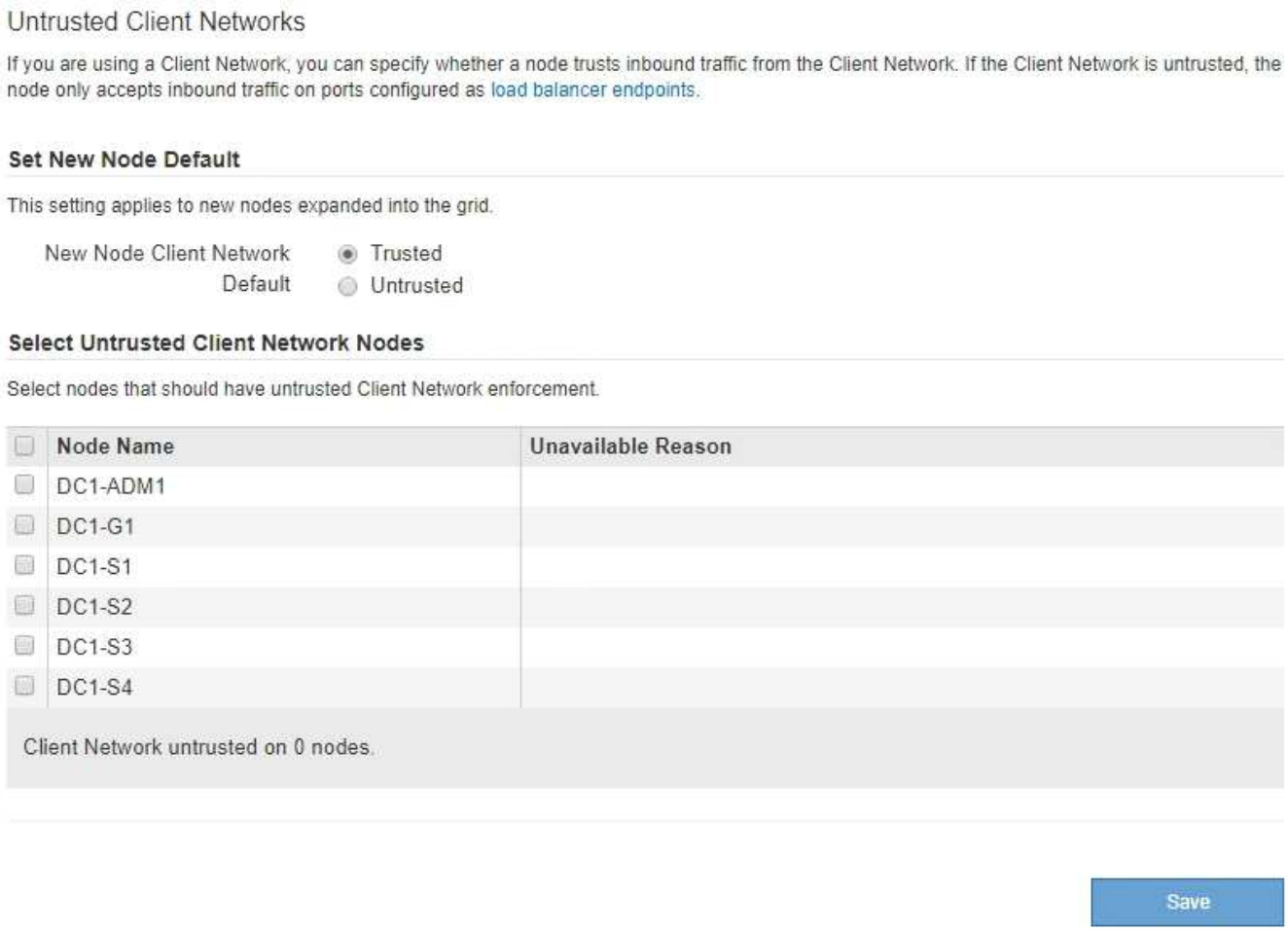
> Les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.

Étapes

1. Sélectionnez **Configuration** > **Paramètres réseau** > **réseau client non fiable**.

   La page réseaux clients non approuvés s'affiche.

   Cette page répertorie tous les nœuds du système StorageGRID. La colonne motif indisponible comprend une entrée si le réseau client du nœud doit être approuvé.



2. Dans la section **Set New Node Default** (définir nouveau nœud par défaut*), indiquez le paramètre par défaut à utiliser lorsque de nouveaux nœuds sont ajoutés à la grille dans une procédure d'extension.

   - **Trusted**: Lorsqu'un noeud est ajouté dans une extension, son réseau client est fiable.
   - **Non fiable** : lorsqu'un nœud est ajouté dans une extension, son réseau client n'est pas fiable. Si

nécessaire, vous pouvez revenir à cette page pour modifier le paramètre d'un nouveau nœud spécifique.

> Ce paramètre n'affecte pas les nœuds existants du système StorageGRID.

3. Dans la section **Sélectionner des nœuds réseau client non approuvés**, sélectionnez les nœuds qui doivent autoriser les connexions client uniquement sur les noeuds finaux de l'équilibreur de charge configurés explicitement.

   Vous pouvez sélectionner ou désélectionner la case à cocher du titre pour sélectionner ou désélectionner tous les nœuds.

4. Cliquez sur **Enregistrer**.

   Les nouvelles règles de pare-feu sont immédiatement ajoutées et appliquées. Les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.

Informations associées

"Configuration des terminaux d'équilibrage de charge"

Gestion des groupes haute disponibilité

Les groupes haute disponibilité peuvent être utilisés pour fournir des connexions de données hautement disponibles pour les clients S3 et Swift. Les groupes HAUTE DISPONIBILITÉ peuvent également être utilisés pour fournir des connexions haute disponibilité au Grid Manager et au tenant Manager.

- "Qu'est-ce qu'un groupe haute disponibilité"
- "Mode d'utilisation des groupes haute disponibilité"
- "Options de configuration pour les groupes haute disponibilité"
- "Création d'un groupe haute disponibilité"
- "Modification d'un groupe haute disponibilité"
- "Suppression d'un groupe haute disponibilité"

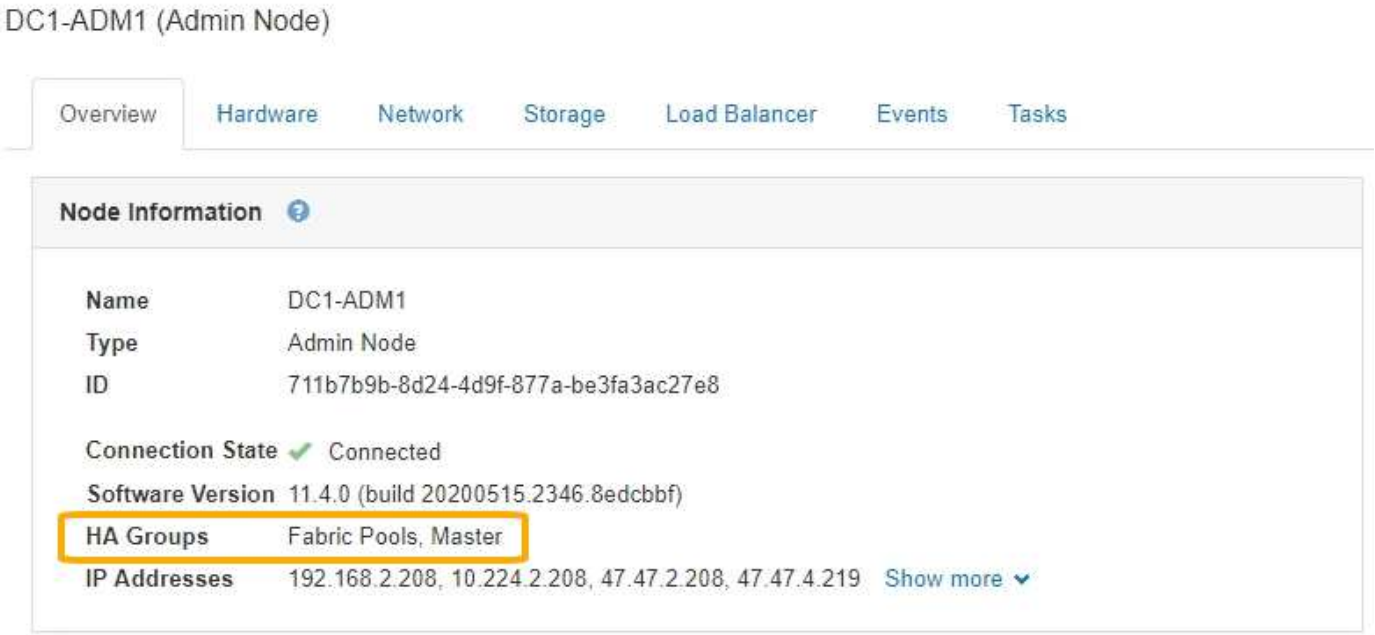
Qu'est-ce qu'un groupe haute disponibilité

Les groupes haute disponibilité utilisent des adresses IP virtuelles (VIP) pour fournir un accès de sauvegarde active aux services de nœud de passerelle ou de nœud d'administration.

Un groupe haute disponibilité comprend une ou plusieurs interfaces réseau sur les nœuds d'administration et les nœuds de passerelle. Lors de la création d'un groupe HA, vous sélectionnez des interfaces réseau appartenant à la grille Network (eth0) ou au réseau client (eth2). Toutes les interfaces d'un groupe haute disponibilité doivent se trouver dans le même sous-réseau réseau réseau.

Un groupe haute disponibilité conserve une ou plusieurs adresses IP virtuelles ajoutées à l'interface active du groupe. Si l'interface active n'est plus disponible, les adresses IP virtuelles sont déplacées vers une autre interface. Ce processus de basculement ne prend généralement que quelques secondes et est suffisamment rapide pour que les applications clientes aient peu d'impact et peuvent compter sur des comportements de tentatives normales pour poursuivre le fonctionnement.

L'interface active d'un groupe HA est désignée comme maître. Toutes les autres interfaces sont désignées comme étant Backup. Pour afficher ces désignations, sélectionnez **nœuds** > ***node*** > **Présentation**.



Lors de la création d'un groupe haute disponibilité, vous spécifiez une interface à utiliser comme maître préféré. Le maître préféré est l'interface active, sauf en cas de défaillance qui entraîne la réaffectation des adresses VIP à une interface de sauvegarde. Lorsque l'échec est résolu, les adresses VIP sont automatiquement retransférées vers le maître préféré.

Le basculement peut être déclenché pour l'une des raisons suivantes :

- Le nœud sur lequel l'interface est configurée s'éteint.
- Le nœud sur lequel l'interface est configurée perd la connectivité sur tous les autres nœuds pendant au moins 2 minutes
- L'interface active tombe en panne.
- Le service Load Balancer s'arrête.
- Le service haute disponibilité s'arrête.

> Le basculement peut ne pas être déclenché par des pannes réseau externes au nœud qui héberge l'interface active. De même, le basculement n'est pas déclenché par la défaillance du service CLB (obsolète) ou des services pour le Grid Manager ou le tenant Manager.

Si le groupe haute disponibilité inclut des interfaces de plus de deux nœuds, l'interface active peut être déplacé vers l'interface d'un autre nœud pendant le basculement.

Mode d'utilisation des groupes haute disponibilité

Vous pouvez utiliser les groupes haute disponibilité (HA) pour plusieurs raisons.

- Un groupe haute disponibilité peut fournir des connexions administratives hautement disponibles vers le Grid Manager ou le tenant Manager.
- Un groupe haute disponibilité peut fournir des connexions de données extrêmement disponibles pour les clients S3 et Swift.

- Un groupe haute disponibilité ne contenant qu'une interface vous permet de fournir de nombreuses adresses VIP et de définir explicitement des adresses IPv6.

Un groupe haute disponibilité peut assurer la haute disponibilité uniquement si tous les nœuds du groupe fournissent les mêmes services. Lorsque vous créez un groupe haute disponibilité, ajoutez des interfaces à partir des types de nœuds qui fournissent les services requis.

- **Nœuds d'administration** : incluez le service Load Balancer et activez l'accès au Grid Manager ou au Gestionnaire de locataires.
- **Gateway Nodes** : inclut le service Load Balancer et le service CLB (obsolète).

Objectif du groupe haute disponibilité	Ajout de nœuds de ce type au groupe haute disponibilité
Accès à Grid Manager	• Nœud d'administration principal (**maître préféré**) • Nœuds d'administration non primaires **Remarque :** le noeud d'administration principal doit être le maître préféré. Certaines procédures de maintenance peuvent uniquement être effectuées depuis le nœud d'administration principal.
Accès au Gestionnaire de locataires uniquement	• Nœuds d'administration primaires ou non primaires
Accès client S3 ou Swift — Service Load Balancer	• Nœuds d'administration • Nœuds de passerelle
Accès client S3 ou Swift — service CLB **Note:** le service CLB est obsolète.	• Nœuds de passerelle

Restrictions liées à l'utilisation de groupes haute disponibilité avec Grid Manager ou tenant Manager

L'échec des services de Grid Manager ou de tenant Manager n'entraîne pas de basculement au sein du groupe haute disponibilité.

Si vous êtes connecté au Grid Manager ou au tenant Manager lors du basculement, vous êtes déconnecté et vous devez vous reconnecter pour reprendre votre tâche.

Certaines procédures de maintenance ne peuvent pas être effectuées lorsque le nœud d'administration principal n'est pas disponible. Pendant le basculement, vous pouvez utiliser le Gestionnaire de grille pour surveiller votre système StorageGRID.

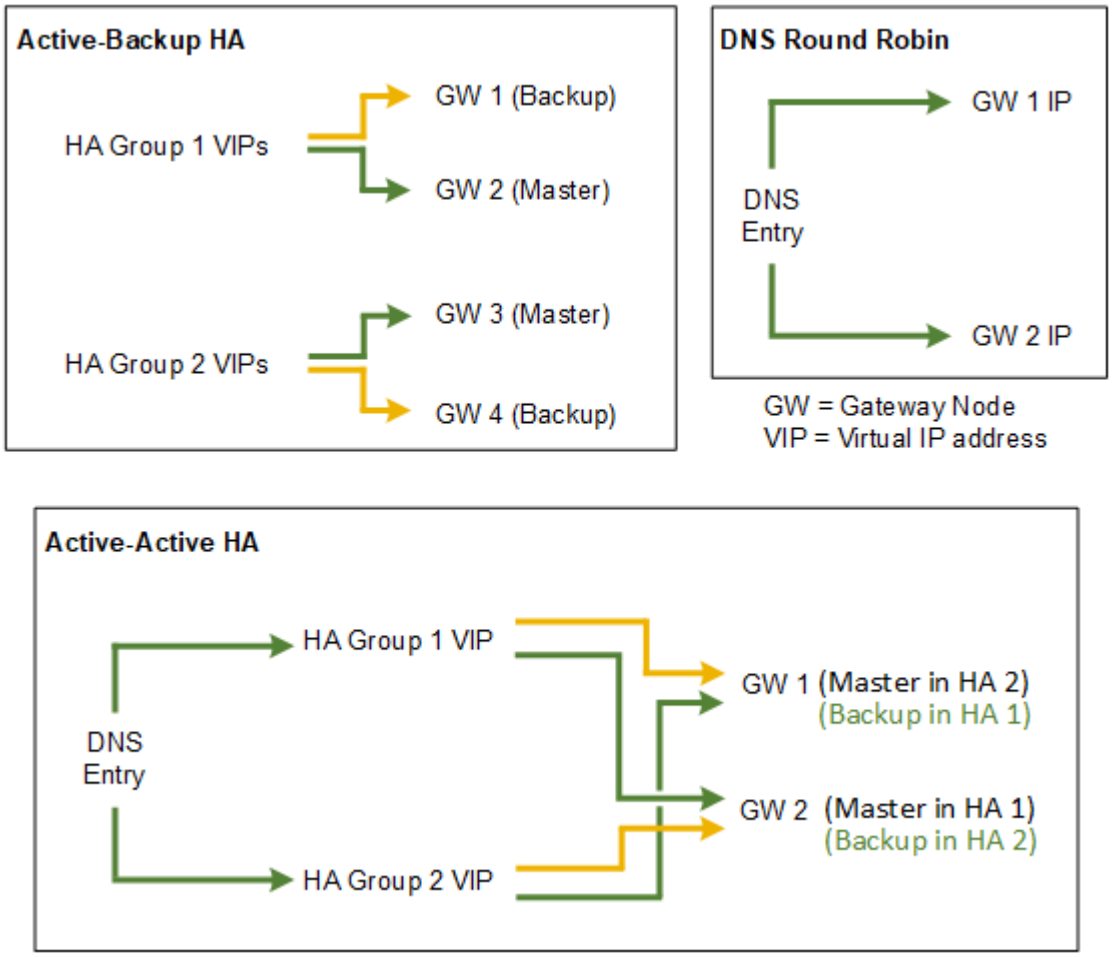
Limites de l'utilisation de groupes HA avec le service CLB

La défaillance du service CLB ne déclenche pas de basculement au sein du groupe HA.

> Le service CLB est obsolète.

Options de configuration pour les groupes haute disponibilité

Les schémas ci-dessous fournissent des exemples de différentes façons de configurer les groupes haute disponibilité. Chaque option présente des avantages et des inconvénients.



Lors de la création de plusieurs groupes HA redondants, comme illustré dans l'exemple HA actif-actif, le débit total évolue avec le nombre de nœuds et de groupes HA. Avec trois nœuds ou plus et trois groupes haute disponibilité ou plus, vous pouvez également continuer à utiliser n'importe quel VIP, même lors des procédures de maintenance nécessitant de mettre un nœud hors ligne.

Le tableau récapitule les avantages de chaque configuration de haute disponibilité illustrée sur le schéma.

Configuration	Avantages	Inconvénients
Active-Backup HA	• Gérées par StorageGRID sans dépendances externes • Basculement rapide	• Un seul nœud d'un groupe haute disponibilité est actif. Au moins un nœud par groupe haute disponibilité sera inactif.

Configuration	Avantages	Inconvénients
DNS Round Robin	• Un débit global supérieur. • Aucun hôte inactif.	• Basculement lent, qui peut dépendre du comportement des clients. • Nécessite une configuration matérielle en dehors du StorageGRID. • Nécessite une vérification de l'état implémentée par le client.
Actif-actif	• Le trafic est réparti entre plusieurs groupes haute disponibilité. • Débit global élevé qui évolue en même temps que le nombre de groupes HA. • Basculement rapide	• Configuration plus complexe. • Nécessite une configuration matérielle en dehors du StorageGRID. • Nécessite une vérification de l'état implémentée par le client.

Création d'un groupe haute disponibilité

Vous pouvez créer un ou plusieurs groupes haute disponibilité pour fournir un accès hautement disponible aux services sur les nœuds d'administration ou les nœuds de passerelle.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation accès racine.

Description de la tâche

Une interface doit respecter les conditions suivantes pour être inclus dans un groupe haute disponibilité :

- L'interface doit être destinée à un nœud de passerelle ou à un nœud d'administration.
- L'interface doit appartenir au réseau Grid Network (eth0) ou au réseau client (eth2).
- L'interface doit être configurée avec un adressage IP fixe ou statique, et non avec DHCP.

Étapes

1. Sélectionnez **Configuration** > **Paramètres réseau** > **groupes haute disponibilité**.

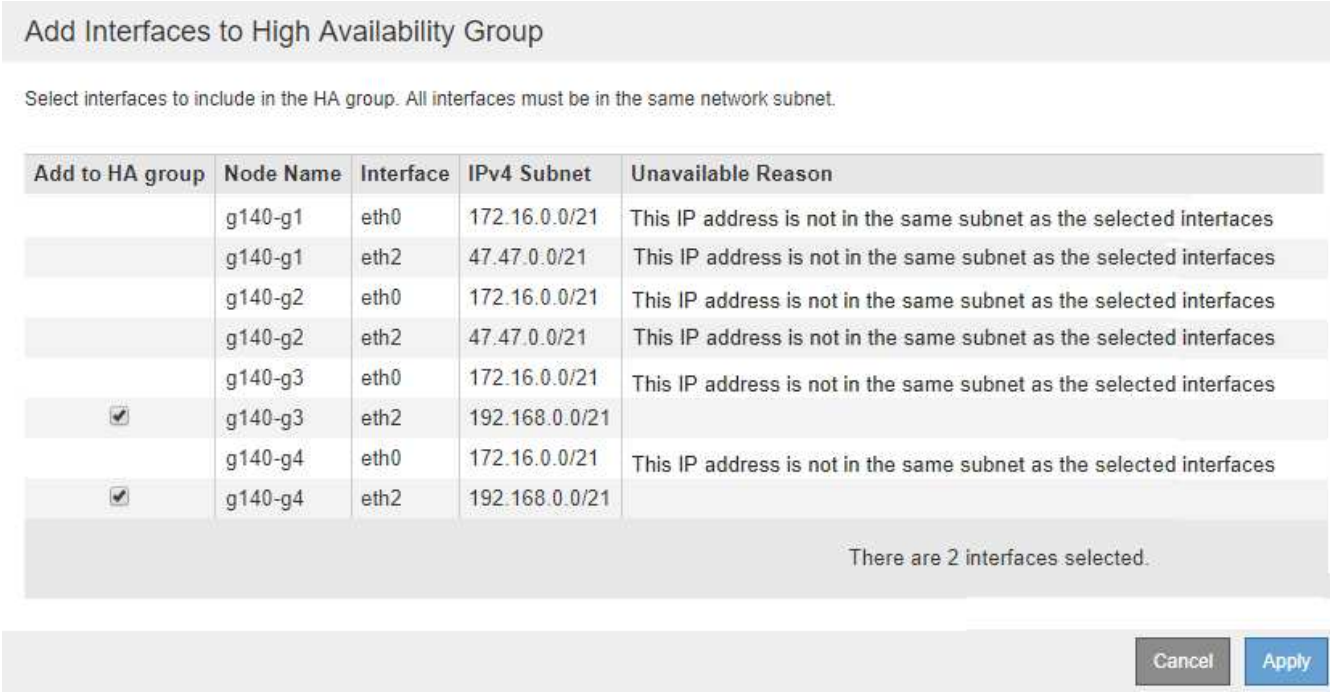
   La page groupes haute disponibilité s'affiche.

2. Cliquez sur **Créer**.

   La boîte de dialogue Créer un groupe haute disponibilité s'affiche.

3. Saisissez un nom et, le cas échéant, une description pour le groupe HA.
4. Cliquez sur **Sélectionner interfaces**.

   La boîte de dialogue Ajouter des interfaces au groupe haute disponibilité s'affiche. Le tableau répertorie les nœuds, les interfaces et les sous-réseaux IPv4 éligibles.



   Une interface n'apparaît pas dans la liste si son adresse IP est attribuée par DHCP.

5. Dans la colonne **Ajouter au groupe HA**, cochez la case de l'interface que vous souhaitez ajouter au groupe HA.

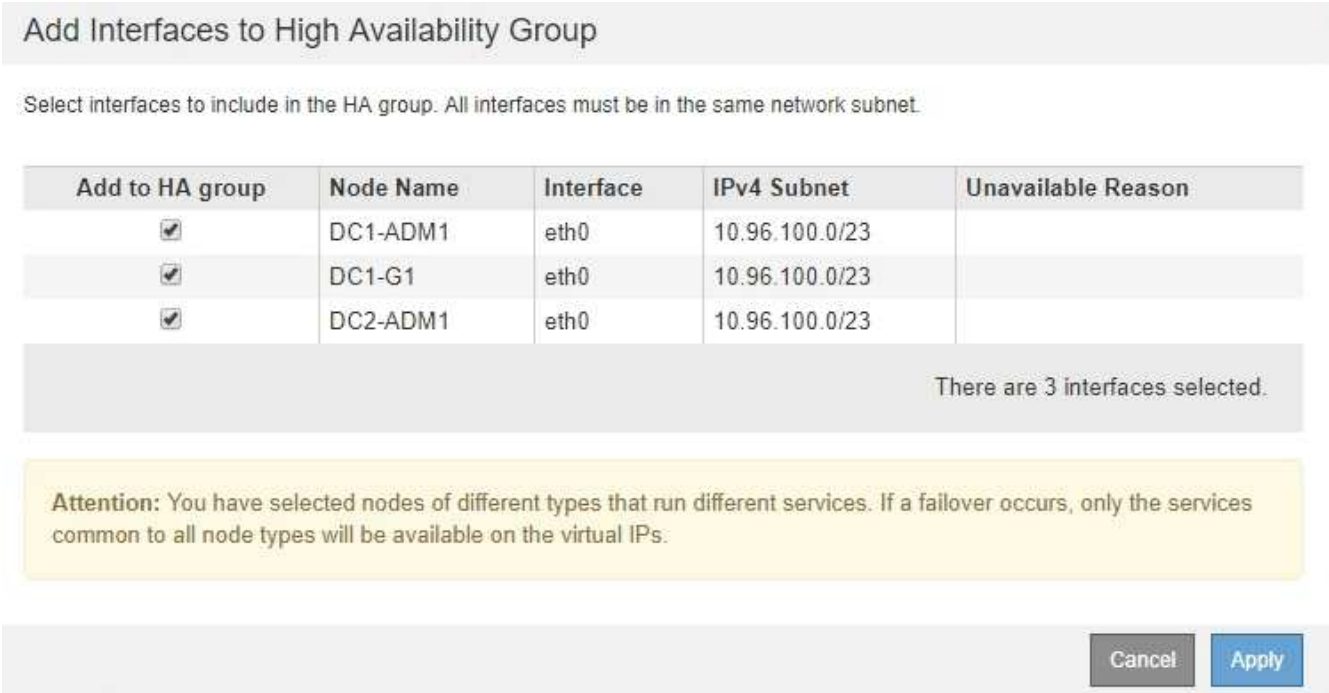
   Notez les consignes suivantes pour la sélection des interfaces :

   - Vous devez sélectionner au moins une interface.
   - Si vous sélectionnez plusieurs interfaces, toutes les interfaces doivent se trouver sur le réseau Grid (eth0) ou sur le réseau client (eth2).
   - Toutes les interfaces doivent se trouver dans le même sous-réseau ou dans des sous-réseaux avec un préfixe commun.

Les adresses IP seront limitées au sous-réseau le plus petit (celui avec le plus grand préfixe).

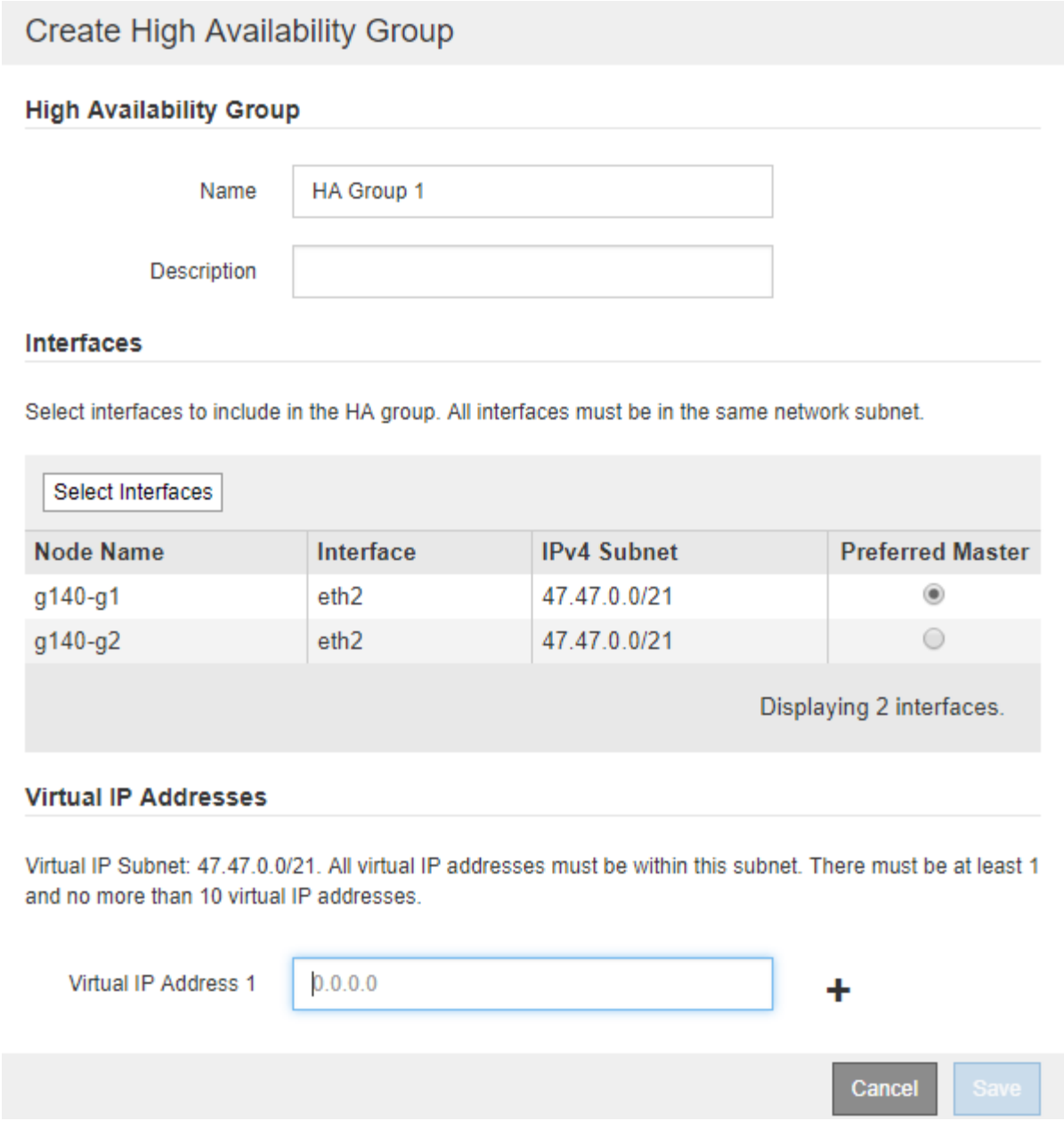
- Si vous sélectionnez des interfaces sur différents types de nœuds et qu'un basculement se produit, seuls les services communs aux nœuds sélectionnés seront disponibles sur les adresses IP virtuelles.
  - Sélectionnez au moins deux nœuds d'administration pour protéger haute disponibilité le Grid Manager ou le tenant Manager.
  - Sélectionnez au moins deux nœuds d'administration et/ou plusieurs nœuds de passerelle pour la protection haute disponibilité du service Load Balancer.
  - Sélectionnez au moins deux nœuds de passerelle pour la protection haute disponibilité du service CLB.

    Le service CLB est obsolète.



6. Cliquez sur **appliquer**.

   Les interfaces sélectionnées sont répertoriées dans la section interfaces de la page Créer un groupe haute disponibilité. Par défaut, la première interface de la liste est sélectionnée comme maître préféré.



7. Si vous souhaitez qu'une interface différente soit le maître préféré, sélectionnez cette interface dans la colonne **Maître préféré**.

   Le maître préféré est l'interface active, sauf en cas de défaillance qui entraîne la réaffectation des adresses VIP à une interface de sauvegarde.

   > Si le groupe HA donne accès à Grid Manager, vous devez sélectionner une interface sur le nœud d'administration principal pour qu'il soit le maître préféré. Certaines procédures de maintenance peuvent uniquement être effectuées depuis le nœud d'administration principal.

8. Dans la section adresses IP virtuelles de la page, entrez une à 10 adresses IP virtuelles pour le groupe HA. Cliquez sur le signe plus (+) Pour ajouter plusieurs adresses IP.

   Vous devez fournir au moins une adresse IPv4. Vous pouvez éventuellement spécifier des adresses IPv4 et IPv6 supplémentaires.

   Les adresses IPv4 doivent se trouver dans le sous-réseau IPv4 partagé par toutes les interfaces membres.

9. Cliquez sur **Enregistrer**.

   Le groupe haute disponibilité est créé et vous pouvez maintenant utiliser les adresses IP virtuelles configurées.

Informations associées

"Installez Red Hat Enterprise Linux ou CentOS"

"Installez VMware"

"Installez Ubuntu ou Debian"

"Gestion de l'équilibrage des charges"

Modification d'un groupe haute disponibilité

Vous pouvez modifier un groupe haute disponibilité (HA) pour modifier son nom et sa description, ajouter ou supprimer des interfaces ou ajouter ou mettre à jour une adresse IP virtuelle.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation accès racine.

Description de la tâche

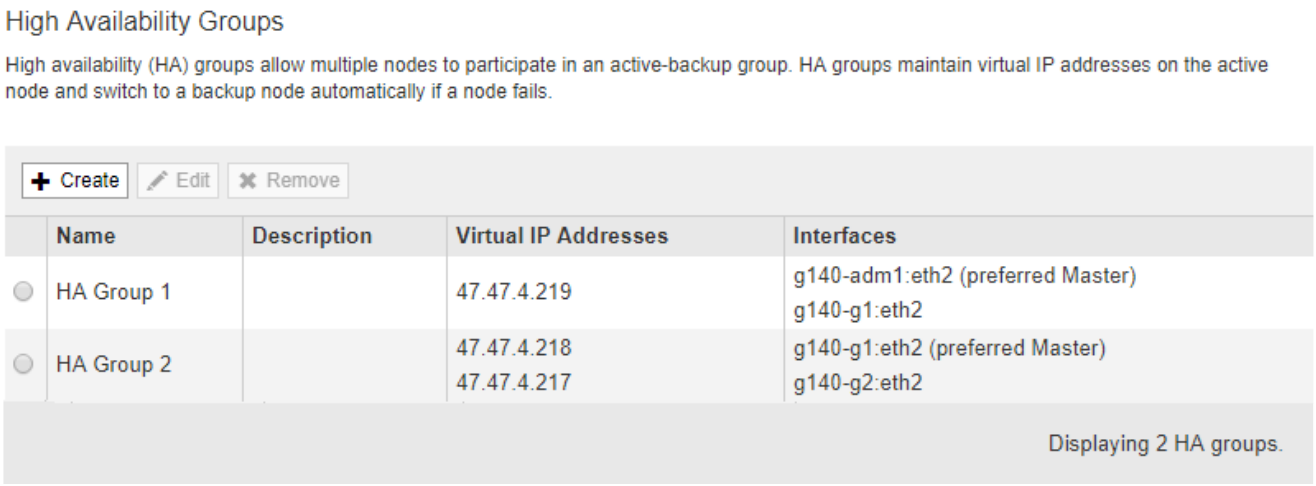
Voici quelques-unes des raisons justifiant la modification d'un groupe haute disponibilité :

- Ajout d'une interface à un groupe existant. L'adresse IP de l'interface doit se trouver dans le même sous-réseau que les autres interfaces déjà attribuées au groupe.
- Suppression d'une interface d'un groupe haute disponibilité. Par exemple, vous ne pouvez pas démarrer une procédure de mise hors service d'un site ou d'un nœud si l'interface d'un nœud pour le réseau Grid ou le réseau client est utilisée dans un groupe HA.

Étapes

1. Sélectionnez **Configuration** > **Paramètres réseau** > **groupes haute disponibilité**.

   La page groupes haute disponibilité s'affiche.

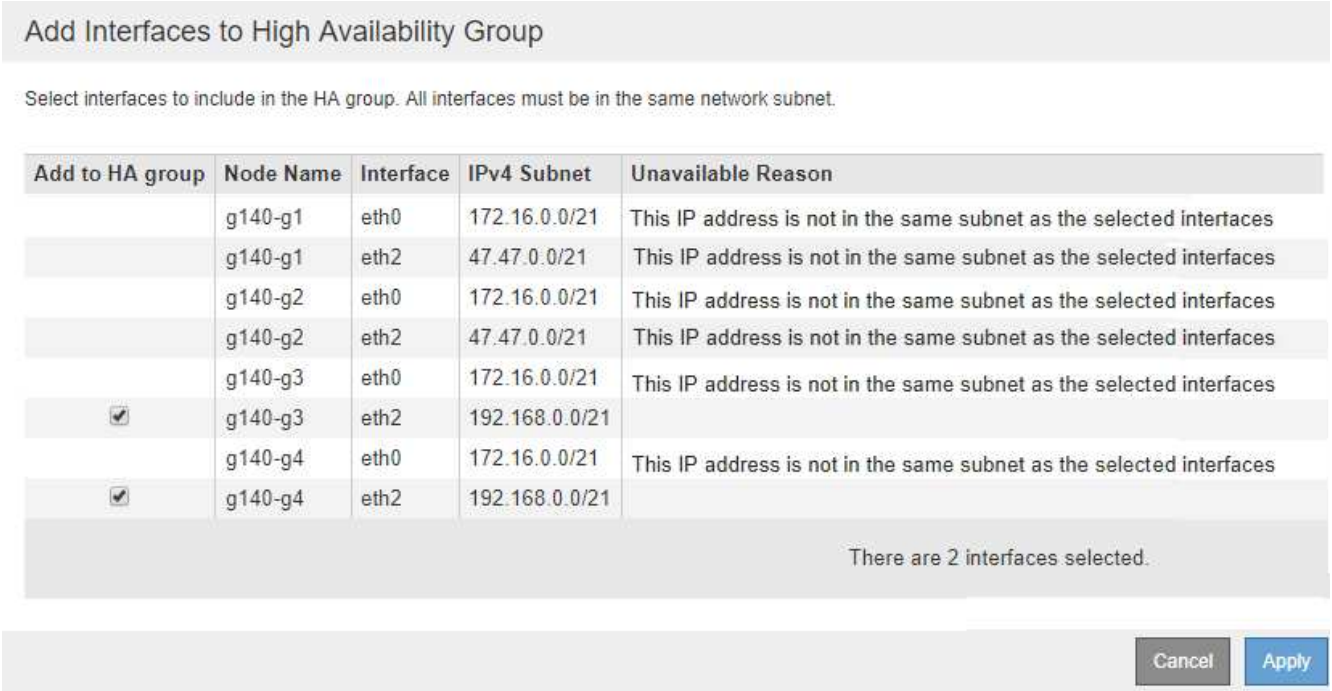


2. Sélectionnez le groupe HA que vous souhaitez modifier et cliquez sur **Modifier**.

   La boîte de dialogue Modifier le groupe haute disponibilité s'affiche.

3. Vous pouvez également mettre à jour le nom ou la description du groupe.
4. Vous pouvez également cliquer sur **Select interfaces** pour modifier les interfaces du groupe HA.

   La boîte de dialogue Ajouter des interfaces au groupe haute disponibilité s'affiche.



   Une interface n'apparaît pas dans la liste si son adresse IP est attribuée par DHCP.

5. Cocher ou décocher les cases pour ajouter ou supprimer des interfaces.

   Notez les consignes suivantes pour la sélection des interfaces :

   - Vous devez sélectionner au moins une interface.
   - Si vous sélectionnez plusieurs interfaces, toutes les interfaces doivent se trouver sur le réseau Grid (eth0) ou sur le réseau client (eth2).
   - Toutes les interfaces doivent se trouver dans le même sous-réseau ou dans des sous-réseaux avec un préfixe commun.

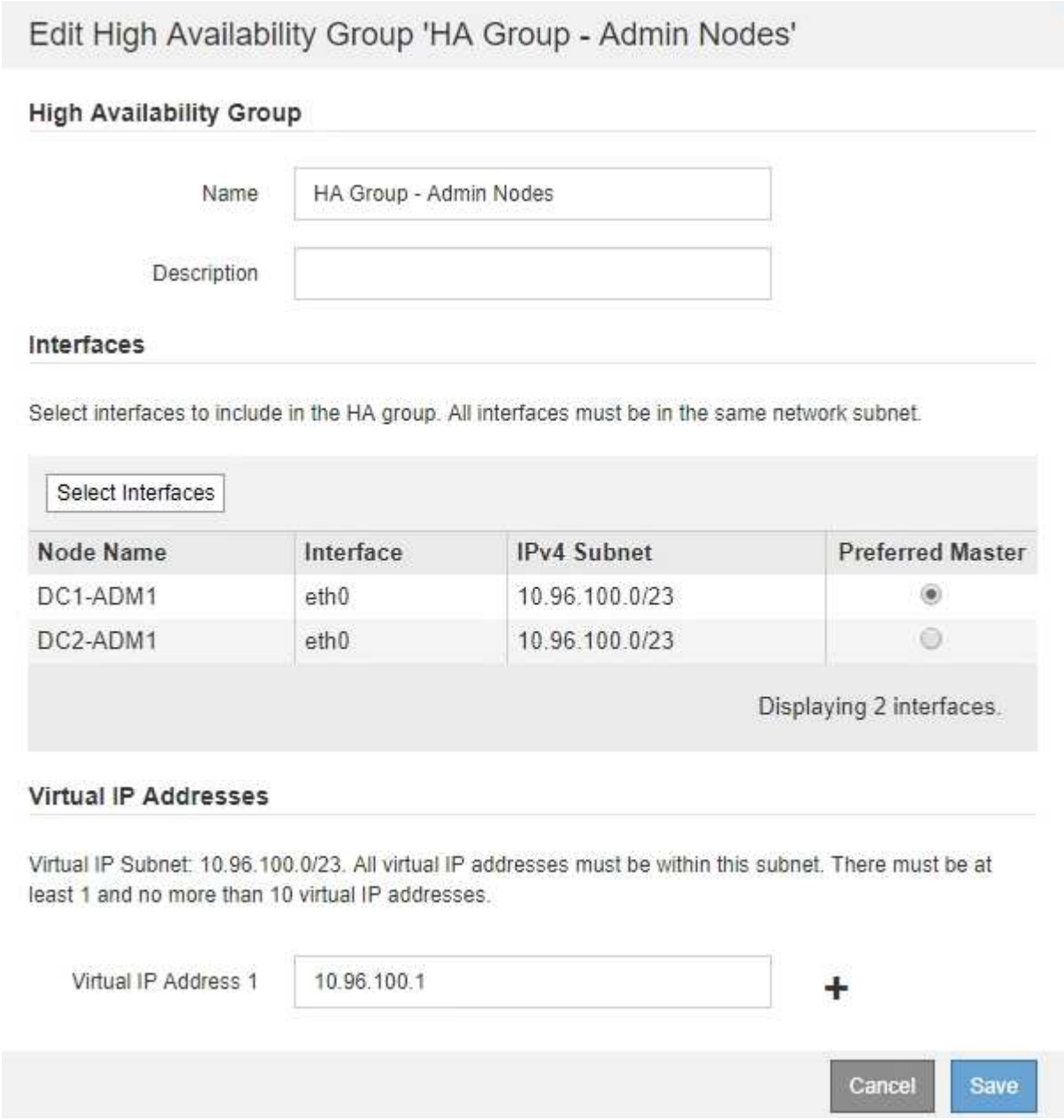
     Les adresses IP seront limitées au sous-réseau le plus petit (celui avec le plus grand préfixe).

   - Si vous sélectionnez des interfaces sur différents types de nœuds et qu'un basculement se produit, seuls les services communs aux nœuds sélectionnés seront disponibles sur les adresses IP virtuelles.
     - Sélectionnez au moins deux nœuds d'administration pour protéger haute disponibilité le Grid Manager ou le tenant Manager.
     - Sélectionnez au moins deux nœuds d'administration et/ou plusieurs nœuds de passerelle pour la protection haute disponibilité du service Load Balancer.
     - Sélectionnez au moins deux nœuds de passerelle pour la protection haute disponibilité du service CLB.

Le service CLB est obsolète.

6. Cliquez sur **appliquer**.

   Les interfaces sélectionnées sont répertoriées dans la section interfaces de la page. Par défaut, la première interface de la liste est sélectionnée comme maître préféré.



7. Si vous souhaitez qu'une interface différente soit le maître préféré, sélectionnez cette interface dans la colonne **Maître préféré**.

   Le maître préféré est l'interface active, sauf en cas de défaillance qui entraîne la réaffectation des adresses VIP à une interface de sauvegarde.

   Si le groupe HA donne accès à Grid Manager, vous devez sélectionner une interface sur le nœud d'administration principal pour qu'il soit le maître préféré. Certaines procédures de maintenance peuvent uniquement être effectuées depuis le nœud d'administration principal.

8. Si vous le souhaitez, mettez à jour les adresses IP virtuelles pour le groupe haute disponibilité.

   Vous devez fournir au moins une adresse IPv4. Vous pouvez éventuellement spécifier des adresses IPv4 et IPv6 supplémentaires.

   Les adresses IPv4 doivent se trouver dans le sous-réseau IPv4 partagé par toutes les interfaces membres.

9. Cliquez sur **Enregistrer**.

   Le groupe haute disponibilité est mis à jour.

Suppression d'un groupe haute disponibilité

Vous pouvez supprimer un groupe haute disponibilité (HA) que vous n'utilisez plus.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation accès racine.

Aboout cette tâche

Si vous supprimez un groupe haute disponibilité, tout client S3 ou Swift configuré pour utiliser l'une des adresses IP virtuelles du groupe ne pourra plus se connecter à StorageGRID. Pour éviter les interruptions de vos clients, nous vous recommandons de mettre à jour toutes les applications des clients S3 ou Swift affectées avant de supprimer un groupe haute disponibilité. Mettre à jour chaque client pour se connecter à l'aide d'une autre adresse IP, par exemple l'adresse IP virtuelle d'un autre groupe haute disponibilité ou l'adresse IP configurée pour une interface lors de l'installation ou à l'aide de DHCP.

Étapes

1. Sélectionnez **Configuration** > **Paramètres réseau** > **groupes haute disponibilité**.

   La page groupes haute disponibilité s'affiche.

   High Availability Groups

   High availability (HA) groups allow multiple nodes to participate in an active-backup group. HA groups maintain virtual IP addresses on the active node and switch to a backup node automatically if a node fails.

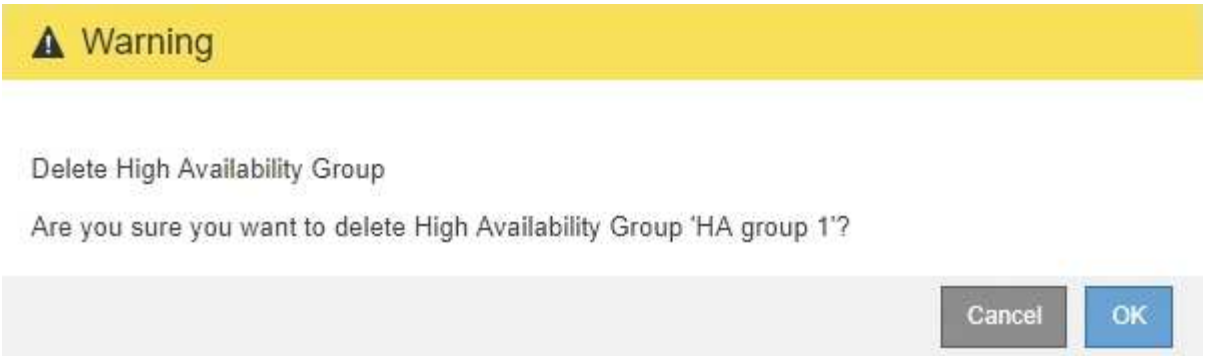
   + Create | Edit | Remove

	Name	Description	Virtual IP Addresses	Interfaces
○	HA Group 1		47.47.4.219	g140-adm1:eth2 (preferred Master) g140-g1:eth2
○	HA Group 2		47.47.4.218 47.47.4.217	g140-g1:eth2 (preferred Master) g140-g2:eth2

   Displaying 2 HA groups.

2. Sélectionnez le groupe HA que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

   L'avertissement Supprimer le groupe haute disponibilité s'affiche.



3. Cliquez sur **OK**.

   Le groupe haute disponibilité est supprimé.

Configuration des noms de domaine de terminaux API S3

Pour prendre en charge les demandes de type hébergement virtuel S3, vous devez utiliser Grid Manager pour configurer la liste des noms de domaine de points de terminaison auxquels les clients S3 se connectent.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir confirmé qu'une mise à niveau de la grille n'est pas en cours.

> Ne modifiez pas la configuration du nom de domaine lorsqu'une mise à niveau de la grille est en cours.

Description de la tâche

Pour permettre aux clients d'utiliser les noms de domaine de terminaux S3, vous devez effectuer toutes les tâches suivantes :

- Utilisez le Gestionnaire de grille pour ajouter les noms de domaine de points de terminaison S3 au système StorageGRID.
- Vérifiez que le certificat utilisé par le client pour les connexions HTTPS à StorageGRID est signé pour tous les noms de domaine requis par le client.

  Par exemple, si le noeud final est `s3.company.com`, Vous devez vous assurer que le certificat utilisé pour les connexions HTTPS inclut le `s3.company.com` Nom de l'alternative (SAN) de l'objet générique du noeud final et du noeud final : `*.s3.company.com`.

- Configurez le serveur DNS utilisé par le client. Inclure les enregistrements DNS pour les adresses IP utilisées par les clients pour établir des connexions et s'assurer que les enregistrements référencent tous les noms de domaine de point final requis, y compris les noms de caractères génériques.

> Les clients peuvent se connecter à StorageGRID à l'aide de l'adresse IP d'un nœud de passerelle, d'un nœud d'administration ou d'un nœud de stockage, ou en se connectant à l'adresse IP virtuelle d'un groupe haute disponibilité. Vous devez comprendre comment les applications client se connectent à la grille pour inclure les adresses IP correctes dans les enregistrements DNS.

Le certificat utilisé par un client pour les connexions HTTPS dépend de la façon dont le client se connecte à la grille :

- Si un client se connecte à l'aide du service Load Balancer, il utilise le certificat pour un noeud final spécifique de l'équilibreur de charge.

  > Chaque noeud final de l'équilibreur de charge possède son propre certificat et chaque noeud final peut être configuré pour reconnaître différents noms de domaine de point final.

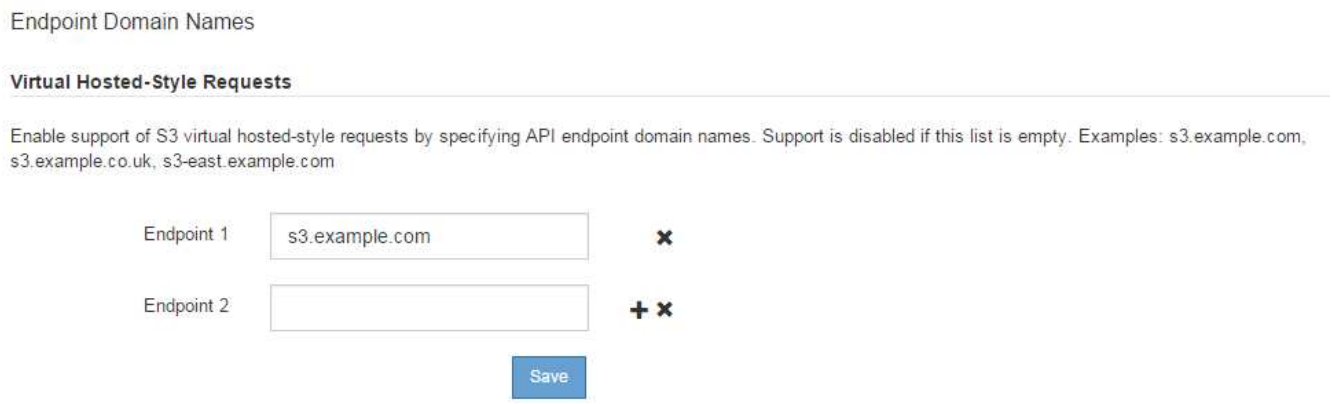
- Si le client se connecte à un nœud de stockage ou au service CLB sur un nœud de passerelle, le client utilise un certificat de serveur personnalisé de grille qui a été mis à jour pour inclure tous les noms de domaine de noeud final requis.

  > Le service CLB est obsolète.

Étapes

1. Sélectionnez **Configuration** > **Paramètres réseau** > **noms de domaine**.

   La page noms de domaine de point final s'affiche.

2. À l'aide de l'icône (+) pour ajouter des champs supplémentaires, entrez la liste des noms de domaine de points de terminaison de l'API S3 dans les champs **Endpoint**.

   Si cette liste est vide, la prise en charge des demandes de type hébergement virtuel S3 est désactivée.

3. Cliquez sur **Enregistrer**.
4. Assurez-vous que les certificats de serveur utilisés par les clients correspondent aux noms de domaine de noeud final requis.
   - Pour les clients qui utilisent le service Load Balancer, mettez à jour le certificat associé au noeud final Load Balancer auquel le client se connecte.
   - Pour les clients qui se connectent directement aux nœuds de stockage ou qui utilisent le service CLB sur les nœuds de passerelle, mettez à jour le certificat de serveur personnalisé pour la grille.

5. Ajoutez les enregistrements DNS requis pour vous assurer que les demandes de nom de domaine de point final peuvent être résolues.

Résultat

Maintenant, lorsque les clients utilisent le noeud final `bucket.s3.company.com`, Le serveur DNS résout le noeud final correct et le certificat authentifie le noeud final comme prévu.

Informations associées

"Utilisation de S3"

"Affichage des adresses IP"

"Création d'un groupe haute disponibilité"

"Configuration d'un certificat de serveur personnalisé pour les connexions au nœud de stockage ou au service CLB"

"Configuration des terminaux d'équilibrage de charge"

Activation du protocole HTTP pour les communications client

Par défaut, les applications clientes utilisent le protocole réseau HTTPS pour toutes les connexions aux nœuds de stockage ou au service CLB obsolète sur les nœuds de passerelle. Vous pouvez éventuellement activer HTTP pour ces connexions, par exemple lors du test d'une grille autre que la production.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Cette tâche doit être effectuée uniquement si les clients S3 et Swift doivent établir des connexions HTTP directement vers les nœuds de stockage ou vers le service CLB obsolète sur les nœuds de passerelle.

Il n'est pas nécessaire d'effectuer cette tâche pour les clients qui utilisent uniquement des connexions HTTPS ou pour les clients qui se connectent au service Load Balancer (parce que vous pouvez configurer chaque noeud final Load Balancer pour utiliser HTTP ou HTTPS). Pour plus d'informations, reportez-vous aux informations sur la configuration des noeuds finaux de l'équilibreur de charge.

Voir "Résumé : adresses IP et ports pour les connexions client" Pour découvrir les ports que les clients S3 et Swift utilisent lors de la connexion aux nœuds de stockage ou au service CLB obsolète via HTTP ou HTTPS

> Soyez prudent lorsque vous activez HTTP pour une grille de production car les requêtes seront envoyées de manière non chiffrée.

Étapes

1. Sélectionnez **Configuration** > **Paramètres système** > **Options de grille**.
2. Dans la section Options réseau, cochez la case **Activer la connexion HTTP**.

3. Cliquez sur **Enregistrer**.

Informations associées

"Configuration des terminaux d'équilibrage de charge"

"Utilisation de S3"

"Utiliser Swift"

Contrôle des opérations client autorisées

Vous pouvez sélectionner l'option empêcher la grille de modification du client pour refuser des opérations client HTTP spécifiques.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Empêcher la modification du client est un paramètre à l'échelle du système. Lorsque l'option empêcher la modification du client est sélectionnée, les demandes suivantes sont refusées :

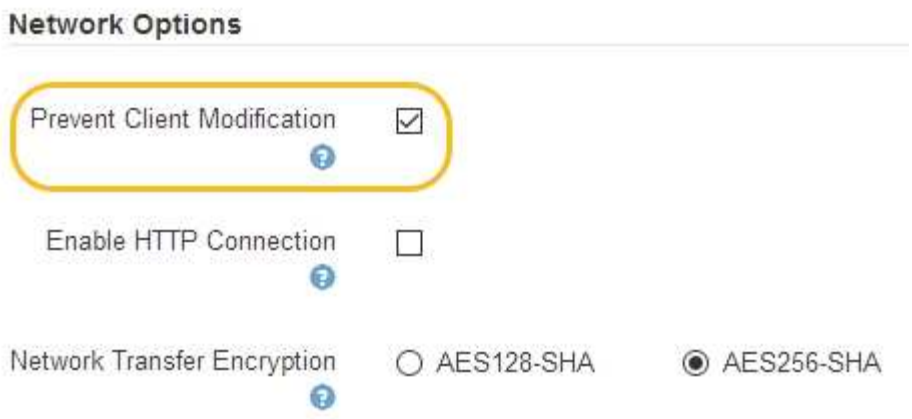
- **API REST S3**
  - Supprimer les demandes de compartiment
  - Toute demande de modification des données d'un objet existant, des métadonnées définies par l'utilisateur ou du balisage d'objets S3

> Ce paramètre ne s'applique pas aux compartiments avec la gestion des versions activée. Le contrôle de version empêche déjà les modifications des données d'objet, des métadonnées définies par l'utilisateur et du balisage d'objets.

- **API REST Swift**
  - Supprimer les demandes de conteneur
  - Demande de modifier tout objet existant. Par exemple, les opérations suivantes sont refusées : remplacement, suppression, mise à jour des métadonnées, etc.

Étapes

1. Sélectionnez **Configuration** > **Paramètres système** > **Options de grille**.
2. Dans la section Options réseau, cochez la case **empêcher la modification du client**.



3. Cliquez sur **Enregistrer**.

Gestion des réseaux et des connexions StorageGRID

Vous pouvez utiliser le Gestionnaire de grille pour configurer et gérer les réseaux et les connexions StorageGRID.

Voir "Configuration des connexions des clients S3 et Swift" Pour apprendre à connecter des clients S3 ou Swift.

- "Instructions pour les réseaux StorageGRID"
- "Affichage des adresses IP"
- "Chiffrement pris en charge pour les connexions TLS sortantes"
- "Modification du chiffrement du transfert réseau"
- "Configuration des certificats de serveur"
- "Configuration des paramètres du proxy de stockage"
- "Configuration des paramètres du proxy d'administration"
- "Gestion des stratégies de classification du trafic"
- "Quels sont les coûts de liaison"

Instructions pour les réseaux StorageGRID

StorageGRID prend en charge jusqu'à trois interfaces réseau par nœud de grid, vous permettant de configurer le réseau pour chaque nœud de grid en fonction de vos besoins de sécurité et d'accès.

> Pour modifier ou ajouter un réseau pour un nœud de grille, reportez-vous aux instructions de récupération et de maintenance. Pour plus d'informations sur la topologie du réseau, reportez-vous aux instructions de mise en réseau.

Réseau Grid

Obligatoire. Le réseau Grid est utilisé pour l'ensemble du trafic StorageGRID interne. Il assure la connectivité entre tous les nœuds de la grille, sur tous les sites et sous-réseaux.

Réseau d'administration

Facultatif. Le réseau d'administration est généralement utilisé pour l'administration et la maintenance du système. Il peut également être utilisé pour l'accès au protocole client. Le réseau Admin est généralement un réseau privé et n'a pas besoin d'être routable entre les sites.

Réseau client

Facultatif. Le réseau client est un réseau ouvert généralement utilisé pour fournir l'accès aux applications client S3 et Swift, de sorte que le réseau Grid puisse être isolé et sécurisé. Le réseau client peut communiquer avec tout sous-réseau accessible via la passerelle locale.

Directives

- Chaque nœud de grid StorageGRID nécessite une interface réseau dédiée, une adresse IP, un masque de sous-réseau et une passerelle pour chaque réseau auquel il est attribué.
- Un nœud de grid ne peut pas avoir plusieurs interfaces sur un réseau.
- Une passerelle unique, par réseau et par nœud grid est prise en charge et doit être sur le même sous-réseau que le nœud. Vous pouvez implémenter un routage plus complexe dans la passerelle, si nécessaire.
- Sur chaque nœud, chaque réseau est mappé à une interface réseau spécifique.

Le réseau	Nom de l'interface
Grille	eth0
Administrateur (en option)	eth1
Client (facultatif)	eth2

- Si le nœud est connecté à une appliance StorageGRID, des ports spécifiques sont utilisés pour chaque réseau. Pour plus de détails, reportez-vous aux instructions d'installation de votre appareil.
- La route par défaut est générée automatiquement, par nœud. Si eth2 est activé, 0.0.0.0/0 utilise le réseau client sur eth2. Si eth2 n'est pas activé, alors 0.0.0.0/0 utilise le réseau Grid sur eth0.
- Le réseau client n'est opérationnel qu'après que le nœud de la grille ait rejoint la grille
- Le réseau Admin peut être configuré pendant le déploiement du nœud grid pour permettre l'accès à l'interface utilisateur d'installation avant que la grille soit entièrement installée.

Informations associées

"Maintenance et récupération"

"Instructions réseau"

Affichage des adresses IP

Vous pouvez afficher l'adresse IP de chaque nœud grid dans votre système StorageGRID. Vous pouvez ensuite utiliser cette adresse IP pour vous connecter au nœud grid en ligne de commande et effectuer diverses procédures de maintenance.

Ce dont vous avez besoin

Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.

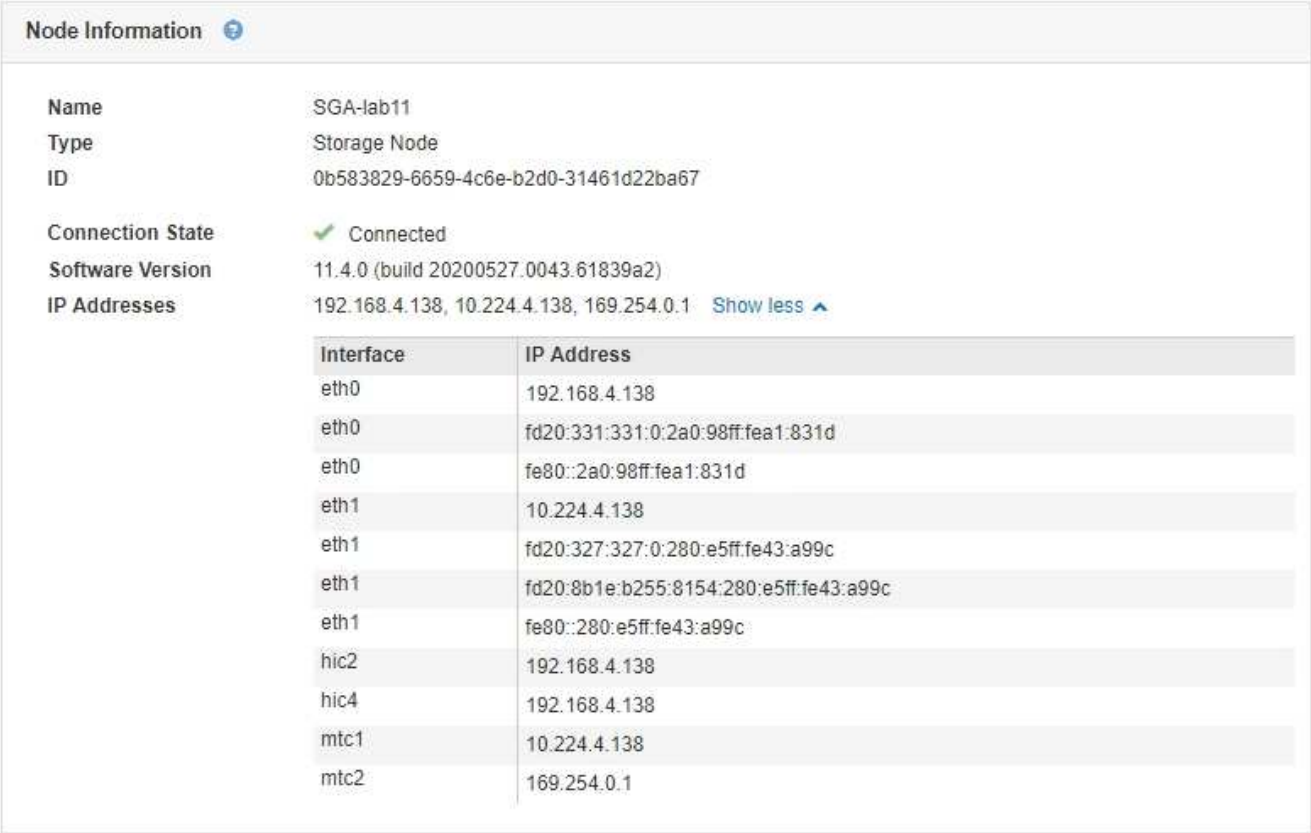
Description de la tâche

Pour plus d'informations sur la modification des adresses IP, reportez-vous aux instructions de reprise et de maintenance.

Étapes

1. Sélectionnez **Nodes** > ***grid node*** > **Overview**.
2. Cliquez sur **Afficher plus** à droite du titre adresses IP.

   Les adresses IP de ce nœud de grille sont répertoriées dans un tableau.



Node Information

Name	SGA-lab11
Type	Storage Node
ID	0b583829-6659-4c6e-b2d0-31461d22ba67
Connection State	Connected
Software Version	11.4.0 (build 20200527.0043.61839a2)
IP Addresses	192.168.4.138, 10.224.4.138, 169.254.0.1 Show less

Interface	IP Address
eth0	192.168.4.138
eth0	fd20:331:331:0:2a0:98ff:fea1:831d
eth0	fe80::2a0:98ff:fea1:831d
eth1	10.224.4.138
eth1	fd20:327:327:0:280:e5ff:fe43:a99c
eth1	fd20:8b1e:b255:8154:280:e5ff:fe43:a99c
eth1	fe80::280:e5ff:fe43:a99c
hic2	192.168.4.138
hic4	192.168.4.138
mtc1	10.224.4.138
mtc2	169.254.0.1

Informations associées

"Maintenance et récupération"

Chiffrement pris en charge pour les connexions TLS sortantes

Le système StorageGRID prend en charge un ensemble limité de suites de chiffrement pour les connexions TLS (transport Layer Security) avec les systèmes externes utilisés pour la fédération des identités et les pools de stockage cloud.

Versions supportées de TLS

StorageGRID prend en charge TLS 1.2 et TLS 1.3 pour les connexions aux systèmes externes utilisés pour la fédération des identités et les pools de stockage cloud.

Les chiffrements TLS qui sont pris en charge pour une utilisation avec des systèmes externes ont été sélectionnés pour assurer la compatibilité avec une gamme de systèmes externes. La liste est plus grande que la liste des chiffrements pris en charge pour une utilisation avec les applications client S3 ou Swift.

> Les options de configuration TLS telles que les versions de protocole, les chiffrements, les algorithmes d'échange de clés et les algorithmes MAC ne sont pas configurables en StorageGRID. Contactez votre ingénieur commercial NetApp pour toute demande spécifique concernant ces paramètres.

Suites de chiffrement TLS 1.2 prises en charge

Les suites de chiffrement TLS 1.2 suivantes sont prises en charge :

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHA20_POLY1305
- TLS_ECDHE_ECDSA_WITH_CHA20_POLY1305
- TLS_RSA_WAS_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

Suites de chiffrement TLS 1.3 prises en charge

Les suites de chiffrement TLS 1.3 suivantes sont prises en charge :

- TLS_AES_256_GCM_SHA384
- TLS_CHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

Modification du chiffrement du transfert réseau

Le système StorageGRID utilise TLS (transport Layer Security) pour protéger le trafic de contrôle interne entre les nœuds de la grille. L'option Network Transfer Encryption définit l'algorithme utilisé par TLS pour chiffrer le trafic de contrôle entre les nœuds de la grille. Ce paramètre n'affecte pas le chiffrement des données.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Par défaut, le chiffrement de transfert réseau utilise l'algorithme AES256-SHA. Le trafic de contrôle peut également être crypté à l'aide de l'algorithme AES128-SHA.

Étapes

1. Sélectionnez **Configuration** > **Paramètres système** > **Options de grille**.

2. Dans la section Options réseau, définissez cryptage de transfert réseau sur **AES128-SHA** ou **AES256-SHA** (par défaut).

3. Cliquez sur **Enregistrer**.

Configuration des certificats de serveur

Vous pouvez personnaliser les certificats de serveur utilisés par le système StorageGRID.

Le système StorageGRID utilise des certificats de sécurité à diverses fins :

- Certificats de serveur de l'interface de gestion : utilisés pour sécuriser l'accès à Grid Manager, au tenant Manager, à l'API de gestion du grid et à l'API de gestion des locataires.
- Certificats de serveur d'API de stockage : utilisés pour sécuriser l'accès aux nœuds de stockage et aux nœuds de passerelle, que les applications client d'API utilisent pour charger et télécharger les données d'objet.

Vous pouvez utiliser les certificats par défaut créés lors de l'installation ou remplacer l'un ou l'autre de ces types de certificats par défaut par vos propres certificats personnalisés.

Types pris en charge de certificat de serveur personnalisé

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

Pour plus d'informations sur la sécurisation des connexions clients par StorageGRID pour l'API REST, consultez les guides d'implémentation S3 ou Swift.

Certificats pour les noeuds finaux de l'équilibreur de charge

StorageGRID gère séparément les certificats utilisés pour les terminaux de l'équilibreur de charge. Pour configurer des certificats d'équilibreur de charge, reportez-vous aux instructions de configuration des noeuds finaux d'équilibreur de charge.

Informations associées

"Utilisation de S3"

"Utiliser Swift"

"Configuration des terminaux d'équilibrage de charge"

Configuration d'un certificat de serveur personnalisé pour le Grid Manager et le tenant Manager

Vous pouvez remplacer le certificat de serveur StorageGRID par défaut par un seul certificat de serveur personnalisé qui permet aux utilisateurs d'accéder au Gestionnaire de grille et au Gestionnaire de locataires sans rencontrer d'avertissements de sécurité.

Description de la tâche

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

Comme un seul certificat de serveur personnalisé est utilisé pour tous les nœuds d'administration, vous devez spécifier le certificat en tant que certificat générique ou multidomaine si les clients doivent vérifier le nom d'hôte lors de la connexion à Grid Manager et au Gestionnaire de locataires. Définissez le certificat personnalisé de sorte qu'il corresponde à tous les nœuds d'administration de la grille.

Vous devez terminer la configuration sur le serveur et, selon l'autorité de certification racine (AC) que vous utilisez, les utilisateurs devront peut-être aussi installer le certificat d'autorité de certification racine dans le navigateur Web qu'ils utiliseront pour accéder au gestionnaire de grille et au gestionnaire de tenant.

> Pour garantir que les opérations ne sont pas interrompues par un certificat de serveur défaillant, l'alerte **expiration du certificat de serveur pour l'interface de gestion** et l'alarme expiration du certificat de l'interface de gestion héritée (MCEP) sont toutes deux déclenchées lorsque ce certificat de serveur est sur le point d'expirer. Si nécessaire, vous pouvez afficher le nombre de jours jusqu'à l'expiration du certificat de service en cours en sélectionnant **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***primary Admin Node*** > **CMN** > **Resources**.

> Si vous accédez à Grid Manager ou au Gestionnaire de locataires à l'aide d'un nom de domaine au lieu d'une adresse IP, le navigateur affiche une erreur de certificat sans option de contournement si l'un des cas suivants se produit :
>
> - Votre certificat de serveur de l'interface de gestion personnalisée expire.
> - Vous restaurez un certificat de serveur d'interface de gestion personnalisée vers le certificat de serveur par défaut.

Étapes

1. Sélectionnez **Configuration** > **Paramètres réseau** > **certificats serveur**.
2. Dans la section certificat du serveur de l'interface de gestion, cliquez sur **installer le certificat personnalisé**.
3. Téléchargez les fichiers de certificat de serveur requis :
   - **Certificat de serveur** : fichier de certificat de serveur personnalisé (`.crt`).
   - **Clé privée de certificat de serveur** : fichier de clé privée de certificat de serveur personnalisé (`.key`).

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

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

4. Cliquez sur **Enregistrer**.

   Les certificats de serveur personnalisés sont utilisés pour toutes les nouvelles connexions client suivantes.

   Sélectionnez un onglet pour afficher des informations détaillées sur le certificat de serveur StorageGRID par défaut ou sur un certificat signé par l'autorité de certification qui a été téléchargé.

   > Après avoir téléchargé un nouveau certificat, autorisez jusqu'à un jour l'effacement des alertes d'expiration de certificat (ou des alarmes héritées) associées.

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

Restauration des certificats de serveur par défaut pour le Grid Manager et le tenant Manager

Vous pouvez revenir à l'utilisation des certificats de serveur par défaut pour le Grid Manager et le tenant Manager.

Étapes

1. Sélectionnez **Configuration** > **Paramètres réseau** > **certificats serveur**.
2. Dans la section gérer le certificat du serveur d'interface, cliquez sur **utiliser les certificats par défaut**.
3. Cliquez sur **OK** dans la boîte de dialogue de confirmation.

   Lorsque vous restaurez les certificats de serveur par défaut, les fichiers de certificat de serveur personnalisés que vous avez configurés sont supprimés et ne peuvent pas être récupérés du système. Les certificats de serveur par défaut sont utilisés pour toutes les nouvelles connexions client suivantes.

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

Configuration d'un certificat de serveur personnalisé pour les connexions au nœud de stockage ou au service CLB

Vous pouvez remplacer le certificat de serveur utilisé pour les connexions des clients S3 ou Swift vers le nœud de stockage ou vers le service CLB (obsolète) sur le nœud de passerelle. Le certificat de serveur personnalisé de remplacement est spécifique à votre organisation.

Description de la tâche

Par défaut, chaque nœud de stockage est doté d'un certificat de serveur X.509 signé par l'autorité de certification de la grille. Ces certificats signés par l'autorité de certification peuvent être remplacés par un seul certificat de serveur personnalisé commun et une clé privée correspondante.

Un seul certificat de serveur personnalisé est utilisé pour tous les nœuds de stockage. Vous devez donc spécifier le certificat comme un certificat générique ou multidomaine si les clients doivent vérifier le nom d'hôte lors de la connexion au noeud final de stockage. Définissez le certificat personnalisé de sorte qu'il corresponde à tous les nœuds de stockage de la grille.

Une fois la configuration terminée sur le serveur, les utilisateurs peuvent également avoir besoin d'installer le certificat d'autorité de certification racine dans le client API S3 ou Swift qu'ils utiliseront pour accéder au système, selon l'autorité de certification racine que vous utilisez.

> Pour garantir que les opérations ne sont pas interrompues par un échec du certificat de serveur, l'alerte **expiration du certificat de serveur pour les noeuds finaux de l'API de stockage** et l'alarme expiration du certificat de noeuds finaux du service de l'API de stockage héritée sont toutes deux déclenchées lorsque le certificat de serveur racine est sur le point d'expirer. Si nécessaire, vous pouvez afficher le nombre de jours jusqu'à l'expiration du certificat de service en cours en sélectionnant **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***primary Admin Node*** > **CMN** > **Resources**.

Les certificats personnalisés sont utilisés uniquement si les clients se connectent à StorageGRID à l'aide du service CLB obsolète sur les nœuds de passerelle ou s'ils se connectent directement aux nœuds de stockage. Les clients S3 ou Swift qui se connectent à StorageGRID via le service Load Balancer sur les nœuds d'administration ou les nœuds de passerelle utilisent le certificat configuré pour le terminal de l'équilibreur de charge.

> L'alerte **expiration du certificat de point final de l'équilibreur de charge** est déclenchée pour les noeuds finaux de l'équilibreur de charge qui expirent bientôt.

Étapes

1. Sélectionnez **Configuration** > **Paramètres réseau** > **certificats serveur**.
2. Dans la section certificat de serveur de noeuds finaux du service API de stockage d'objets, cliquez sur **installer le certificat personnalisé**.
3. Téléchargez les fichiers de certificat de serveur requis :
   - **Certificat de serveur** : fichier de certificat de serveur personnalisé (`.crt`).
   - **Clé privée de certificat de serveur** : fichier de clé privée de certificat de serveur personnalisé (`.key`).

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

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

   Le certificat de serveur personnalisé est utilisé pour toutes les nouvelles connexions client API suivantes.

   Sélectionnez un onglet pour afficher des informations détaillées sur le certificat de serveur StorageGRID par défaut ou sur un certificat signé par l'autorité de certification qui a été téléchargé.

   > Après avoir téléchargé un nouveau certificat, autorisez jusqu'à un jour l'effacement des alertes d'expiration de certificat (ou des alarmes héritées) associées.

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

Informations associées

"Utilisation de S3"

"Utiliser Swift"

"Configuration des noms de domaine de terminaux API S3"

Restauration des certificats de serveur par défaut pour les terminaux API REST S3 et Swift

Vous pouvez revenir à l'utilisation des certificats de serveur par défaut pour les terminaux API REST S3 et Swift.

Étapes

1. Sélectionnez **Configuration** > **Paramètres réseau** > **certificats serveur**.
2. Dans la section certificat de serveur de noeuds finaux du service API de stockage d'objets, cliquez sur **utiliser les certificats par défaut**.
3. Cliquez sur **OK** dans la boîte de dialogue de confirmation.

   Lorsque vous restaurez les certificats de serveur par défaut pour les noeuds finaux de l'API de stockage d'objets, les fichiers de certificat de serveur personnalisés que vous avez configurés sont supprimés et ne peuvent pas être récupérés du système. Les certificats de serveur par défaut sont utilisés pour toutes les nouvelles connexions client API suivantes.

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

Copie du certificat de l'autorité de certification du système StorageGRID

StorageGRID utilise une autorité de certification interne pour sécuriser le trafic interne. Ce certificat ne change pas si vous téléchargez vos propres certificats.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

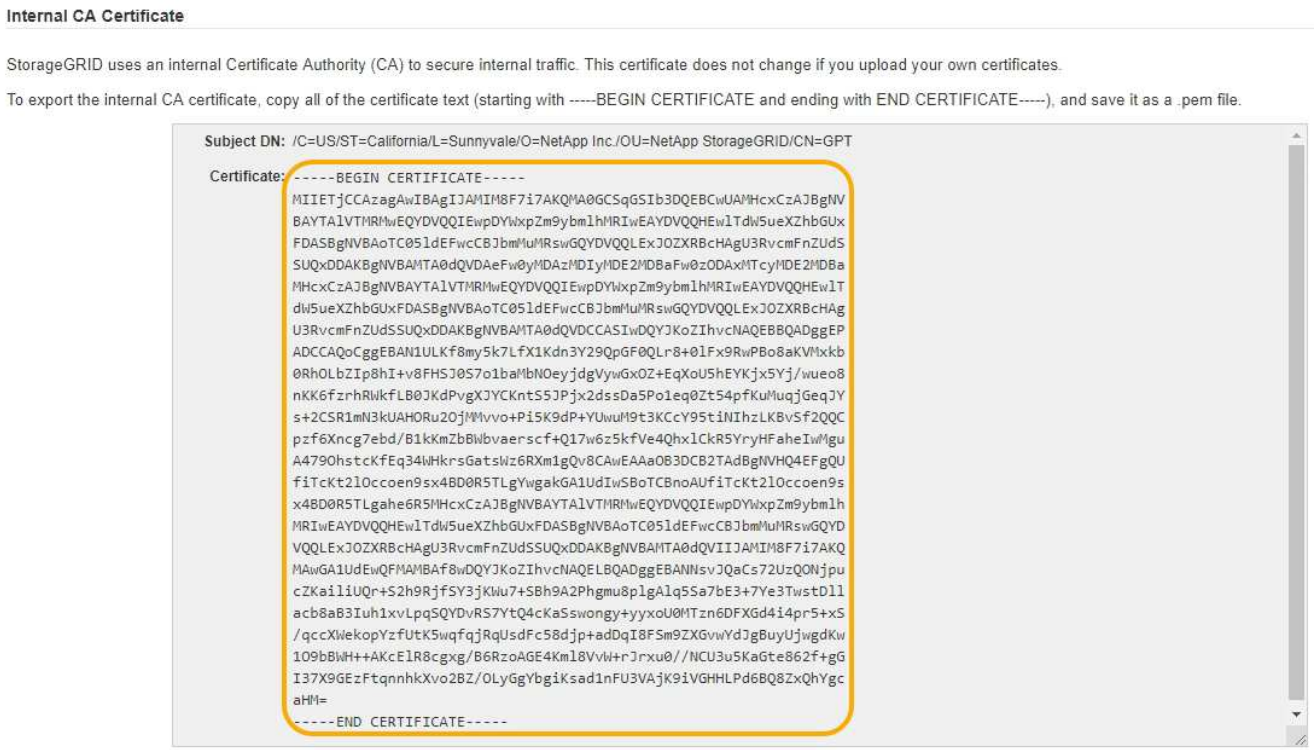
Description de la tâche

Si un certificat de serveur personnalisé a été configuré, les applications client doivent vérifier le serveur à l'aide du certificat de serveur personnalisé. Ils ne doivent pas copier le certificat de l'autorité de certification depuis le système StorageGRID.

Étapes

1. Sélectionnez **Configuration** > **Paramètres réseau** > **certificats serveur**.
2. Dans la section **certificat CA interne**, sélectionnez tout le texte du certificat.

   Vous devez inclure `-----BEGIN CERTIFICATE-----` et `-----END CERTIFICATE-----` dans votre sélection.



3. Cliquez avec le bouton droit de la souris sur le texte sélectionné et sélectionnez **Copier**.
4. Collez le certificat copié dans un éditeur de texte.
5. Enregistrez le fichier avec l'extension `.pem`.

   Par exemple : `storagegrid_certificate.pem`

Configuration des certificats StorageGRID pour FabricPool

Pour les clients S3 qui effectuent une validation stricte du nom d'hôte et qui ne prennent pas en charge la désactivation de la validation stricte du nom d'hôte, comme les clients ONTAP utilisant FabricPool, vous pouvez générer ou charger un certificat de serveur lors de la configuration du point de terminaison de l'équilibreur de charge.

Ce dont vous avez besoin

- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.

Description de la tâche

Lorsque vous créez un noeud final de l'équilibreur de charge, vous pouvez générer un certificat de serveur auto-signé ou télécharger un certificat signé par une autorité de certification connue. Dans les environnements de production, vous devez utiliser un certificat signé par une autorité de certification connue. Les certificats signés par une autorité de certification peuvent être pivotés sans interruption. Elles sont également plus sécurisées parce qu'elles offrent une meilleure protection contre les attaques de l'homme au milieu.

Les étapes suivantes fournissent des instructions d'ordre général pour les clients S3 qui utilisent FabricPool. Pour plus d'informations et de procédures, reportez-vous aux instructions de configuration de StorageGRID pour FabricPool.

> Le service distinct Connection Load Balancer (CLB) sur les nœuds de passerelle est obsolète et n'est plus recommandé pour une utilisation avec FabricPool.

Étapes

1. Configurez également un groupe haute disponibilité (HA) pour FabricPool à utiliser.
2. Créez un terminal d'équilibrage de charge S3 pour FabricPool.

   Lorsque vous créez un noeud final d'équilibreur de charge HTTPS, vous êtes invité à télécharger votre certificat de serveur, votre clé privée de certificat et votre bundle CA.

3. Association de StorageGRID en tant que Tier cloud dans ONTAP

   Spécifiez le port de point final de l'équilibreur de charge et le nom de domaine complet utilisé dans le certificat de l'autorité de certification que vous avez téléchargé. Ensuite, indiquez le certificat de l'autorité de certification.

   > Si une autorité de certification intermédiaire a émis le certificat StorageGRID, vous devez fournir le certificat CA intermédiaire. Si le certificat StorageGRID a été émis directement par l'autorité de certification racine, vous devez fournir le certificat d'autorité de certification racine.

Informations associées

"Configuration de StorageGRID pour FabricPool"

Génération d'un certificat de serveur auto-signé pour l'interface de gestion

Vous pouvez utiliser un script pour générer un certificat de serveur auto-signé pour les clients de l'API de gestion nécessitant une validation stricte du nom d'hôte.

Ce dont vous avez besoin

- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir le `Passwords.txt` fichier.

Description de la tâche

Dans les environnements de production, vous devez utiliser un certificat signé par une autorité de certification connue. Les certificats signés par une autorité de certification peuvent être pivotés sans interruption. Elles sont également plus sécurisées parce qu'elles offrent une meilleure protection contre les attaques de l'homme au milieu.

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. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

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

3. Configurez StorageGRID avec un nouveau certificat auto-signé.

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

   - Pour `--domains`, Utilisez des caractères génériques pour représenter les noms de domaine complets de tous les nœuds d'administration. Par exemple : `*.ui.storagegrid.example.com` utilise le caractère générique * pour représenter `admin1.ui.storagegrid.example.com` et `admin2.ui.storagegrid.example.com`.
   - Réglez `--type` à `management` Pour configurer le certificat utilisé par Grid Manager et tenant Manager.
   - Par défaut, les certificats générés sont valables pendant un an (365 jours) et doivent être recréés avant leur expiration. Vous pouvez utiliser le `--days` argument pour remplacer la période de validité par défaut.

> La période de validité d'un certificat commence quand `make-certificate` est exécuté. Vous devez vous assurer que le client de l'API de gestion est synchronisé avec la même source que StorageGRID ; sinon, le client peut rejeter le certificat.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 365
```

   Le résultat contient le certificat public requis par votre client de l'API de gestion.

4. Sélectionnez et copiez le certificat.

   Incluez les étiquettes DE DÉBUT et DE FIN dans votre sélection.

5. Déconnectez-vous du shell de commande. `$ exit`
6. Vérifiez que le certificat a été configuré :
   a. Accédez au Grid Manager.
   b. Sélectionnez **Configuration** > **certificats de serveur** > **certificat de serveur d'interface de gestion**.
7. Configurez votre client de l'API de gestion pour utiliser le certificat public que vous avez copié. Incluez les balises DE DÉBUT et DE FIN.

Configuration des paramètres du proxy de stockage

Si vous utilisez des services de plateforme ou des pools de stockage cloud, vous pouvez configurer un proxy non transparent entre les nœuds de stockage et les terminaux S3 externes. Par exemple, vous aurez peut-être besoin d'un proxy non transparent pour permettre l'envoi de messages de services de plate-forme vers des noeuds finaux externes, tels qu'un noeud final sur Internet.

Ce dont vous avez besoin

- Vous devez disposer d'autorisations d'accès spécifiques.

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.

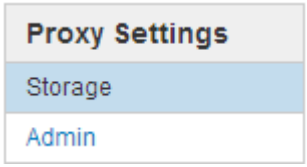
Description de la tâche

Vous pouvez configurer les paramètres d'un proxy de stockage unique.

Étapes

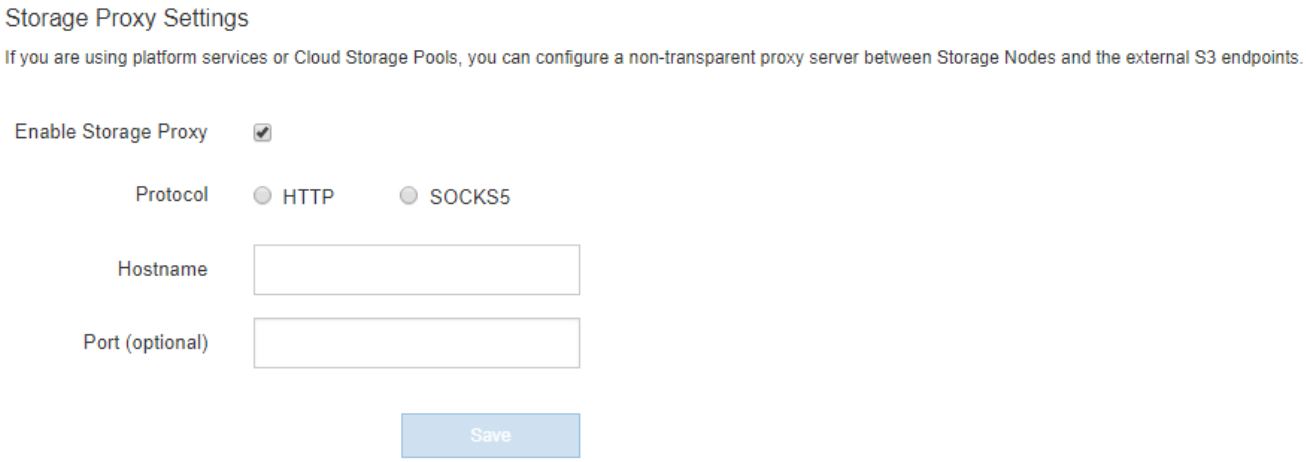
1. Sélectionnez **Configuration** > **Paramètres réseau** > **Paramètres proxy**.

   La page Paramètres du proxy de stockage s'affiche. Par défaut, **Storage** est sélectionné dans le menu de la barre latérale.

2. Cochez la case **Activer le proxy de stockage**.

   Les champs de configuration d'un proxy de stockage s'affichent.

3. Sélectionnez le protocole du proxy de stockage non transparent.
4. Entrez le nom d'hôte ou l'adresse IP du serveur proxy.
5. Vous pouvez également saisir le port utilisé pour vous connecter au serveur proxy.

   Vous pouvez laisser ce champ vide si vous utilisez le port par défaut pour le protocole : 80 pour HTTP ou 1080 pour SOCKS5.

6. Cliquez sur **Enregistrer**.

   Une fois le proxy de stockage enregistré, de nouveaux terminaux pour les services de plateforme ou les pools de stockage cloud peuvent être configurés et testés.

   > Les modifications de proxy peuvent prendre jusqu'à 10 minutes.

7. Vérifiez les paramètres de votre serveur proxy pour vous assurer que les messages relatifs au service de la plate-forme de StorageGRID ne seront pas bloqués.

Une fois que vous avez terminé

Si vous devez désactiver un proxy de stockage, décochez la case **Activer le proxy de stockage**, puis cliquez sur **Enregistrer**.

Informations associées

"Réseaux et ports pour les services de plate-forme"

"Gestion des objets avec ILM"

Configuration des paramètres du proxy d'administration

Si vous envoyez des messages AutoSupport via HTTP ou HTTPS, vous pouvez configurer un serveur proxy non transparent entre les nœuds d'administration et le support technique (AutoSupport).

Ce dont vous avez besoin

- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.

Description de la tâche

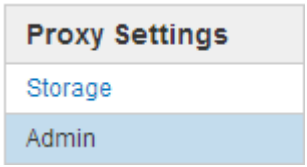
Vous pouvez configurer les paramètres d'un proxy d'administration unique.

Étapes

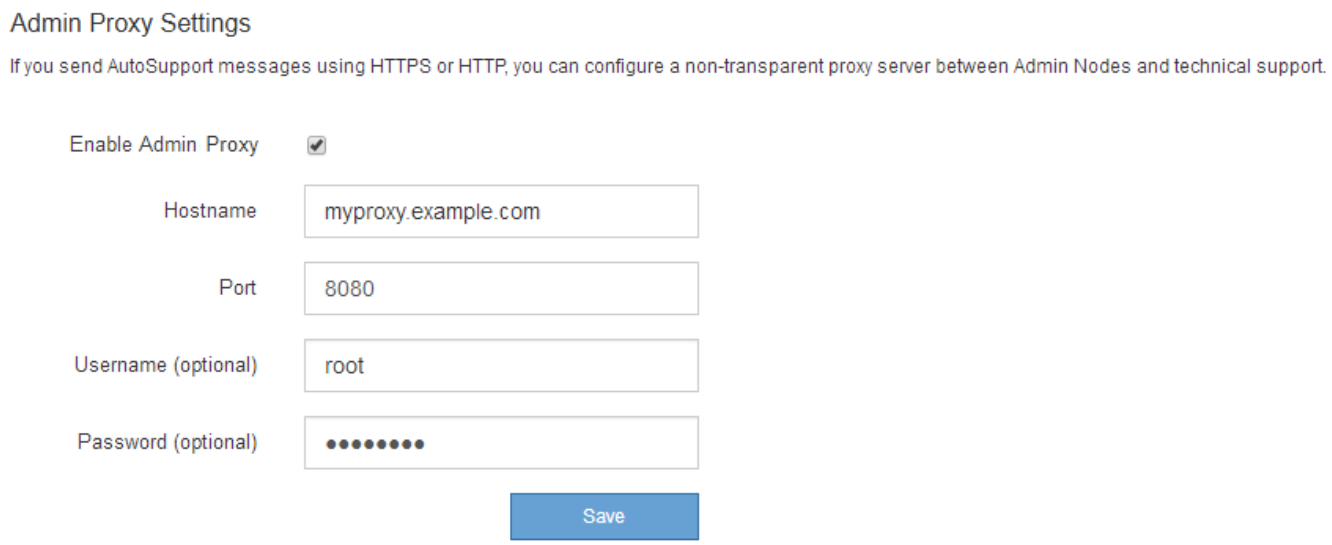
1. Sélectionnez **Configuration** > **Paramètres réseau** > **Paramètres proxy**.

   La page Paramètres du proxy administrateur s'affiche. Par défaut, **Storage** est sélectionné dans le menu de la barre latérale.

2. Dans le menu barre latérale, sélectionnez **Admin**.

3. Cochez la case **Activer le proxy d'administration**.



4. Entrez le nom d'hôte ou l'adresse IP du serveur proxy.
5. Entrez le port utilisé pour se connecter au serveur proxy.
6. Vous pouvez également saisir le nom d'utilisateur du proxy.

   Laissez ce champ vide si votre serveur proxy ne nécessite pas de nom d'utilisateur.

7. Vous pouvez également saisir le mot de passe du proxy.

   Laissez ce champ vide si votre serveur proxy ne nécessite pas de mot de passe.

8. Cliquez sur **Enregistrer**.

   Une fois le proxy d'administration enregistré, le serveur proxy entre les nœuds d'administration et le support technique est configuré.

   > Les modifications de proxy peuvent prendre jusqu'à 10 minutes.

9. Si vous devez désactiver le proxy, décochez la case **Activer le proxy d'administration**, puis cliquez sur **Enregistrer**.

Informations associées

"Spécification du protocole des messages AutoSupport"

Gestion des stratégies de classification du trafic

Pour améliorer vos offres de qualité de service (QoS), vous pouvez créer des stratégies de classification du trafic afin d'identifier et de surveiller différents types de trafic réseau. Ces règles peuvent vous aider à limiter le trafic et à surveiller le trafic.

Les règles de classification du trafic sont appliquées aux terminaux du service StorageGRID Load Balancer pour les nœuds de passerelle et les nœuds d'administration. Pour créer des stratégies de classification de trafic, vous devez avoir déjà créé des points d'extrémité d'équilibreur de charge.

Règles de mise en correspondance et limites facultatives

Chaque règle de classification de trafic contient une ou plusieurs règles de correspondance permettant d'identifier le trafic réseau lié à une ou plusieurs des entités suivantes :

- Seaux
- Locataires
- Sous-réseaux (sous-réseaux IPv4 contenant le client)
- Terminaux (terminaux d'équilibrage de charge)

StorageGRID surveille le trafic qui correspond à n'importe quelle règle de la stratégie conformément aux objectifs de la règle. Tout trafic qui correspond à une règle d'une stratégie est géré par cette règle. Inversement, vous pouvez définir des règles qui correspondent à tout le trafic, à l'exception d'une entité spécifiée.

Vous pouvez également définir des limites pour une stratégie en fonction des paramètres suivants :

- Bande passante agrégée dans
- Bande passante de l'agrégat sortie
- Demandes de lecture simultanée
- Demandes d'écriture simultanées
- Bande passante par demande dans
- Bande passante à la demande
- Taux de demande de lecture
- Taux de demandes d'écriture

> Vous pouvez créer des règles pour limiter la bande passante agrégée ou limiter la bande passante par requête. Cependant, StorageGRID ne peut pas limiter simultanément les deux types de bande passante. Les limites de bande passante globales peuvent imposer un impact mineur supplémentaire sur les performances du trafic non limité.

Limitation du trafic

Lorsque vous avez créé des politiques de classification du trafic, le trafic est limité en fonction du type de règles et de limites que vous avez définies. Pour les limites de bande passante globale ou par requête, les demandes sont envoyées vers l'intérieur ou vers l'extérieur au débit défini. StorageGRID ne peut appliquer qu'une seule vitesse. La correspondance des règles la plus spécifique, par type de contrôleur, est donc la plus appliquée. Pour tous les autres types de limite, les demandes des clients sont retardées de 250 millisecondes et reçoivent une réponse lente de 503 pour les demandes dépassant toute limite de stratégie correspondante.

Dans Grid Manager, vous pouvez afficher les diagrammes de trafic et vérifier que les stratégies appliquent les limites de trafic que vous attendez.

Utilisation de stratégies de classification du trafic avec des contrats de niveau de service

Vous pouvez utiliser des règles de classification du trafic en association avec les limites de capacité et la protection des données pour appliquer des accords de niveau de service (SLA) qui fournissent des spécificités en matière de capacité, de protection des données et de performances.

Les limites de classification du trafic sont mises en œuvre par équilibreur de charge. Si le trafic est réparti

simultanément sur plusieurs équilibreurs de charge, les débits maximaux totaux sont un multiple des limites de débit que vous spécifiez.

L'exemple suivant montre trois niveaux d'un SLA. Vous pouvez créer des règles de classification du trafic pour atteindre les objectifs de performances de chaque niveau de contrat de niveau de service.

Niveau de service	Puissance	La protection des données	Performance	Le coût
Or	1 po de stockage autorisé	Règle ILM de 3 copies	25 000 demandes/s Bande passante de 5 Go/s (40 Gbit/s)	par mois
Argent	Stockage de 250 To autorisé	Règle ILM 2 copies	10 000 demandes/s Bande passante de 1.25 Go/s (10 Gbit/s)	$$ par mois
Bronze	Stockage de 100 To autorisé	Règle ILM 2 copies	5 000 demandes/s Bande passante de 1 Go/s (8 Gbit/s)	$ par mois

Création de stratégies de classification de trafic

Vous créez des règles de classification du trafic pour surveiller et limiter, éventuellement, le trafic réseau par compartiment, locataire, sous-réseau IP ou point de terminaison d'équilibrage de la charge. Vous pouvez également définir des limites pour une stratégie en fonction de la bande passante, du nombre de demandes simultanées ou du taux de demande.

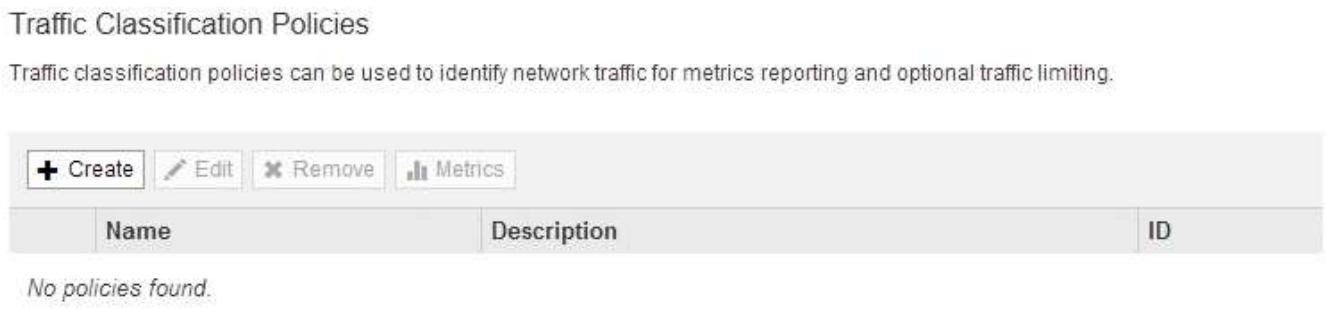
Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation accès racine.
- Vous devez avoir créé tous les noeuds finaux de l'équilibreur de charge que vous souhaitez associer.
- Vous devez avoir créé les locataires que vous souhaitez associer.

Étapes

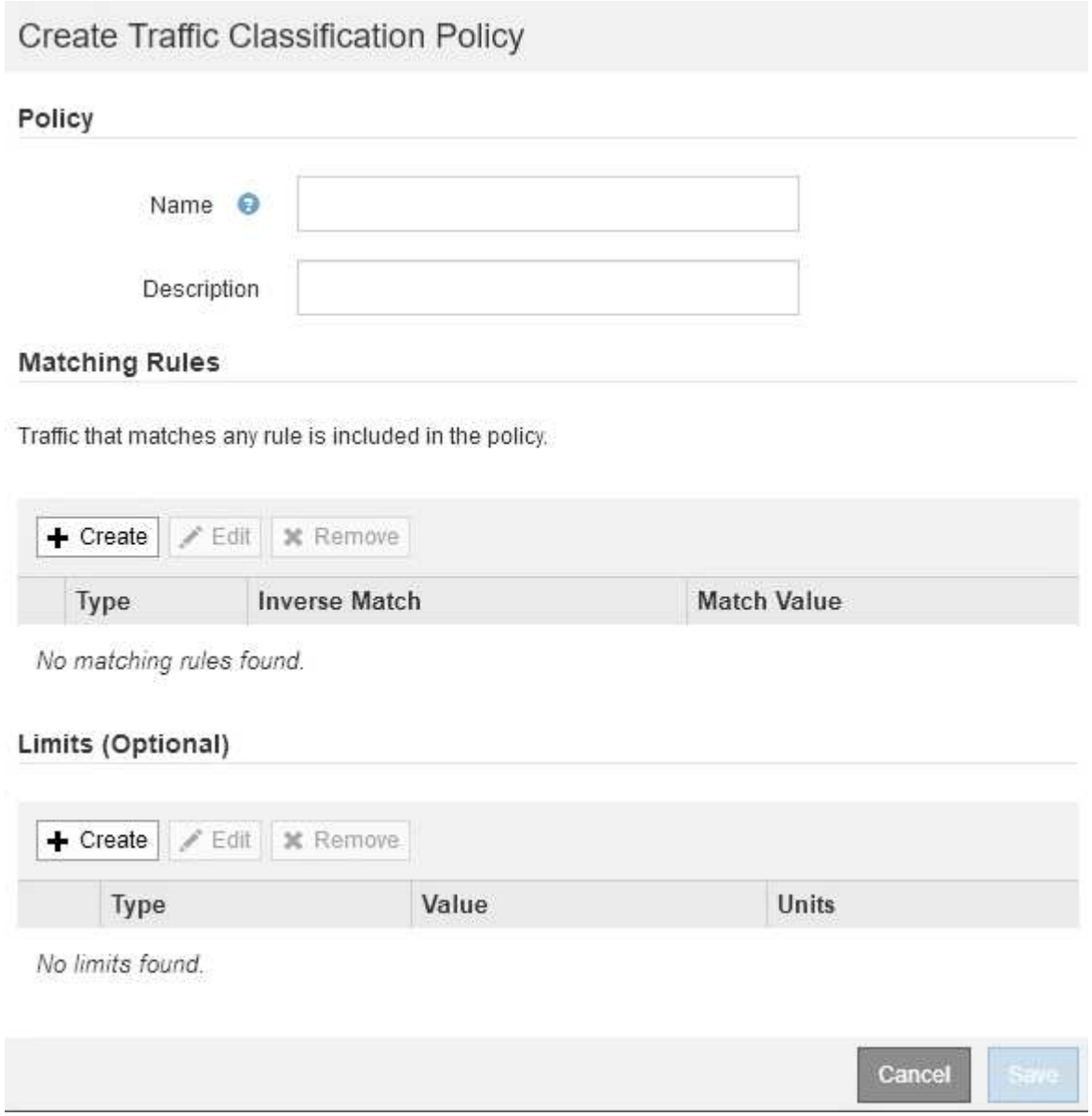
1. Sélectionnez **Configuration** > **Paramètres réseau** > **Classification du trafic**.

   La page règles de classification du trafic s'affiche.



2. Cliquez sur **Créer**.

   La boîte de dialogue Créer une stratégie de classification de trafic s'affiche.



3. Dans le champ **Nom**, entrez un nom pour la stratégie.

   Entrez un nom descriptif pour reconnaître la stratégie.

4. Vous pouvez également ajouter une description de la stratégie dans le champ **Description**.

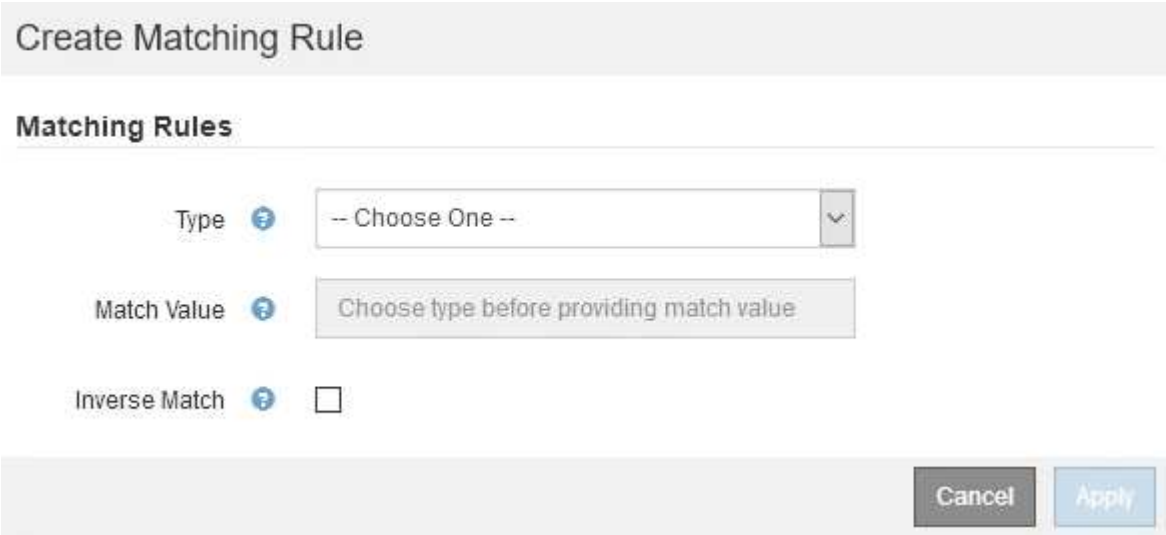
   Par exemple, décrivez à quoi s'applique cette politique de classification de trafic et à quoi elle limite.

5. Créer une ou plusieurs règles de correspondance pour la règle.

   Les règles de correspondance contrôlent les entités qui seront affectées par cette politique de classification du trafic. Par exemple, sélectionnez tenant si vous souhaitez que cette stratégie s'applique au trafic réseau d'un locataire spécifique. Ou sélectionnez point final si vous souhaitez que cette stratégie s'applique au trafic réseau sur un point final d'équilibreur de charge spécifique.

   a. Cliquez sur **Créer** dans la section **règles de correspondance**.

      La boîte de dialogue Créer une règle de correspondance s'affiche.



   b. Dans la liste déroulante **Type**, sélectionnez le type d'entité à inclure dans la règle correspondante.
   c. Dans le champ **valeur de correspondance**, entrez une valeur de correspondance basée sur le type d'entité que vous avez choisi.
      - Compartiment : entrez un nom de compartiment.
      - Regex du compartiment : saisissez une expression régulière qui sera utilisée pour correspondre à un ensemble de noms de compartiment.

        L'expression régulière n'est pas ancrée. Utilisez l'ancre ^ pour faire correspondre au début du nom du compartiment, et utilisez l'ancre $ pour correspondre à la fin du nom.

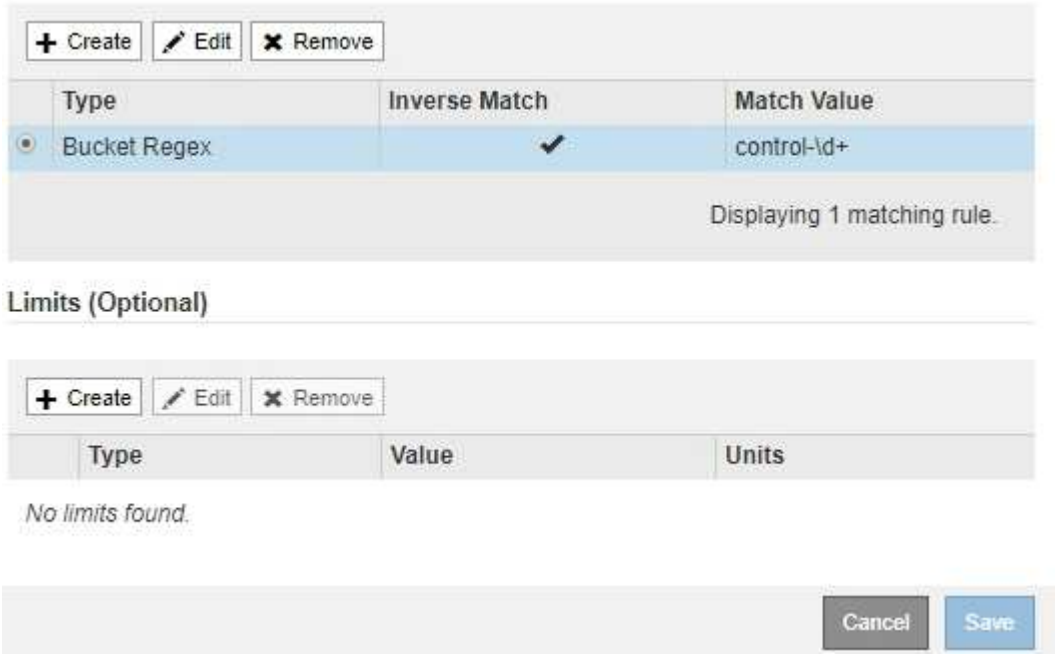
      - CIDR : saisissez un sous-réseau IPv4, en notation CIDR, qui correspond au sous-réseau souhaité.
      - Noeud final : sélectionnez un noeud final dans la liste des noeuds finaux existants. Il s'agit des noeuds finaux de l'équilibreur de charge que vous avez définis sur la page noeuds finaux de l'équilibreur de charge.
      - Locataire : sélectionnez un locataire dans la liste des locataires existants. La correspondance établie entre les locataires dépend de la propriété du compartiment utilisé. L'accès anonyme à un compartiment correspond au locataire qui détient le compartiment.
   d. Si vous souhaitez faire correspondre tout le trafic réseau *exception* trafic correspondant au type et à la valeur de correspondance que vous venez de définir, cochez la case **inverse**. Sinon, ne cochez pas la case.

Par exemple, si vous souhaitez que cette stratégie s'applique à tous les noeuds finaux de l'équilibreur de charge sauf un, spécifiez le noeud final de l'équilibreur de charge à exclure et sélectionnez **inverse**.

> Dans le cas d'une règle contenant plusieurs matcheurs où au moins un est un matcher inverse, veillez à ne pas créer une règle qui correspond à toutes les demandes.

e. Cliquez sur **appliquer**.

La règle est créée et répertoriée dans le tableau règles de correspondance.



a. Répétez ces étapes pour chaque règle que vous souhaitez créer pour la règle.

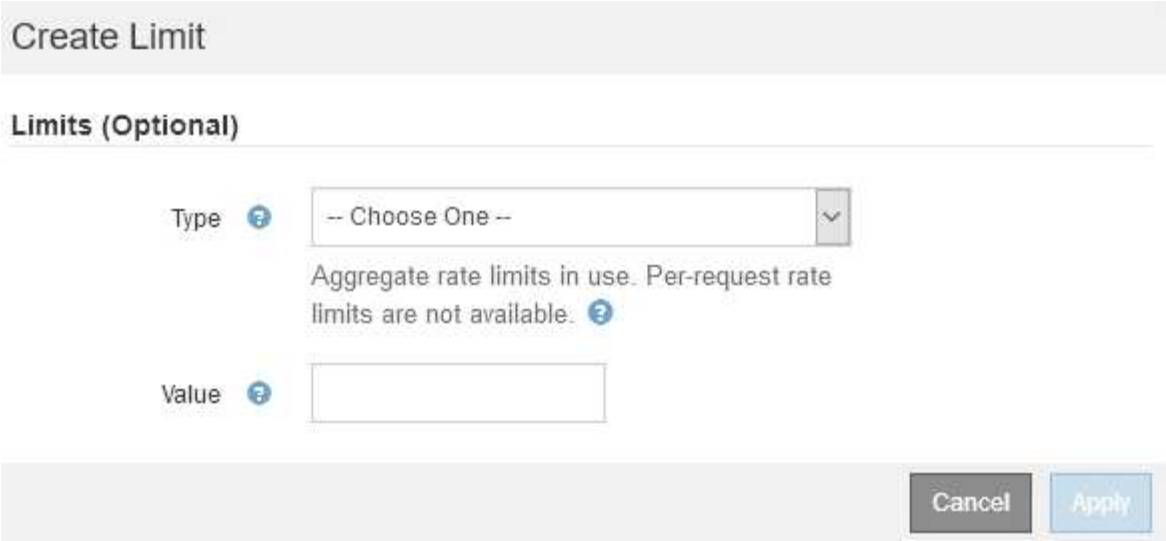
> Le trafic correspondant à n'importe quelle règle est géré par la règle.

6. Vous avez la possibilité de créer des limites pour la règle.

> Même si vous ne créez pas de limites, StorageGRID collecte des mesures pour vous permettre de surveiller le trafic réseau qui correspond à la stratégie.

a. Cliquez sur **Créer** dans la section **limites**.

La boîte de dialogue Créer limite s'affiche.



b. Dans la liste déroulante **Type**, sélectionnez le type de limite que vous souhaitez appliquer à la stratégie.

   Dans la liste suivante, **in** désigne le trafic des clients S3 ou Swift vers l'équilibreur de charge StorageGRID et **OUT** désigne le trafic de l'équilibreur de charge vers les clients S3 ou Swift.

   - Bande passante agrégée dans
   - Bande passante de l'agrégat sortie
   - Demandes de lecture simultanée
   - Demandes d'écriture simultanées
   - Bande passante par demande dans
   - Bande passante à la demande
   - Taux de demande de lecture
   - Taux de demandes d'écriture

   > Vous pouvez créer des règles pour limiter la bande passante agrégée ou limiter la bande passante par requête. Cependant, StorageGRID ne peut pas limiter simultanément les deux types de bande passante. Les limites de bande passante globales peuvent imposer un impact mineur supplémentaire sur les performances du trafic non limité.

   Pour les limites de bande passante, StorageGRID applique la règle qui correspond le mieux au type de limite défini. Par exemple, si vous avez une stratégie qui limite le trafic dans une seule direction, alors le trafic dans la direction opposée sera illimité, même s'il y a un trafic qui correspond à des stratégies supplémentaires qui ont des limites de bande passante. StorageGRID met en œuvre des correspondances « meilleures » pour les limites de bande passante dans l'ordre suivant :

   - Adresse IP exacte (/32 masque)
   - Nom exact du compartiment
   - Seau regex
   - Locataire

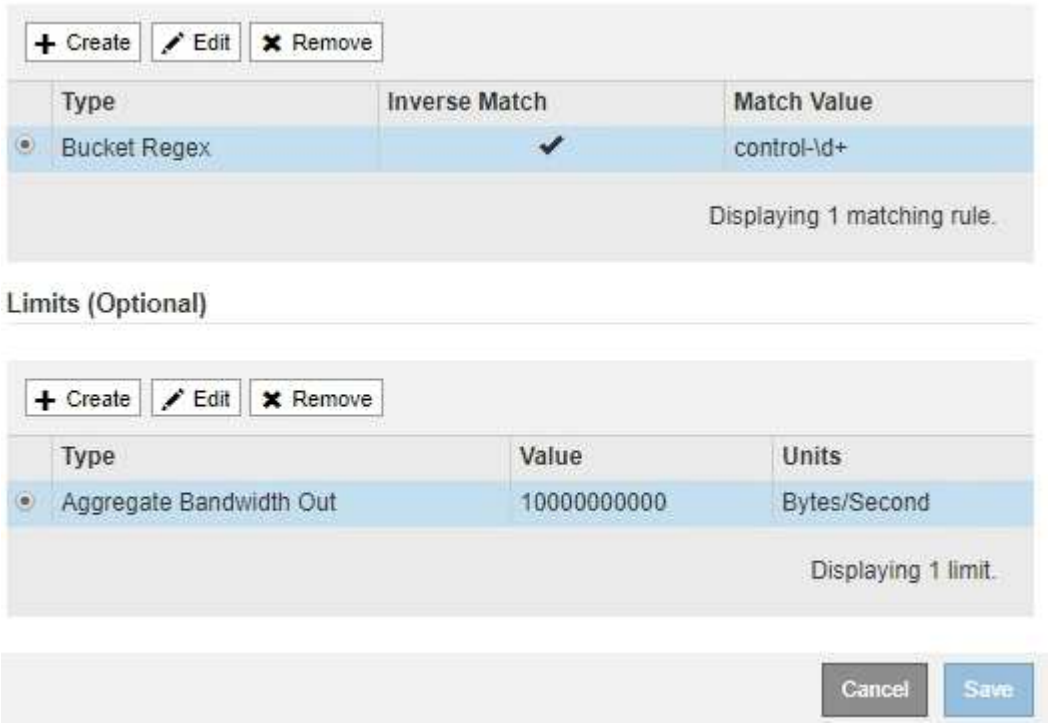
- Point final
- Correspondances CIDR non exactes (pas /32)
- Correspondances inverses

c. Dans le champ **valeur**, entrez une valeur numérique pour le type de limite que vous avez choisi.

   Les unités attendues s'affichent lorsque vous sélectionnez une limite.

d. Cliquez sur **appliquer**.

   La limite est créée et est répertoriée dans le tableau limites.



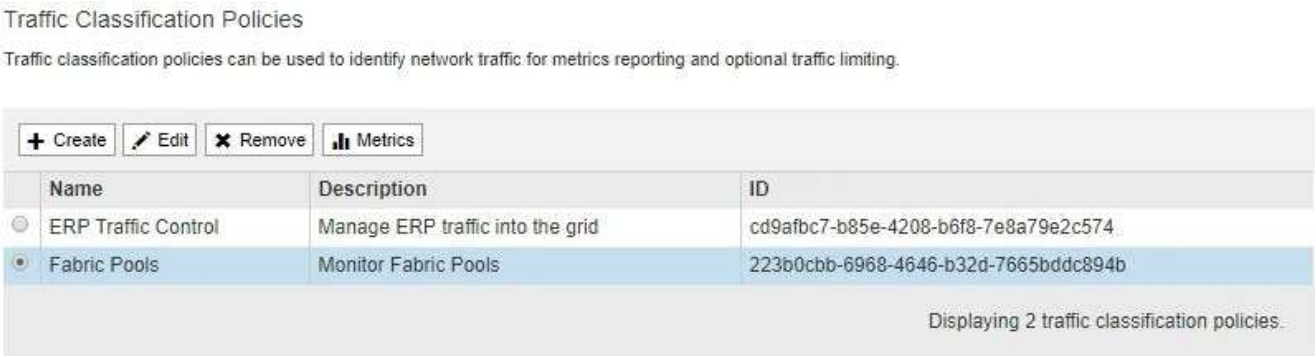
e. Répétez ces étapes pour chaque limite que vous souhaitez ajouter à la stratégie.

   Par exemple, si vous souhaitez créer une limite de bande passante de 40 Gbits/s pour un niveau de contrat de niveau de service, créez une limite de bande passante agrégée et une limite de bande passante agrégée OUT et définissez chacune sur 40 Gbits/s.

   Pour convertir les mégaoctets par seconde en gigabits par seconde, multipliez par huit. Par exemple, 125 Mo/s équivaut à 1,000 Mbit/s ou 1 Gbit/s.

7. Lorsque vous avez terminé de créer des règles et des limites, cliquez sur **Enregistrer**.

   La police est enregistrée et est répertoriée dans le tableau règles de classification du trafic.



Le trafic client S3 et Swift est désormais géré conformément aux règles de classification du trafic. Vous pouvez afficher les diagrammes de trafic et vérifier que les stratégies appliquent les limites de trafic auxquelles vous vous attendez.

Informations associées

"Gestion de l'équilibrage des charges"

"Affichage des metrics de trafic réseau"

Modification d'une règle de classification du trafic

Vous pouvez modifier une stratégie de classification de trafic pour modifier son nom ou sa description, ou pour créer, modifier ou supprimer des règles ou des limites de la stratégie.

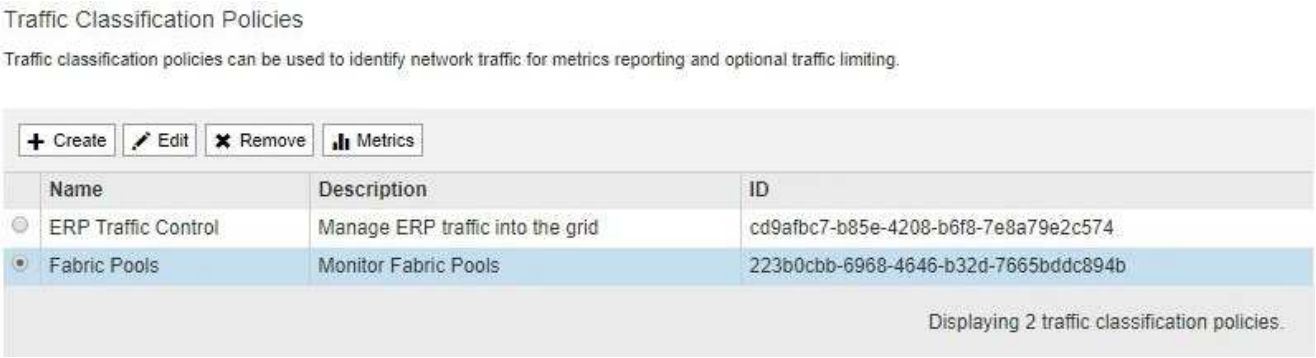
Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation accès racine.

Étapes

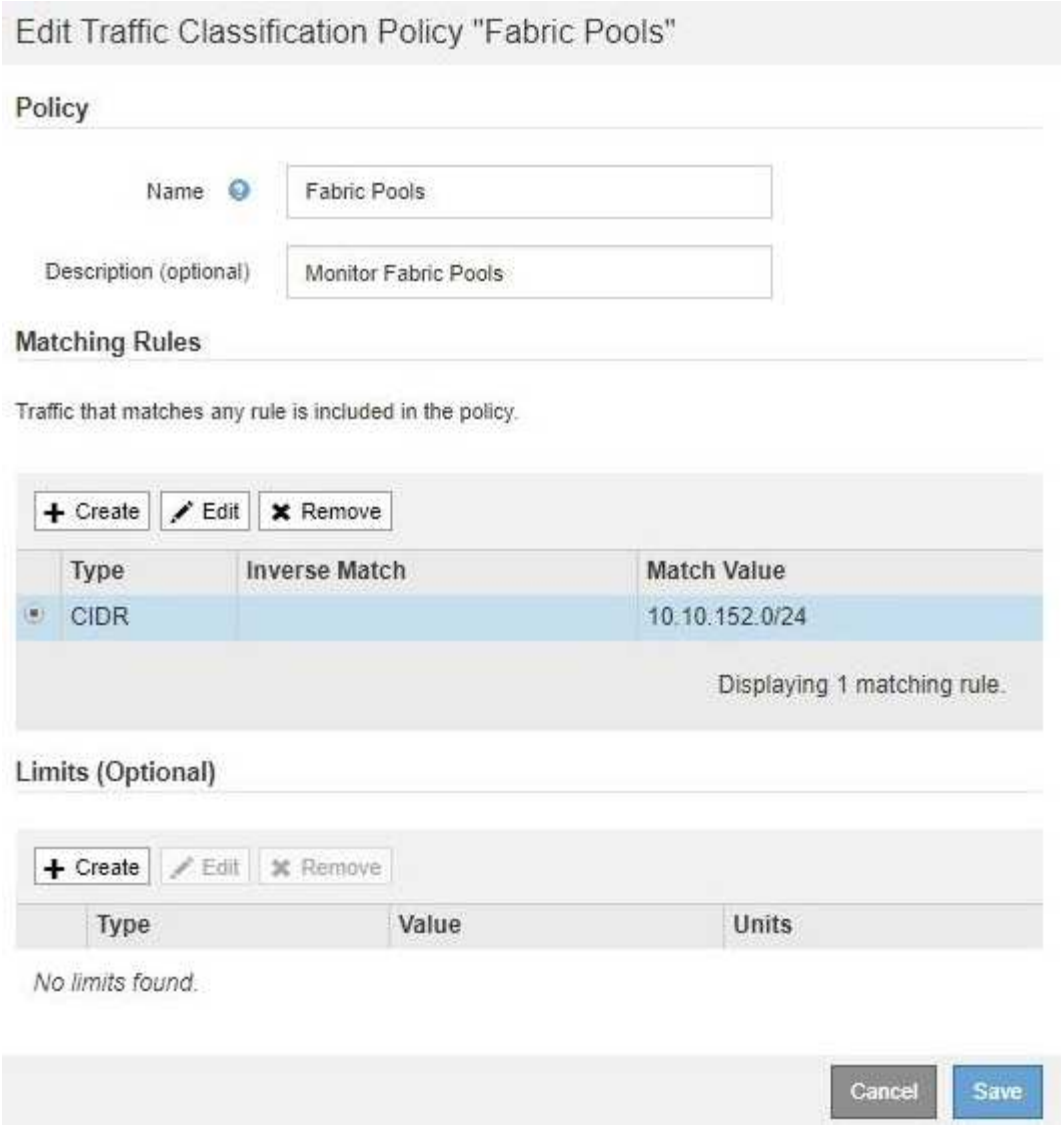
1. Sélectionnez **Configuration** > **Paramètres réseau** > **Classification du trafic**.

   La page règles de classification du trafic s'affiche et les stratégies existantes sont répertoriées dans le tableau.



2. Sélectionnez le bouton radio à gauche de la police que vous souhaitez modifier.
3. Cliquez sur **Modifier**.

   La boîte de dialogue Modifier la stratégie de classification de trafic s'affiche.



4. Créez, modifiez ou supprimez des règles et des limites de correspondance selon les besoins.
   a. Pour créer une règle ou une limite de correspondance, cliquez sur **Créer** et suivez les instructions pour créer une règle ou créer une limite.
   b. Pour modifier une règle ou une limite de correspondance, sélectionnez le bouton radio de la règle ou de la limite, cliquez sur **Modifier** dans la section **règles de mise en correspondance** ou **limites** et suivez les instructions pour créer une règle ou créer une limite.
   c. Pour supprimer une règle ou une limite correspondante, sélectionnez le bouton radio de la règle ou de la limite, puis cliquez sur **Supprimer**. Cliquez ensuite sur **OK** pour confirmer que vous souhaitez supprimer la règle ou la limite.
5. Lorsque vous avez terminé de créer ou de modifier une règle ou une limite, cliquez sur **appliquer**.
6. Lorsque vous avez terminé de modifier la stratégie, cliquez sur **Enregistrer**.

   Les modifications apportées à la stratégie sont enregistrées et le trafic réseau est désormais géré conformément aux règles de classification du trafic. Vous pouvez afficher les diagrammes de trafic et vérifier que les stratégies appliquent les limites de trafic auxquelles vous vous attendez.

Suppression d'une stratégie de classification du trafic

Si vous n'avez plus besoin d'une règle de classification du trafic, vous pouvez la supprimer.

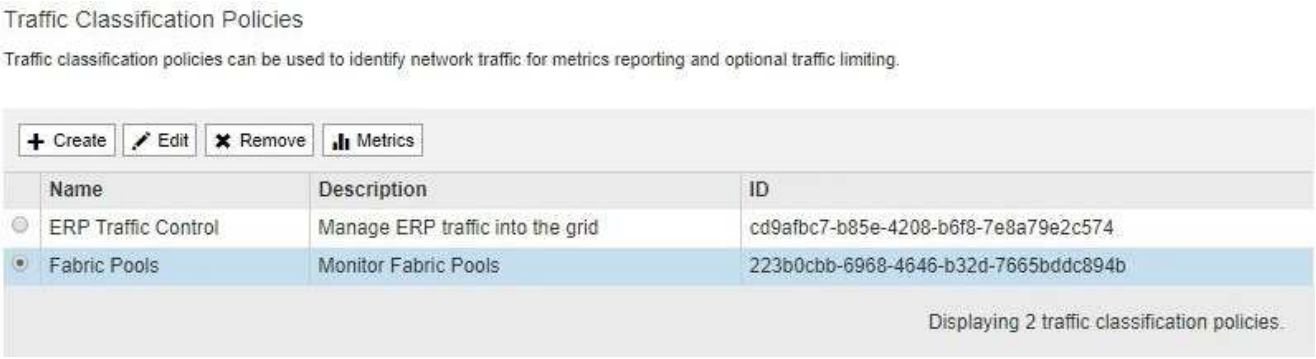
Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation accès racine.

Étapes

1. Sélectionnez **Configuration** > **Paramètres réseau** > **Classification du trafic**.

   La page règles de classification du trafic s'affiche et les stratégies existantes sont répertoriées dans le tableau.

2. Sélectionnez le bouton radio à gauche de la police que vous souhaitez supprimer.
3. Cliquez sur **Supprimer**.

   Une boîte de dialogue Avertissement s'affiche.

4. Cliquez sur **OK** pour confirmer que vous souhaitez supprimer la stratégie.

   La stratégie est supprimée.

Affichage des metrics de trafic réseau

Vous pouvez surveiller le trafic réseau en consultant les graphiques disponibles à partir de la page règles de classification du trafic.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation accès racine.

Description de la tâche

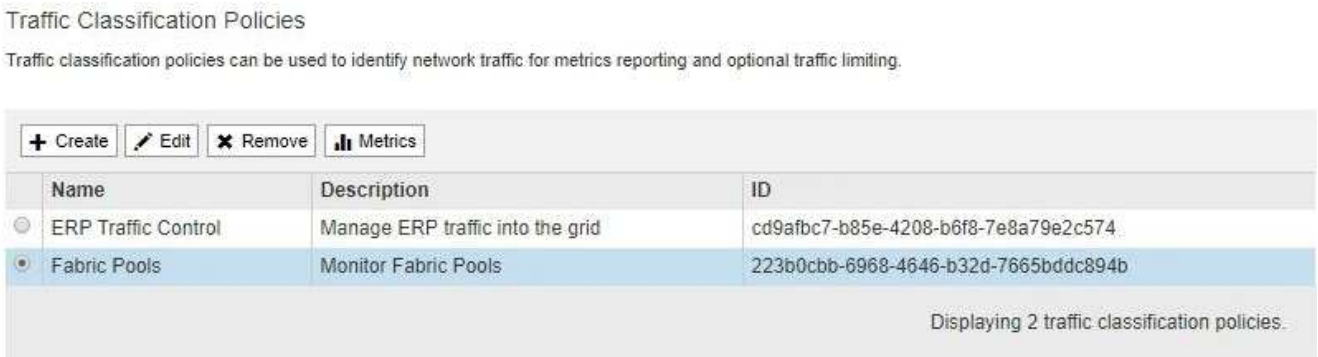
Pour toute règle de classification de trafic existante, vous pouvez afficher les mesures du service Load Balancer afin de déterminer si la stratégie limite le trafic sur le réseau. Les données des graphiques peuvent vous aider à déterminer si vous devez ajuster la stratégie.

Même si aucune limite n'est définie pour une stratégie de classification du trafic, des mesures sont recueillies et les graphiques fournissent des informations utiles pour comprendre les tendances du trafic.

Étapes

1. Sélectionnez **Configuration** > **Paramètres réseau** > **Classification du trafic**.

   La page règles de classification du trafic s'affiche et les stratégies existantes sont répertoriées dans le tableau.



2. Sélectionnez le bouton radio à gauche de la police pour laquelle vous souhaitez afficher les mesures.
3. Cliquez sur **métriques**.

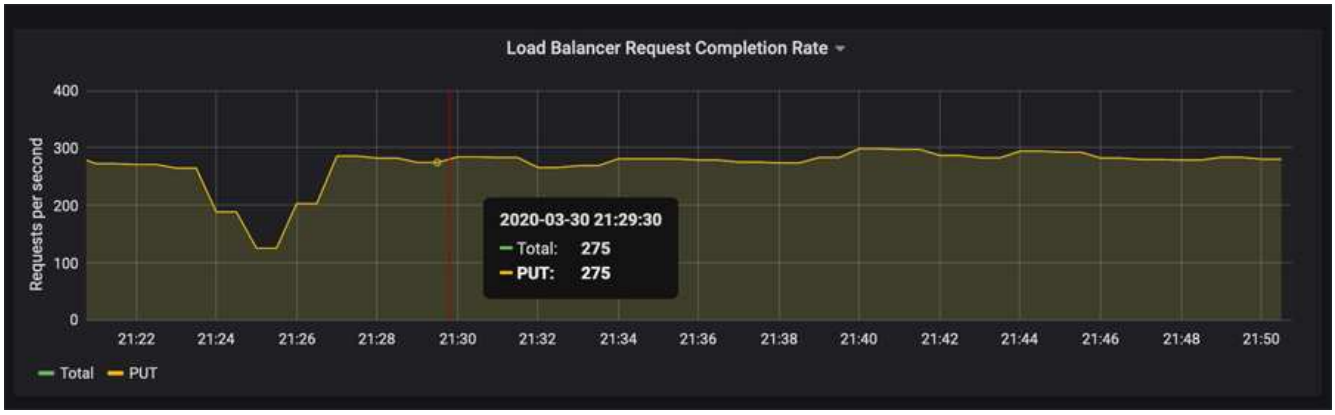
   Une nouvelle fenêtre de navigateur s'ouvre et les graphiques de la politique de classification du trafic s'affichent. Les graphiques affichent des mesures uniquement pour le trafic correspondant à la stratégie sélectionnée.

   Vous pouvez sélectionner d'autres stratégies à afficher à l'aide de la liste déroulante **policy**.

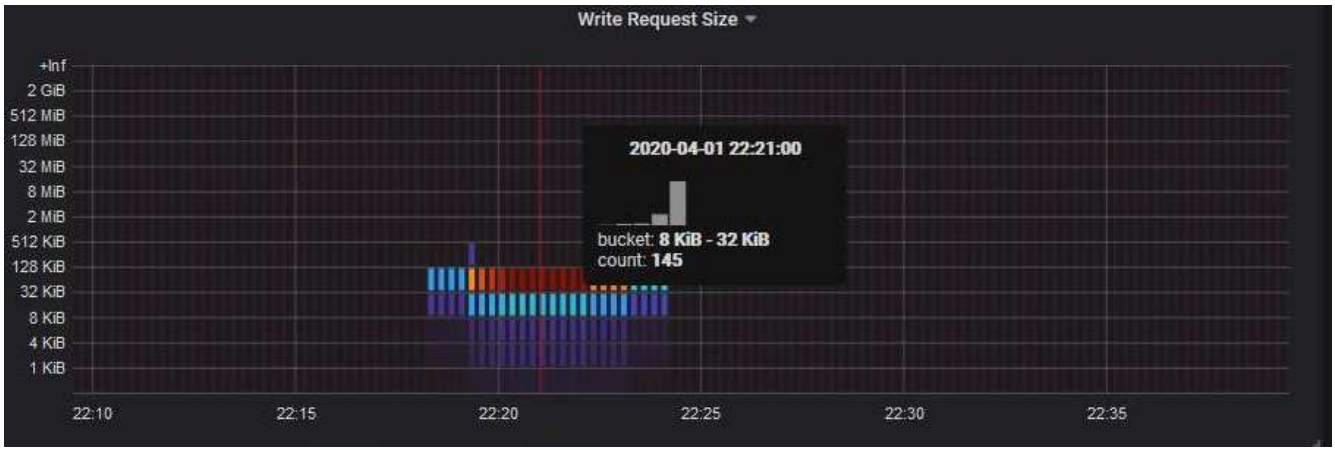
Les graphiques suivants sont inclus sur la page Web.

- Trafic des demandes d'équilibrage de charge : ce graphique fournit une moyenne mobile de 3 minutes du débit des données transmises entre les terminaux d'équilibreur de charge et les clients effectuant les demandes, en bits par seconde.
- Taux d'exécution de la demande d'équilibrage de charge : ce graphique fournit une moyenne mobile de 3 minutes du nombre de demandes terminées par seconde, ventilées par type de demande (GET, PUT, HEAD et DELETE). Cette valeur est mise à jour lorsque les en-têtes d'une nouvelle demande ont été validés.
- Taux de réponse d'erreur : ce graphique fournit une moyenne mobile de 3 minutes du nombre de réponses d'erreur renvoyées aux clients par seconde, ventilées par le code de réponse d'erreur.
- Durée moyenne de la demande (non-erreur) : ce graphique fournit une moyenne mobile de 3 minutes de durée de la demande, ventilées par type de demande (OBTENIR, PLACER, TÊTE et SUPPRIMER). Chaque durée de la demande commence lorsqu'un en-tête de requête est analysé par le service Load Balancer et se termine lorsque le corps de réponse complet est renvoyé au client.
- Taux de demande d'écriture par taille d'objet : cette configuration fournit une moyenne mobile de 3 minutes du taux de traitement des demandes d'écriture basé sur la taille de l'objet. Dans ce contexte, les demandes d'écriture ne font référence qu'à DES requêtes PUT.
- Taux de demande de lecture par taille d'objet : cette carte thermique fournit une moyenne mobile de 3 minutes du taux de traitement des demandes de lecture en fonction de la taille de l'objet. Dans ce contexte, les demandes de lecture ne font référence qu'à L'OBTENTION des demandes. Les couleurs de la carte de chaleur indiquent la fréquence relative d'une taille d'objet dans un graphique individuel. Les couleurs plus froides (par exemple, le violet et le bleu) indiquent des taux relatifs plus bas, et les couleurs plus chaudes (par exemple, l'orange et le rouge) indiquent des taux relatifs plus élevés.

4. Placez le curseur sur un graphique linéaire pour afficher une fenêtre contextuelle de valeurs sur une partie spécifique du graphique.



5. Placez le curseur sur une carte de chaleur pour afficher une fenêtre contextuelle indiquant la date et l'heure de l'échantillon, les tailles d'objet agrégées dans le compte et le nombre de demandes par seconde pendant cette période.



6. Utilisez le menu déroulant **Policy** en haut à gauche pour sélectionner une autre stratégie.

   Les graphiques de la stratégie sélectionnée s'affichent.

7. Vous pouvez également accéder aux graphiques à partir du menu **support**.
   a. Sélectionnez **support** > **Outils** > **métriques**.
   b. Dans la section **Grafana** de la page, sélectionnez **politique de classification du trafic**.
   c. Sélectionnez la police dans le menu déroulant situé en haut à gauche de la page.

      Les politiques de classification du trafic sont identifiées par leur ID. Les ID de police sont répertoriés sur la page règles de classification de la circulation.

8. Analysez les graphiques pour déterminer à quelle fréquence la stratégie limite le trafic et si vous devez ajuster la stratégie.

Informations associées

"Moniteur et amp ; dépannage"

Quels sont les coûts de liaison

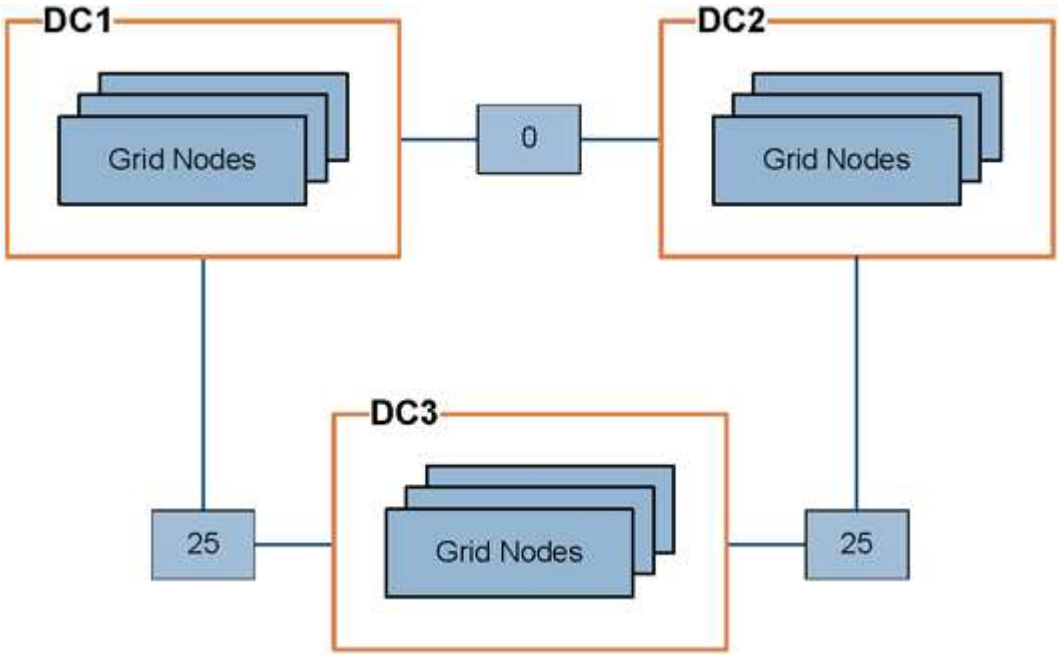
Les coûts de liaison vous permettent de définir la priorité du site de data Center qui fournit un service demandé lorsqu'au moins deux sites de data Center existent. Vous

pouvez ajuster les coûts de liaison pour refléter la latence entre les sites.

- Les coûts des liens permettent de classer par ordre de priorité la copie d'objet utilisée pour les récupérations d'objets.
- Les coûts des liaisons sont utilisés par l'API de gestion du grid et l'API de gestion des locataires pour déterminer quels services StorageGRID internes utiliser.
- Les coûts de liaison sont utilisés par le service CLB sur les nœuds de passerelle pour diriger les connexions client.

> Le service CLB est obsolète.

Le schéma présente une grille de trois sites avec des coûts de liaison configurés entre les sites :



- Le service CLB sur les nœuds de passerelle distribue également les connexions client à tous les nœuds de stockage du même site de data Center et à tous les sites de data Center dont le coût de liaison est de 0.

  Dans l'exemple, un nœud passerelle du site de data Center 1 (DC1) distribue également les connexions client aux nœuds de stockage du DC1 et aux nœuds de stockage du DC2. Un nœud de passerelle du DC3 envoie des connexions client uniquement aux nœuds de stockage du DC3.

- Lors de la récupération d'un objet existant sous forme de plusieurs copies répliquées, StorageGRID récupère la copie au niveau du data Center présentant le coût de liaison le plus faible.

  Dans l'exemple, si une application client de DC2 récupère un objet stocké à la fois à DC1 et DC3, l'objet est récupéré de DC1, car le coût de liaison de DC1 à D2 est 0, ce qui est inférieur au coût de liaison de DC3 à DC2 (25).

Les coûts de liaison sont des nombres relatifs arbitraires sans unité de mesure spécifique. Par exemple, un coût de lien de 50 est utilisé de manière moins préférentielle qu'un coût de lien de 25. Le tableau indique les coûts de liaison couramment utilisés.

Lien	Coût des liens	Remarques
Entre les sites de data centers physiques	25 (par défaut)	Data centers connectés par une liaison WAN.
Entre des sites de data centers logiques au même emplacement physique	0	Data centers logiques dans le même bâtiment physique ou campus connecté par un réseau LAN.

Informations associées

"Fonctionnement de l'équilibrage de charge - service CLB"

Mise à jour des coûts de lien

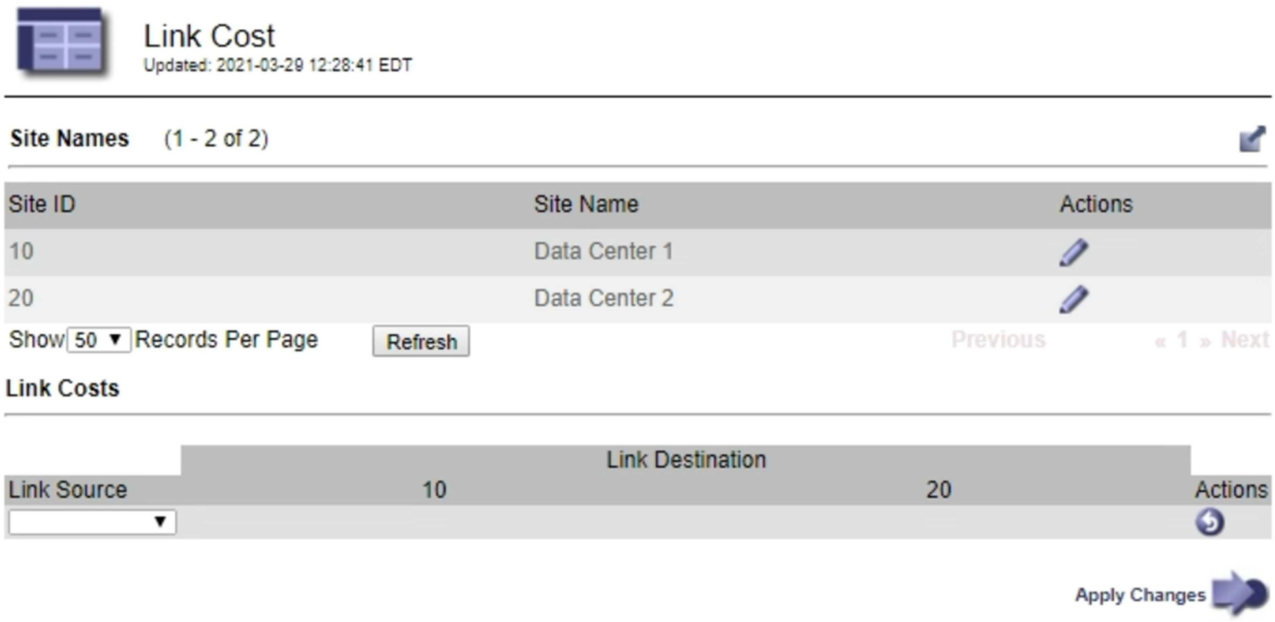
Vous pouvez mettre à jour les coûts de liaison entre les sites de data Center afin de refléter la latence entre les sites.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation Configuration de la page de topologie de la grille.

Étapes

1. Sélectionnez **Configuration** > **Paramètres réseau** > **coût lien**.



2. Sélectionnez un site sous **Link Source** et entrez une valeur de coût comprise entre 0 et 100 sous **Link destination**.

   Vous ne pouvez pas modifier le coût du lien si la source est identique à la destination.

   Pour annuler les modifications, cliquez sur **Retour**.

3. Cliquez sur **appliquer les modifications**.

Configuration d'AutoSupport en cours

La fonctionnalité AutoSupport permet à votre système StorageGRID d'envoyer des messages d'état et d'état au support technique. L'utilisation de AutoSupport peut considérablement accélérer l'identification et la résolution des problèmes. Le support technique peut également surveiller les besoins en stockage de votre système et vous aider à déterminer si vous devez ajouter de nouveaux nœuds ou sites. Vous pouvez également configurer l'envoi des messages AutoSupport à une destination supplémentaire.

Informations incluses dans les messages AutoSupport

Les messages AutoSupport incluent des informations telles que :

- Version du logiciel StorageGRID
- Version du système d'exploitation
- Informations sur les attributs au niveau du système et de l'emplacement
- Alertes et alarmes récentes (système hérité)
- État actuel de toutes les tâches de la grille, y compris les données historiques
- Informations sur les événements répertoriées sur la page **Nodes** > ***Grid Node*** > **Events**
- Utilisation de la base de données du nœud d'administration
- Nombre d'objets perdus ou manquants
- Paramètres de configuration de la grille
- Entités NMS
- Règle ILM active
- Fichier de spécification de grille provisionné
- Les mesures de diagnostic

Vous pouvez activer la fonctionnalité AutoSupport et les options AutoSupport individuelles lors de la première installation de StorageGRID, ou vous pouvez les activer ultérieurement. Si AutoSupport n'est pas activé, un message s'affiche dans le tableau de bord du gestionnaire de grille. Le message inclut un lien vers la page de configuration de AutoSupport.

Vous pouvez sélectionner le symbole « x » pour fermer le message. Le message ne s'affichera plus tant que le cache de votre navigateur n'aura pas été effacé, même si AutoSupport reste désactivé.

Utilisation de Active IQ

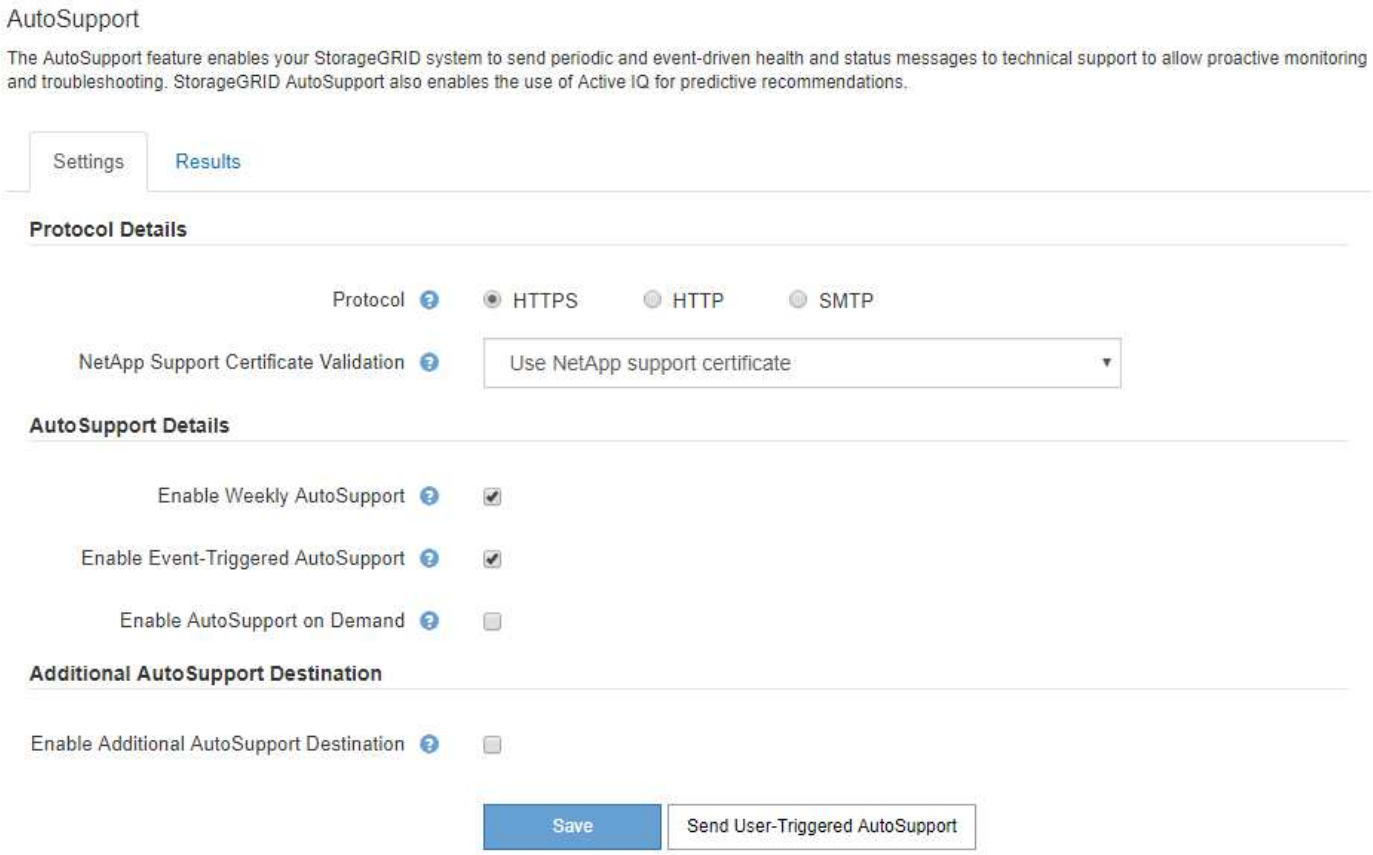
Active IQ est un conseiller digital basé dans le cloud qui exploite l'analytique prédictive et les connaissances de la communauté issues de la base installée de NetApp. Les évaluations continues des risques, les alertes prédictives, les conseils normatifs et les actions automatisées vous aident à anticiper les problèmes, ce qui permet d'améliorer l'état et la disponibilité du système.

Vous devez activer AutoSupport si vous souhaitez utiliser les tableaux de bord et la fonctionnalité Active IQ sur le site de support NetApp.

"Documentation Active IQ sur le conseiller digital"

Accès aux paramètres AutoSupport

Vous configurez AutoSupport à l'aide du Gestionnaire de grille (**support Outils AutoSupport**). La page **AutoSupport** comporte deux onglets : **Paramètres** et **Résultats**.



Protocoles pour l'envoi des messages AutoSupport

Vous pouvez choisir l'un des trois protocoles pour l'envoi des messages AutoSupport :

- HTTPS
- HTTP
- SMTP

Si vous envoyez des messages AutoSupport via HTTPS ou HTTP, vous pouvez configurer un serveur proxy non transparent entre les nœuds d'administration et le support technique.

Si vous utilisez SMTP comme protocole pour les messages AutoSupport, vous devez configurer un serveur de messagerie SMTP.

Options AutoSupport

Toutes les combinaisons d'options suivantes vous permettent d'envoyer des messages AutoSupport au support technique :

- **Hebdomadaire**: Envoyer automatiquement des messages AutoSupport une fois par semaine. Paramètre par défaut : activé.
- **Event-déclenché** : envoie automatiquement des messages AutoSupport toutes les heures ou lorsque des événements système importants se produisent. Paramètre par défaut : activé.
- **On Demand**: Laissez le support technique demander à votre système StorageGRID d'envoyer automatiquement des messages AutoSupport, ce qui est utile lorsqu'ils travaillent activement en cas de problème (nécessite le protocole de transmission HTTPS AutoSupport). Paramètre par défaut : Désactivé.
- **Déclenché par l'utilisateur** : envoyez manuellement des messages AutoSupport à tout moment.

Informations associées

"Support NetApp"

Spécification du protocole des messages AutoSupport

Vous pouvez utiliser l'un des trois protocoles pour envoyer des messages AutoSupport.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation accès racine ou autre configuration grille.
- Si vous utilisez le protocole HTTPS ou HTTP pour l'envoi des messages AutoSupport, vous devez avoir fourni un accès Internet sortant au nœud d'administration principal, soit directement, soit à l'aide d'un serveur proxy (connexions entrantes non requises).
- Si vous utilisez le protocole HTTPS ou HTTP et que vous souhaitez utiliser un serveur proxy, vous devez avoir configuré un serveur proxy Admin.
- Si vous utilisez SMTP comme protocole pour les messages AutoSupport, vous devez avoir configuré un serveur de messagerie SMTP. La même configuration de serveur de messagerie est utilisée pour les notifications par e-mail d'alarme (système hérité).

Description de la tâche

Vous pouvez envoyer des messages AutoSupport via l'un des protocoles suivants :

- **HTTPS** : il s'agit du paramètre par défaut et recommandé pour les nouvelles installations. Le protocole HTTPS utilise le port 443. Pour activer la fonctionnalité AutoSupport On Demand, vous devez utiliser le protocole HTTPS.
- **HTTP**: Ce protocole n'est pas sécurisé, sauf s'il est utilisé dans un environnement de confiance où le serveur proxy se convertit en HTTPS lors de l'envoi de données via Internet. Le protocole HTTP utilise le port 80.
- **SMTP**: Utilisez cette option si vous souhaitez que les messages AutoSupport soient envoyés par e-mail. Si vous utilisez SMTP comme protocole pour les messages AutoSupport, vous devez configurer un serveur de messagerie SMTP sur la page Configuration de l'e-mail héritée (**support** > **alarmes (hérité)** > **Configuration de l'e-mail héritée**).

> SMTP était le seul protocole disponible pour les messages AutoSupport avant la version de StorageGRID 11.2. Si vous avez installé une version antérieure de StorageGRID au départ, SMTP est peut-être le protocole sélectionné.

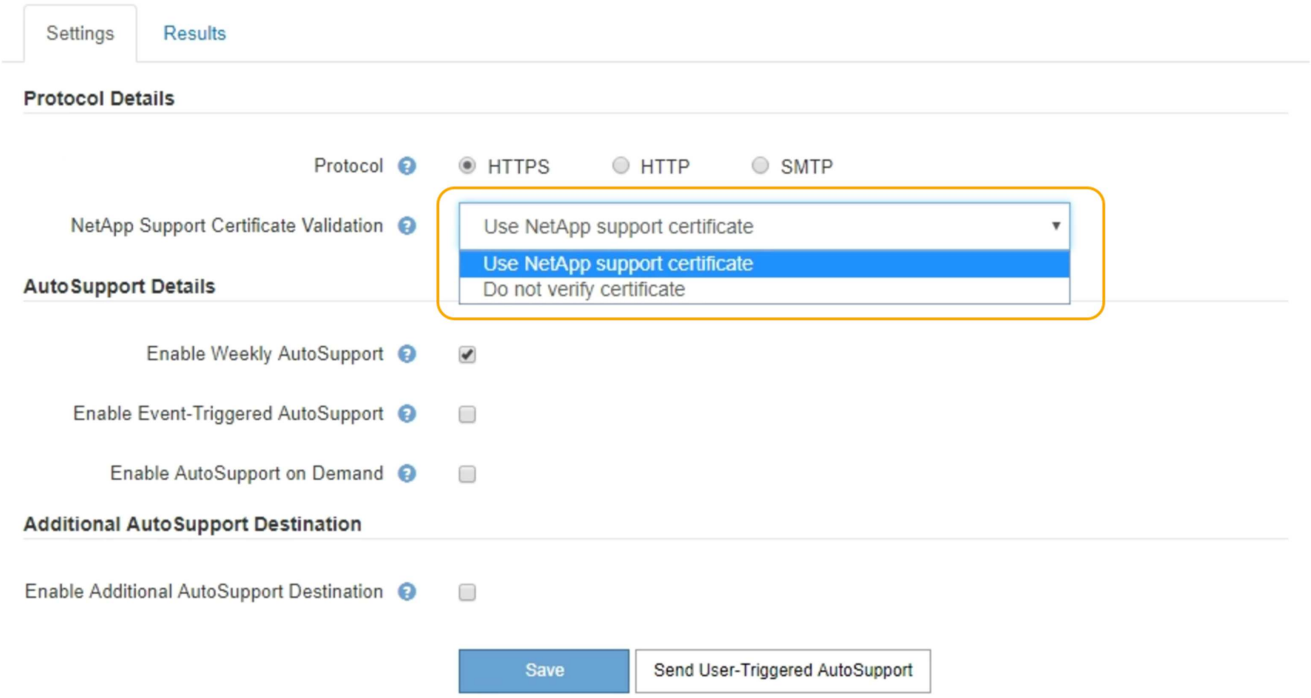
Le protocole que vous définissez permet d'envoyer tous les types de messages AutoSupport.

Étapes

1. Sélectionnez **support** > **Outils** > **AutoSupport**.

   La page AutoSupport s'affiche et l'onglet **Paramètres** est sélectionné.

2. Sélectionnez le protocole à utiliser pour envoyer des messages AutoSupport.



3. Sélectionnez votre choix pour **validation de certificat de support NetApp**.
   - Utilisez le certificat de support NetApp (par défaut) : la validation du certificat permet de sécuriser la transmission des messages AutoSupport. Le certificat de support NetApp est déjà installé avec le logiciel StorageGRID.
   - Ne pas vérifier le certificat : sélectionnez cette option uniquement si vous avez une bonne raison de ne pas utiliser la validation de certificat, par exemple lorsqu'il y a un problème temporaire avec un certificat.
4. Sélectionnez **Enregistrer**.

   Tous les messages hebdomadaires, déclenchés par l'utilisateur et déclenchés par des événements sont envoyés à l'aide du protocole sélectionné.

Informations associées

"Configuration des paramètres du proxy d'administration"

Activation d’AutoSupport à la demande

AutoSupport On Demand peut vous aider à résoudre les problèmes sur lesquels le support technique travaille activement. Lorsque vous activez AutoSupport On Demand, le support technique peut demander l’envoi des messages AutoSupport sans intervention de votre part.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l’aide d’un navigateur pris en charge.
- Vous devez disposer de l’autorisation accès racine ou autre configuration grille.
- Vous devez avoir activé les messages AutoSupport hebdomadaires.
- Vous devez avoir défini le protocole de transport sur HTTPS.

Description de la tâche

Lorsque vous activez cette fonctionnalité, le support technique peut demander à votre système StorageGRID d’envoyer automatiquement des messages AutoSupport. Le support technique peut également définir l’intervalle d’interrogation pour les requêtes AutoSupport On Demand.

Le support technique ne peut ni activer ni désactiver AutoSupport On Demand.

Étapes

1. Sélectionnez **support** > **Outils** > **AutoSupport**.

   La page AutoSupport s’affiche avec l’onglet **Paramètres** sélectionné.

2. Sélectionnez le bouton d’option HTTPS dans la section **Protocol Details** de la page.

3. Cochez la case **Activer AutoSupport hebdomadaire**.
4. Cochez la case **Activer AutoSupport On Demand**.
5. Sélectionnez **Enregistrer**.

   AutoSupport On Demand est activé et le support technique peut envoyer des demandes AutoSupport On Demand à StorageGRID.

Désactivation des messages AutoSupport hebdomadaires

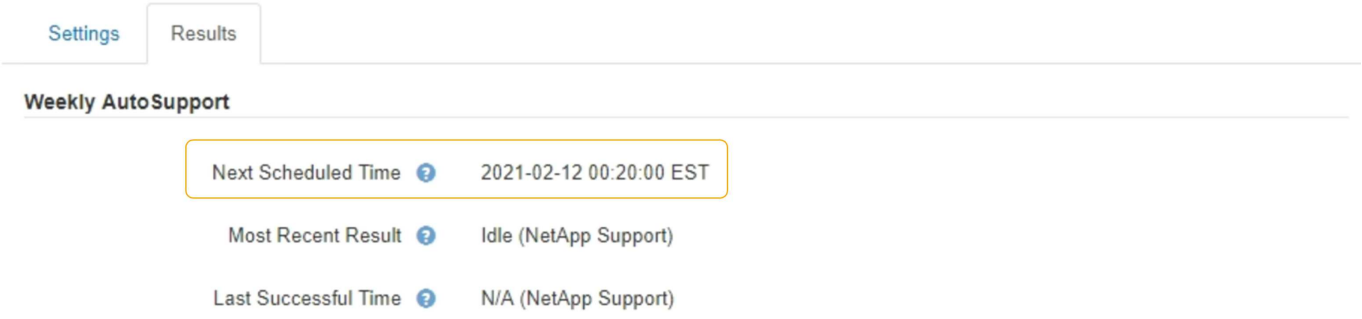
Par défaut, le système StorageGRID est configuré pour envoyer un message AutoSupport au support NetApp une fois par semaine.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l’aide d’un navigateur pris en charge.
- Vous devez disposer de l’autorisation accès racine ou autre configuration grille.

Description de la tâche

Pour déterminer à quel moment le message AutoSupport hebdomadaire est envoyé, reportez-vous à la section **prochaine heure programmée** sous **AutoSupport hebdomadaire** de la page **AutoSupport** > **Résultats**.



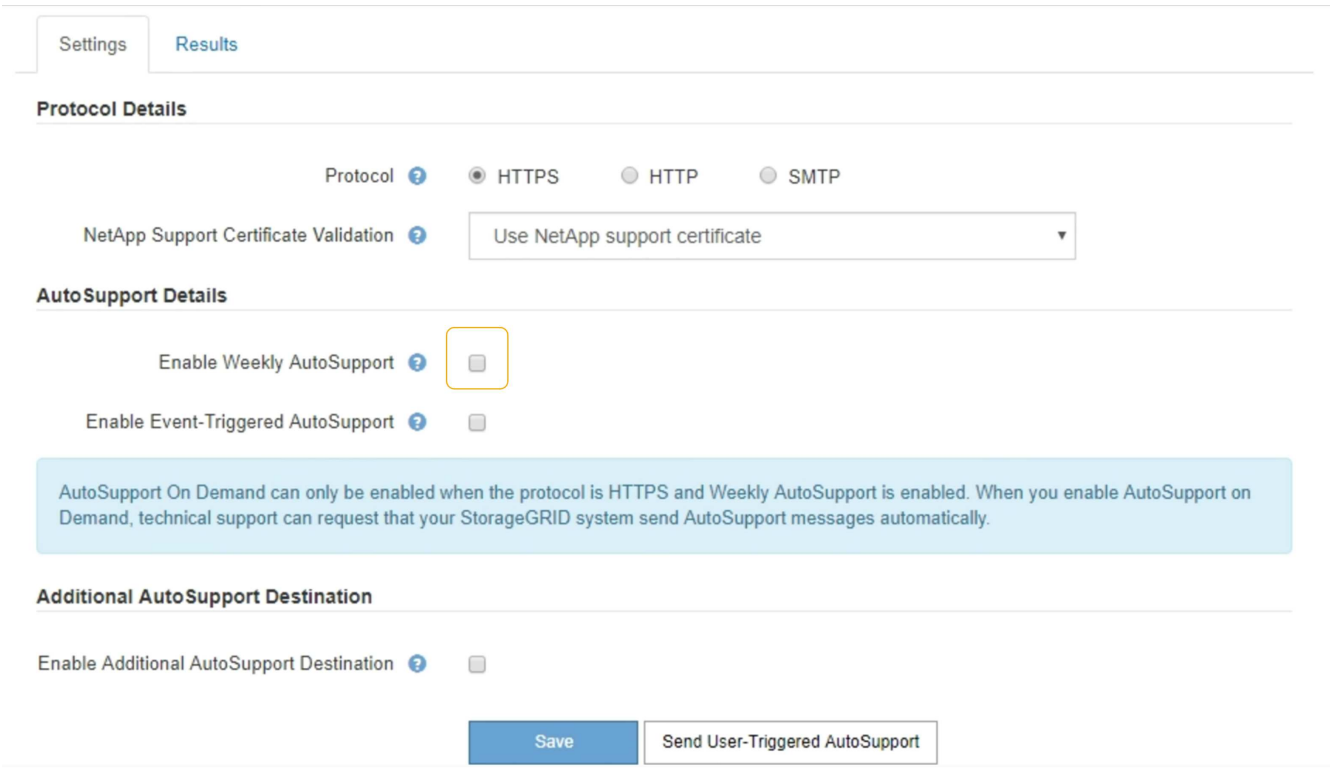
Vous pouvez désactiver l'envoi automatique d'un message AutoSupport à tout moment.

Étapes

1. Sélectionnez **support** > **Outils** > **AutoSupport**.

   La page AutoSupport s'affiche avec l'onglet **Paramètres** sélectionné.

2. Décochez la case **Activer AutoSupport hebdomadaire**.



3. Sélectionnez **Enregistrer**.

Désactivation des messages AutoSupport déclenchés par les événements

Par défaut, le système StorageGRID est configuré de manière à envoyer un message AutoSupport au support NetApp lorsqu'une alerte importante ou un autre événement système important se produit.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation accès racine ou autre configuration grille.

Description de la tâche

Vous pouvez désactiver à tout moment les messages AutoSupport déclenchés par les événements.

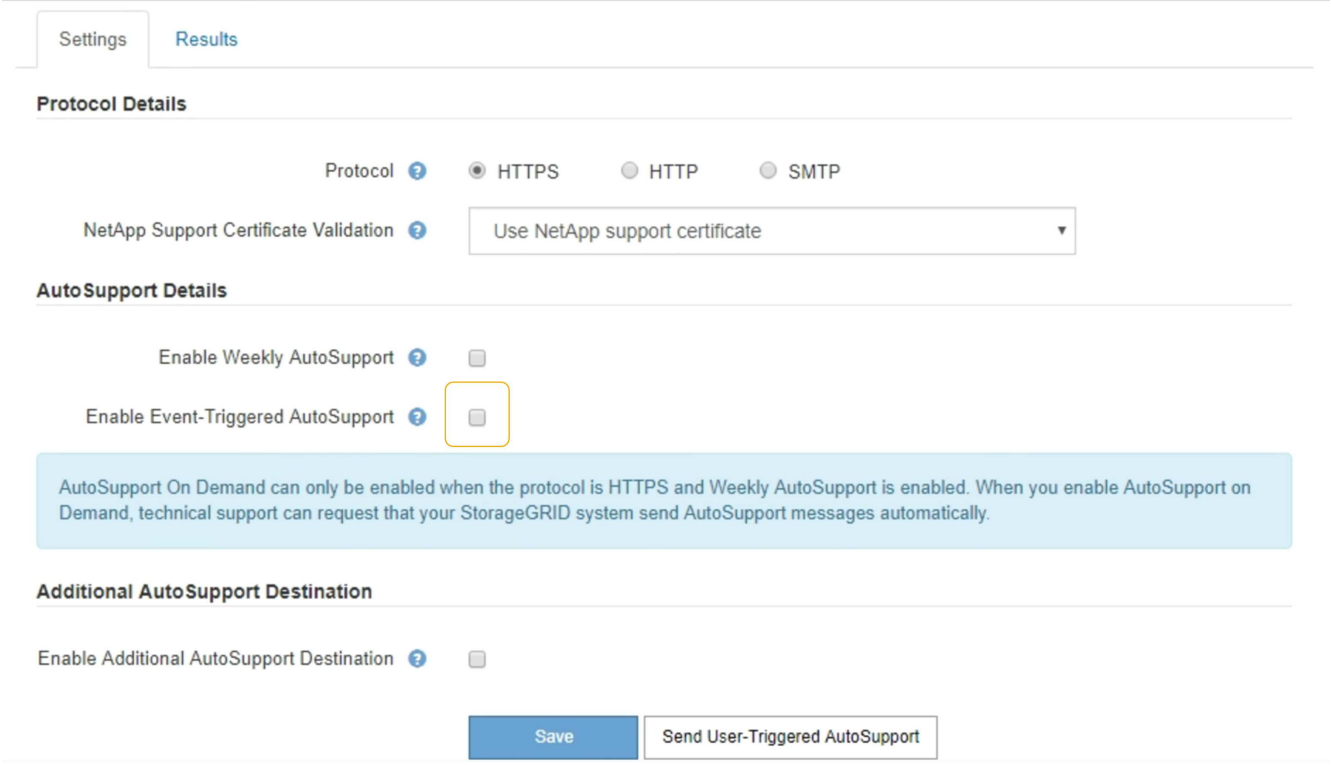
> Les messages AutoSupport déclenchés par des événements sont également supprimés lorsque vous supprimez des notifications par e-mail dans tout le système. (Sélectionnez **Configuration** > **Paramètres système** > **Options d'affichage**. Sélectionnez ensuite **Supprimer toutes les notifications**.)

Étapes

1. Sélectionnez **support** > **Outils** > **AutoSupport**.

   La page AutoSupport s'affiche avec l'onglet **Paramètres** sélectionné.

2. Décochez la case **Activer AutoSupport déclenchée par événement**.



3. Sélectionnez **Enregistrer**.

Déclenchement manuel de l'un des messages AutoSupport

Pour aider le support technique à résoudre les problèmes liés à votre système StorageGRID, vous pouvez déclencher manuellement un message AutoSupport à envoyer.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.

- Vous devez disposer de l'autorisation accès racine ou autre configuration grille.

Étapes

1. Sélectionnez **support** > **Outils** > **AutoSupport**.

   La page AutoSupport s'affiche avec l'onglet **Paramètres** sélectionné.

2. Sélectionnez **Envoyer AutoSupport déclenchée par l'utilisateur**.

   StorageGRID tente d'envoyer un message AutoSupport au support technique. Si la tentative réussit, les valeurs **résultat le plus récent** et **dernier temps** réussi dans l'onglet **Résultats** sont mises à jour. En cas de problème, la valeur **résultat** la plus récente est mise à jour sur "échec" et StorageGRID n'essaie pas d'envoyer à nouveau le message AutoSupport.

   > Après avoir envoyé un message AutoSupport déclenché par l'utilisateur, actualisez la page AutoSupport de votre navigateur après 1 minute pour accéder aux résultats les plus récents.

Ajout d'une destination AutoSupport supplémentaire

Lorsque vous activez AutoSupport, les messages d'état et d'état sont envoyés au support NetApp. Vous pouvez indiquer une destination supplémentaire pour tous les messages AutoSupport.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation accès racine ou autre configuration grille.

Description de la tâche

Pour vérifier ou modifier le protocole utilisé pour envoyer des messages AutoSupport, reportez-vous aux instructions de spécification d'un protocole AutoSupport.

> Vous ne pouvez pas utiliser le protocole SMTP pour envoyer des messages AutoSupport à une destination supplémentaire.

"Spécification du protocole des messages AutoSupport"

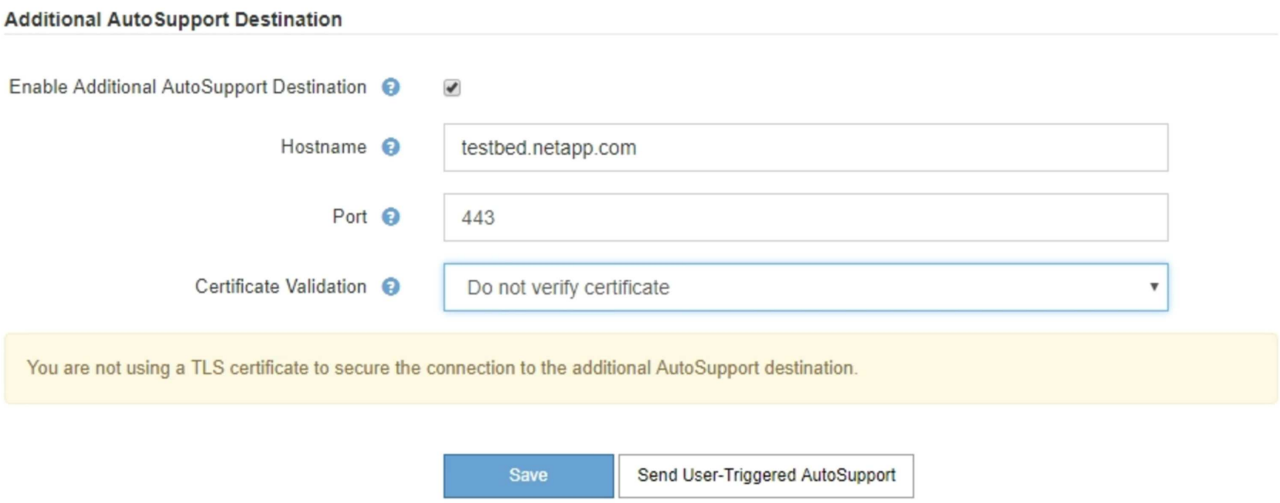
Étapes

1. Sélectionnez **support** > **Outils** > **AutoSupport**.

   La page AutoSupport s'affiche avec l'onglet **Paramètres** sélectionné.

2. Sélectionnez **Activer une destination AutoSupport supplémentaire**.

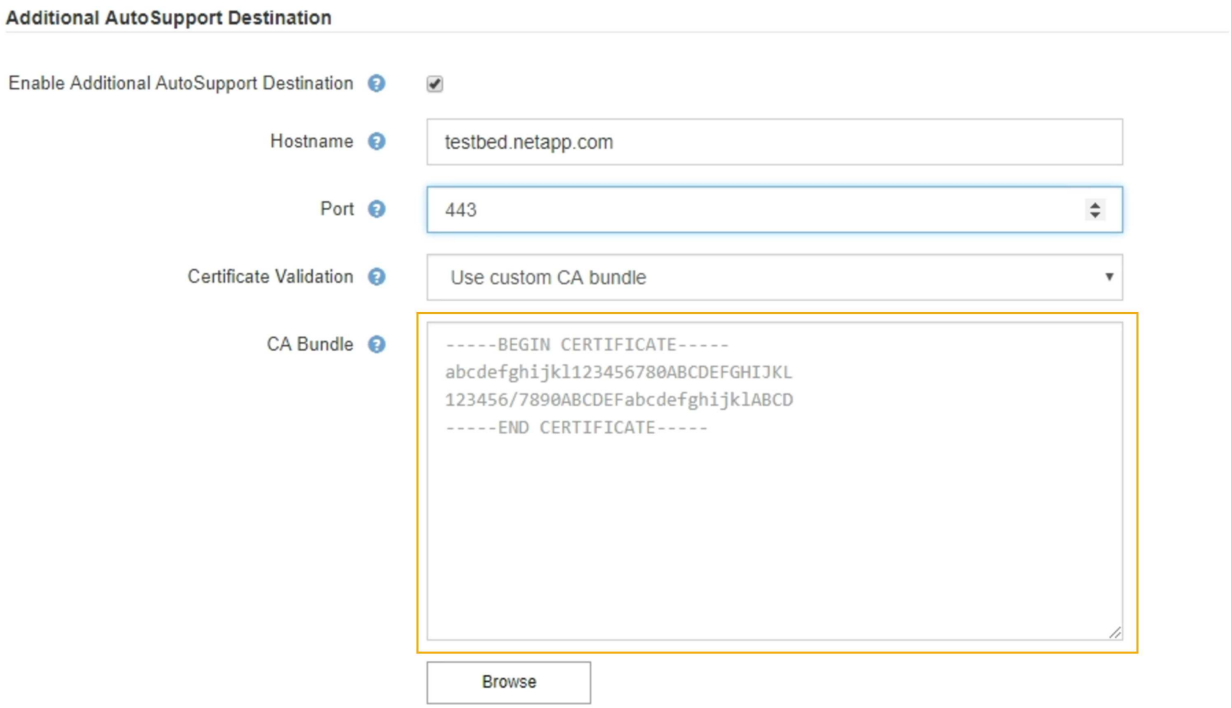
   Les champs destination AutoSupport supplémentaire s'affichent.



3. Entrez le nom d'hôte ou l'adresse IP du serveur d'un serveur de destination AutoSupport supplémentaire.

   Vous ne pouvez entrer qu'une destination supplémentaire.

4. Entrez le port utilisé pour la connexion à un serveur de destination AutoSupport supplémentaire (le port par défaut est le port 80 pour HTTP ou le port 443 pour HTTPS).
5. Pour envoyer vos messages AutoSupport avec validation de certificat, sélectionnez **utiliser le bundle de CA personnalisé** dans la liste déroulante **validation de certificat**. Puis, effectuez l'une des opérations suivantes :
   - Utilisez un outil d'édition pour copier et coller tout le contenu de chacun des fichiers de certificat d'autorité de certification codés au PEM dans le champ **CA bundle**, concaténé dans l'ordre de la chaîne de certificats. Vous devez inclure `----BEGIN CERTIFICATE----` et `----END CERTIFICATE----` dans votre sélection.



   - Sélectionnez **Parcourir**, naviguez jusqu'au fichier contenant les certificats, puis sélectionnez **Ouvrir** pour télécharger le fichier. La validation du certificat garantit que la transmission des messages

AutoSupport est sécurisée.

6. Pour envoyer vos messages AutoSupport sans validation de certificat, sélectionnez **ne pas vérifier le certificat** dans la liste déroulante **validation de certificat**.

   Sélectionnez cette option uniquement si vous avez une bonne raison de ne pas utiliser la validation de certificat, par exemple en cas de problème temporaire avec un certificat.

   Un message d'avertissement s'affiche : « vous n'utilisez pas de certificat TLS pour sécuriser la connexion à la destination AutoSupport supplémentaire. »

7. Sélectionnez **Enregistrer**.

   Tous les futurs messages AutoSupport hebdomadaires, déclenchés par les événements et déclenchés par l'utilisateur seront envoyés à la destination supplémentaire.

Envoi de messages AutoSupport E-Series via StorageGRID

Vous pouvez envoyer des messages AutoSupport E-Series SANtricity System Manager au support technique par l'intermédiaire d'un nœud d'administration StorageGRID plutôt que du port de gestion de l'appliance de stockage.

Ce dont vous avez besoin

- Vous êtes connecté à Grid Manager à l'aide d'un navigateur Web pris en charge.
- Vous disposez de l'autorisation Administrateur de l'appliance de stockage ou de l'autorisation accès racine.

> Vous devez disposer d'un firmware SANtricity 8.70 ou supérieur pour accéder à SANtricity System Manager à l'aide de Grid Manager.

Description de la tâche

Les messages AutoSupport E-Series contiennent des informations détaillées sur le matériel de stockage. Ils sont plus spécifiques que les autres messages AutoSupport envoyés par le système StorageGRID.

Configurez une adresse de serveur proxy spéciale dans SANtricity System Manager pour que les messages AutoSupport soient transmis par l'intermédiaire d'un nœud d'administration StorageGRID sans utiliser le port de gestion de l'appliance. Les messages AutoSupport transmis de cette façon respectent les paramètres de proxy d'expéditeur et d'administration préférés qui peuvent avoir été configurés dans le Gestionnaire de grille.

Si vous souhaitez configurer le serveur proxy d'administration dans Grid Manager, reportez-vous aux instructions de configuration des paramètres proxy d'administration.

"Configuration des paramètres du proxy d'administration"

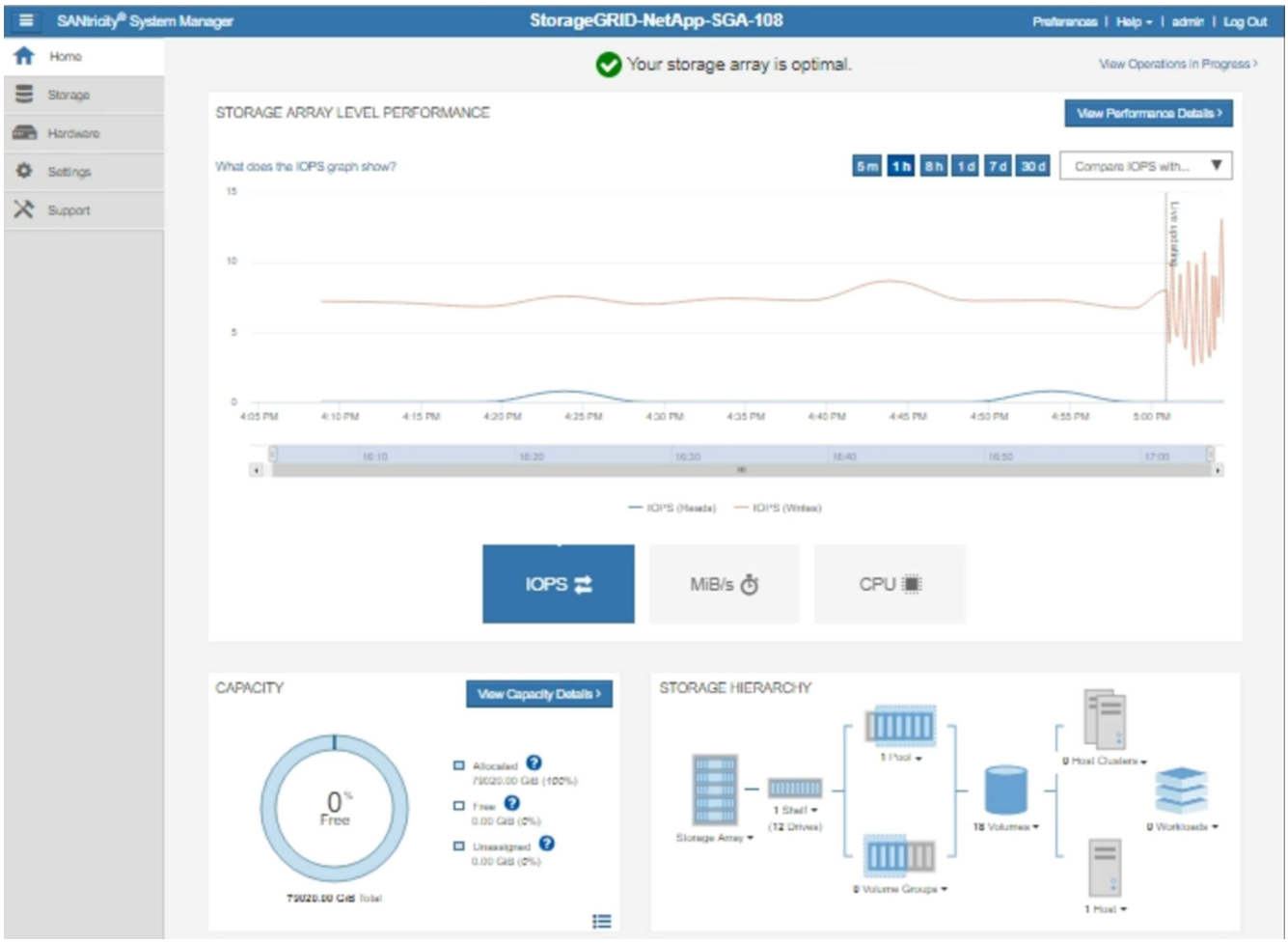
> Cette procédure permet uniquement de configurer un serveur proxy StorageGRID pour les messages AutoSupport E-Series. Pour en savoir plus sur la configuration des baies E-Series AutoSupport, consultez le centre de documentation E-Series.
>
> "Centre de documentation des systèmes NetApp E-Series"

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **noeuds**.

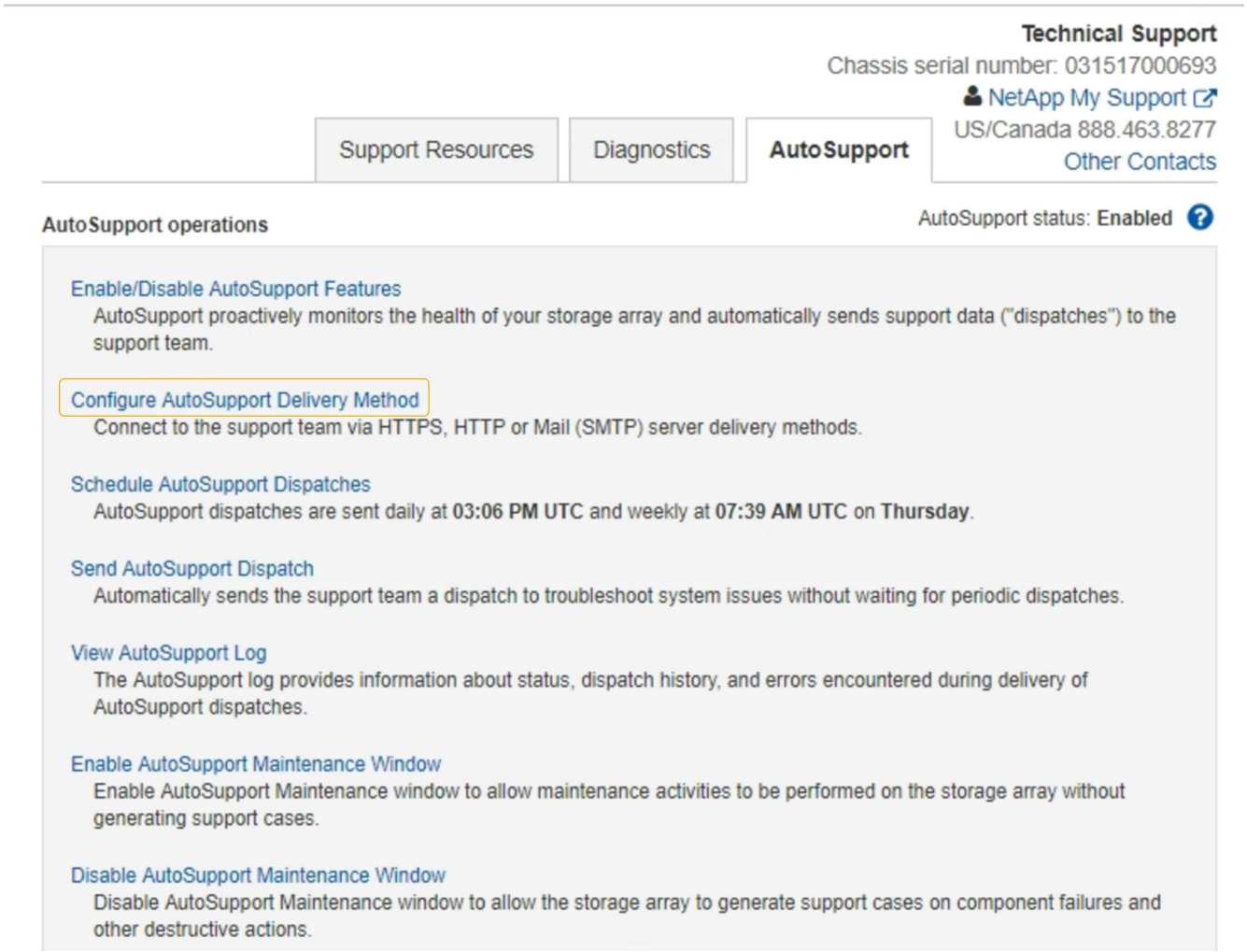
2. Dans la liste des nœuds de gauche, sélectionnez le nœud d'appliance de stockage à configurer.
3. Sélectionnez **SANtricity System Manager**.

   La page d'accueil de SANtricity System Manager s'affiche.



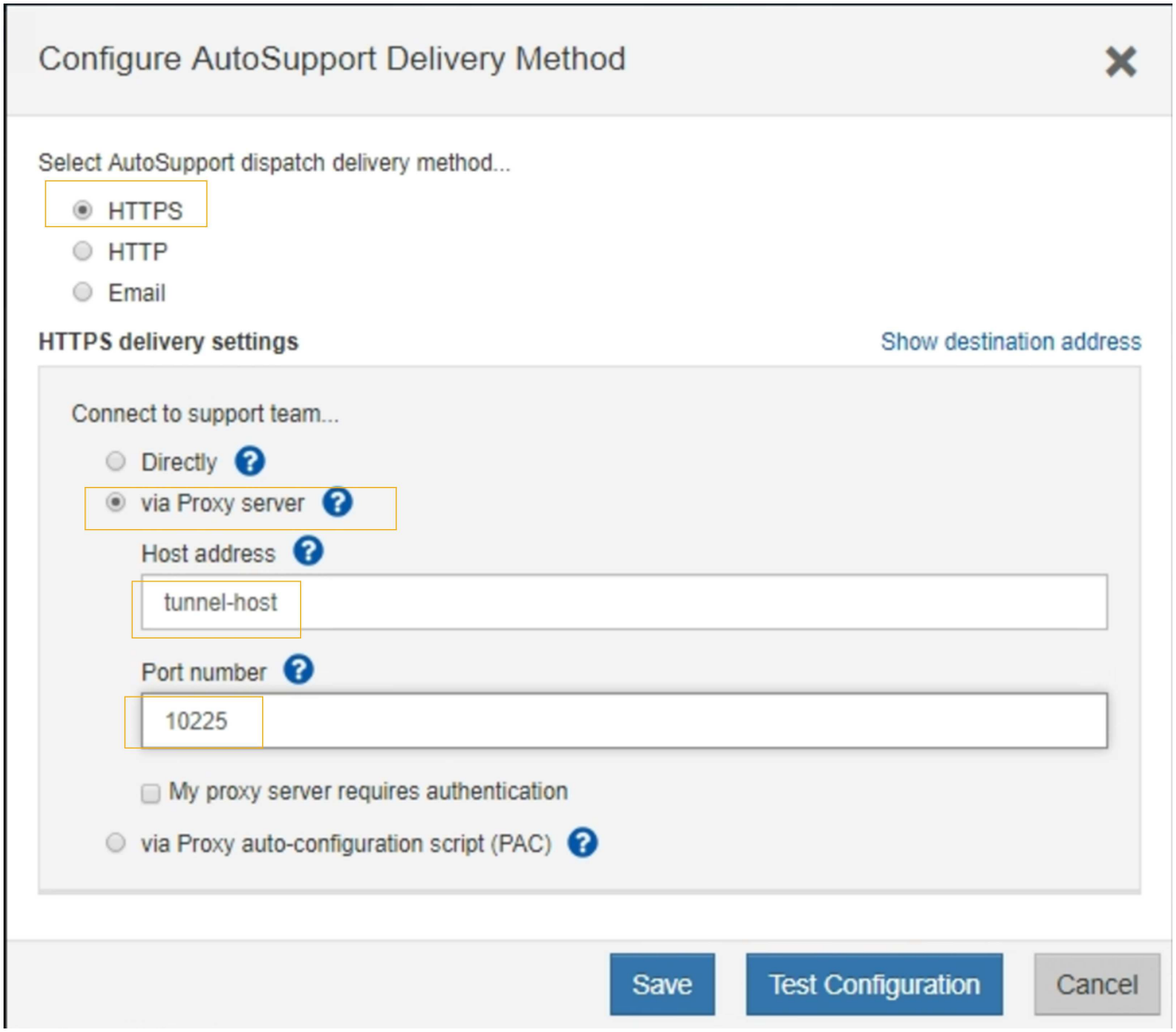
4. Sélectionnez **support** > **support Center** > **AutoSupport**.

   La page opérations AutoSupport s'affiche.



5. Sélectionnez **configurer la méthode de livraison AutoSupport**.

   La page configurer la méthode de livraison AutoSupport s'affiche.



6. Sélectionnez **HTTPS** pour la méthode de livraison.

   Le certificat qui active le protocole HTTPS est préinstallé.

7. Sélectionnez **via le serveur proxy**.
8. Entrez `tunnel-host` Pour l'adresse **hôte**.

   `tunnel-host` Est l'adresse spéciale pour utiliser un nœud d'administration pour envoyer les messages AutoSupport E-Series.

9. Entrez `10225` Pour le **Numéro de port**.

   `10225` Numéro de port sur le serveur proxy StorageGRID qui reçoit des messages AutoSupport du contrôleur E-Series de l'appliance.

10. Sélectionnez **Tester la configuration** pour tester le routage et la configuration de votre serveur proxy AutoSupport.

    Si c'est le cas, un message apparaît dans une bannière verte : « votre configuration AutoSupport a été

vérifiée ».

Si le test échoue, un message d'erreur s'affiche dans une bannière rouge. Vérifiez les paramètres DNS de StorageGRID et la mise en réseau, assurez-vous que le nœud d'administration d'expéditeur privilégié peut se connecter au site du support NetApp, puis réessayez.

11. Sélectionnez **Enregistrer**.

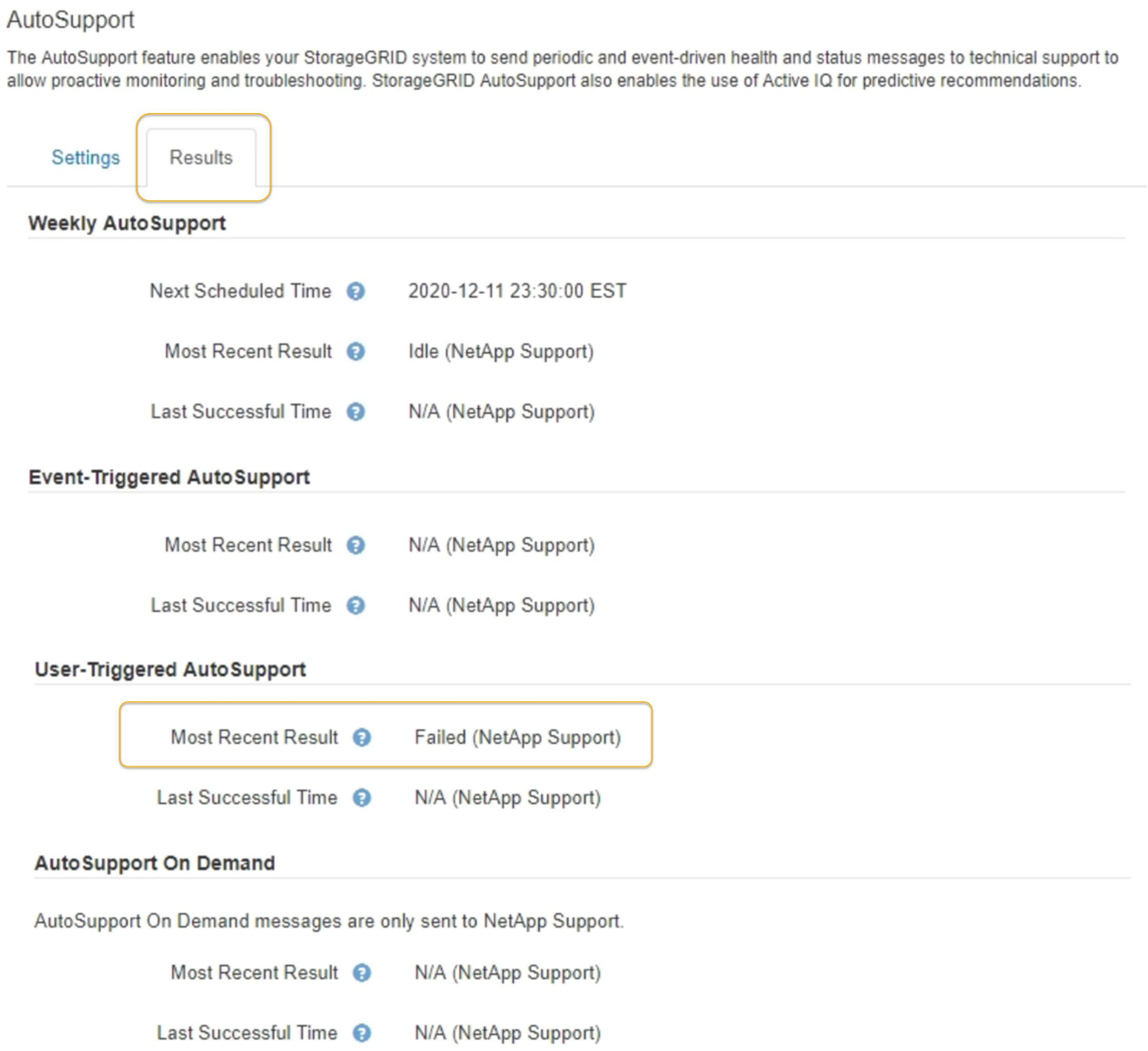
    La configuration est enregistrée et un message de confirmation apparaît : « la méthode de livraison AutoSupport a été configurée ».

Dépannage des messages AutoSupport

Si la tentative d'envoi d'un message AutoSupport échoue, le système StorageGRID effectue différentes actions en fonction du type de message AutoSupport. Vous pouvez vérifier l'état des messages AutoSupport en sélectionnant **support** > **Outils** > **AutoSupport** > **Résultats**.

> Les messages AutoSupport déclenchés par des événements sont supprimés lorsque vous supprimez des notifications par e-mail dans tout le système. (Sélectionnez **Configuration** > **Paramètres système** > **Options d'affichage**. Sélectionnez ensuite **Supprimer toutes les notifications**.)

Lorsque le message AutoSupport ne parvient pas à envoyer, ""FAILED"" s'affiche dans l'onglet **Résultats** de la page **AutoSupport**.



Échec hebdomadaire du message AutoSupport

Si un message AutoSupport hebdomadaire ne parvient pas à s'envoyer, le système StorageGRID prend les actions suivantes :

1. Met à jour l'attribut de résultat le plus récent pour réessayer.
2. Tente de renvoyer le message AutoSupport 15 fois toutes les quatre minutes pendant une heure.
3. Après une heure d'échec d'envoi, met à jour l'attribut de résultat le plus récent sur échec.
4. Tente à nouveau d'envoyer un message AutoSupport à l'heure programmée suivante.
5. Maintient le programme AutoSupport normal si le message échoue parce que le service NMS n'est pas disponible et si un message est envoyé avant sept jours.
6. Lorsque le service NMS est de nouveau disponible, envoie immédiatement un message AutoSupport si aucun message n'a été envoyé pendant sept jours ou plus.

Échec du message AutoSupport déclenché par l'utilisateur ou déclenché par un événement

Si l'envoi d'un message AutoSupport déclenché par l'utilisateur ou un événement ne parvient pas à s'effectuer, le système StorageGRID prend les actions suivantes :

1. Affiche un message d'erreur si l'erreur est connue. Par exemple, si un utilisateur sélectionne le protocole SMTP sans fournir les paramètres de configuration corrects de la messagerie, l'erreur suivante s'affiche : `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. Ne tente pas d'envoyer le message à nouveau.
3. Consigne l'erreur dans `nms.log`.

En cas de défaillance et si SMTP est le protocole sélectionné, vérifiez que le serveur de messagerie du système StorageGRID est correctement configuré et que votre serveur de messagerie est en cours d'exécution (**support** > **alarmes (hérité)** > **> Configuration de l'e-mail héritée**). Le message d'erreur suivant peut apparaître sur la page AutoSupport : `AutoSupport messages 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 dans le "moniteur et amp ; instructions de dépannage".

Échec de la correction d'un message AutoSupport

En cas d'échec et si SMTP est le protocole sélectionné, vérifiez que le serveur de messagerie du système StorageGRID est correctement configuré et que votre serveur de messagerie est en cours d'exécution. Le message d'erreur suivant peut apparaître sur la page AutoSupport : `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Informations associées

"Moniteur et amp ; dépannage"

Gestion des nœuds de stockage

Des nœuds de stockage fournissent de la capacité de stockage sur disque et des services. La gestion des nœuds de stockage consiste à contrôler la quantité d'espace utilisable sur chaque nœud, à l'aide des paramètres de filigrane et à appliquer les paramètres de configuration du nœud de stockage.

- "Qu'est-ce qu'un noeud de stockage"
- "Gestion des options de stockage"
- "Gestion du stockage des métadonnées d'objet"
- "Configuration des paramètres globaux des objets stockés"
- "Paramètres de configuration du nœud de stockage"
- "Gestion des nœuds de stockage complets"

Qu'est-ce qu'un noeud de stockage

Des nœuds de stockage gèrent et stockent les données et les métadonnées d'objets. Chaque système StorageGRID doit disposer d'au moins trois nœuds de stockage. Si

vous avez plusieurs sites, chaque site de votre système StorageGRID doit également disposer de trois nœuds de stockage.

Un nœud de stockage inclut les services et les processus nécessaires pour stocker, déplacer, vérifier et récupérer les données d'objet et les métadonnées sur le disque. Vous pouvez afficher des informations détaillées sur les nœuds de stockage sur la page **Nodes**.

Qu'est-ce que le service ADC

Le service contrôleur de domaine d'administration (ADC) authentifie les nœuds de la grille et leurs connexions entre eux. Le service ADC est hébergé sur chacun des trois premiers nœuds de stockage d'un site.

Le service ADC conserve les informations de topologie, notamment l'emplacement et la disponibilité des services. Lorsqu'un nœud de grille nécessite des informations provenant d'un autre nœud de grille ou qu'une action soit effectuée par un autre nœud de grille, il contacte un service ADC pour trouver le nœud de grille le plus adapté au traitement de sa demande. De plus, le service ADC conserve une copie des packs de configuration du déploiement StorageGRID, ce qui permet à n'importe quel nœud de la grille de récupérer les informations de configuration actuelles.vous pouvez afficher les informations ADC d'un nœud de stockage sur la page topologie de la grille (**support** > **topologie de grille**).

Pour faciliter les opérations distribuées et en attente, chaque service ADC synchronise les certificats, les lots de configuration et les informations sur les services et la topologie avec les autres services ADC du système StorageGRID.

En général, tous les nœuds de la grille maintiennent une connexion à au moins un service ADC. Les nœuds du grid accèdent ainsi aux informations les plus récentes. Lorsque les nœuds de la grille se connectent, ils mettent en cache les certificats d'autres nœuds de la grille, ce qui permet aux systèmes de continuer à fonctionner avec les nœuds de la grille connus même lorsqu'un service ADC n'est pas disponible. Les nouveaux nœuds de grille ne peuvent établir de connexions qu'à l'aide d'un service ADC.

La connexion de chaque nœud de grille permet au service ADC de collecter les informations de topologie. Ces informations sur le nœud de la grille incluent la charge CPU, l'espace disque disponible (si le système dispose de stockage), les services pris en charge et l'ID de site du nœud de la grille. D'autres services demandent au service ADC d'obtenir des informations sur la topologie par le biais de requêtes de topologie. Le service ADC répond à chaque requête avec les dernières informations reçues du système StorageGRID.

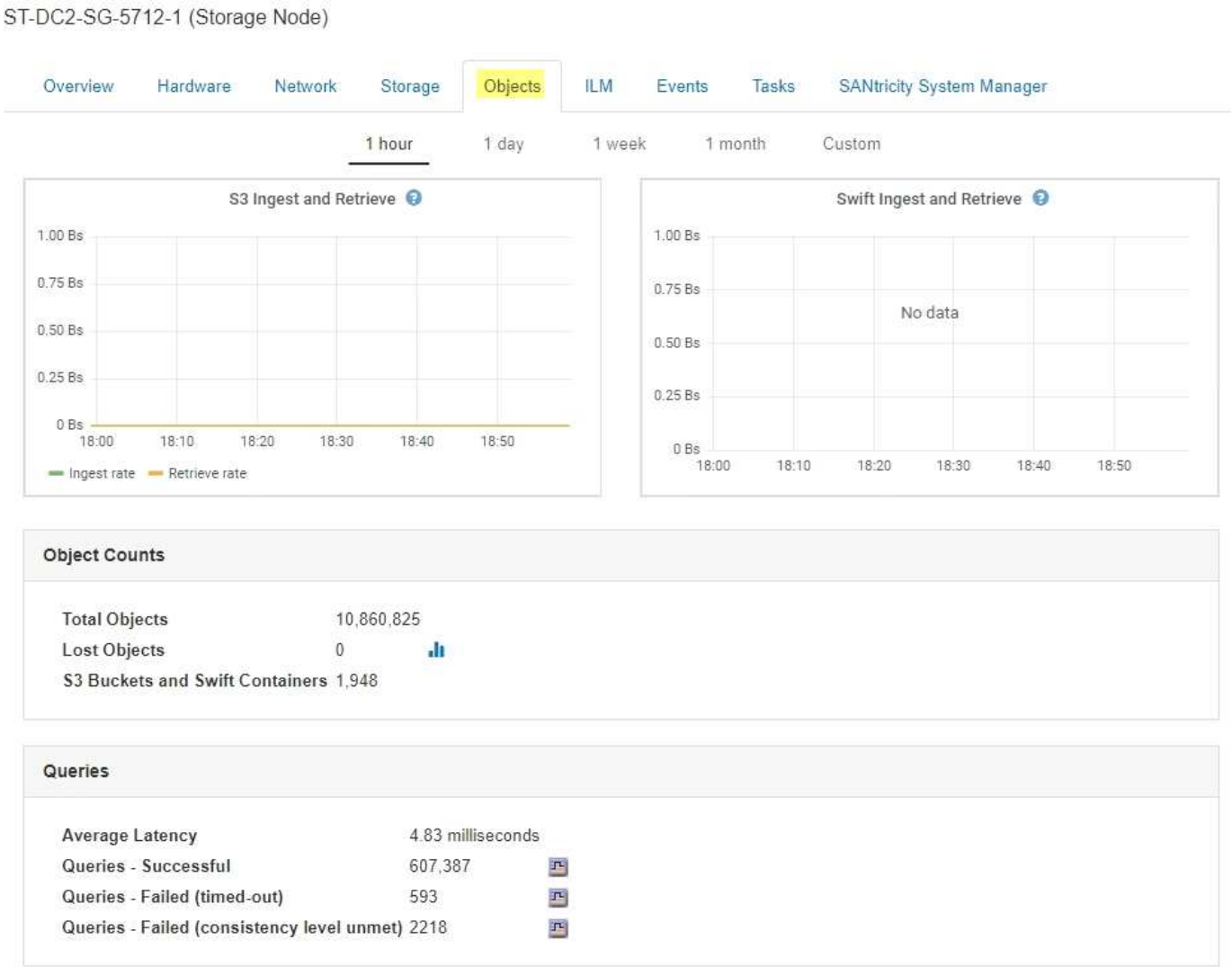
Qu'est-ce que le service DDS

Hébergé par un nœud de stockage, le service DDS (Distributed Data Store) s'interface avec la base de données Cassandra pour effectuer des tâches en arrière-plan sur les métadonnées d'objet stockées dans le système StorageGRID.

Nombre d'objets

Le service DDS suit le nombre total d'objets ingérés dans le système StorageGRID, ainsi que le nombre total d'objets ingérés par chacune des interfaces prises en charge par le système (S3 ou Swift).

Vous pouvez voir le nombre total d'objets sur la page nœuds > onglet objets pour n'importe quel nœud de stockage.



Requêtes

Vous pouvez identifier le temps moyen d'exécution d'une requête sur le magasin de métadonnées par le biais du service DDS spécifique, du nombre total de requêtes réussies et du nombre total de requêtes ayant échoué en raison d'un problème de délai d'attente.

Un examen des informations de requête peut être nécessaire afin de contrôler l'état du datastore Cassandra, ce qui a un impact sur les performances d'entrée et de récupération du système. Par exemple, si la latence d'une requête moyenne est lente et que le nombre de requêtes ayant échoué en raison de délais d'attente est élevé, le magasin de métadonnées peut rencontrer une charge plus élevée ou effectuer une autre opération.

Vous pouvez également afficher le nombre total de requêtes ayant échoué en raison d'échecs de cohérence. Les échecs de niveau de cohérence résultent d'un nombre insuffisant de magasins de métadonnées disponibles au moment où une requête est effectuée par le biais du service DDS spécifique.

Vous pouvez utiliser la page Diagnostics pour obtenir des informations supplémentaires sur l'état actuel de votre grille. Voir "Exécution des diagnostics".

Garanties et contrôles de cohérence

StorageGRID garantit la cohérence de lecture après écriture pour les nouveaux objets. Toute opération GET après une opération PUT réussie sera capable de lire les données récemment écrites. Les écrasements

d’objets existants, les mises à jour de métadonnées et les suppressions restent cohérents.

Est ce que est le service LDR

Hébergé par chaque nœud de stockage, le service LDR (local distribution Router) gère le transport de contenu pour le système StorageGRID. Le transport de contenu englobe de nombreuses tâches, dont le stockage des données, le routage et le traitement des demandes. Le service LDR fait la majorité des efforts considérables du système StorageGRID en gérant les charges de transfert de données et les fonctions de trafic de données.

Le service LDR gère les tâches suivantes :

- Requêtes
- Activité liée à la gestion du cycle de vie des informations (ILM)
- Suppression d’objet
- Stockage des données objet
- Transferts de données objet à partir d’un autre service LDR (nœud de stockage)
- Gestion du stockage des données
- Interfaces de protocole (S3 et Swift)

Le service LDR gère également le mappage d’objets S3 et Swift vers des UUID (« content handle ») uniques que le système StorageGRID attribue à chaque objet ingéré.

Requêtes

Les requêtes LDR incluent des requêtes pour l’emplacement des objets lors des opérations de récupération et d’archivage. Vous pouvez identifier le temps moyen d’exécution d’une requête, le nombre total de requêtes réussies et le nombre total de requêtes ayant échoué en raison d’un problème de délai d’attente.

Vous pouvez examiner les informations de requête afin de contrôler l’état du magasin de métadonnées, ce qui a un impact sur les performances d’entrée et de récupération du système. Par exemple, si la latence d’une requête moyenne est lente et que le nombre de requêtes ayant échoué en raison de délais d’attente est élevé, le magasin de métadonnées peut rencontrer une charge plus élevée ou effectuer une autre opération.

Vous pouvez également afficher le nombre total de requêtes ayant échoué en raison d’échecs de cohérence. Les défaillances de niveau de cohérence résultent d’un nombre insuffisant de magasins de métadonnées disponibles au moment où une requête est exécutée via le service LDR spécifique.

Vous pouvez utiliser la page Diagnostics pour obtenir des informations supplémentaires sur l’état actuel de votre grille. Voir "Exécution des diagnostics".

Activité des règles ILM

Les metrics de gestion du cycle de vie des informations vous permettent de surveiller la vitesse à laquelle les objets sont évalués pour la mise en œuvre de ILM. Vous pouvez afficher ces mesures dans le tableau de bord ou sur la page nœuds > l’onglet ILM de chaque nœud de stockage.

Magasins d’objets

Le stockage sous-jacent d’un service LDR est divisé en un nombre fixe de magasins d’objets (aussi appelés volumes de stockage). Chaque magasin d’objets est un point de montage distinct.

Les magasins d’objets d’un nœud de stockage s’affichent sur la page nœuds > onglet stockage.

Object Stores

ID	Size	Available	Replicated Data	EC Data	Object Data (%)	Health
0000	4.40 TB	1.35 TB	43.99 GB	0 bytes	1.00%	No Errors
0001	1.97 TB	1.57 TB	44.76 GB	351.14 GB	20.09%	No Errors
0002	1.97 TB	1.46 TB	43.29 GB	465.20 GB	25.81%	No Errors
0003	1.97 TB	1.70 TB	43.51 GB	223.98 GB	13.58%	No Errors
0004	1.97 TB	1.92 TB	44.03 GB	0 bytes	2.23%	No Errors
0005	1.97 TB	1.46 TB	43.67 GB	463.36 GB	25.73%	No Errors
0006	1.97 TB	1.92 TB	43.10 GB	1.61 GB	2.27%	No Errors
0007	1.97 TB	1.35 TB	46.05 GB	575.24 GB	31.53%	No Errors
0008	1.97 TB	1.81 TB	46.00 GB	112.84 GB	8.06%	No Errors
0009	1.97 TB	1.57 TB	43.91 GB	352.72 GB	20.13%	No Errors
000A	1.97 TB	1.70 TB	44.31 GB	226.81 GB	13.76%	No Errors
000B	1.97 TB	1.92 TB	43.17 GB	780.07 MB	2.23%	No Errors
000C	1.97 TB	1.58 TB	44.32 GB	339.56 GB	19.48%	No Errors
000D	1.97 TB	1.82 TB	44.47 GB	107.34 GB	7.70%	No Errors
000E	1.97 TB	1.68 TB	43.07 GB	241.70 GB	14.45%	No Errors
000F	2.03 TB	1.50 TB	44.57 GB	475.47 GB	25.67%	No Errors

Les magasins d'objets d'un nœud de stockage sont identifiés par un nombre hexadécimal compris entre 0000 et 002F, appelé ID de volume. L'espace est réservé dans le premier magasin d'objets (volume 0) pour les métadonnées d'objet dans une base de données Cassandra. Tout espace restant sur ce volume est utilisé pour les données d'objet. Tous les autres magasins d'objets sont exclusivement utilisés pour les données d'objet, notamment les copies répliquées et les fragments avec code d'effacement.

Pour garantir même l'utilisation de l'espace pour les copies répliquées, les données d'objet d'un objet donné sont stockées dans un magasin d'objets basé sur l'espace de stockage disponible. Lorsqu'un ou plusieurs magasins d'objets sont remplis à la capacité, les magasins d'objets restants continuent de stocker des objets jusqu'à ce qu'il n'y ait plus d'espace sur le nœud de stockage.

Protection des métadonnées

Les métadonnées de l'objet sont des informations liées ou une description d'un objet. Par exemple, l'heure de modification de l'objet ou l'emplacement de stockage. StorageGRID stocke les métadonnées d'objet dans une base de données Cassandra, qui assure l'interface avec le service LDR.

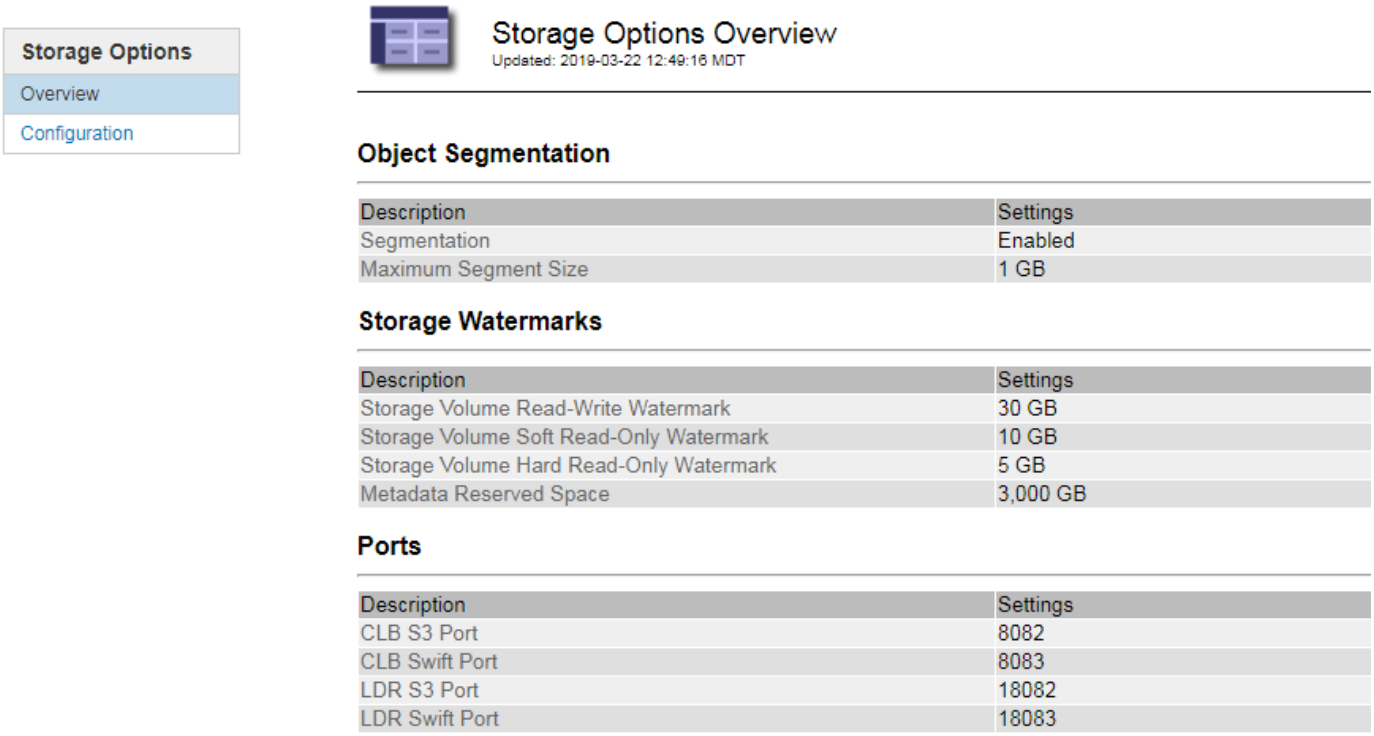
Pour assurer la redondance et ainsi la protection contre la perte, trois copies des métadonnées d'objet sont conservées sur chaque site. Les copies sont réparties de manière homogène sur tous les nœuds de stockage de chaque site. Cette réplication n'est pas configurable et se fait automatiquement.

"Gestion du stockage des métadonnées d'objet"

Gestion des options de stockage

Vous pouvez afficher et configurer les options de stockage à l'aide du menu Configuration du Gestionnaire de grille. Les options de stockage incluent les paramètres de segmentation des objets et les valeurs actuelles pour les filigranes de stockage. Vous pouvez également afficher les ports S3 et Swift utilisés par le service CLB obsolète sur les nœuds de passerelle et par le service LDR sur les nœuds de stockage.

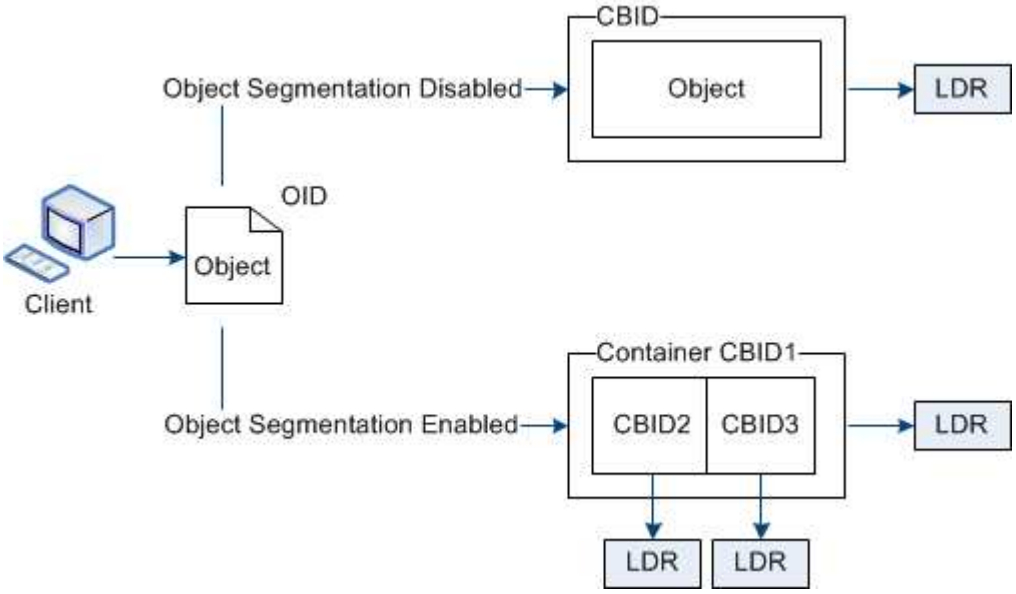
Pour plus d'informations sur les affectations de ports, reportez-vous à la section "Résumé : adresses IP et ports pour les connexions client".



La segmentation des objets

La segmentation d'objet consiste à diviser un objet en un ensemble d'objets de plus petite taille afin d'optimiser l'utilisation des ressources et du stockage pour les objets volumineux. Le téléchargement multi-pièces S3 crée également des objets segmentés, avec un objet représentant chaque pièce.

Lorsqu'un objet est ingéré dans le système StorageGRID, le service LDR divise l'objet en segments et crée un conteneur de segments qui répertorie les informations d'en-tête de tous les segments en tant que contenu.



Si votre système StorageGRID inclut un nœud d'archivage dont le type cible est NetApp Cloud Tiering — simple Storage Service et le système de stockage d'archives ciblé est Amazon Web Services (AWS), la taille de segment maximale doit être inférieure ou égale à 4.5 Gio (4,831,838,208 octets). Cette limite supérieure garantit que la limite DE cinq Go D'AWS PUT n'est pas dépassée. Les demandes vers AWS qui dépassent cette valeur ont échoué.

Lors de la récupération d'un conteneur de segments, le service LDR assemble l'objet original à partir de ses segments et renvoie l'objet au client.

Le conteneur et les segments ne sont pas nécessairement stockés sur le même noeud de stockage. Le conteneur et les segments peuvent être stockés sur n'importe quel nœud de stockage.

Chaque segment est traité indépendamment par le système StorageGRID et contribue au nombre d'attributs tels que les objets gérés et les objets stockés. Par exemple, si un objet stocké dans le système StorageGRID est divisé en deux segments, la valeur des objets gérés augmente de trois après la fin de l'acquisition, comme suit :

conteneur de segments + segment 1 + segment 2 = trois objets stockés

Vous pouvez améliorer les performances lors de la manipulation d'objets volumineux en vous assurant que :

- Chaque passerelle et nœud de stockage dispose d'une bande passante réseau suffisante pour le débit requis. Par exemple, configurez des réseaux Grid et client distincts sur des interfaces Ethernet 10 Gbits/s.
- Suffisamment de nœuds de passerelle et de stockage sont déployés pour le débit requis.
- Chaque nœud de stockage dispose de performances d'E/S de disque suffisantes pour le débit requis.

Quels sont les filigranes du volume de stockage

StorageGRID utilise des filigranes du volume de stockage qui permettent de surveiller la quantité d'espace utilisable disponible sur les nœuds de stockage. Si la quantité d'espace disponible sur un nœud est inférieure à un paramètre de filigrane configuré, l'alarme Storage Status (SSTS) est déclenchée pour vous permettre de déterminer si vous devez ajouter des nœuds de stockage.

Pour afficher les paramètres actuels des filigranes du volume de stockage, sélectionnez **Configuration** > **Options de stockage** > **Présentation**.

Storage Options Overview

Updated: 2019-10-09 13:09:30 MDT

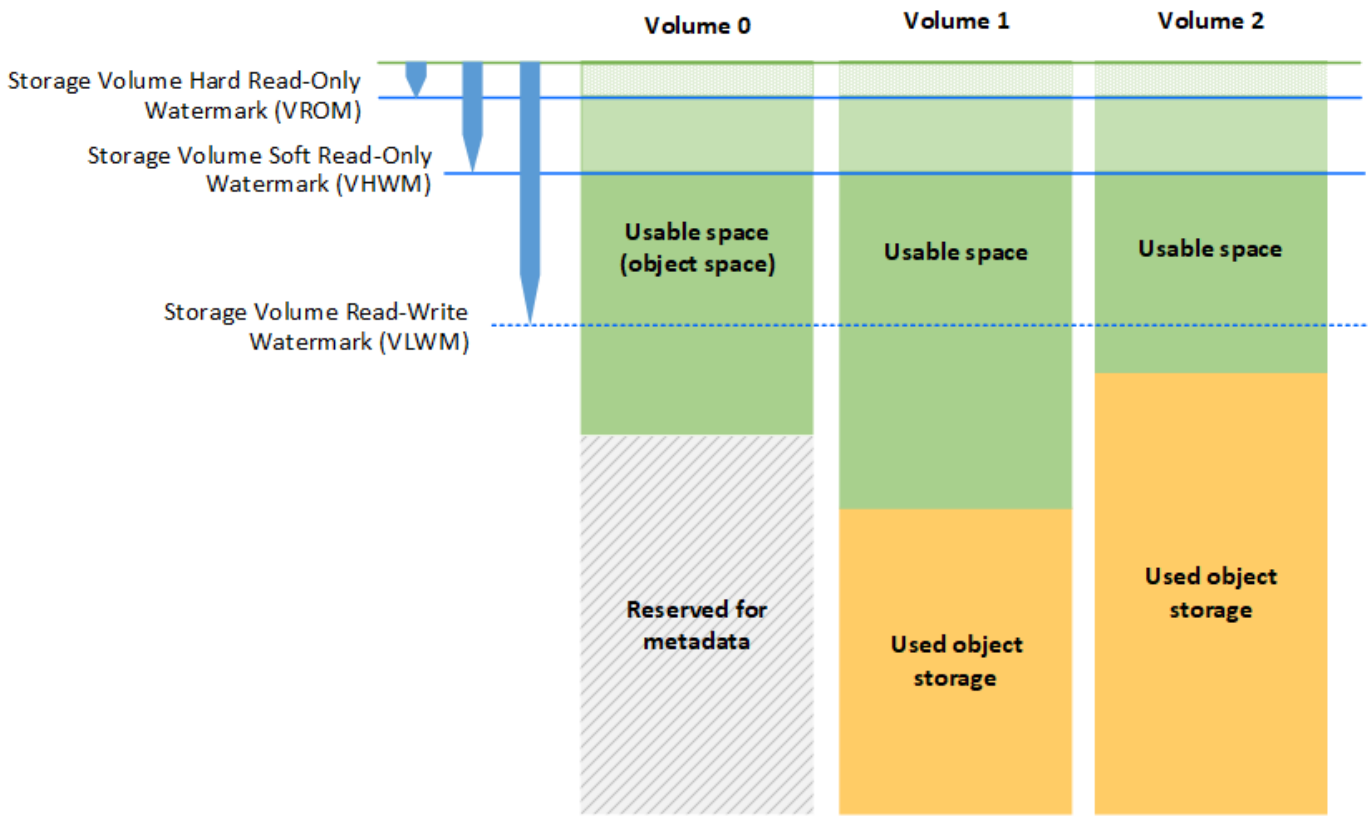
Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	3,000 GB

La figure suivante représente un nœud de stockage avec trois volumes et indique la position relative des trois filigranes du volume de stockage. Dans chaque nœud de stockage, StorageGRID se réserve l'espace sur le volume 0 pour les métadonnées d'objet. Tout espace restant sur ce volume est utilisé pour les données d'objet. Tous les autres volumes sont utilisés exclusivement pour les données d'objet, notamment les copies répliquées et les fragments avec code d'effacement.



Les filigranes du volume de stockage sont des valeurs par défaut qui indiquent la quantité minimale d'espace libre requise sur chaque volume du nœud de stockage afin d'empêcher les StorageGRID de modifier le comportement de lecture/écriture du nœud ou de déclencher une alarme. Notez que tous les volumes doivent atteindre le filigrane avant que StorageGRID ne prenne l'action. Si certains volumes ont plus que la quantité minimale d'espace disponible requise, l'alarme n'est pas déclenchée et le comportement de lecture/écriture du nœud ne change pas.

Filigrane volume de stockage en lecture seule (VHWM)

Le filigrane en lecture seule programmable du volume de stockage est le premier filigrane indiquant que l'espace utilisable d'un nœud pour les données d'objet est en train de devenir plein. Ce filigrane représente la quantité d'espace disponible sur chaque volume d'un nœud de stockage pour empêcher le nœud de passer en « mode de lecture seule par logiciel libre ». Le mode de lecture seule souple signifie que le nœud de stockage annonce des services en lecture seule au reste du système StorageGRID, mais remplit toutes les demandes d'écriture en attente.

Si la quantité d'espace disponible sur chaque volume est inférieure à la valeur définie pour ce filigrane, l'alarme Storage Status (SSTS) est déclenchée au niveau Notice et et le nœud de stockage passe en mode lecture seule souple.

Par exemple, supposons que le filigrane de volume de stockage en lecture seule soit défini sur 10 Go, ce qui est sa valeur par défaut. Si moins de 10 Go d'espace libre reste sur chaque volume du nœud de stockage, l'alarme SSTS est déclenchée au niveau Avertissement et le nœud de stockage passe en mode lecture seule souple.

Filigrane en lecture seule (VROM) du volume de stockage

Le filigrane en lecture seule matérielle du volume de stockage est le filigrane suivant pour indiquer que l'espace utilisable d'un nœud pour les données d'objet est en train de devenir plein. Ce filigrane représente la quantité d'espace disponible sur chaque volume d'un nœud de stockage pour empêcher le nœud de passer en mode « lecture seule matérielle ». Le mode lecture seule matériel signifie que le nœud de stockage est en lecture seule et n'accepte plus les demandes d'écriture.

Si la quantité d'espace disponible sur chaque volume d'un nœud de stockage est inférieure au paramètre de ce filigrane, l'alarme Storage Status (SSTS) est déclenchée au niveau majeur et le nœud de stockage passe en mode lecture seule.

Par exemple, supposons que le filigrane du volume de stockage en lecture seule est défini sur 5 Go, ce qui est sa valeur par défaut. Si moins de 5 Go d'espace libre reste sur chaque volume de stockage du nœud de stockage, l'alarme SSTS est déclenchée au niveau principal et le nœud de stockage passe en mode lecture seule matériel.

La valeur du filigrane du volume de stockage en lecture seule matérielle doit être inférieure à la valeur du filigrane du volume de stockage en lecture seule.

Filigrane de lecture/écriture du volume de stockage (VLWM)

Le filigrane en lecture-écriture du volume de stockage ne s'applique qu'aux nœuds de stockage ayant migré en mode lecture seule. Ce filigrane détermine quand le noeud de stockage est autorisé à revenir en lecture/écriture.

Supposons par exemple qu'un nœud de stockage est passé en mode lecture seule rigide. Si le filigrane en lecture/écriture du volume de stockage est défini sur 30 Go (valeur par défaut), l'espace libre de chaque volume de stockage du nœud de stockage doit passer de 5 Go à 30 Go avant que le nœud ne puisse à nouveau lire/écrire.

La valeur du filigrane de lecture-écriture du volume de stockage doit être supérieure à la valeur du filigrane de lecture seule programmable du volume de stockage.

Informations associées

"Gestion des nœuds de stockage complets"

Gestion du stockage des métadonnées d'objet

La capacité des métadonnées d'objet d'un système StorageGRID contrôle le nombre maximal d'objets qui peuvent être stockés sur le système en question. Pour s'assurer que votre système StorageGRID dispose d'un espace suffisant pour stocker les nouveaux objets, vous devez comprendre où et comment StorageGRID stocke les métadonnées d'objet.

Qu'est-ce que les métadonnées d'objet ?

Les métadonnées d'objet constituent toutes les informations qui décrivent un objet. StorageGRID utilise les métadonnées d'objet pour suivre l'emplacement de tous les objets de la grille, et pour gérer le cycle de vie de chaque objet au fil du temps.

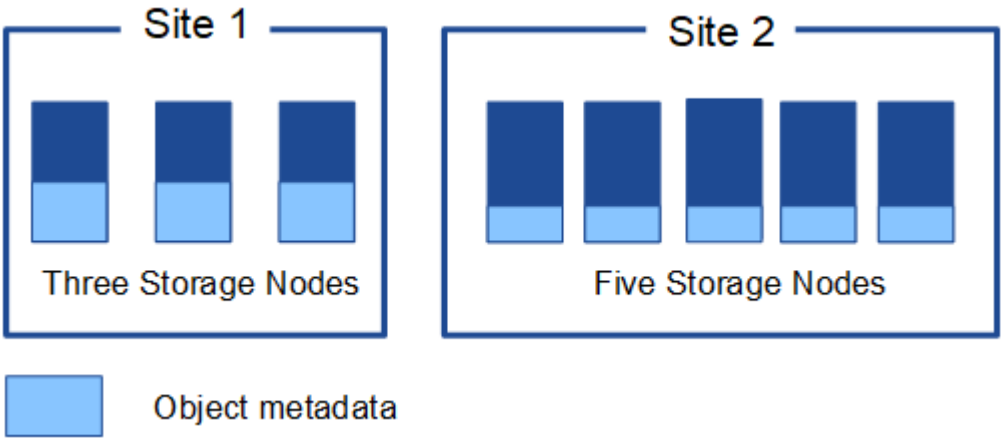
Pour un objet dans StorageGRID, les métadonnées d'objet incluent les types d'information suivants :

- Les métadonnées du système, y compris un ID unique pour chaque objet (UUID), le nom de l'objet, le nom du compartiment S3 ou du conteneur Swift, le nom ou l'ID 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 de clé-valeur de métadonnées utilisateur personnalisées associées à l'objet.
- Pour les objets S3, toutes les paires de clé-valeur de balise d'objet associées à l'objet.
- Pour les copies d'objet répliquées, emplacement de stockage actuel de chaque copie.
- Pour les copies d'objets avec code d'effacement, l'emplacement de stockage actuel de chaque fragment.
- Pour les copies d'objet dans Cloud Storage Pool, l'emplacement de l'objet, notamment le nom du compartiment externe et l'identifiant unique de l'objet.
- Pour les objets segmentés et les objets à plusieurs parties, les identificateurs de segment et la taille des données.

Comment les métadonnées d'objet sont-elles stockées ?

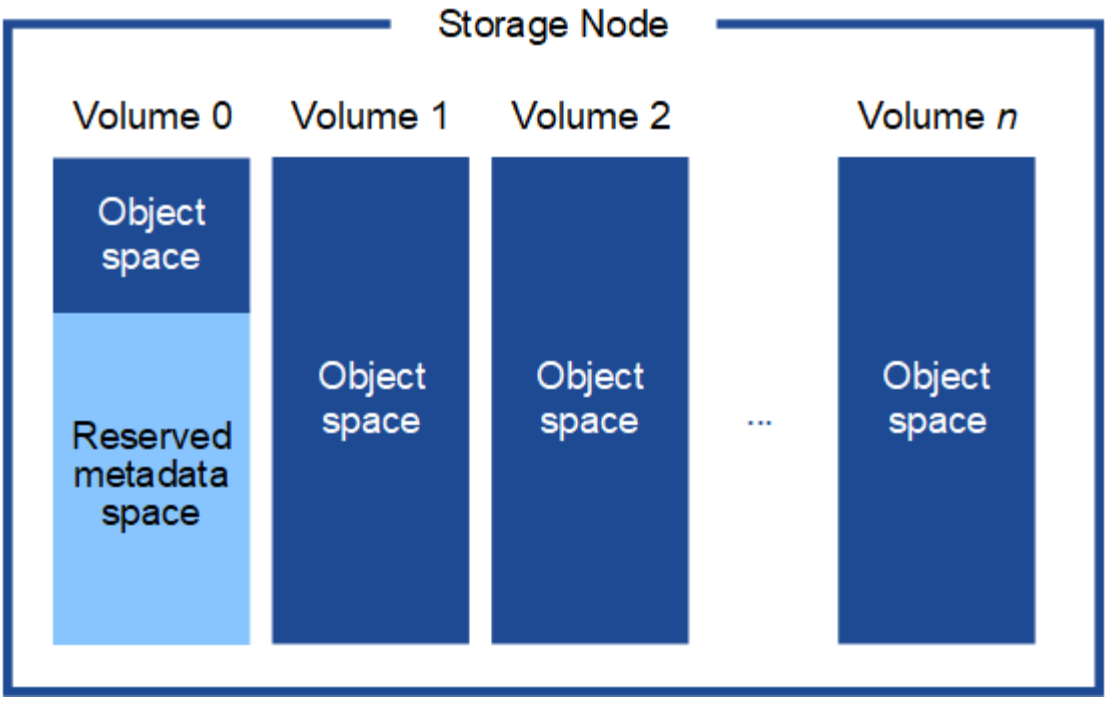
Les métadonnées d'objet sont conservées dans une base de données Cassandra, stockée indépendamment des données d'objet. StorageGRID Pour assurer la redondance et protéger les métadonnées d'objet contre la perte, StorageGRID stocke trois copies des métadonnées de tous les objets du système sur chaque site. Les trois copies de métadonnées d'objet sont réparties de manière uniforme sur tous les nœuds de stockage de chaque site.

Cette figure représente les nœuds de stockage sur deux sites. Chaque site dispose de la même quantité de métadonnées d'objet, qui sont réparties de la même manière sur les nœuds de stockage sur ce site.



Où sont stockées les métadonnées d'objet ?

Cette figure représente les volumes de stockage d'un seul nœud de stockage.



Comme illustré dans la figure, StorageGRID réserve l'espace des métadonnées d'objet sur le volume de stockage 0 de chaque nœud de stockage. Il utilise l'espace réservé pour stocker les métadonnées d'objet et effectuer les opérations essentielles de la base de données. Tout espace restant sur le volume de stockage 0 et tous les autres volumes du nœud de stockage sont utilisés exclusivement pour les données d'objet (copies répliquées et fragments avec code d'effacement).

La quantité d'espace réservé aux métadonnées d'objet sur un nœud de stockage particulier dépend d'un certain nombre de facteurs, décrits ci-dessous.

Paramètre Metadata Reserved Space

Le paramètre *Metadata Reserved Space* 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 noeud de stockage. Comme indiqué dans le tableau, la valeur par défaut de ce paramètre pour StorageGRID 11.5 est basée sur les éléments suivants :

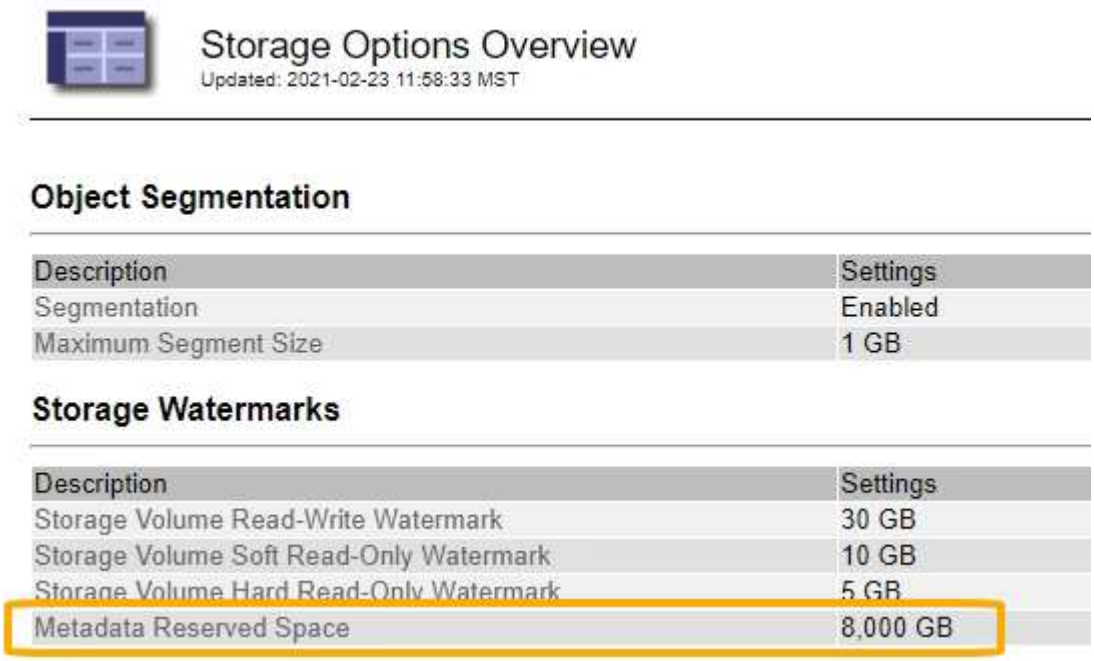
- La version du logiciel que vous utilisiez lors de l'installation initiale de StorageGRID.
- Quantité de RAM sur chaque nœud de stockage.

Version utilisée pour l'installation initiale de StorageGRID	Quantité de RAM sur les nœuds de stockage	Paramètre d'espace réservé aux métadonnées par défaut pour StorageGRID 11.5
11.5	Au moins 128 Go sur chaque nœud de stockage de la grille	8 TO (8,000 GO)
	Moins de 128 Go sur n'importe quel nœud de stockage de la grille	3 TO (3,000 GO)
11.1 à 11.4	128 Go ou plus sur chaque nœud de stockage sur un site	4 TO (4,000 GO)

Version utilisée pour l'installation initiale de StorageGRID	Quantité de RAM sur les nœuds de stockage	Paramètre d'espace réservé aux métadonnées par défaut pour StorageGRID 11.5
	Moins de 128 Go sur n'importe quel nœud de stockage de chaque site	3 TO (3,000 GO)
11.0 ou antérieure	Tout montant	2 TO (2,000 GO)

Pour afficher le paramètre espace réservé aux métadonnées de votre système StorageGRID :

1. Sélectionnez **Configuration** > **Paramètres système** > **Options de stockage**.
2. Dans le tableau des filigranes de stockage, localisez **espace réservé de métadonnées**.



Dans la capture d'écran, la valeur **Metadata Reserved Space** est de 8,000 Go (8 To). Il s'agit du paramètre par défaut pour une nouvelle installation StorageGRID 11.5 dans laquelle chaque nœud de stockage dispose d'au moins 128 Go de RAM.

Espace réservé réel pour les métadonnées

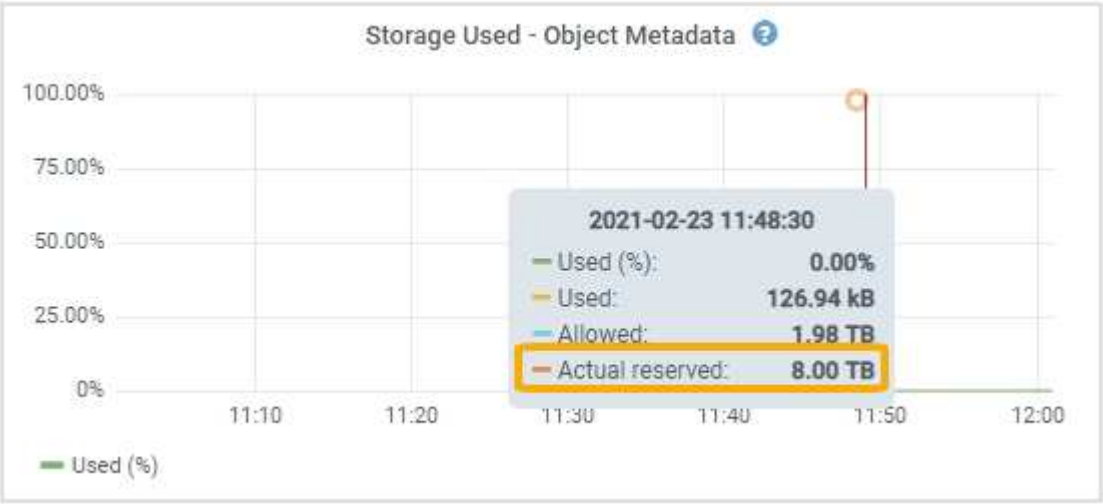
Contrairement au paramètre espace réservé aux métadonnées pour l'ensemble du système, le paramètre *espace réservé réel* pour les métadonnées d'objet est déterminé pour chaque nœud de stockage. Pour un nœud de stockage donné, l'espace réservé réel pour les métadonnées dépend de la taille du volume 0 pour le nœud et du paramètre espace réservé * métadonnées * pour l'ensemble du système.

Taille du volume 0 pour le nœud	Espace réservé réel pour les métadonnées
Moins de 500 Go (non utilisé en production)	10 % du volume 0

Taille du volume 0 pour le nœud	Espace réservé réel pour les métadonnées
500 Go ou plus	Plus ces valeurs sont faibles : • Volume 0 • Paramètre Metadata Reserved Space

Pour afficher l'espace réservé réel pour les métadonnées sur un nœud de stockage particulier :

1. Dans Grid Manager, sélectionnez **noeuds** > ***Storage Node***.
2. Sélectionnez l'onglet **stockage**.
3. Placez le curseur sur le diagramme stockage utilisé — métadonnées objet et localisez la valeur **réservé réelle**.



Dans la capture d'écran, la valeur **réelle réservée** est de 8 To. Cette copie d'écran concerne un nœud de stockage grand format dans une nouvelle installation de StorageGRID 11.5. Étant donné que le paramètre espace réservé aux métadonnées pour l'ensemble du système est inférieur au volume 0 pour ce nœud de stockage, l'espace réservé réel pour ce nœud est égal au paramètre espace réservé aux métadonnées.

La valeur **réservation réelle** correspond à cette mesure Prometheus :

```
storagegrid_storage_utilization_metadata_reserved_bytes
```

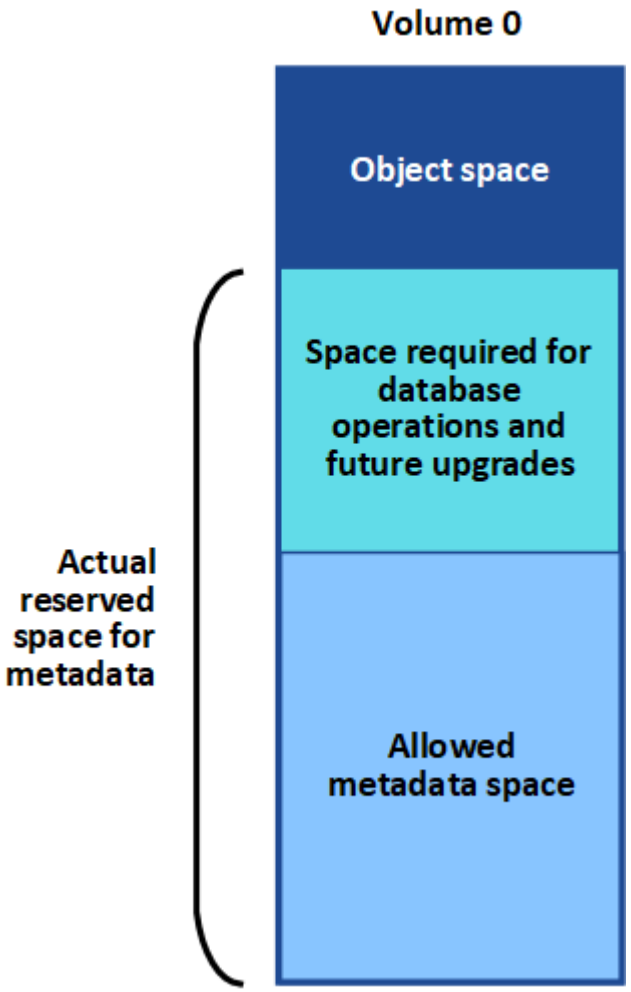
Exemple d'espace de métadonnées réservé réel

Supposons que vous installiez un nouveau système StorageGRID à l'aide de la version 11.5. Dans cet exemple, supposons que chaque nœud de stockage dispose de plus de 128 Go de RAM et que le volume 0 du nœud de stockage 1 (SN1) est de 6 To. Sur la base de ces valeurs :

- L'espace réservé * métadonnées* pour l'ensemble du système est défini sur 8 To. (Il s'agit de la valeur par défaut pour une nouvelle installation StorageGRID 11.5 si chaque nœud de stockage dispose de plus de 128 Go de RAM.)
- L'espace réservé réel pour les métadonnées pour SN1 est de 6 To. (Le volume entier est réservé car le volume 0 est inférieur au paramètre **Metadata Reserved Space**.)

Espace de métadonnées autorisé

L'espace réservé réel de chaque nœud de stockage pour les métadonnées est divisé en l'espace disponible pour les métadonnées d'objet (l'espace *autorisé metadata space*) et l'espace requis pour les opérations essentielles de bases de données (telles que la compaction et la réparation) et les mises à niveau matérielles et logicielles futures. L'espace de métadonnées autorisé régit la capacité globale des objets.



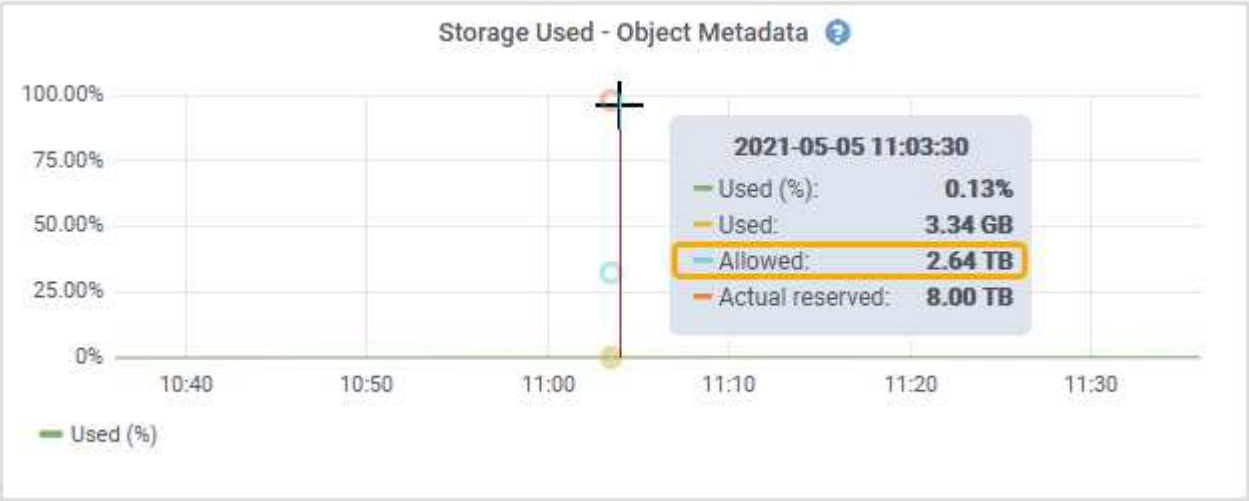
Le tableau suivant récapitule la valeur d'espace de métadonnées autorisé pour un nœud de stockage StorageGRID.

Espace réservé réel pour les métadonnées	Espace de métadonnées autorisé
4 To ou moins	60 % de l'espace réservé réel pour les métadonnées, jusqu'à un maximum de 1.98 To
Plus de 4 To	(Espace réservé réel pour les métadonnées − 1 To) × 60 %, jusqu'à un maximum de 2.64 To

Si votre système StorageGRID stocke (ou doit stocker) plus de 2.64 To de métadonnées sur un nœud de stockage, l'espace de métadonnées autorisé peut être augmenté dans certains cas. Si vos nœuds de stockage disposent chacun de plus de 128 Go de RAM et d'espace disponible sur le volume de stockage 0, contactez votre représentant NetApp. Nous examinerons vos besoins et augmenterons l'espace de métadonnées autorisé pour chaque nœud de stockage, si possible.

Pour afficher l'espace de métadonnées autorisé pour un nœud de stockage :

1. Dans Grid Manager, sélectionnez **Node** > ***Storage Node***.
2. Sélectionnez l'onglet **stockage**.
3. Placez le curseur sur le diagramme stockage utilisé — métadonnées objet et localisez la valeur **autorisé**.



Dans la capture d'écran, la valeur **autorisé** est de 2.64 To, ce qui est la valeur maximale pour un noeud de stockage dont l'espace réservé réel pour les métadonnées est supérieur à 4 To.

La valeur **autorisé** correspond à cette métrique Prometheus :

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Exemple d'espace de métadonnées autorisé

Supposons que vous installez un système StorageGRID avec la version 11.5. Dans cet exemple, supposons que chaque nœud de stockage dispose de plus de 128 Go de RAM et que le volume 0 du nœud de stockage 1 (SN1) est de 6 To. Sur la base de ces valeurs :

- L'espace réservé * métadonnées* pour l'ensemble du système est défini sur 8 To. (Il s'agit de la valeur par défaut pour StorageGRID 11.5 lorsque chaque nœud de stockage dispose de plus de 128 Go de RAM.)
- L'espace réservé réel pour les métadonnées pour SN1 est de 6 To. (Le volume entier est réservé car le volume 0 est inférieur au paramètre **Metadata Reserved Space**.)
- L'espace autorisé pour les métadonnées sur SN1 est de 2.64 To. (Il s'agit de la valeur maximale de l'espace réservé réel.)

La façon dont les nœuds de stockage de différentes tailles affectent la capacité des objets

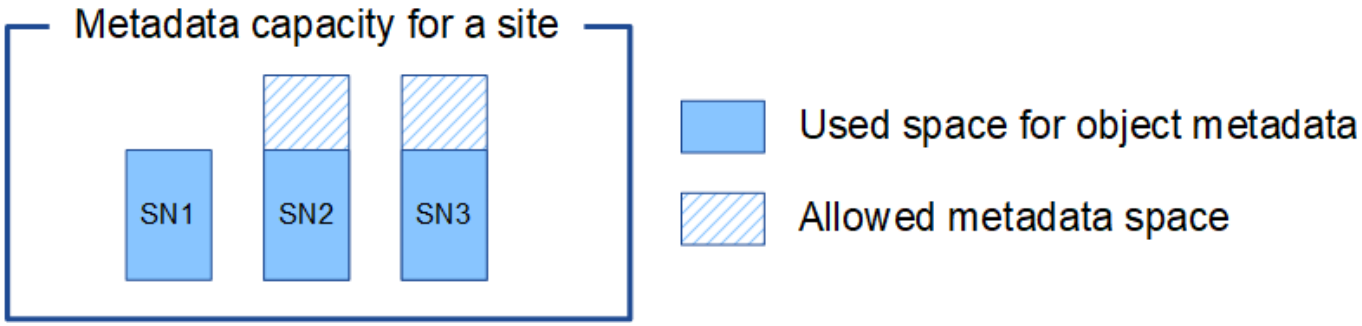
Comme décrit ci-dessus, StorageGRID distribue uniformément les métadonnées d'objet sur les nœuds de stockage sur chaque site. Par conséquent, si un site contient des nœuds de stockage de différentes tailles, le plus petit nœud du site détermine la capacité des métadonnées du site.

Prenons l'exemple suivant :

- Une grille sur un seul site contient trois nœuds de stockage de tailles différentes.
- Le paramètre **Metadata Reserved Space** est de 4 To.
- Les nœuds de stockage ont les valeurs suivantes pour l'espace réservé réel des métadonnées et l'espace autorisé pour les métadonnées.

Nœud de stockage	Taille du volume 0	Espace réservé réel des métadonnées	Espace de métadonnées autorisé
SN1	2.2 TO	2.2 TO	1.32 TO
SN2	5 TO	4 TO	1.98 TO
SN3	6 To	4 TO	1.98 TO

Les métadonnées de l'objet sont réparties de manière uniforme sur les nœuds de stockage d'un site. En effet, chaque nœud de cet exemple ne peut contenir que 1.32 To de métadonnées. Les 0.66 To supplémentaires d'espace de métadonnées autorisé pour SN2 et SN3 ne peuvent pas être utilisés.



De même, puisque StorageGRID conserve toutes les métadonnées d'objet d'un système StorageGRID sur chaque site, la capacité globale des métadonnées d'un système StorageGRID est déterminée par la capacité des métadonnées d'objet du plus petit site.

Étant donné que la capacité des métadonnées contrôle le nombre maximal d'objets, lorsqu'un nœud vient à manquer de capacité de métadonnées, la grille est véritablement pleine.

Informations associées

- Pour apprendre à contrôler la capacité de métadonnées d'objet pour chaque nœud de stockage :

  "Moniteur et amp ; dépannage"

- Pour augmenter la capacité des métadonnées des objets de votre système, vous devez ajouter de nouveaux nœuds de stockage :

"Développez votre grille"

Configuration des paramètres globaux des objets stockés

Vous pouvez utiliser les options de grille pour configurer les paramètres de tous les objets stockés dans votre système StorageGRID, y compris la compression des objets stockés et le chiffrement des objets stockés. et objet stocké hachage.

- "Configuration de la compression des objets stockés"
- "Configuration du chiffrement des objets stockés"
- "Configuration du hachage de l'objet stocké"

Configuration de la compression des objets stockés

Vous pouvez utiliser l'option de grille Compress objets stockés pour réduire la taille des objets stockés dans StorageGRID, de sorte que les objets consomment moins de stockage.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Par défaut, l'option de grille de compression des objets stockés est désactivée. Si vous activez cette option, StorageGRID tente de compresser chaque objet lors de son enregistrement, en utilisant la compression sans perte.

> Si vous modifiez ce paramètre, il faudra environ une minute pour appliquer le nouveau paramètre. La valeur configurée est mise en cache pour les performances et l'évolutivité.

Avant d'activer cette option, tenez compte des points suivants :

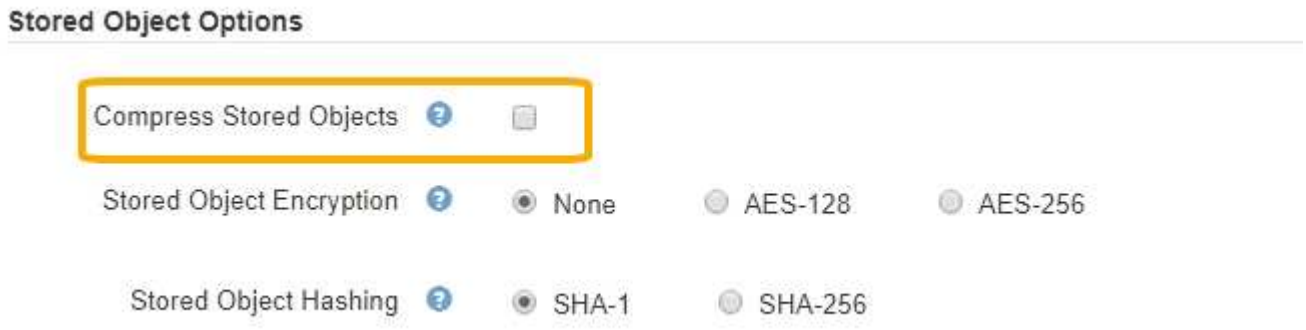
- Vous ne devez pas activer la compression, sauf si vous savez que les données stockées sont compressibles.
- Les applications qui enregistrent des objets dans StorageGRID peuvent compresser les objets avant de les enregistrer. Si une application client a déjà compressé un objet avant de l'enregistrer dans StorageGRID, l'activation de la compression des objets stockés ne réduira pas davantage la taille d'un objet.
- N'activez pas la compression si vous utilisez NetApp FabricPool avec StorageGRID.
- Si l'option de grille objets stockés de compression est activée, les applications client S3 et Swift doivent éviter d'exécuter des opérations GET Object qui indiquent une plage d'octets à renvoyer. Ces opérations de « lecture à plage » sont inefficaces, car StorageGRID doit décompresser efficacement les objets pour accéder aux octets demandés. LES opérations GET Object qui demandent une petite plage d'octets provenant d'un objet très volumineux sont particulièrement inefficaces. Par exemple, il est inefficace de lire une plage de 10 Mo sur un objet compressé de 50 Go.

  Si les plages sont lues à partir d'objets compressés, les demandes client peuvent être en attente.

> Si vous devez compresser des objets et que votre application client doit utiliser des lectures de plage, augmentez le délai de lecture de l'application.

Étapes

1. Sélectionnez **Configuration** > **Paramètres système** > **Options de grille**.
2. Dans la section Options des objets stockés, cochez la case **Compresser objets enregistrés**.



3. Cliquez sur **Enregistrer**.

Configuration du chiffrement des objets stockés

Vous pouvez crypter les objets stockés si vous souhaitez vous assurer que les données ne peuvent pas être récupérées sous une forme lisible si un magasin d'objets est compromis. Par défaut, les objets ne sont pas chiffrés.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Le chiffrement d'objets stocké permet le chiffrement de toutes les données d'objet à leur entrée via S3 ou Swift. Lorsque vous activez le paramètre, tous les objets récemment acquis sont chiffrés, mais aucun changement n'est apporté aux objets stockés existants. Si vous désactivez le chiffrement, les objets chiffrés restent chiffrés, mais les objets récemment ingérées ne sont pas chiffrés.

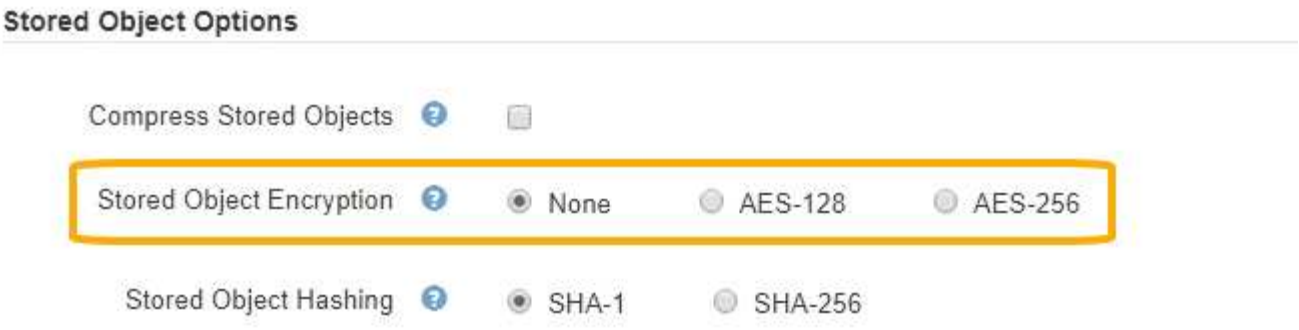
> Si vous modifiez ce paramètre, il faudra environ une minute pour appliquer le nouveau paramètre. La valeur configurée est mise en cache pour les performances et l'évolutivité.

Les objets stockés peuvent être cryptés à l'aide de l'algorithme de cryptage AES-128 ou AES-256.

Le paramètre de chiffrement d'objet stocké s'applique uniquement aux objets S3 qui n'ont pas été chiffrés par chiffrement au niveau du compartiment ou de l'objet.

Étapes

1. Sélectionnez **Configuration** > **Paramètres système** > **Options de grille**.
2. Dans la section Options d'objet stocké, définissez le chiffrement d'objet stocké sur **None** (par défaut), **AES-128** ou **AES-256**.



3. Cliquez sur **Enregistrer**.

Configuration du hachage de l'objet stocké

L'option de hachage d'objet stocké spécifie l'algorithme de hachage utilisé pour vérifier l'intégrité des objets.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Par défaut, les données d'objet sont hachées à l'aide de l'algorithme SHA-1. L'algorithme SHA-256 nécessite des ressources CPU supplémentaires et n'est généralement pas recommandé pour la vérification de l'intégrité.

> Si vous modifiez ce paramètre, il faudra environ une minute pour appliquer le nouveau paramètre. La valeur configurée est mise en cache pour les performances et l'évolutivité.

Étapes

1. Sélectionnez **Configuration** > **Paramètres système** > **Options de grille**.
2. Dans la section Options des objets stockés, définissez hachage de l'objet stocké sur **SHA-1** (par défaut) ou **SHA-256**.

3. Cliquez sur **Enregistrer**.

Paramètres de configuration du nœud de stockage

Chaque nœud de stockage utilise un certain nombre de paramètres de configuration et

de compteurs. Vous devrez peut-être afficher les paramètres actuels ou réinitialiser les compteurs pour effacer les alarmes (système hérité).

> Sauf en cas d'instruction spécifique dans la documentation, consultez le support technique avant de modifier les paramètres de configuration des nœuds de stockage. Si nécessaire, vous pouvez réinitialiser les compteurs d'événements pour effacer les alarmes héritées.

Pour accéder aux paramètres de configuration et aux compteurs d'un nœud de stockage :

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez ***site*** > ***Storage Node***.
3. Développez le nœud de stockage et sélectionnez le service ou le composant.
4. Sélectionnez l'onglet **Configuration**.

Les tableaux suivants résument les paramètres de configuration du nœud de stockage.

LDR

Nom d'attribut	Code	Description
État HTTP	HSTE	État actuel du protocole HTTP pour S3, Swift et autre trafic StorageGRID interne : • Hors ligne : aucune opération n'est autorisée et toute application client qui tente d'ouvrir une session HTTP au service LDR reçoit un message d'erreur. Les sessions actives sont normalement fermées. • En ligne : le fonctionnement se poursuit normalement
Démarrage automatique HTTP	HTA	• Si cette option est sélectionnée, l'état du système au redémarrage dépend de l'état du composant **LDR** > **Storage**. Si le composant **LDR** > **Storage** est en lecture seule au redémarrage, l'interface HTTP est également en lecture seule. Si le composant **LDR** > **Storage** est en ligne, HTTP est également en ligne. Dans le cas contraire, l'interface HTTP reste à l'état hors ligne. • Si elle n'est pas sélectionnée, l'interface HTTP reste hors ligne jusqu'à ce qu'elle soit explicitement activée.

LDR > datastore

Nom d'attribut	Code	Description
Réinitialiser le nombre d'objets perdus	RCOR	Réinitialisez le compteur du nombre d'objets perdus sur ce service.

LDR > stockage

Nom d'attribut	Code	Description
État de stockage — souhaité	SSD	Paramètre configurable par l'utilisateur pour l'état souhaité du composant de stockage. Le service LDR lit cette valeur et tente de faire correspondre l'état indiqué par cet attribut. La valeur est persistante entre les redémarrages. Par exemple, vous pouvez utiliser ce paramètre pour forcer le stockage à devenir en lecture seule, même en présence d'un espace de stockage disponible suffisant. Ceci peut être utile pour le dépannage. L'attribut peut prendre l'une des valeurs suivantes : • Hors ligne : lorsque l'état souhaité est hors ligne, le service LDR met le composant **LDR** > **Storage** hors ligne. • Lecture seule : lorsque l'état souhaité est en lecture seule, le service LDR déplace l'état du stockage en lecture seule et arrête d'accepter le nouveau contenu. Notez que le contenu peut continuer à être enregistré sur le nœud de stockage pendant une courte période jusqu'à la fermeture des sessions ouvertes. • En ligne : conservez la valeur sur Online pendant le fonctionnement normal du système. L'état de stockage — le courant du composant de stockage sera défini de manière dynamique par le service en fonction de l'état du service LDR, comme le volume de l'espace de stockage objet disponible. Si l'espace est faible, le composant devient lecture seule.
Délai de vérification de l'état dépassé	SHCT	La limite de temps en secondes pendant laquelle un test de vérification de l'état doit s'effectuer pour que le volume de stockage soit considéré comme sain. Ne modifiez cette valeur que si vous y êtes invité par le support.

LDR > Vérification

Nom d'attribut	Code	Description
Réinitialiser le nombre d'objets manquants	VCMI	Réinitialise le nombre d'objets manquants détectés (OMIS). Utiliser uniquement une fois la vérification de premier plan terminée. Les données d'objet répliqué manquantes sont restaurées automatiquement par le système StorageGRID.

Nom d’attribut	Code	Description
La vérification	FVV	Sélectionnez les magasins d’objets sur lesquels effectuer la vérification de premier plan.
Taux de vérification	VPRI	Définissez la vitesse à laquelle la vérification des antécédents a lieu. Voir les informations sur la configuration du taux de vérification des antécédents.
Réinitialiser le nombre d’objets corrompus	VCCR	Réinitialisez le compteur pour les données d’objet répliqué corrompues trouvées lors de la vérification en arrière-plan. Cette option peut être utilisée pour effacer la condition d’alarme des objets corrompus détectés (OCOR). Pour plus d’informations, reportez-vous aux instructions de surveillance et de dépannage de StorageGRID.
Supprimer des objets en quarantaine	OQRT	Supprimez des objets corrompus du répertoire de quarantaine, réinitialisez le nombre d’objets mis en quarantaine et effacez l’alarme OQRT (Quarquarantaine Objects détectés). Cette option est utilisée après la restauration automatique par le système StorageGRID d’objets corrompus. Si une alarme objets perdus est déclenchée, le support technique peut vouloir accéder aux objets mis en quarantaine. Dans certains cas, les objets mis en quarantaine peuvent être utiles pour la récupération des données ou pour le débogage des problèmes sous-jacents à l’origine des copies d’objet corrompues.

LDR > codage d’effacement

Nom d’attribut	Code	Description
Réinitialiser le nombre d’échecs d’écriture	RSWF	Réinitialisez le compteur pour les échecs d’écriture des données d’objet avec code d’effacement sur le nœud de stockage.
Réinitialiser le nombre d’échecs de lecture	RSRF	Réinitialisez le compteur pour les échecs de lecture des données d’objet avec code d’effacement à partir du nœud de stockage.
Réinitialiser supprime le nombre d’échecs	RSDF	Réinitialisez le compteur pour les échecs de suppression des données d’objet avec code d’effacement du nœud de stockage.

Nom d’attribut	Code	Description
Réinitialiser le nombre de copies corrompues détectées	RSCC	Réinitialisez le compteur du nombre de copies corrompues de données d’objet avec code d’effacement sur le nœud de stockage.
Réinitialiser le nombre de fragments corrompus détectés	RSCD	Réinitialisez le compteur en cas de fragments endommagés de données d’objet avec code d’effacement sur le nœud de stockage.
Réinitialiser le nombre de fragments manquants détectés	RSMD	Réinitialisez le compteur en cas de fragments manquants de données d’objet avec code d’effacement sur le nœud de stockage. Utiliser uniquement une fois la vérification de premier plan terminée.

LDR > réplication

Nom d’attribut	Code	Description
Réinitialiser le nombre d’échecs de réplication entrante	RICR	Réinitialisez le compteur pour les échecs de réplication entrants. Il peut être utilisé pour effacer l’alarme RIRF (réplication entrante — échouée).
Réinitialiser le nombre d’échecs de réplication sortante	ROCR	Réinitialisez le compteur pour les échecs de réplication sortants. Cette fonction permet d’effacer l’alarme RORF (réplications sortantes — en échec).
Désactiver la réplication entrante	DSIR	Sélectionnez cette option pour désactiver la réplication entrante dans le cadre d’une procédure de maintenance ou de test. Laisser non vérifié pendant le fonctionnement normal. Lorsque la réplication entrante est désactivée, les objets peuvent être récupérés depuis le nœud de stockage pour être copiés vers d’autres emplacements du système StorageGRID, mais les objets ne peuvent pas être copiés vers ce nœud de stockage à partir d’autres emplacements : le service LDR est en lecture seule.

Nom d'attribut	Code	Description
Désactiver la réplication sortante	DSOR	Sélectionnez cette option pour désactiver la réplication sortante (y compris les demandes de contenu pour les récupérations HTTP) dans le cadre d'une procédure de maintenance ou de test. Laisser non vérifié pendant le fonctionnement normal. Lorsque la réplication sortante est désactivée, les objets peuvent être copiés vers ce noeud de stockage, mais les objets ne peuvent pas être récupérés depuis le noeud de stockage pour être copiés vers d'autres emplacements du système StorageGRID. Le service LDR est en écriture seule.

Informations associées

"Moniteur et amp ; dépannage"

Gestion des nœuds de stockage complets

Lorsque les nœuds de stockage atteignent leur capacité maximale, ils doivent étendre le système StorageGRID en ajoutant du nouveau stockage. Trois options sont disponibles : ajout de volumes de stockage, ajout de tiroirs d'extension de stockage et ajout de nœuds de stockage.

Ajout de volumes de stockage

Chaque nœud de stockage prend en charge un nombre maximal de volumes de stockage. Le maximum défini varie selon la plate-forme. Si un nœud de stockage contient moins de volumes de stockage que le nombre maximum, vous pouvez ajouter des volumes pour augmenter sa capacité. Voir les instructions d'extension d'un système StorageGRID.

Ajout de tiroirs d'extension de stockage

Certains nœuds de stockage StorageGRID, comme le SG6060, peuvent prendre en charge des tiroirs de stockage supplémentaires. Si vos appliances StorageGRID bénéficient de fonctionnalités d'extension qui n'ont pas encore été étendues à leur capacité maximale, vous pouvez ajouter des tiroirs de stockage pour augmenter la capacité. Voir les instructions d'extension d'un système StorageGRID.

Ajout de nœuds de stockage

L'ajout de nœuds de stockage permet d'augmenter la capacité de stockage. L'ajout de stockage nécessite de prendre en compte les règles ILM et les exigences de capacité actuellement actives. Voir les instructions d'extension d'un système StorageGRID.

Informations associées

"Développez votre grille"

Gestion des nœuds d'administration

Chaque site d'un déploiement StorageGRID peut avoir un ou plusieurs nœuds

d’administration.

- "Qu’est-ce qu’un nœud d’administration"
- "Utilisation de plusieurs nœuds d’administration"
- "Identification du nœud d’administration principal"
- "Sélection d’un expéditeur préféré"
- "Affichage de l’état des notifications et des files d’attente"
- "Affichage des alarmes acquittées par les nœuds d’administration (système hérité)"
- "Configuration de l’accès client d’audit"

Qu’est-ce qu’un nœud d’administration

Des nœuds d’administration qui assurent les services de gestion tels que la configuration du système, la surveillance et la journalisation. Chaque grid doit être connecté à un nœud d’administration principal et doit comporter un nombre quelconque de nœuds d’administration non primaires pour assurer la redondance.

Lorsque vous vous connectez à Grid Manager ou au Gestionnaire de locataires, vous vous connectez à un noeud d’administration. Vous pouvez vous connecter à n’importe quel nœud d’administration et chaque nœud d’administration affiche une vue similaire du système StorageGRID. Cependant, les procédures de maintenance doivent être effectuées à l’aide du nœud d’administration principal.

Les nœuds d’administration peuvent également être utilisés pour équilibrer la charge du trafic des clients S3 et Swift.

Les nœuds d’administration hébergent les services suivants :

- Service AMS
- Service CMN
- Service NMS
- Service Prometheus
- Services d’équilibrage de la charge et haute disponibilité (pour prendre en charge le trafic des clients S3 et Swift)

Les nœuds d’administration prennent également en charge l’API de gestion (Management application Program interface) pour traiter les requêtes depuis l’API de gestion du grid et l’API de gestion des locataires.

Qu’est-ce que le service AMS

Le service du système de gestion de la vérification (AMS) suit l’activité et les événements du système.

Qu’est-ce que le service CMN

Le service de nœud de gestion de la configuration (CMN) gère les configurations de connectivité et de protocoles à l’échelle du système nécessaires à tous les services. De plus, le service CMN est utilisé pour exécuter et surveiller les tâches de la grille. Il n’y a qu’un seul service CMN par déploiement StorageGRID. Le nœud d’administration qui héberge le service CMN est appelé nœud d’administration principal.

En quoi consiste le service NMS

Le service Network Management System (NMS) alimente les options de surveillance, de rapport et de configuration affichées via le gestionnaire de grille, l'interface navigateur du système StorageGRID.

Définition du service Prometheus

Le service Prometheus collecte les metrics de séries chronologiques des services sur tous les nœuds.

Informations associées

"Via l'API de gestion du grid"

"Utilisez un compte de locataire"

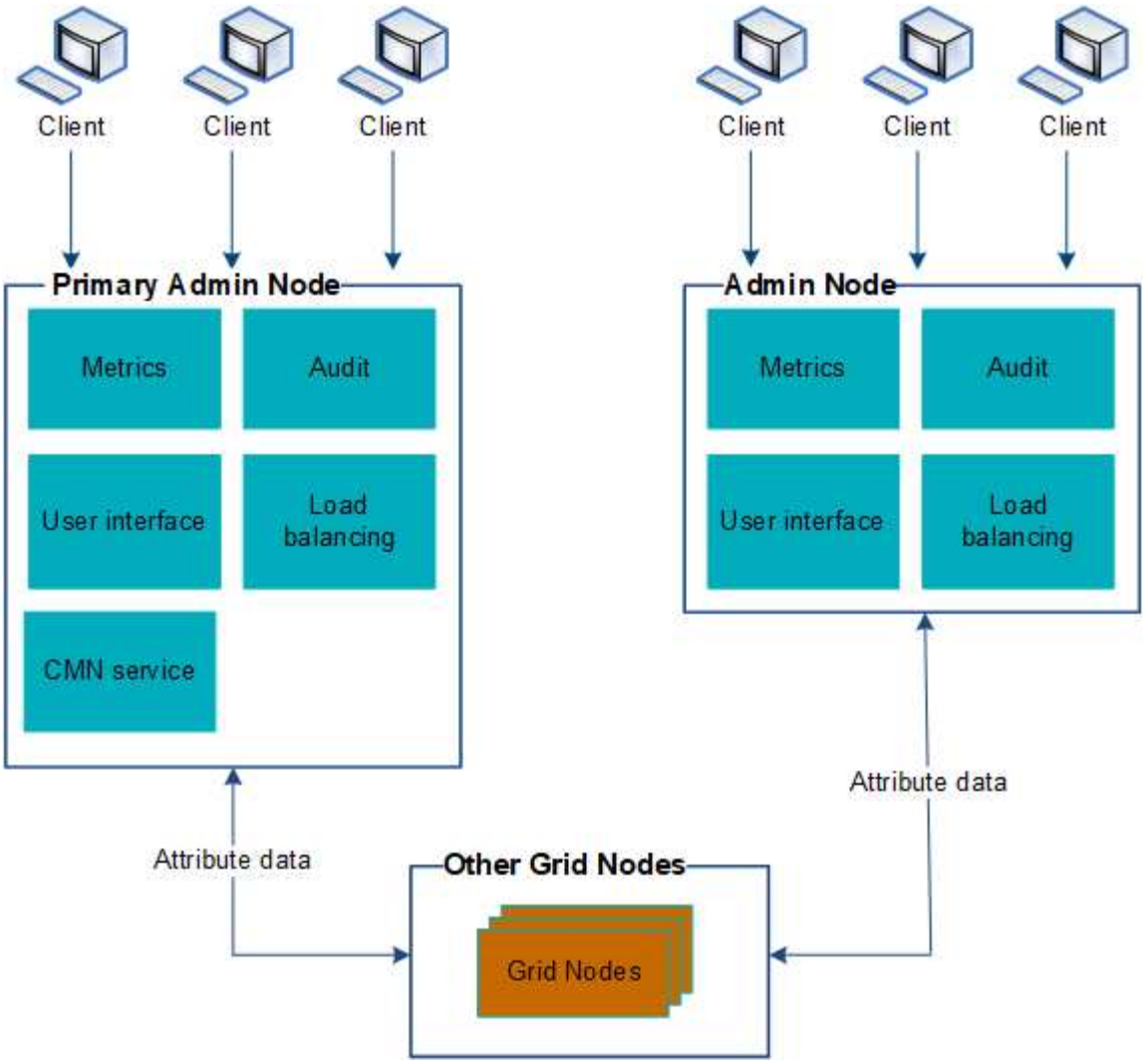
"Gestion de l'équilibrage des charges"

"Gestion des groupes haute disponibilité"

Utilisation de plusieurs nœuds d'administration

Un système StorageGRID peut inclure plusieurs nœuds d'administration pour vous permettre de contrôler et de configurer en continu votre système StorageGRID, même en cas de panne d'un nœud d'administration.

Si un nœud d'administration devient indisponible, le traitement des attributs continue, les alertes et les alarmes (système hérité) sont toujours déclenchées et les notifications par e-mail et les messages AutoSupport sont toujours envoyés. Toutefois, plusieurs nœuds d'administration n'assurent pas la protection du basculement, à l'exception des notifications et des messages AutoSupport. En particulier, les accusés de réception d'alarme d'un nœud d'administration ne sont pas copiés sur d'autres nœuds d'administration.



Deux options s'offrent à vous pour continuer à afficher et à configurer le système StorageGRID en cas de défaillance d'un nœud d'administration :

- Les clients Web peuvent se reconnecter à tout autre nœud d'administration disponible.
- Si un administrateur système a configuré un groupe de nœuds d'administration haute disponibilité, les clients Web peuvent continuer à accéder à Grid Manager ou au Gestionnaire de locataires à l'aide de l'adresse IP virtuelle du groupe HA.

> Lors de l'utilisation d'un groupe haute disponibilité, l'accès est interrompu en cas de défaillance du nœud d'administration principal. Les utilisateurs doivent se reconnecter une fois que l'adresse IP virtuelle du groupe HA bascule vers un autre noeud d'administration du groupe.

Certaines tâches de maintenance peuvent uniquement être effectuées à l'aide du nœud d'administration principal. En cas de panne du nœud d'administration principal, celui-ci doit être restauré avant que le système StorageGRID ne fonctionne à nouveau entièrement.

Informations associées

"Gestion des groupes haute disponibilité"

Identification du nœud d’administration principal

Le nœud d’administration principal héberge le service CMN. Certaines procédures de maintenance peuvent uniquement être effectuées à l’aide du nœud d’administration principal.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l’aide d’un navigateur pris en charge.
- Vous devez disposer d’autorisations d’accès spécifiques.

Étapes

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez ***site*** > **Admin Node**, puis cliquez sur ➕ Pour développer l’arborescence de la topologie et afficher les services hébergés sur ce nœud d’administration.

   Le nœud d’administration principal héberge le service CMN.

3. Si ce nœud d’administration n’héberge pas le service CMN, vérifiez les autres nœuds d’administration.

Sélection d’un expéditeur préféré

Si votre déploiement StorageGRID inclut plusieurs nœuds d’administration, vous pouvez sélectionner le nœud d’administration qui doit être l’expéditeur préféré des notifications. Par défaut, le nœud d’administration principal est sélectionné, mais n’importe quel nœud d’administration peut être l’expéditeur préféré.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l’aide d’un navigateur pris en charge.
- Vous devez disposer d’autorisations d’accès spécifiques.

Description de la tâche

La page **Configuration** > **Paramètres système** > **Options d’affichage** indique quel nœud d’administration est actuellement sélectionné comme expéditeur préféré. Le nœud d’administration principal est sélectionné par défaut.

Dans des conditions normales de fonctionnement du système, seul l’expéditeur préféré envoie les notifications suivantes :

- Messages AutoSupport
- Notifications SNMP
- E-mails d’alerte
- E-mails d’alarme (système hérité)

Cependant, tous les autres nœuds d’administration (expéditeurs de secours) surveillent l’expéditeur préféré. Si un problème est détecté, un expéditeur en attente peut également envoyer ces notifications.

Dans les cas suivants, l’expéditeur préféré et l’expéditeur de secours peuvent envoyer des notifications :

- Si les nœuds d’administration deviennent « en attente » les uns des autres, l’expéditeur préféré et les

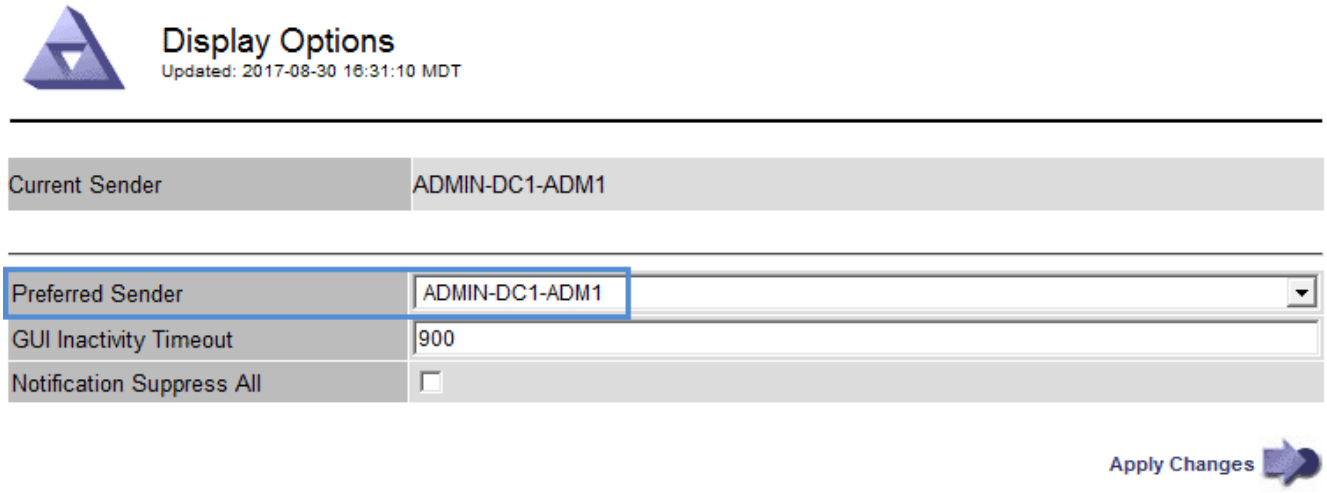
expéditeurs de secours tenteront d'envoyer des notifications, et plusieurs copies de notifications peuvent être reçues.

- Lorsqu'un expéditeur en veille détecte des problèmes avec l'expéditeur préféré et commence à envoyer des notifications, il est possible que l'expéditeur préféré puisse récupérer sa capacité à envoyer des notifications. Dans ce cas, des notifications en double peuvent être envoyées. L'expéditeur en attente interrompt l'envoi des notifications lorsqu'il ne détecte plus d'erreurs sur l'expéditeur préféré.

> Lorsque vous testez les notifications d'alarme et les messages AutoSupport, tous les nœuds Admin envoient l'e-mail de test. Lorsque vous testez les notifications d'alertes, vous devez vous connecter à chaque nœud d'administration pour vérifier la connectivité.

Étapes

1. Sélectionnez **Configuration** > **Paramètres système** > **Options d'affichage**.
2. Dans le menu Options d'affichage, sélectionnez **Options**.
3. Sélectionnez le noeud d'administration que vous souhaitez définir comme expéditeur préféré dans la liste déroulante.



4. Cliquez sur **appliquer les modifications**.

   Le nœud d'administration est défini comme l'expéditeur préféré des notifications.

Affichage de l'état des notifications et des files d'attente

Le service NMS sur les nœuds d'administration envoie des notifications au serveur de messagerie. Vous pouvez afficher l'état actuel du service NMS ainsi que la taille de sa file d'attente de notifications sur la page moteur d'interface.

Pour accéder à la page moteur d'interface, sélectionnez **support** > **Outils** > **topologie de grille**. Enfin, sélectionnez ***site*** > ***Admin Node*** > **NMS** > **interface Engine**.

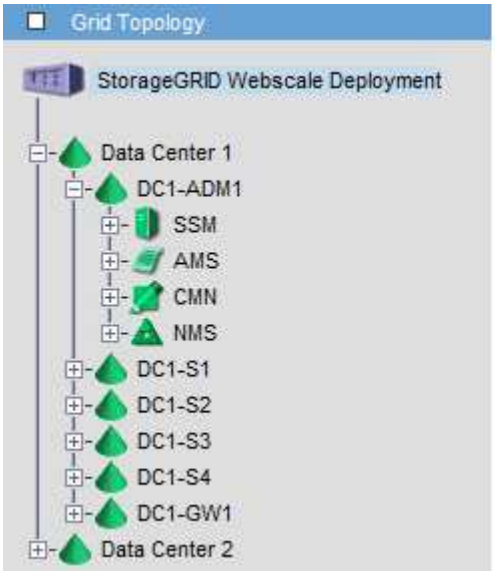
Les notifications sont traitées via la file d'attente de notifications par e-mail et sont envoyées au serveur de messagerie l'une après l'autre dans l'ordre dans lequel elles sont déclenchées. En cas de problème (par exemple, une erreur de connexion réseau) et si le serveur de messagerie n'est pas disponible lors de la tentative d'envoi de la notification, une tentative de renvoi de la notification au serveur de messagerie se poursuit pendant une période de 60 secondes. Si la notification n'est pas envoyée au serveur de messagerie

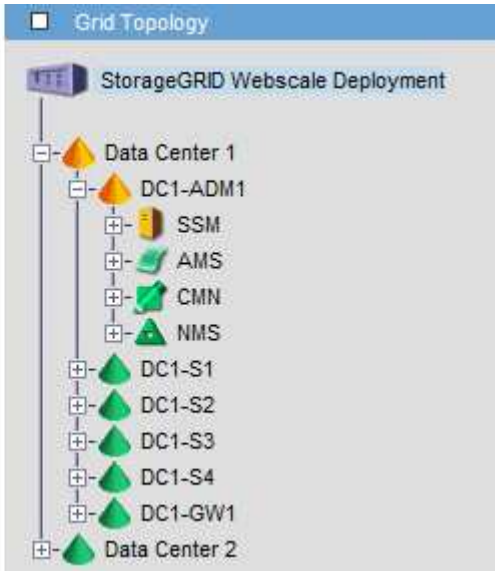
après 60 secondes, elle est supprimée de la file d'attente de notifications et une tentative d'envoi de la notification suivante dans la file d'attente est effectuée. Comme les notifications peuvent être supprimées de la file d'attente de notifications sans être envoyées, il est possible qu'une alarme puisse être déclenchée sans qu'une notification soit envoyée. Dans le cas où une notification est supprimée de la file d'attente sans être envoyée, l'alarme mineure EN MINUTES (état de notification par e-mail) est déclenchée.

Affichage des alarmes acquittées par les nœuds d'administration (système hérité)

Lorsque vous accusez réception d'une alarme sur un nœud d'administration, l'alarme acquittée n'est copiée sur aucun autre nœud d'administration. Comme les accusés de réception ne sont pas copiés sur d'autres nœuds d'administration, il est possible que l'arborescence de la topologie de grille ne soit pas identique pour chaque nœud d'administration.

Cette différence peut être utile lors de la connexion de clients Web. Les clients Web peuvent avoir différentes vues du système StorageGRID selon les besoins de l'administrateur.





Notez que les notifications sont envoyées depuis le nœud d'administration où l'accusé de réception a lieu.

Configuration de l'accès client d'audit

Le nœud d'administration, via le service AMS (Audit Management System), consigne tous les événements système vérifiés dans un fichier journal disponible via le partage d'audit, qui est ajouté à chaque nœud d'administration lors de l'installation. Pour faciliter l'accès aux journaux d'audit, vous pouvez configurer l'accès des clients aux partages d'audit pour CIFS et NFS.

Le système StorageGRID utilise une reconnaissance positive pour éviter toute perte de messages d'audit avant qu'ils ne soient écrits dans le fichier journal. Un message reste placé dans la file d'attente d'un service jusqu'à ce que le service AMS ou un service de relais d'audit intermédiaire en ait reconnu le contrôle.

Pour plus d'informations, reportez-vous aux instructions de compréhension des messages d'audit.

Si vous avez la possibilité d'utiliser CIFS ou NFS, choisissez NFS.

L'exportation d'audit via CIFS/Samba a été obsolète et sera supprimée dans une future version de StorageGRID.

Informations associées

"Qu'est-ce qu'un nœud d'administration"

"Examiner les journaux d'audit"

"Mise à niveau du logiciel"

Configuration des clients d'audit pour CIFS

La procédure utilisée pour configurer un client d'audit dépend de la méthode d'authentification Windows Workgroup ou Windows Active Directory (AD). Lorsqu'il est ajouté, le partage d'audit est automatiquement activé en tant que partage en lecture seule.

L'exportation d'audit via CIFS/Samba a été obsolète et sera supprimée dans une future version de StorageGRID.

Informations associées

"Mise à niveau du logiciel"

Configuration des clients d'audit pour Workgroup

Effectuez cette procédure pour chaque nœud d'administration d'un déploiement StorageGRID à partir duquel vous souhaitez récupérer des messages d'audit.

Ce dont vous avez besoin

- Vous devez avoir le `Passwords.txt` Fichier avec le mot de passe du compte root/admin (disponible dans LEDIT paquet).
- Vous devez avoir le `Configuration.txt` Fichier (disponible dans LEDIT paquet).

Description de la tâche

L'exportation d'audit via CIFS/Samba a été obsolète et sera supprimée dans une future version de StorageGRID.

Étapes

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
2. Vérifiez que tous les services sont en cours d'exécution ou vérifiés : `storagegrid-status`

Si tous les services ne sont pas en cours d'exécution ou vérifiés, résolvez les problèmes avant de continuer.

3. Revenez à la ligne de commande, appuyez sur **Ctrl+C**.
4. Démarrez l'utilitaire de configuration CIFS : `config_cifs.rb`

```
----------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
----------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
----------------------------------------------------------------------
```

5. Définissez l'authentification pour le groupe de travail Windows :

   Si l'authentification a déjà été définie, un message d'avertissement s'affiche. Si l'authentification a déjà été définie, passez à l'étape suivante.

   a. Entrez : `set-authentication`
   b. Lorsque vous êtes invité à installer Windows Workgroup ou Active Directory, entrez : `workgroup`
   c. Lorsque vous y êtes invité, entrez le nom du groupe de travail : *`workgroup_name`*
   d. Lorsque vous y êtes invité, créez un nom NetBIOS significatif : *`netbios_name`*

      ou

      Appuyez sur **entrée** pour utiliser le nom d'hôte du noeud d'administration comme nom NetBIOS.

   Le script redémarre le serveur Samba et des modifications sont appliquées. Cela devrait prendre moins d'une minute. Une fois l'authentification définie, ajoutez un client d'audit.

   a. Lorsque vous y êtes invité, appuyez sur **entrée**.

      L'utilitaire de configuration CIFS s'affiche.

6. Ajouter un client d'audit :

   a. Entrez : `add-audit-share`

      > Le partage est automatiquement ajouté en lecture seule.

   b. Lorsque vous y êtes invité, ajoutez un utilisateur ou un groupe : *`user`*
   c. Lorsque vous y êtes invité, entrez le nom d'utilisateur de l'audit : *`audit_user_name`*

d. Lorsque vous y êtes invité, entrez un mot de passe pour l'utilisateur d'audit : *`password`*

e. Lorsque vous y êtes invité, saisissez à nouveau le même mot de passe pour le confirmer : *`password`*

f. Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

> Il n'est pas nécessaire d'entrer un répertoire. Le nom du répertoire d'audit est prédéfini.

7. Si plusieurs utilisateurs ou groupes sont autorisés à accéder au partage d'audit, ajoutez-les :

a. Entrez : `add-user-to-share`

Une liste numérotée des partages activés s'affiche.

b. Lorsque vous y êtes invité, entrez le numéro du partage audit-exportation : *`share_number`*

c. Lorsque vous y êtes invité, ajoutez un utilisateur ou un groupe : `user`

ou `group`

d. Lorsque vous y êtes invité, entrez le nom de l'utilisateur ou du groupe d'audit : *`audit_user or audit_group`*

e. Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

f. Répétez ces sous-étapes pour chaque utilisateur ou groupe supplémentaire ayant accès au partage d'audit.

8. Vérifiez éventuellement votre configuration : `validate-config`

Les services sont vérifiés et affichés. Vous pouvez ignorer en toute sécurité les messages suivants :

```
Can't find include file /etc/samba/includes/cifs-interfaces.inc
Can't find include file /etc/samba/includes/cifs-filesystem.inc
Can't find include file /etc/samba/includes/cifs-custom-config.inc
Can't find include file /etc/samba/includes/cifs-shares.inc
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
(16384)
```

a. Lorsque vous y êtes invité, appuyez sur **entrée**.

La configuration du client d'audit s'affiche.

b. Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

9. Fermez l'utilitaire de configuration CIFS : `exit`

10. Démarrez le service Samba : `service smbd start`

11. Si le déploiement de StorageGRID est un site unique, passez à l'étape suivante.

    ou

    Si le déploiement de StorageGRID inclut des nœuds d'administration sur d'autres sites, activez ce partage d'audit comme requis :

    a. Connectez-vous à distance au nœud d'administration d'un site :
        i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
        ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
        iii. Entrez la commande suivante pour passer à la racine : `su -`
        iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
    b. Répétez les étapes pour configurer le partage d'audit pour chaque nœud d'administration supplémentaire.
    c. Fermez la connexion du shell sécurisé distant au nœud d'administration distant : `exit`
12. Déconnectez-vous du shell de commande : `exit`

Informations associées

"Mise à niveau du logiciel"

Configuration des clients d'audit pour Active Directory

Effectuez cette procédure pour chaque nœud d'administration d'un déploiement StorageGRID à partir duquel vous souhaitez récupérer des messages d'audit.

Ce dont vous avez besoin

- Vous devez avoir le `Passwords.txt` Fichier avec le mot de passe du compte root/admin (disponible dans LEDIT paquet).
- Vous devez disposer du nom d'utilisateur et du mot de passe CIFS Active Directory.
- Vous devez avoir le `Configuration.txt` Fichier (disponible dans LEDIT paquet).

> L'exportation d'audit via CIFS/Samba a été obsolète et sera supprimée dans une future version de StorageGRID.

Étapes

1. Connectez-vous au nœud d'administration principal :
    a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
    b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
    c. Entrez la commande suivante pour passer à la racine : `su -`
    d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

    Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
2. Vérifiez que tous les services sont en cours d'exécution ou vérifiés : `storagegrid-status`

Si tous les services ne sont pas en cours d'exécution ou vérifiés, résolvez les problèmes avant de continuer.

3. Revenez à la ligne de commande, appuyez sur **Ctrl**+**C**.
4. Démarrez l'utilitaire de configuration CIFS : `config_cifs.rb`

```
---------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
---------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
---------------------------------------------------------------------
```

5. Définissez l'authentification pour Active Directory : `set-authentication`

   Dans la plupart des déploiements, vous devez définir l'authentification avant d'ajouter le client d'audit. Si l'authentification a déjà été définie, un message d'avertissement s'affiche. Si l'authentification a déjà été définie, passez à l'étape suivante.

   a. Lorsque vous êtes invité à installer Workgroup ou Active Directory : `ad`
   b. À l'invite, entrez le nom du domaine AD (nom de domaine court).
   c. Indiquez l'adresse IP ou le nom d'hôte DNS du contrôleur de domaine.
   d. Lorsque vous y êtes invité, entrez le nom de domaine de domaine complet.

      Utilisez des lettres majuscules.

   e. Lorsque vous êtes invité à activer la prise en charge de winbind, tapez **y**.

      Winbind est utilisé pour résoudre les informations utilisateur et de groupe à partir des serveurs AD.

   f. Lorsque vous y êtes invité, entrez le nom NetBIOS.
   g. Lorsque vous y êtes invité, appuyez sur **entrée**.

      L'utilitaire de configuration CIFS s'affiche.

6. Rejoindre le domaine :
   a. Si ce n'est pas déjà fait, démarrez l'utilitaire de configuration CIFS : `config_cifs.rb`
   b. Rejoindre le domaine : `join-domain`
   c. Vous êtes invité à tester si le nœud d'administration est actuellement un membre valide du domaine. Si ce nœud d'administration n'a pas déjà rejoint le domaine, entrez : `no`
   d. Indiquez le nom d'utilisateur de l'administrateur lorsque vous y êtes invité :

administrator_username

où *administrator_username* Est le nom d'utilisateur CIFS Active Directory, pas le nom d'utilisateur StorageGRID.

e. Lorsque vous y êtes invité, indiquez le mot de passe de l'administrateur : *administrator_password*

l'ont été *administrator_password* Est le nom d'utilisateur CIFS Active Directory, et non le mot de passe StorageGRID.

f. Lorsque vous y êtes invité, appuyez sur **entrée**.

L'utilitaire de configuration CIFS s'affiche.

7. Vérifiez que vous avez correctement joint le domaine :
   a. Rejoindre le domaine : `join-domain`
   b. Lorsque vous êtes invité à tester si le serveur est actuellement un membre valide du domaine, entrez : `y`

      Si vous recevez le message « rejoindre est OK », vous avez rejoint le domaine avec succès. Si vous n'obtenez pas cette réponse, essayez de définir l'authentification et de rejoindre à nouveau le domaine.

   c. Lorsque vous y êtes invité, appuyez sur **entrée**.

      L'utilitaire de configuration CIFS s'affiche.

8. Ajouter un client d'audit : `add-audit-share`
   a. Lorsque vous êtes invité à ajouter un utilisateur ou un groupe, entrez : `user`
   b. Lorsque vous êtes invité à saisir le nom d'utilisateur de l'audit, entrez le nom d'utilisateur de l'audit.
   c. Lorsque vous y êtes invité, appuyez sur **entrée**.

      L'utilitaire de configuration CIFS s'affiche.

9. Si plusieurs utilisateurs ou groupes sont autorisés à accéder au partage d'audit, ajoutez des utilisateurs supplémentaires : `add-user-to-share`

   Une liste numérotée des partages activés s'affiche.

   a. Entrez le numéro du partage audit-exportation.
   b. Lorsque vous êtes invité à ajouter un utilisateur ou un groupe, entrez : `group`

      Vous êtes invité à entrer le nom du groupe d'audit.

   c. Lorsque vous êtes invité à entrer le nom du groupe d'audit, entrez le nom du groupe d'utilisateurs d'audit.
   d. Lorsque vous y êtes invité, appuyez sur **entrée**.

      L'utilitaire de configuration CIFS s'affiche.

   e. Répétez cette étape pour chaque utilisateur ou groupe supplémentaire ayant accès au partage d'audit.

10. Vérifiez éventuellement votre configuration : `validate-config`

    Les services sont vérifiés et affichés. Vous pouvez ignorer en toute sécurité les messages suivants :

    - Impossible de trouver le fichier d'inclure `/etc/samba/includes/cifs-interfaces.inc`
    - Impossible de trouver le fichier d'inclure `/etc/samba/includes/cifs-filesystem.inc`
    - Impossible de trouver le fichier d'inclure `/etc/samba/includes/cifs-interfaces.inc`
    - Impossible de trouver le fichier d'inclure `/etc/samba/includes/cifs-custom-config.inc`
    - Impossible de trouver le fichier d'inclure `/etc/samba/includes/cifs-shares.inc`
    - rlimiit_max : augmentation de rlimit_max (1024) à la limite Windows minimale (16384)

      > Ne pas combiner le paramètre 'Security=ADS' avec le paramètre 'Password Server'. (Par défaut, Samba détecte le bon DC à contacter automatiquement).

      i. Lorsque vous y êtes invité, appuyez sur **entrée** pour afficher la configuration du client d'audit.
      ii. Lorsque vous y êtes invité, appuyez sur **entrée**.

      L'utilitaire de configuration CIFS s'affiche.

11. Fermez l'utilitaire de configuration CIFS : `exit`
12. Si le déploiement de StorageGRID est un site unique, passez à l'étape suivante.

    ou

    Si le déploiement de StorageGRID inclut des nœuds d'administration sur d'autres sites, activez ces partages d'audit comme requis :

    a. Connectez-vous à distance au nœud d'administration d'un site :
       i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
       ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
       iii. Entrez la commande suivante pour passer à la racine : `su -`
       iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
    b. Répétez cette procédure pour configurer les partages d'audit pour chaque nœud d'administration.
    c. Fermez la connexion du shell sécurisé distant au nœud d'administration : `exit`

13. Déconnectez-vous du shell de commande : `exit`

Informations associées

"Mise à niveau du logiciel"

Ajout d'un utilisateur ou d'un groupe à un partage d'audit CIFS

Vous pouvez ajouter un utilisateur ou un groupe à un partage d'audit CIFS intégré à l'authentification AD.

Ce dont vous avez besoin

- Vous devez avoir le `Passwords.txt` Fichier avec le mot de passe du compte root/admin (disponible dans LEDIT paquet).
- Vous devez avoir le `Configuration.txt` Fichier (disponible dans LEDIT paquet).

Description de la tâche

La procédure suivante concerne un partage d'audit intégré à l'authentification AD.

> L'exportation d'audit via CIFS/Samba a été obsolète et sera supprimée dans une future version de StorageGRID.

Étapes

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
2. Vérifiez que tous les services sont en cours d'exécution ou vérifiés. Entrez : `storagegrid-status`

   Si tous les services ne sont pas en cours d'exécution ou vérifiés, résolvez les problèmes avant de continuer.
3. Revenez à la ligne de commande, appuyez sur **Ctrl**+**C**.
4. Démarrez l'utilitaire de configuration CIFS : `config_cifs.rb`

```
----------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
----------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
----------------------------------------------------------------------
```

5. Commencez à ajouter un utilisateur ou un groupe : `add-user-to-share`

   Une liste numérotée de partages d'audit qui ont été configurés s'affiche.
6. Lorsque vous y êtes invité, entrez le numéro du partage d'audit (audit-export) : *`audit_share_number`*

   On vous demande si vous souhaitez donner un accès à ce partage d'audit à un utilisateur ou à un groupe.

7. Lorsque vous y êtes invité, ajoutez un utilisateur ou un groupe : `user` ou `group`
8. Lorsque vous êtes invité à entrer le nom de l'utilisateur ou du groupe pour ce partage d'audit AD, entrez le nom.

   L'utilisateur ou le groupe est ajouté en lecture seule pour le partage d'audit à la fois dans le système d'exploitation du serveur et dans le service CIFS. La configuration Samba est rechargée pour permettre à l'utilisateur ou au groupe d'accéder au partage du client d'audit.

9. Lorsque vous y êtes invité, appuyez sur **entrée**.

   L'utilitaire de configuration CIFS s'affiche.

10. Répétez ces étapes pour chaque utilisateur ou groupe ayant accès au partage d'audit.
11. Vérifiez éventuellement votre configuration : `validate-config`

    Les services sont vérifiés et affichés. Vous pouvez ignorer en toute sécurité les messages suivants :

    - Impossible de trouver le fichier /etc/samba/include/cifs-interfaces.inc
    - Impossible de trouver le fichier /etc/samba/include/cifs-filesystem.inc
    - Impossible de trouver le fichier /etc/samba/include/cifs-custom-config.inc
    - Impossible de trouver le fichier /etc/samba/include/cifs-shares.inc
      i. Lorsque vous y êtes invité, appuyez sur **entrée** pour afficher la configuration du client d'audit.
      ii. Lorsque vous y êtes invité, appuyez sur **entrée**.
12. Fermez l'utilitaire de configuration CIFS : `exit`
13. Déterminez si vous devez activer des partages d'audit supplémentaires, comme suit :
    - Si le déploiement de StorageGRID est un site unique, passez à l'étape suivante.
    - Si le déploiement de StorageGRID inclut des nœuds d'administration sur d'autres sites, activez ces partages d'audit si nécessaire :
      i. Connectez-vous à distance au nœud d'administration d'un site :
        A. Saisissez la commande suivante : `ssh admin@grid_node_IP`
        B. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
        C. Entrez la commande suivante pour passer à la racine : `su -`
        D. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
      ii. Répétez cette procédure pour configurer les partages d'audit pour chaque nœud d'administration.
      iii. Fermez la connexion du shell sécurisé distant au nœud d'administration distant : `exit`
14. Déconnectez-vous du shell de commande : `exit`

Suppression d'un utilisateur ou d'un groupe d'un partage d'audit CIFS

Vous ne pouvez pas supprimer le dernier utilisateur ou groupe autorisé à accéder au partage d'audit.

Ce dont vous avez besoin

- Vous devez avoir le `Passwords.txt` Fichier avec les mots de passe du compte racine (disponible dans

LEDIT package).

- Vous devez avoir le `Configuration.txt` Fichier (disponible dans LEDIT paquet).

Description de la tâche

L'exportation d'audit via CIFS/Samba a été obsolète et sera supprimée dans une future version de StorageGRID.

Étapes

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

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

2. Démarrez l'utilitaire de configuration CIFS : `config_cifs.rb`

```
----------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
----------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
----------------------------------------------------------------------
```

3. Commencez à supprimer un utilisateur ou un groupe : `remove-user-from-share`

   Une liste numérotée des partages d'audit disponibles pour le nœud d'administration s'affiche. Le partage d'audit est étiqueté audit-export.

4. Entrez le numéro du partage d'audit : *`audit_share_number`*
5. Lorsque vous êtes invité à supprimer un utilisateur ou un groupe : `user` ou `group`

   Une liste numérotée d'utilisateurs ou de groupes pour le partage d'audit s'affiche.

6. Entrez le numéro correspondant à l'utilisateur ou au groupe que vous souhaitez supprimer : *`number`*

   Le partage d'audit est mis à jour et l'utilisateur ou le groupe n'est plus autorisé à accéder au partage d'audit. Par exemple :

```
Enabled shares
 1. audit-export
Select the share to change: 1
Remove user or group? [User/group]: User
Valid users for this share
1. audituser
2. newaudituser
Select the user to remove: 1

Removed user "audituser" from share "audit-export".

Press return to continue.
```

7. Fermez l'utilitaire de configuration CIFS : `exit`
8. Si le déploiement StorageGRID inclut des nœuds d'administration sur d'autres sites, désactivez le partage d'audit sur chaque site selon les besoins.
9. Déconnectez-vous de chaque shell de commande une fois la configuration terminée : `exit`

Informations associées

"Mise à niveau du logiciel"

Modification du nom d'utilisateur ou de groupe d'un audit CIFS

Vous pouvez modifier le nom d'un utilisateur ou d'un groupe pour un partage d'audit CIFS en ajoutant un nouvel utilisateur ou un nouveau groupe, puis en supprimant l'ancien.

Description de la tâche

L'exportation d'audit via CIFS/Samba a été obsolète et sera supprimée dans une future version de StorageGRID.

Étapes

1. Ajoutez un nouvel utilisateur ou un nouveau groupe portant le nom mis à jour au partage d'audit.
2. Supprimez l'ancien nom d'utilisateur ou de groupe.

Informations associées

"Mise à niveau du logiciel"

"Ajout d'un utilisateur ou d'un groupe à un partage d'audit CIFS"

"Suppression d'un utilisateur ou d'un groupe d'un partage d'audit CIFS"

Vérification de l'intégration d'un audit CIFS

Le partage d'audit est en lecture seule. Les fichiers journaux sont destinés à être lus par des applications informatiques et la vérification ne comprend pas l'ouverture d'un fichier. Il est considéré comme suffisant de vérifier que les fichiers journaux d'audit apparaissent dans une fenêtre de l'Explorateur Windows. Après vérification de la connexion, fermez

toutes les fenêtres.

Configuration du client d'audit pour NFS

Le partage d'audit est automatiquement activé en tant que partage en lecture seule.

Ce dont vous avez besoin

- Vous devez avoir le `Passwords.txt` Fichier avec le mot de passe root/admin (disponible dans LEDIT paquet).
- Vous devez avoir le `Configuration.txt` Fichier (disponible dans LEDIT paquet).
- Le client d'audit doit utiliser NFS version 3 (NFSv3).

Description de la tâche

Effectuez cette procédure pour chaque nœud d'administration d'un déploiement StorageGRID à partir duquel vous souhaitez récupérer des messages d'audit.

Étapes

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

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

2. Vérifiez que tous les services sont en cours d'exécution ou vérifiés. Entrez : `storagegrid-status`

   Si des services ne sont pas répertoriés comme en cours d'exécution ou vérifiés, résolvez les problèmes avant de continuer.

3. Revenez à la ligne de commande. Appuyez sur **Ctrl+C**.
4. Démarrez l'utilitaire de configuration NFS. Entrez : `config_nfs.rb`

```
-----------------------------------------------------------------
| Shares                | Clients               | Config          |
-----------------------------------------------------------------
| add-audit-share       | add-ip-to-share       | validate-config |
| enable-disable-share  | remove-ip-from-share  | refresh-config  |
|                       |                       | help            |
|                       |                       | exit            |
-----------------------------------------------------------------
```

5. Ajouter le client d'audit : `add-audit-share`
   a. Lorsque vous y êtes invité, entrez l'adresse IP ou la plage d'adresses IP du client d'audit pour le partage d'audit : `client_IP_address`

b. Lorsque vous y êtes invité, appuyez sur **entrée**.

6. Si plusieurs clients d'audit sont autorisés à accéder au partage d'audit, ajoutez l'adresse IP de l'utilisateur supplémentaire : `add-ip-to-share`

   a. Entrez le numéro du partage d'audit : *`audit_share_number`*

   b. Lorsque vous y êtes invité, entrez l'adresse IP ou la plage d'adresses IP du client d'audit pour le partage d'audit : *`client_IP_address`*

   c. Lorsque vous y êtes invité, appuyez sur **entrée**.

      L'utilitaire de configuration NFS s'affiche.

   d. Répétez ces sous-étapes pour chaque client d'audit supplémentaire ayant accès au partage d'audit.

7. Vérifiez éventuellement votre configuration.

   a. Saisissez les informations suivantes : `validate-config`

      Les services sont vérifiés et affichés.

   b. Lorsque vous y êtes invité, appuyez sur **entrée**.

      L'utilitaire de configuration NFS s'affiche.

   c. Fermez l'utilitaire de configuration NFS : `exit`

8. Déterminez si vous devez activer des partages d'audit sur d'autres sites.

   - Si le déploiement de StorageGRID est un site unique, passez à l'étape suivante.
   - Si le déploiement de StorageGRID inclut des nœuds d'administration sur d'autres sites, activez ces partages d'audit si nécessaire :

     i. Connectez-vous à distance au nœud d'administration du site :

        A. Saisissez la commande suivante : `ssh admin@`*`grid_node_IP`*

        B. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

        C. Entrez la commande suivante pour passer à la racine : `su -`

        D. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

     ii. Répétez cette procédure pour configurer les partages d'audit pour chaque nœud d'administration supplémentaire.

     iii. Fermez la connexion du shell sécurisé distant au nœud d'administration distant. Entrez : `exit`

9. Déconnectez-vous du shell de commande : `exit`

   Les clients d'audit NFS ont accès à un partage d'audit en fonction de leur adresse IP. Accordez l'accès au partage d'audit à un nouveau client d'audit NFS en ajoutant son adresse IP au partage ou supprimez un client d'audit existant en supprimant son adresse IP.

Ajout d'un client d'audit NFS à un partage d'audit

Les clients d'audit NFS ont accès à un partage d'audit en fonction de leur adresse IP. Accorder l'accès au partage d'audit à un nouveau client d'audit NFS en ajoutant son adresse IP au partage d'audit.

Ce dont vous avez besoin

- Vous devez avoir le `Passwords.txt` Fichier avec le mot de passe du compte root/admin (disponible dans LEDIT paquet).
- Vous devez avoir le `Configuration.txt` Fichier (disponible dans LEDIT paquet).
- Le client d'audit doit utiliser NFS version 3 (NFSv3).

Étapes

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@`*`primary_Admin_Node_IP`*
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

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

2. Démarrez l'utilitaire de configuration NFS : `config_nfs.rb`

```
-----------------------------------------------------------------
| Shares                | Clients               | Config          |
-----------------------------------------------------------------
| add-audit-share       | add-ip-to-share       | validate-config |
| enable-disable-share  | remove-ip-from-share  | refresh-config  |
|                       |                       | help            |
|                       |                       | exit            |
-----------------------------------------------------------------
```

3. Entrez : `add-ip-to-share`

   La liste des partages d'audit NFS activés sur le nœud d'administration s'affiche. Le partage d'audit est répertorié comme suit : `/var/local/audit/export`

4. Entrez le numéro du partage d'audit : *`audit_share_number`*
5. Lorsque vous y êtes invité, entrez l'adresse IP ou la plage d'adresses IP du client d'audit pour le partage d'audit : *`client_IP_address`*

   Le client d'audit est ajouté au partage d'audit.

6. Lorsque vous y êtes invité, appuyez sur **entrée**.

   L'utilitaire de configuration NFS s'affiche.

7. Répétez les étapes pour chaque client d'audit qui doit être ajouté au partage d'audit.
8. Vérifiez éventuellement votre configuration : `validate-config`

   Les services sont vérifiés et affichés.

a. Lorsque vous y êtes invité, appuyez sur **entrée**.

   L'utilitaire de configuration NFS s'affiche.

9. Fermez l'utilitaire de configuration NFS : `exit`
10. Si le déploiement de StorageGRID est un site unique, passez à l'étape suivante.

    Si le déploiement StorageGRID inclut des nœuds d'administration sur d'autres sites, activez éventuellement ces partages d'audit si nécessaire :

    a. Connectez-vous à distance au nœud d'administration d'un site :
       i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
       ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
       iii. Entrez la commande suivante pour passer à la racine : `su -`
       iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
    b. Répétez cette procédure pour configurer les partages d'audit pour chaque nœud d'administration.
    c. Fermez la connexion du shell sécurisé distant au nœud d'administration distant : `exit`
11. Déconnectez-vous du shell de commande : `exit`

Vérification de l'intégration d'un audit NFS

Après avoir configuré un partage d'audit et ajouté un client d'audit NFS, vous pouvez monter le partage client d'audit et vérifier que les fichiers sont disponibles à partir du partage d'audit.

Étapes

1. Vérifiez la connectivité (ou la variante du système client) à l'aide de l'adresse IP côté client du nœud d'administration hébergeant le service AMS. Entrez : `ping IP_address`

   Vérifiez que le serveur répond, indiquant la connectivité.

2. Montez le partage d'audit en lecture seule à l'aide d'une commande appropriée au système d'exploitation client. Un exemple de commande Linux est (entrez sur une ligne) :

   `mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/audit/export myAudit`

   Utilisez l'adresse IP du nœud d'administration hébergeant le service AMS et le nom de partage prédéfini pour le système d'audit. Le point de montage peut être n'importe quel nom sélectionné par le client (par exemple, `myAudit` dans la commande précédente).

3. Vérifiez que les fichiers sont disponibles à partir du partage d'audit. Entrez : `ls myAudit /*`

   où `myAudit` est le point de montage du partage d'audit. Au moins un fichier journal doit être répertorié.

Suppression d'un client d'audit NFS du partage d'audit

Les clients d'audit NFS ont accès à un partage d'audit en fonction de leur adresse IP.

Vous pouvez supprimer un client d'audit existant en supprimant son adresse IP.

Ce dont vous avez besoin

- Vous devez avoir le `Passwords.txt` Fichier avec le mot de passe du compte root/admin (disponible dans LEDIT paquet).
- Vous devez avoir le `Configuration.txt` Fichier (disponible dans LEDIT paquet).

Description de la tâche

Vous ne pouvez pas supprimer la dernière adresse IP autorisée à accéder au partage d'audit.

Étapes

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@`*`primary_Admin_Node_IP`*
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

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

2. Démarrez l'utilitaire de configuration NFS : `config_nfs.rb`

```
-------------------------------------------------------------------
| Shares                | Clients               | Config          |
-------------------------------------------------------------------
| add-audit-share       | add-ip-to-share       | validate-config |
| enable-disable-share  | remove-ip-from-share  | refresh-config  |
|                       |                       | help            |
|                       |                       | exit            |
-------------------------------------------------------------------
```

3. Supprimez l'adresse IP du partage d'audit : `remove-ip-from-share`

   Une liste numérotée de partages d'audit configurés sur le serveur s'affiche. Le partage d'audit est répertorié comme suit : `/var/local/audit/export`

4. Saisissez le numéro correspondant au partage d'audit : *`audit_share_number`*

   Une liste numérotée d'adresses IP autorisées à accéder au partage d'audit s'affiche.

5. Saisissez le numéro correspondant à l'adresse IP que vous souhaitez supprimer.

   Le partage d'audit est mis à jour et l'accès n'est plus autorisé à partir d'un client d'audit possédant cette adresse IP.

6. Lorsque vous y êtes invité, appuyez sur **entrée**.

   L'utilitaire de configuration NFS s'affiche.

7. Fermez l'utilitaire de configuration NFS : `exit`
8. Si votre déploiement StorageGRID est un déploiement de plusieurs sites de data Center avec des nœuds d'administration supplémentaires sur les autres sites, désactivez les partages d'audit suivants :
   a. Connectez-vous à distance au nœud d'administration de chaque site :
      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
      iii. Entrez la commande suivante pour passer à la racine : `su -`
      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   b. Répétez cette procédure pour configurer les partages d'audit pour chaque nœud d'administration supplémentaire.
   c. Fermez la connexion du shell sécurisé distant au nœud d'administration distant : `exit`
9. Déconnectez-vous du shell de commande : `exit`

Modification de l'adresse IP d'un client d'audit NFS

1. Ajouter une nouvelle adresse IP à un partage d'audit NFS existant.
2. Supprimez l'adresse IP d'origine.

Informations associées

"Ajout d'un client d'audit NFS à un partage d'audit"

"Suppression d'un client d'audit NFS du partage d'audit"

Gestion des nœuds d'archivage

En option, vous pouvez déployer chacun des sites de data Center de votre système StorageGRID à l'aide d'un nœud d'archivage, ce qui vous permet de vous connecter à un système de stockage d'archivage externe ciblé, tel que Tivoli Storage Manager (TSM).

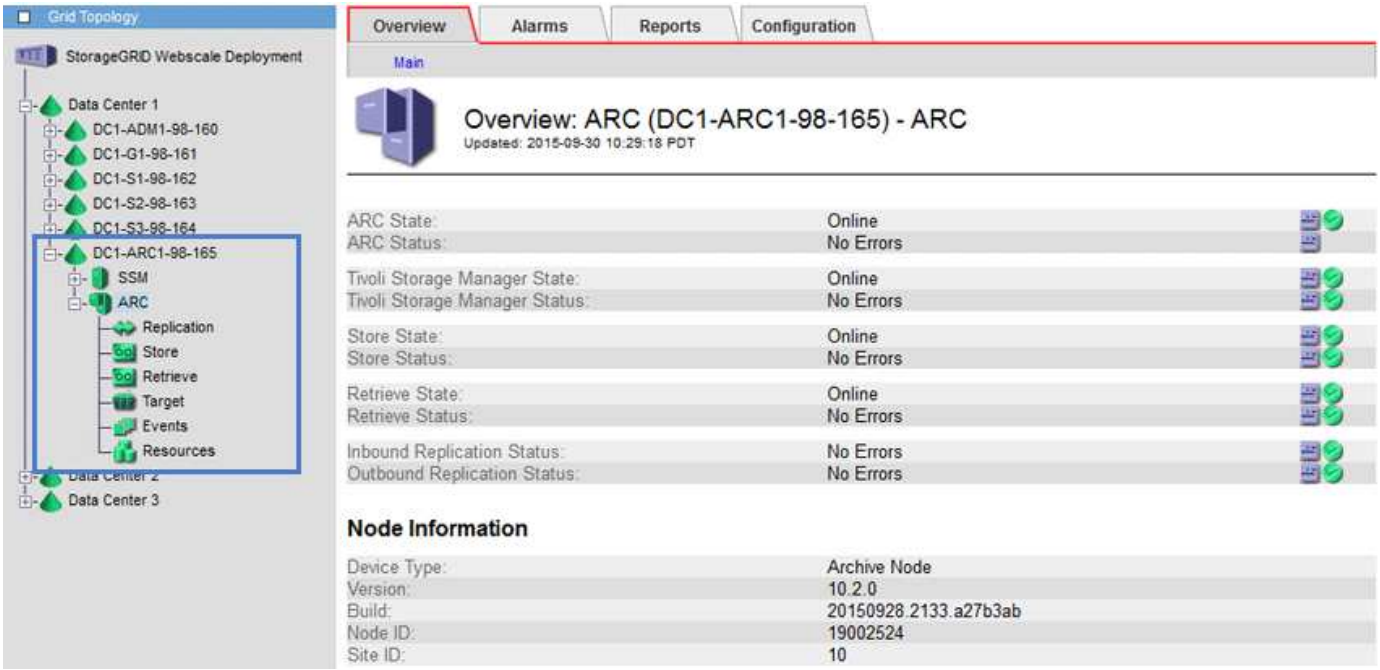
Après avoir configuré les connexions à la cible externe, vous pouvez configurer le nœud d'archivage pour optimiser les performances TSM, mettre un nœud d'archivage hors ligne lorsqu'un serveur TSM atteint sa capacité ou est indisponible, et configurer les paramètres de réplication et de récupération. Vous pouvez également définir des alarmes personnalisées pour le nœud d'archivage.

- "Qu'est-ce qu'un nœud d'archivage"
- "Configuration des connexions du nœud d'archivage au stockage d'archivage"
- "Définition d'alarmes personnalisées pour le nœud d'archivage"
- "Intégration de Tivoli Storage Manager"

Qu'est-ce qu'un nœud d'archivage

Le nœud d'archivage fournit une interface par le biais de laquelle vous pouvez cibler un système de stockage d'archives externe pour le stockage à long terme des données d'objet. Le nœud d'archivage surveille également cette connexion et le transfert des données d'objet entre le système StorageGRID et le système de stockage d'archives

externes ciblé.



Les données d'objet qui ne peuvent pas être supprimées, mais qui ne sont pas régulièrement utilisées, peuvent à tout moment être déplacées hors des disques rotatifs d'un nœud de stockage, vers un stockage d'archivage externe tel que le cloud ou la bande. Cet archivage des données d'objet s'effectue via la configuration du nœud d'archivage d'un site de data Center, puis la configuration des règles ILM sur lesquelles ce nœud d'archivage est sélectionné comme « cible » pour les instructions de placement de contenu. Le nœud d'archivage ne gère pas les données d'objet archivées lui-même, ce qui est réalisé par le dispositif d'archivage externe.

> Les métadonnées de l'objet ne sont pas archivées, mais restent sur les nœuds de stockage.

Qu'est-ce que le service ARC

Le service ARC (Archive Node) fournit l'interface de gestion que vous pouvez utiliser pour configurer les connexions au stockage d'archivage externe, comme les bandes via le middleware TSM.

Il s'agit du service ARC qui interagit avec un système de stockage d'archives externe, en envoyant des données d'objet pour le stockage secondaire et en effectuant des récupérations lorsqu'une application client demande un objet archivé. Lorsqu'une application client demande un objet archivé, un nœud de stockage demande les données de l'objet au service ARC. Le service ARC envoie une demande au système de stockage d'archives externe, qui récupère les données de l'objet demandé et les envoie au service ARC. Le service ARC vérifie les données de l'objet et les transfère au nœud de stockage, qui renvoie alors l'objet à l'application client requérant.

Les demandes de données d'objet archivées sur bande via un middleware TSM sont gérées pour optimiser les récupérations. Les demandes peuvent être commandées de façon à ce que les objets stockés dans l'ordre séquentiel sur bande soient demandés dans le même ordre séquentiel. Les demandes sont alors mises en file d'attente pour soumission à l'unité de stockage. En fonction du périphérique d'archivage, plusieurs demandes d'objets sur différents volumes peuvent être traitées simultanément.

Configuration des connexions du nœud d'archivage au stockage d'archivage

Lorsque vous configurez un nœud d'archivage pour qu'il se connecte à une archive externe, vous devez sélectionner le type cible.

Le système StorageGRID prend en charge l'archivage des données d'objet dans le cloud via une interface S3 ou sur bande via le logiciel médiateur Tivoli Storage Manager (TSM).

> Une fois le type de cible d'archivage configuré pour un nœud d'archivage, le type de cible ne peut pas être modifié.

- "Archivage dans le cloud via l'API S3"
- "Archivage sur bande via le logiciel médiateur TSM"
- "Configuration des paramètres de récupération du nœud d'archivage"
- "Configuration de la réplication du noeud d'archivage"

Archivage dans le cloud via l'API S3

Vous pouvez configurer un nœud d'archivage pour qu'il se connecte directement à Amazon Web Services (AWS) ou à tout autre système capable de s'interfacer avec le système StorageGRID via l'API S3.

> Le déplacement d'objets d'un nœud d'archivage vers un système de stockage d'archivage externe via l'API S3 a été remplacé par les pools de stockage cloud ILM, offrant ainsi plus de fonctionnalités. L'option **Cloud Tiering - simple Storage Service (S3)** est toujours prise en charge, mais vous préférez peut-être implémenter des pools de stockage cloud.

Si vous utilisez actuellement un nœud d'archivage avec l'option **Cloud Tiering - simple Storage Service (S3)**, envisagez de migrer vos objets vers un pool de stockage cloud. Voir les instructions de gestion des objets avec la gestion du cycle de vie des informations.

Informations associées

"Gestion des objets avec ILM"

Configuration des paramètres de connexion pour l'API S3

Si vous vous connectez à un noeud d'archivage à l'aide de l'interface S3, vous devez configurer les paramètres de connexion de l'API S3. Tant que ces paramètres ne sont pas configurés, le service ARC reste dans un état d'alarme majeur car il ne parvient pas à communiquer avec le système de stockage d'archives externe.

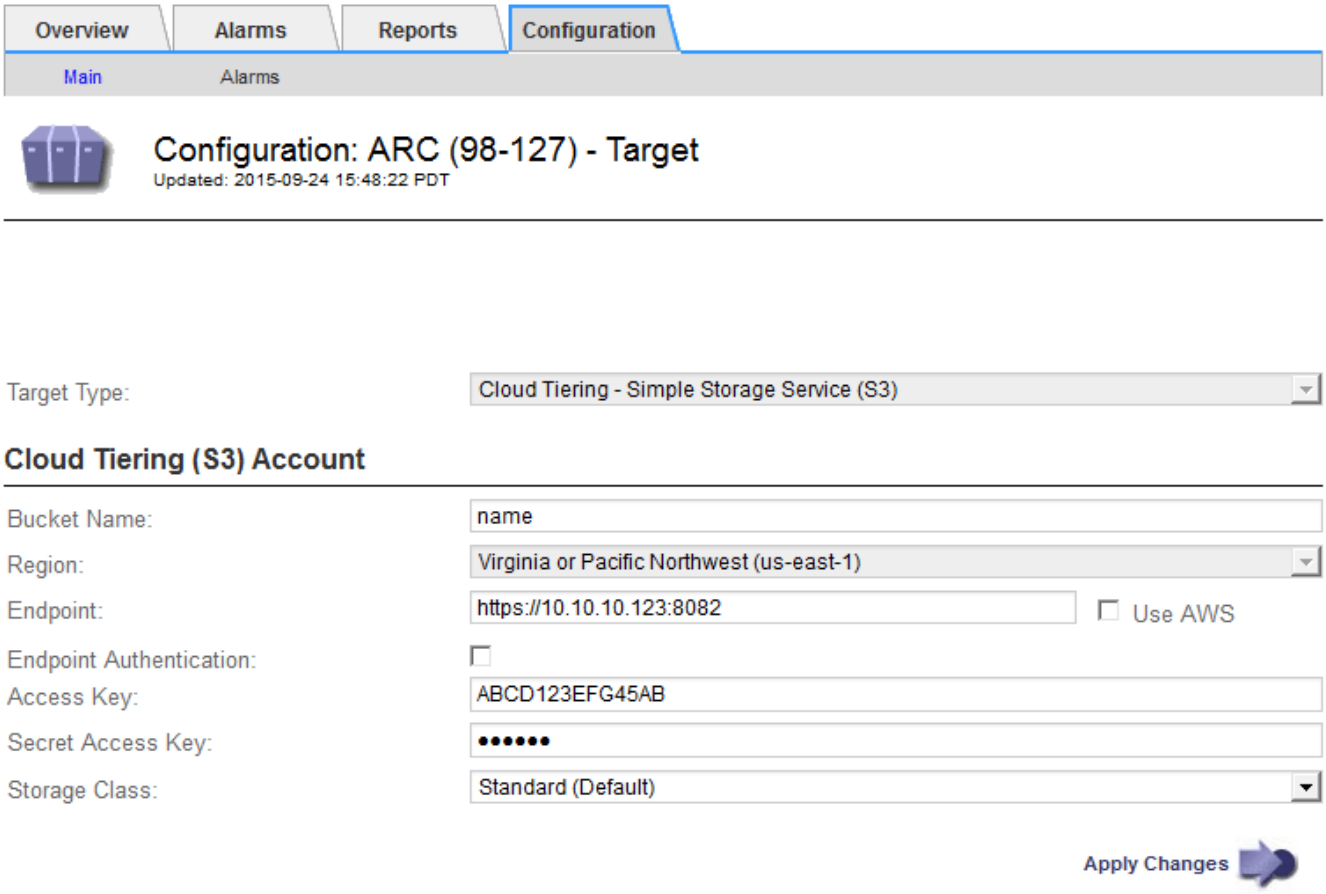
> Le déplacement d'objets d'un nœud d'archivage vers un système de stockage d'archivage externe via l'API S3 a été remplacé par les pools de stockage cloud ILM, offrant ainsi plus de fonctionnalités. L'option **Cloud Tiering - simple Storage Service (S3)** est toujours prise en charge, mais vous préférez peut-être implémenter des pools de stockage cloud.
>
> Si vous utilisez actuellement un nœud d'archivage avec l'option **Cloud Tiering - simple Storage Service (S3)**, envisagez de migrer vos objets vers un pool de stockage cloud. Voir les instructions de gestion des objets avec la gestion du cycle de vie des informations.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.
- Il faut avoir créé un compartiment sur le système de stockage d'archivage cible :
  - Le compartiment doit être dédié à un seul nœud d'archivage. Il ne peut pas être utilisé par d'autres nœuds d'archivage ou d'autres applications.
  - La région du godet doit être sélectionnée pour votre emplacement.
  - Le compartiment doit être configuré avec une gestion des versions suspendue.
- La segmentation d'objet doit être activée et la taille de segment maximale doit être inférieure ou égale à 4.5 Gio (4,831,838,208 octets). Les demandes d'API S3 qui dépassent cette valeur échouent si S3 est utilisé comme système de stockage d'archivage externe.

Étapes

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez **Archive Node** > **ARC** > **Target**.
3. Sélectionnez **Configuration** > **main**.



4. Sélectionnez **Cloud Tiering - simple Storage Service (S3)** dans la liste déroulante Type de cible.

> Les paramètres de configuration ne sont pas disponibles tant que vous n'avez pas sélectionné de type cible.

5. Configurez le compte de Tiering cloud (S3) via lequel le nœud d'archivage se connecte au système de

stockage d'archivage externe cible compatible S3.

La plupart des champs de cette page sont explicites. La section suivante décrit les champs pour lesquels vous avez peut-être besoin d'aide.

- **Région** : disponible uniquement si **Use AWS** est sélectionné. La région que vous sélectionnez doit correspondre à la région du compartiment.
- **Endpoint** et **use AWS** : pour Amazon Web Services (AWS), sélectionnez **use AWS**. **Endpoint** est alors automatiquement renseigné avec une URL de point de terminaison en fonction des attributs Nom du compartiment et région. Par exemple :

  ```
  https://bucket.region.amazonaws.com
  ```

  Pour une cible non AWS, entrez l'URL du système hébergeant le compartiment, y compris le numéro de port. Par exemple :

```
https://system.com:1080
```

- **Authentification par point de terminaison** : activée par défaut. Si le réseau vers le système de stockage d'archives externe est approuvé, vous pouvez désélectionner la case à cocher pour désactiver le certificat SSL de point final et la vérification du nom d'hôte pour le système de stockage d'archives externe cible. Si une autre instance d'un système StorageGRID est le périphérique de stockage d'archives cible et que le système est configuré avec des certificats signés publiquement, vous pouvez maintenir la case à cocher sélectionnée.
- **Classe de stockage** : sélectionnez **Standard (par défaut)** pour le stockage normal. Sélectionnez **réduction de redondance** uniquement pour les objets qui peuvent être facilement recréés. **Redondance réduite** fournit un stockage moins coûteux et moins fiable. Si le système de stockage d'archives cible est une autre instance du système StorageGRID, **Storage Class** contrôle le nombre de copies intermédiaires de l'objet à l'entrée sur le système cible, si la double validation est utilisée lors de l'ingestion d'objets.

6. Cliquez sur **appliquer les modifications**.

   Les paramètres de configuration spécifiés sont validés et appliqués à votre système StorageGRID. Une fois configurée, la cible ne peut plus être modifiée.

Informations associées

"Gestion des objets avec ILM"

Modification des paramètres de connexion pour l'API S3

Une fois que le nœud d'archivage est configuré pour se connecter à un système de stockage d'archives externe via l'API S3, vous pouvez modifier certains paramètres en cas de modification de la connexion.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

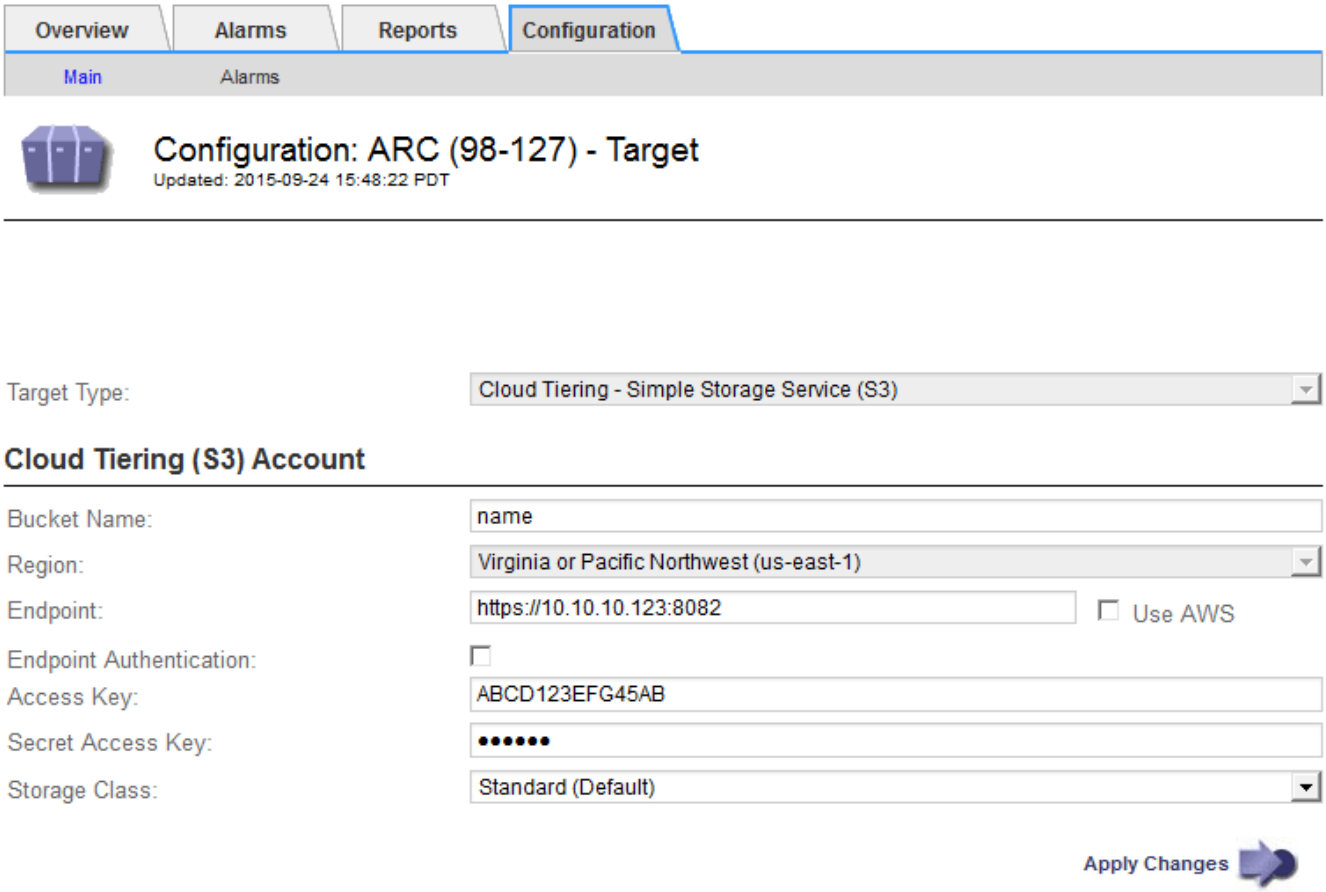
Description de la tâche

Si vous modifiez le compte Cloud Tiering (S3), vous devez vous assurer que les identifiants d'accès utilisateur ont un accès en lecture/écriture au compartiment, y compris tous les objets précédemment ingérées par le

nœud d'archivage vers le compartiment.

Étapes

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez ***Archive Node*** > **ARC** > **cible**.
3. Sélectionnez **Configuration** > **main**.



4. Modifiez les informations de compte si nécessaire.

   Si vous modifiez la classe de stockage, les nouvelles données d'objet sont stockées avec la nouvelle classe de stockage. Un objet existant reste stocké sous la classe de stockage définie lors de l'ingestion.

   > Le nom du compartiment, la région et le point de terminaison utilisent les valeurs AWS et ne peuvent pas être modifiés.

5. Cliquez sur **appliquer les modifications**.

Modification de l'état du service NetApp Cloud Tiering

Vous pouvez contrôler la capacité de lecture et d'écriture du nœud d'archivage sur le système de stockage d'archives externe ciblé qui se connecte via l'API S3 en modifiant l'état du service de Tiering cloud.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.

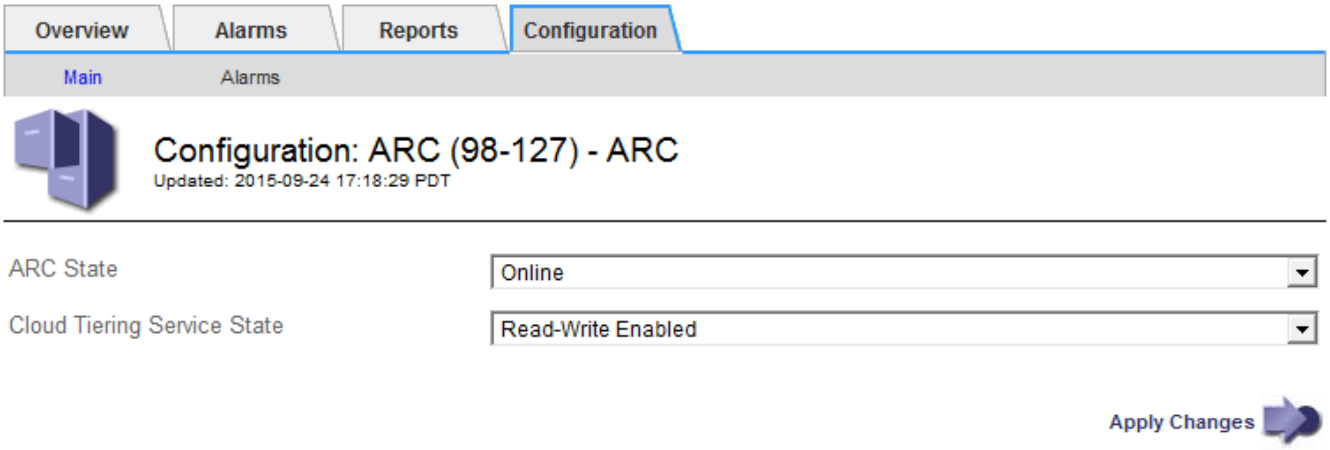
- Vous devez disposer d'autorisations d'accès spécifiques.
- Le nœud d'archivage doit être configuré.

Description de la tâche

Vous pouvez mettre le nœud d'archivage hors ligne en changeant l'état du service de Tiering cloud sur **Read-Write Disabled**.

Étapes

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez ***Archive Node*** > **ARC**.
3. Sélectionnez **Configuration** > **main**.



4. Sélectionnez un **Cloud Tiering Service State**.
5. Cliquez sur **appliquer les modifications**.

Réinitialisation du nombre d'échecs de stockage pour la connexion API S3

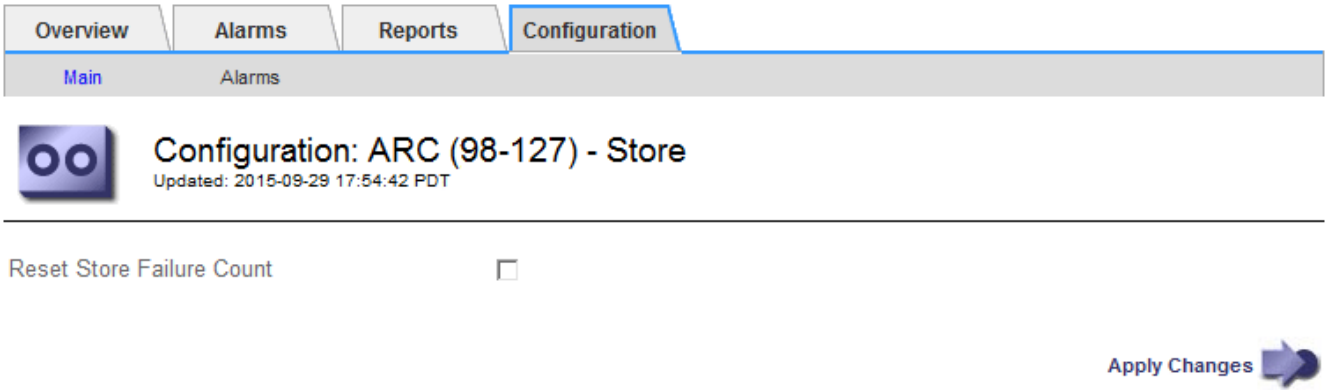
Si votre nœud d'archivage se connecte à un système de stockage d'archives via l'API S3, vous pouvez réinitialiser le nombre d'échecs de stockage, qui peut être utilisé pour effacer l'alarme ARVF (échecs de stockage).

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez ***Archive Node*** > **ARC** > **Store**.
3. Sélectionnez **Configuration** > **main**.



4. Sélectionnez **Réinitialiser le nombre d'échecs de stockage**.
5. Cliquez sur **appliquer les modifications**.

   L'attribut Store Failures se réinitialise sur zéro.

Migration d'objets à partir de Cloud Tiering - S3 vers un pool de stockage cloud

Si vous utilisez actuellement la fonctionnalité **Cloud Tiering - simple Storage Service (S3)** pour hiérarchiser les données d'objet vers un compartiment S3, envisagez de migrer vos objets vers un pool de stockage cloud. Les pools de stockage cloud offrent une approche évolutive qui tire parti de tous les nœuds de stockage dans votre système StorageGRID.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.
- Des objets sont déjà stockés dans le compartiment S3 configuré pour le Tiering dans le cloud.

> Avant de migrer les données d'objet, contactez votre ingénieur commercial NetApp pour comprendre et gérer les coûts éventuels associés.

Description de la tâche

Le pool de stockage cloud est similaire à celui d'un pool de stockage du point de vue ILM. Toutefois, si les pools de stockage sont constitués de nœuds de stockage ou de nœuds d'archivage dans le système StorageGRID, un pool de stockage cloud est constitué d'un compartiment S3 externe.

Avant de migrer les objets depuis Cloud Tiering - S3 vers un pool de stockage cloud, vous devez d'abord créer un compartiment S3, puis créer le pool de stockage cloud dans StorageGRID. Vous pouvez ensuite créer une nouvelle règle ILM et remplacer la règle ILM utilisée pour stocker les objets dans le compartiment Cloud Tiering par une règle ILM clonée qui stocke les mêmes objets dans le pool de stockage cloud.

> Lorsque des objets sont stockés dans un pool de stockage cloud, des copies de ces objets ne peuvent pas également être stockées dans StorageGRID. Si la règle ILM que vous utilisez actuellement pour Cloud Tiering est configurée pour stocker les objets en même temps, déterminez si vous souhaitez toujours effectuer cette migration facultative, car elle sera perdue. Si vous continuez cette migration, vous devez créer de nouvelles règles au lieu de cloner les règles existantes.

Étapes

1. Création d'un pool de stockage cloud.

   Utilisez un nouveau compartiment S3 pour le pool de stockage cloud afin de garantir que celui-ci contient uniquement les données gérées par le pool de stockage cloud.

2. Recherchez toutes les règles ILM de la règle ILM active qui entraîne le stockage des objets dans le compartiment de NetApp Cloud Tiering.
3. Clonez chacune de ces règles.
4. Dans les règles clonées, modifiez l'emplacement de placement dans le nouveau pool de stockage cloud.
5. Enregistrez les règles clonées.
6. Création d'une nouvelle règle qui utilise les nouvelles règles
7. Simuler et activer la nouvelle règle.

   Lorsque la nouvelle règle est activée et que l'évaluation ILM est effectuée, les objets sont déplacés du compartiment S3 configuré pour NetApp Cloud Tiering vers le compartiment S3 configuré pour le pool de stockage cloud. L'espace utilisable sur la grille n'est pas affecté. Une fois les objets déplacés vers le pool de stockage cloud, ils sont supprimés du compartiment de NetApp Cloud Tiering.

Informations associées

"Gestion des objets avec ILM"

Archivage sur bande via le logiciel médiateur TSM

Vous pouvez configurer un nœud d'archivage pour qu'il cible un serveur Tivoli Storage Manager (TSM) qui fournit une interface logique permettant de stocker et de récupérer des données d'objet sur des unités de stockage à accès aléatoire ou séquentiel, y compris des librairies de bandes.

Le service ARC du nœud d'archivage sert de client au serveur TSM, utilisant Tivoli Storage Manager comme logiciel médiateur pour communiquer avec le système de stockage d'archives.

Cours de gestion TSM

Les classes de gestion définies par le middleware TSM décrivent le fonctionnement des opérations de sauvegarde et d'archivage de TSM's et peuvent être utilisées pour spécifier les règles du contenu appliqué par le serveur TSM. Ces règles fonctionnent indépendamment de la politique ILM du système StorageGRID et doivent rester cohérentes avec StorageGRID la condition que les objets soient stockés de manière permanente et soient toujours disponibles pour la récupération par le nœud d'archivage. Une fois les données d'objet envoyées à un serveur TSM par le nœud d'archivage, les règles de cycle de vie et de conservation TSM sont appliquées pendant que les données de l'objet sont stockées sur bande gérée par le serveur TSM.

La classe de gestion TSM est utilisée par le serveur TSM pour appliquer des règles pour l'emplacement ou la conservation des données après que les objets soient envoyés au serveur TSM par le nœud d'archivage. Par exemple, les objets identifiés comme sauvegardes de bases de données (contenu temporaire pouvant être remplacé par des données plus récentes) peuvent être traités différemment des données d'application (contenu fixe qui doit être conservé indéfiniment).

Avant que le nœud d'archivage puisse communiquer avec le middleware Tivoli Storage Manager (TSM), vous devez configurer un certain nombre de paramètres.

Ce dont vous avez besoin

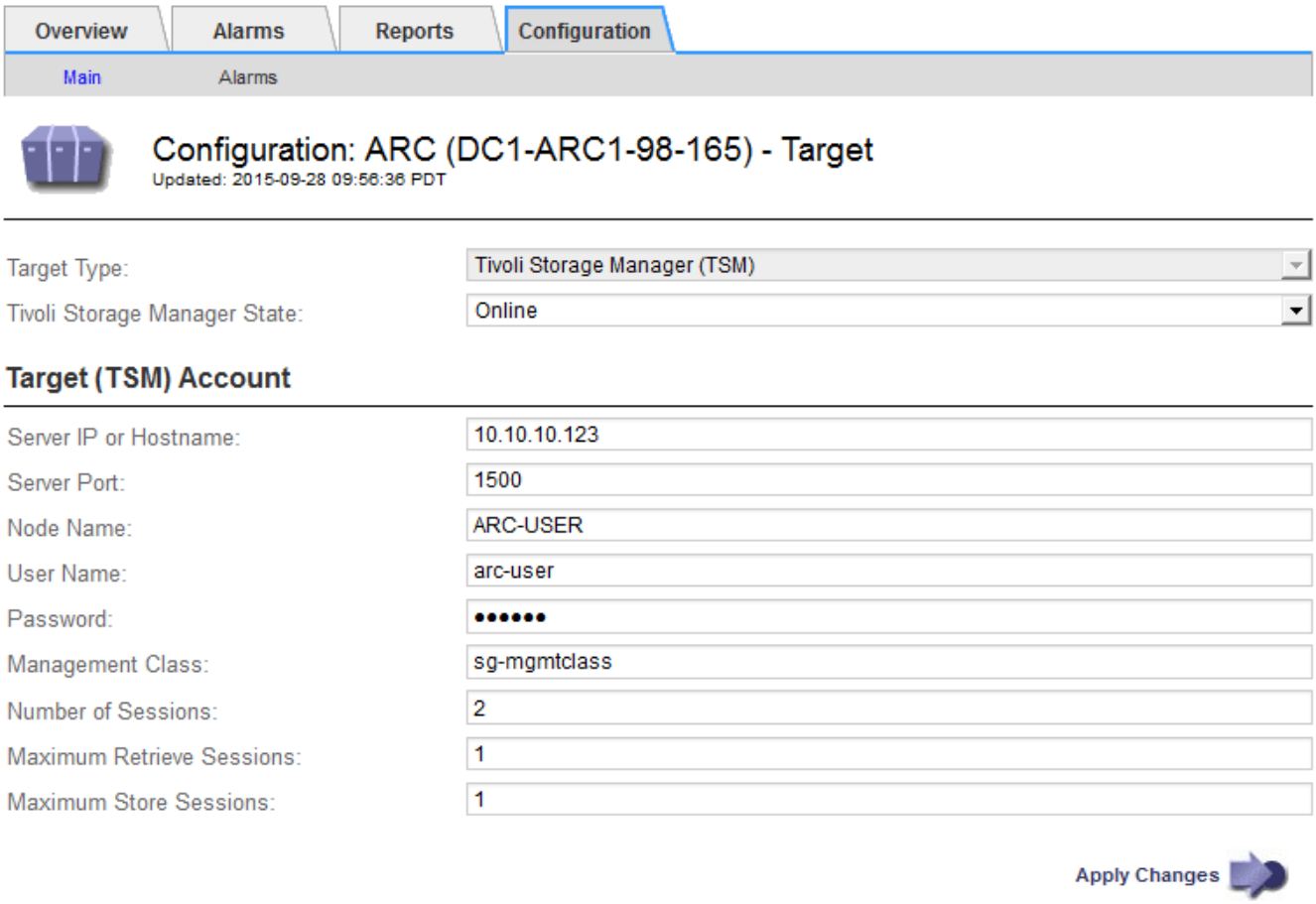
- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Tant que ces paramètres ne sont pas configurés, le service ARC reste dans un état d'alarme majeur car il ne peut pas communiquer avec Tivoli Storage Manager.

Étapes

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez ***Archive Node*** > **ARC** > **cible**.
3. Sélectionnez **Configuration** > **main**.



4. Dans la liste déroulante **Type cible**, sélectionnez **Tivoli Storage Manager (TSM)**.
5. Pour l'état **Tivoli Storage Manager**, sélectionnez **Offline** pour empêcher les récupérations du serveur middleware TSM.

   Par défaut, l'état Tivoli Storage Manager est défini sur en ligne, ce qui signifie que le noeud d'archivage peut récupérer des données d'objet à partir du serveur middleware TSM.

6. Complétez les informations suivantes :

   - **IP ou Nom d'hôte du serveur** : spécifiez l'adresse IP ou le nom de domaine complet du serveur middleware TSM utilisé par le service ARC. L'adresse IP par défaut est 127.0.0.1.
   - **Port serveur** : spécifiez le numéro de port sur le serveur middleware TSM auquel le service ARC se connectera. La valeur par défaut est 1500.
   - **Nom du noeud** : spécifiez le nom du noeud d'archive. Vous devez entrer le nom (utilisateur d'arc) que vous avez enregistré sur le serveur middleware TSM.
   - **Nom d'utilisateur** : spécifiez le nom d'utilisateur utilisé par le service ARC pour se connecter au serveur TSM. Entrez le nom d'utilisateur par défaut (utilisateur d'arc) ou l'utilisateur administratif spécifié pour le noeud d'archivage.
   - **Mot de passe** : Indiquez le mot de passe utilisé par le service ARC pour se connecter au serveur TSM.
   - **Classe de gestion** : spécifiez la classe de gestion par défaut à utiliser si une classe de gestion n'est pas spécifiée lors de l'enregistrement de l'objet sur le système StorageGRID ou si la classe de gestion spécifiée n'est pas définie sur le serveur middleware TSM.
   - **Nombre de sessions** : spécifiez le nombre de lecteurs de bande sur le serveur middleware TSM dédié au nœud d'archivage. Le nœud d'archivage crée simultanément un maximum d'une session par point de montage et un petit nombre de sessions supplémentaires (moins de cinq).

     Vous devez modifier cette valeur pour qu'elle soit identique à la valeur définie pour MAXNUMMP (nombre maximal de points de montage) lorsque le nœud d'archivage a été enregistré ou mis à jour. (Dans la commande REGISTER, la valeur par défaut de MAXNUMMP utilisée est 1, si aucune valeur n'est définie.)

   Vous devez également modifier la valeur de MAXSESSIONS pour le serveur TSM à un nombre au moins aussi important que le nombre de sessions défini pour le service ARC. La valeur par défaut de MAXSESSIONS sur le serveur TSM est 25.

   - **Nombre maximal de sessions de récupération** : spécifiez le nombre maximal de sessions que le service ARC peut ouvrir sur le serveur middleware TSM pour les opérations de récupération. Dans la plupart des cas, la valeur appropriée est le nombre de sessions moins le nombre maximal de sessions en magasin. Si vous devez partager un lecteur de bande pour le stockage et la récupération, spécifiez une valeur égale au nombre de sessions.
   - **Nombre maximal de sessions de stockage** : spécifiez le nombre maximal de sessions simultanées que le service ARC peut ouvrir sur le serveur middleware TSM pour les opérations d'archivage.

     Cette valeur doit être définie sur une seule, sauf lorsque le système de stockage d'archives ciblé est plein et que seules les récupérations peuvent être effectuées. Définissez cette valeur sur zéro pour utiliser toutes les sessions pour les récupérations.

7. Cliquez sur **appliquer les modifications**.

Optimisation d'un nœud d'archivage pour les sessions middleware TSM

Vous pouvez optimiser les performances d'un noeud d'archivage qui se connecte à Tivoli Server Manager (TSM) en configurant les sessions du noeud d'archivage.

Ce dont vous avez besoin

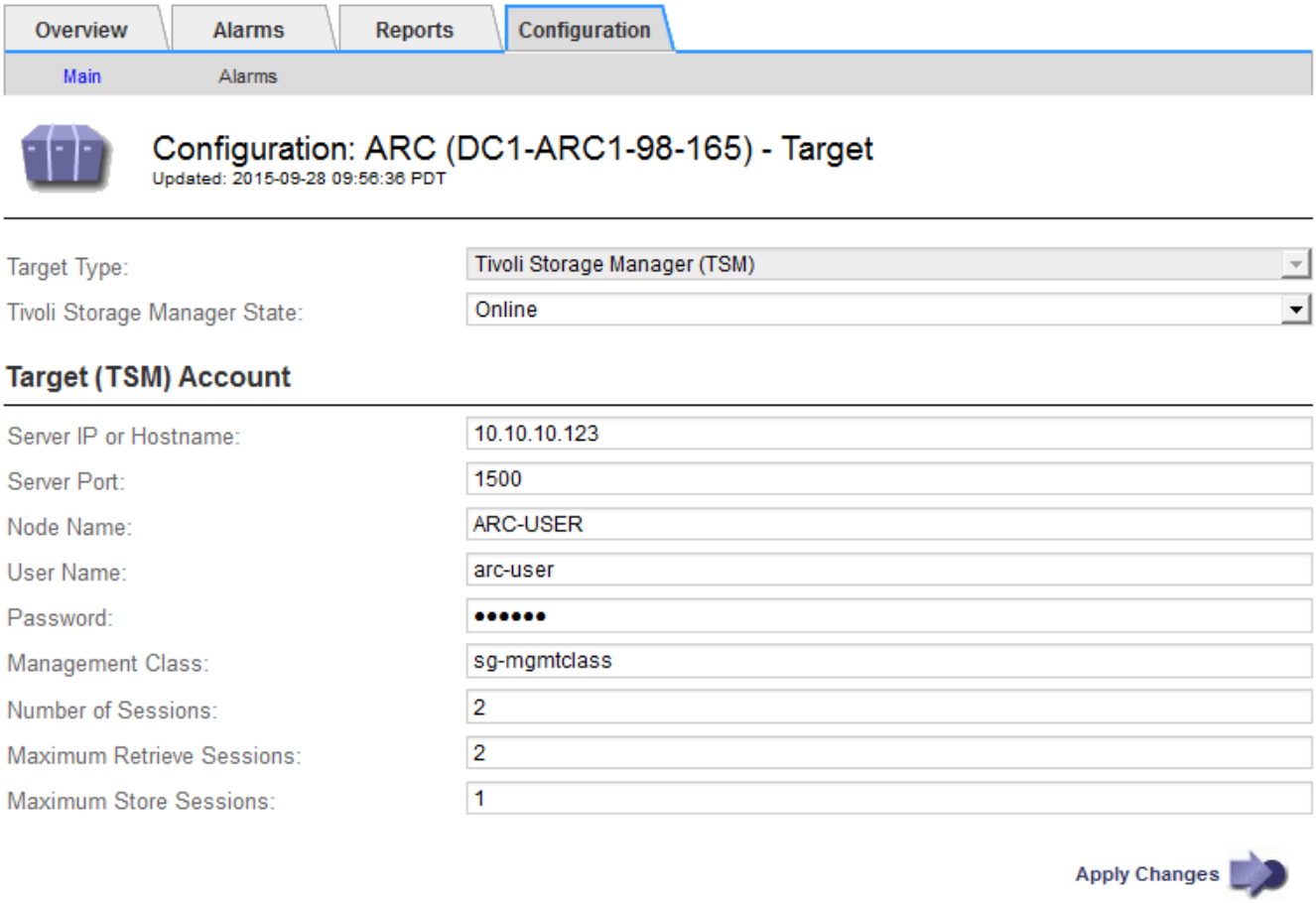
- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

En général, le nombre de sessions simultanées que le nœud d'archivage a ouvertes au serveur middleware TSM est défini sur le nombre de lecteurs de bande que le serveur TSM a dédiés au nœud d'archivage. Un lecteur de bande est alloué au stockage tandis que le reste est alloué à la récupération. Toutefois, lorsqu'un nœud de stockage est en cours de reconstruction à partir de copies de nœud d'archivage ou que le nœud d'archivage fonctionne en mode lecture seule, vous pouvez optimiser les performances du serveur TSM en définissant le nombre maximal de sessions d'extraction à identique au nombre de sessions simultanées. Il en résulte que tous les disques peuvent être utilisés simultanément pour la récupération et, au plus, un de ces lecteurs peut également être utilisé pour le stockage, le cas échéant.

Étapes

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez ***Archive Node*** > **ARC** > **cible**.
3. Sélectionnez **Configuration** > **main**.
4. Modifier **nombre maximal de sessions de récupération** pour être le même que **nombre de sessions**.



5. Cliquez sur **appliquer les modifications**.

Configuration de l'état d'archivage et des compteurs pour TSM

Si votre nœud d'archivage se connecte à un serveur middleware TSM, vous pouvez configurer l'état du magasin d'archives d'un nœud d'archivage sur en ligne ou hors ligne. Vous pouvez également désactiver le magasin d'archives lors du premier démarrage du nœud d'archivage ou réinitialiser le nombre d'échecs en cours de suivi pour l'alarme

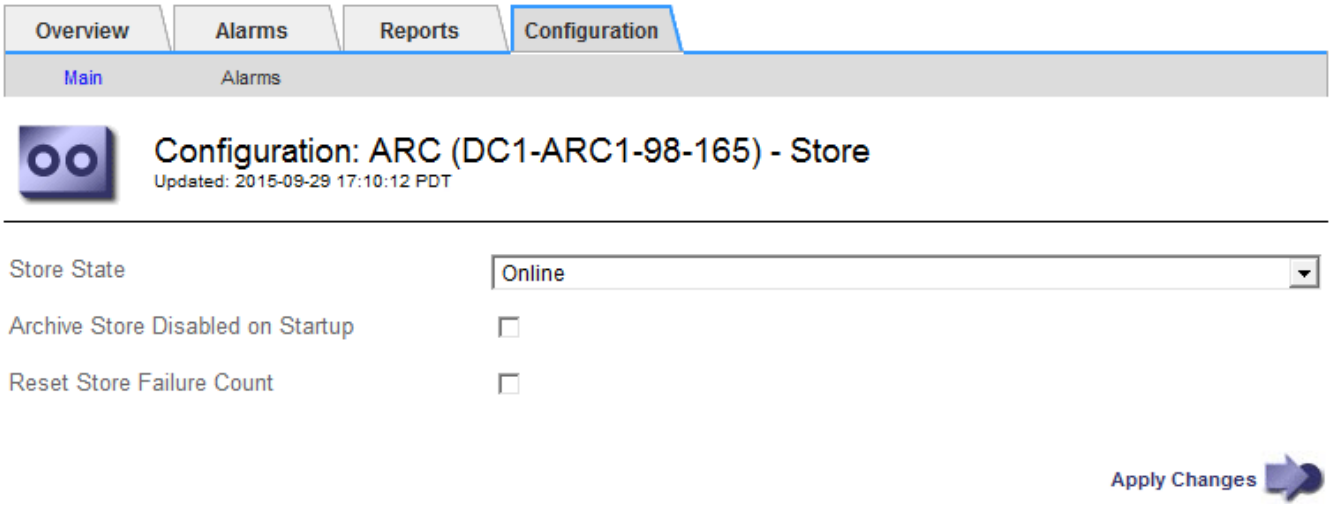
associée.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez ***Archive Node*** > **ARC** > **Store**.
3. Sélectionnez **Configuration** > **main**.



4. Modifiez les paramètres suivants, si nécessaire :
   - État du stockage : définissez l'état du composant sur :
     - En ligne : le nœud d'archivage est disponible pour traiter les données d'objet pour le stockage vers le système de stockage d'archivage.
     - Hors ligne : le nœud d'archivage n'est pas disponible pour traiter les données d'objet pour le stockage vers le système de stockage d'archives.
   - Magasin d'archives désactivé au démarrage : lorsque cette option est sélectionnée, le composant stockage d'archives reste en lecture seule lors du redémarrage. Utilisé pour désactiver de manière persistante le stockage vers le système cible de stockage d'archives. Utile lorsque la cible est ciblée, le système de stockage d'archives ne peut pas accepter de contenu.
   - Réinitialiser le nombre d'échecs du magasin : réinitialisez le compteur pour les échecs du magasin. Il peut être utilisé pour effacer l'alarme ARVF (Store Failure).
5. Cliquez sur **appliquer les modifications**.

Informations associées

"Gestion d'un nœud d'archivage lorsque le serveur TSM atteint sa capacité"

Gestion d'un nœud d'archivage lorsque le serveur TSM atteint sa capacité

Le serveur TSM n'a aucun moyen d'informer le nœud d'archivage lorsque la base de données TSM ou le stockage des supports d'archivage gérés par le serveur TSM atteint sa capacité maximale. Le nœud d'archivage continue à accepter les données d'objet

pour le transfert vers le serveur TSM une fois que le serveur TSM a arrêté d'accepter le nouveau contenu. Ce contenu ne peut pas être écrit sur un support géré par le serveur TSM. Une alarme est déclenchée si cela se produit. Cette situation peut être évitée grâce à la surveillance proactive du serveur TSM.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Pour empêcher le service ARC d'envoyer du contenu supplémentaire au serveur TSM, vous pouvez mettre le nœud d'archivage hors ligne en mettant hors ligne son composant **ARC** > **Store**. Cette procédure peut également être utile pour empêcher les alarmes lorsque le serveur TSM n'est pas disponible pour la maintenance.

Étapes

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez ***Archive Node*** > **ARC** > **Store**.
3. Sélectionnez **Configuration** > **main**.

4. Définissez **Etat du magasin** sur `Offline`.
5. Sélectionnez **Archive Store Disabled au démarrage**.
6. Cliquez sur **appliquer les modifications**.

Configuration du nœud d'archivage en lecture seule si le middleware TSM atteint sa capacité maximale

Si le serveur middleware TSM cible atteint sa capacité, le nœud d'archivage peut être optimisé pour effectuer uniquement des récupérations.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **support** > **Outils** > **topologie de grille**.

2. Sélectionnez ***Archive Node*** > **ARC** > **cible**.
3. Sélectionnez **Configuration** > **main**.
4. Modifiez le nombre maximal de sessions de récupération pour qu'il soit identique au nombre de sessions simultanées répertoriées dans nombre de sessions.
5. Définissez le nombre maximum de sessions de stockage sur 0.

> Il n'est pas nécessaire de modifier le nombre maximal de sessions de stockage sur 0 si le nœud d'archivage est en lecture seule. Les sessions de magasin ne seront pas créées.

6. Cliquez sur **appliquer les modifications**.

Configuration des paramètres de récupération du nœud d'archivage

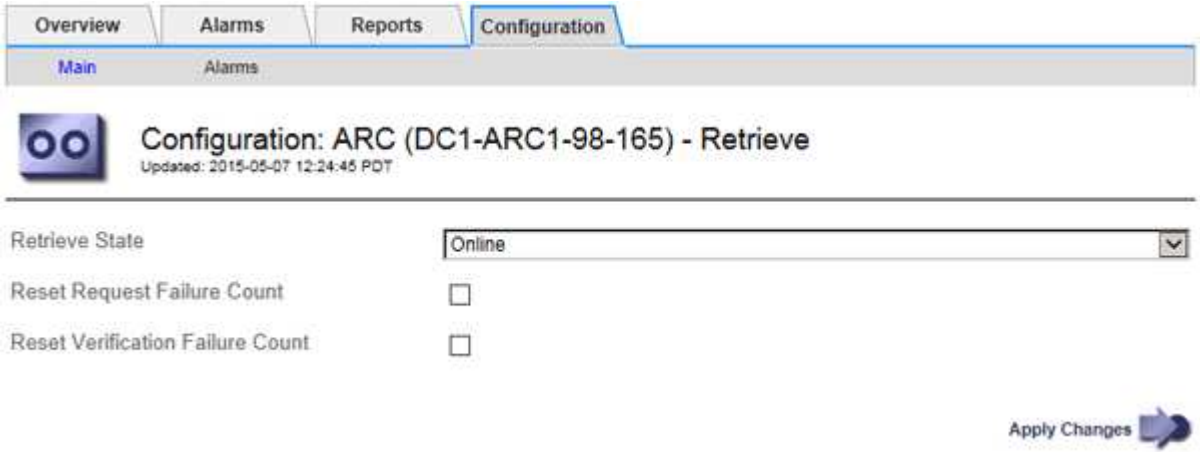
Vous pouvez configurer les paramètres de récupération d'un nœud d'archivage pour définir l'état en ligne ou hors ligne, ou réinitialiser le nombre d'échecs en cours de suivi pour les alarmes associées.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez **Archive Node** > **ARC** > **Retrieve**.
3. Sélectionnez **Configuration** > **main**.



4. Modifiez les paramètres suivants, si nécessaire :
   - **Récupérer l'état** : définissez l'état du composant sur :
     - En ligne : le nœud de grille est disponible pour récupérer les données d'objet à partir du périphérique de support d'archivage.
     - Hors ligne : le nœud grid n'est pas disponible pour récupérer les données d'objet.
   - Réinitialiser le nombre d'échecs de la demande : cochez la case pour réinitialiser le compteur pour les échecs de la demande. Il peut être utilisé pour effacer l'alarme ARRF (demandes d'échecs).

- Réinitialiser le nombre d'échecs de vérification : cochez cette case pour réinitialiser le compteur d'échecs de vérification sur les données d'objet récupérées. Il peut être utilisé pour effacer l'alarme ARRV (échecs de vérification).

5. Cliquez sur **appliquer les modifications**.

Configuration de la réplication du noeud d'archivage

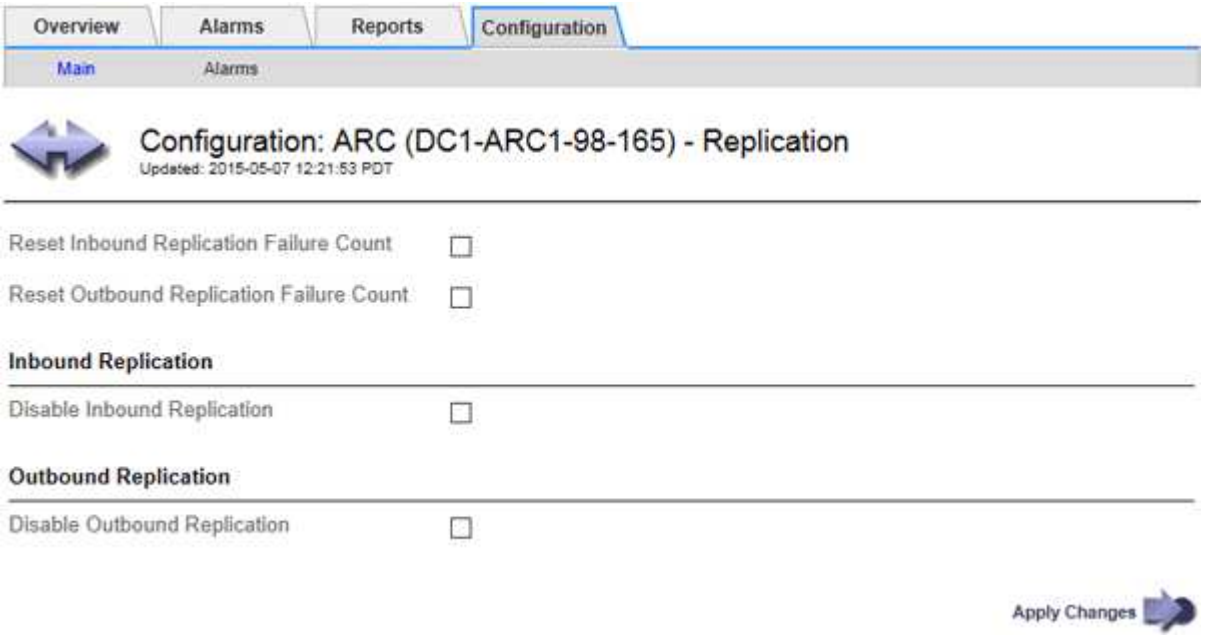
Vous pouvez configurer les paramètres de réplication d'un nœud d'archivage et désactiver la réplication entrante et sortante, ou réinitialiser le nombre d'échecs en cours de suivi pour les alarmes associées.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **support** > **Outils** > **topologie de grille**.
2. Sélectionnez ***Archive Node*** > **ARC** > **Replication**.
3. Sélectionnez **Configuration** > **main**.



4. Modifiez les paramètres suivants, si nécessaire :
   - **Réinitialiser le nombre d'échecs de réplication entrant** : sélectionnez cette option pour réinitialiser le compteur pour les échecs de réplication entrants. Cette fonction permet d'effacer l'alarme RRF (Replications entrantes — FAILED).
   - **Réinitialiser le nombre d'échecs de réplication sortante** : sélectionnez cette option pour réinitialiser le compteur des échecs de réplication sortants. Cette fonction permet d'effacer l'alarme RORF (réplications sortantes — en échec).
   - **Désactiver la réplication entrante** : sélectionnez cette option pour désactiver la réplication entrante dans le cadre d'une procédure de maintenance ou de test. Laisser effacé pendant le fonctionnement normal.

Lorsque la réplication entrante est désactivée, les données d'objet peuvent être extraites du service ARC pour la réplication vers d'autres emplacements du système StorageGRID, mais les objets ne peuvent pas être répliqués vers ce service ARC à partir d'autres emplacements du système. Le service ARC est en lecture seule.

- **Désactiver la réplication sortante** : cochez cette case pour désactiver la réplication sortante (y compris les demandes de contenu pour les récupérations HTTP) dans le cadre d'une procédure de maintenance ou de test. Laisser non vérifié pendant le fonctionnement normal.

  Lorsque la réplication sortante est désactivée, les données d'objet peuvent être copiées vers ce service ARC afin de satisfaire aux règles ILM, mais les données d'objet ne peuvent pas être récupérées à partir du service ARC pour être copiées vers d'autres emplacements du système StorageGRID. Le service ARC est en écriture uniquement.

5. Cliquez sur **appliquer les modifications**.

Définition d'alarmes personnalisées pour le nœud d'archivage

Vous devez établir des alarmes personnalisées pour les attributs ARQL et ARRL utilisés pour surveiller la vitesse et l'efficacité de la récupération des données d'objet à partir du système de stockage d'archives par le nœud d'archivage.

- ARQL : longueur moyenne de la file d'attente. Durée moyenne, en microsecondes, de la mise en file d'attente des données de cet objet pour la récupération à partir du système de stockage d'archivage.
- ARRL : latence moyenne de la requête. Temps moyen, en microsecondes, requis par le nœud d'archivage pour récupérer les données d'objet à partir du système de stockage d'archivage.

Les valeurs acceptables pour ces attributs dépendent de la configuration et de l'utilisation du système de stockage d'archives. (Allez à **ARC** > **Retrieve** > **Présentation** > **main**.) Les valeurs définies pour les délais de requête et le nombre de sessions disponibles pour les demandes de récupération sont particulièrement influentes.

Une fois l'intégration terminée, surveillez les récupérations de données d'objet du nœud d'archivage pour établir des valeurs pour les temps de récupération normaux et la longueur de file d'attente. Ensuite, créez des alarmes personnalisées pour ARQL et ARRL qui se déclencheront en cas de condition de fonctionnement anormale.

Informations associées

"Moniteur et amp ; dépannage"

Intégration de Tivoli Storage Manager

Cette section comprend les meilleures pratiques et les informations de configuration pour l'intégration d'un nœud d'archivage à un serveur Tivoli Storage Manager (TSM), notamment les détails opérationnels du nœud d'archivage qui affectent la configuration du serveur TSM.

- "Configuration et fonctionnement du nœud d'archivage"
- "Bonnes pratiques pour la configuration"
- "Fin de la configuration du nœud d'archivage"

Configuration et fonctionnement du nœud d’archivage

Votre système StorageGRID gère le nœud d’archivage comme un emplacement dans lequel les objets sont stockés indéfiniment et sont toujours accessibles.

À l’ingestion d’un objet, des copies sont effectuées dans tous les emplacements nécessaires, y compris les nœuds d’archivage, en fonction des règles de gestion du cycle de vie des informations (ILM) définies pour votre système StorageGRID. Le nœud d’archivage agit comme un client sur un serveur TSM, et les bibliothèques clientes TSM sont installées sur le nœud d’archivage par le processus d’installation du logiciel StorageGRID. Les données d’objet dirigées vers le nœud d’archivage pour le stockage sont enregistrées directement sur le serveur TSM au moment de leur réception. Le nœud d’archivage n’exécute pas les données d’objet avant de les enregistrer sur le serveur TSM, ni l’agrégation d’objets. Cependant, le nœud d’archivage peut envoyer plusieurs copies au serveur TSM en une seule transaction lorsque le taux de données le garantit.

Une fois que le nœud d’archivage enregistre les données d’objet sur le serveur TSM, les données d’objet sont gérées par le serveur TSM à l’aide de ses politiques de cycle de vie/rétention. Ces règles de conservation doivent être définies pour être compatibles avec le fonctionnement du nœud d’archivage. En d’autres termes, les données d’objet enregistrées par le nœud d’archivage doivent être stockées indéfiniment et doivent toujours être accessibles par le nœud d’archivage, à moins qu’elles ne soient supprimées par le nœud d’archivage.

Il n’y a aucune connexion entre les règles ILM du système StorageGRID et les politiques de cycle de vie/conservation du serveur TSM. Chaque système fonctionne de manière indépendante ; cependant, lorsque chaque objet est ingéré dans le système StorageGRID, vous pouvez lui attribuer une classe de gestion TSM. Cette classe de gestion est transmise au serveur TSM avec les données d’objet. L’affectation de classes de gestion à différents types d’objets vous permet de configurer le serveur TSM pour placer les données d’objet dans différents pools de stockage, ou d’appliquer différentes règles de migration ou de conservation, le cas échéant. Par exemple, les objets identifiés comme sauvegardes de bases de données (le contenu temporaire pouvant être remplacé par des données plus récentes) peuvent être traités différemment des données applicatives (contenu fixe qui doit être conservé indéfiniment).

Le nœud d’archivage peut être intégré à un nouveau serveur TSM ou à un serveur TSM existant ; il ne nécessite pas de serveur TSM dédié. Les serveurs TSM peuvent être partagés avec d’autres clients, à condition que la taille du serveur TSM soit adaptée à la charge maximale attendue. TSM doit être installé sur un serveur ou une machine virtuelle distincte du nœud d’archivage.

Il est possible de configurer plusieurs nœuds d’archivage pour écrire sur le même serveur TSM. Cependant, cette configuration n’est recommandée que si les nœuds d’archivage écrivent différents ensembles de données sur le serveur TSM. Il n’est pas recommandé de configurer plusieurs nœuds d’archivage pour écrire sur le même serveur TSM lorsque chaque nœud d’archivage écrit des copies des mêmes données d’objet dans l’archive. Dans ce dernier scénario, les deux copies sont soumises à un point de défaillance unique (le serveur TSM), pour les copies redondantes et indépendantes des données d’objet.

Les nœuds d’archivage n’utilisent pas le composant HSM (Hierarchical Storage Management) de TSM.

Bonnes pratiques pour la configuration

Lorsque vous dimensionnez et configurez votre serveur TSM, il existe les meilleures pratiques que vous devez appliquer pour l’optimiser afin qu’il fonctionne avec le nœud d’archivage.

Lors du dimensionnement et de la configuration du serveur TSM, il est important de prendre en compte les facteurs suivants :

- Comme le nœud d'archivage ne agrège pas les objets avant de les enregistrer sur le serveur TSM, la base de données TSM doit être dimensionnée pour contenir les références à tous les objets qui seront écrits sur le nœud d'archivage.
- Le logiciel Archive Node ne peut pas tolérer la latence impliquée dans l'écriture d'objets directement sur bande ou sur un autre support amovible. Par conséquent, le serveur TSM doit être configuré avec un pool de stockage sur disque pour le stockage initial des données sauvegardées par le nœud d'archivage chaque fois que des supports amovibles sont utilisés.
- Vous devez configurer les règles de conservation TSM pour utiliser la conservation basée sur les événements. Le nœud d'archivage ne prend pas en charge les politiques de conservation TSM basées sur la création. Utilisez les paramètres recommandés suivants de retmin=0 et retver=0 dans la stratégie de rétention (ce qui indique que la rétention commence lorsque le noeud d'archivage déclenche un événement de rétention et est conservé pendant 0 jours après cela). Toutefois, ces valeurs pour le retmin et le retver sont facultatives.

Le pool de disques doit être configuré pour migrer les données vers le pool de bandes (c'est-à-dire que le pool de bandes doit être le NXTSTGPOOL du pool de disques). Le pool de bandes ne doit pas être configuré en tant que pool de copies du pool de disques avec écriture simultanée sur les deux pools (c'est-à-dire que le pool de bandes ne peut pas être COPYSTGPOOL pour le pool de disques). Pour créer des copies hors ligne des bandes contenant les données du nœud d'archivage, configurez le serveur TSM avec un deuxième pool de bandes qui est un pool de copies du pool de bandes utilisé pour les données du nœud d'archivage.

Fin de la configuration du nœud d'archivage

Le nœud d'archivage ne fonctionne pas après avoir terminé le processus d'installation. Avant que le système StorageGRID puisse enregistrer des objets sur le nœud d'archivage TSM, vous devez terminer l'installation et la configuration du serveur TSM et configurer le nœud d'archivage pour qu'il communique avec le serveur TSM.

Pour plus d'informations sur l'optimisation des sessions de récupération et de stockage TSM, consultez les informations sur la gestion du stockage d'archives.

- "Gestion des nœuds d'archivage"

Si nécessaire, reportez-vous à la documentation IBM suivante lorsque vous préparez votre serveur TSM pour l'intégration au nœud d'archivage d'un système StorageGRID :

- "Guide d'installation et d'utilisation des pilotes de périphérique de bande IBM"
- "Référence de programmation des pilotes de périphériques de bande IBM"

Installation d'un nouveau serveur TSM

Vous pouvez intégrer le nœud d'archivage à un nouveau serveur TSM ou à un serveur TSM existant. Si vous installez un nouveau serveur TSM, suivez les instructions de la documentation TSM pour terminer l'installation.

> Un noeud d'archive ne peut pas être co-hébergé avec un serveur TSM.

Configuration du serveur TSM

Cette section comprend des exemples d'instructions pour préparer un serveur TSM conformément aux meilleures pratiques TSM.

Les instructions suivantes vous guident tout au long du processus :

- Définition d'un pool de stockage sur disque et d'un pool de stockage sur bandes (le cas échéant) sur le serveur TSM
- Définition d'une stratégie de domaine qui utilise la classe de gestion TSM pour les données enregistrées à partir du nœud d'archivage et enregistrement d'un nœud pour utiliser cette stratégie de domaine

Ces instructions sont fournies à titre indicatif uniquement. Elles ne sont pas destinées à remplacer la documentation TSM ou à fournir des instructions complètes et complètes adaptées à toutes les configurations. Des instructions spécifiques à un déploiement doivent être fournies par un administrateur TSM qui connaît à la fois vos exigences détaillées et la documentation complète de TSM Server.

Définition de pools de stockage sur disque et sur bande TSM

Le nœud d'archivage écrit dans un pool de stockage sur disque. Pour archiver du contenu sur bande, vous devez configurer le pool de stockage sur disque afin de déplacer le contenu vers un pool de stockage sur bande.

Description de la tâche

Pour un serveur TSM, vous devez définir un pool de stockage sur bandes et un pool de stockage sur disque dans Tivoli Storage Manager. Une fois le pool de disques défini, créez un volume de disque et affectez-le au pool de disques. Un pool de bandes n'est pas nécessaire si votre serveur TSM utilise du stockage sur disque uniquement.

Vous devez effectuer plusieurs étapes sur votre serveur TSM avant de pouvoir créer un pool de stockage sur bandes. (Créez une bibliothèque de bandes et au moins un lecteur dans la bibliothèque de bandes. Définissez un chemin entre le serveur et la bibliothèque et entre le serveur et les lecteurs, puis définissez une classe de périphériques pour les lecteurs.) Les détails de ces étapes peuvent varier en fonction de la configuration matérielle et des besoins de stockage du site. Pour plus d'informations, consultez la documentation TSM.

Le jeu d'instructions ci-dessous illustre le processus. Vous devez savoir que les besoins spécifiques à votre site peuvent varier en fonction des besoins de votre déploiement. Pour plus d'informations sur la configuration et pour obtenir des instructions, consultez la documentation TSM.

> Vous devez vous connecter au serveur avec des privilèges d'administration et utiliser l'outil dsmadmc pour exécuter les commandes suivantes.

Étapes

1. Créez une bibliothèque de bandes.

   `define library` *`tapelibrary`* `libtype=`*`scsi`*

   Où *`tapelibrary`* est un nom arbitraire choisi pour la bibliothèque de bandes et la valeur de `libtype` peut varier selon le type de bibliothèque de bandes.

2. Définissez un chemin entre le serveur et la bibliothèque de bandes.

   `define path` *`servername tapelibrary`* `srctype=server desttype=library device=`*`lib-devicename`*

   - *`servername`* Est le nom du serveur TSM
   - *`tapelibrary`* est le nom de bibliothèque de bandes que vous avez défini

- *lib-devicename* est le nom du périphérique de la bibliothèque de bandes

3. Définissez un lecteur pour la bibliothèque.

   ```
   define drive tapelibrary drivename
   ```

   - *drivename* est le nom que vous souhaitez spécifier pour le lecteur
   - *tapelibrary* est le nom de bibliothèque de bandes que vous avez défini

     Il est possible que vous souhaitiez configurer un ou plusieurs lecteurs supplémentaires, en fonction de la configuration de votre matériel. (Par exemple, si le serveur TSM est connecté à un commutateur Fibre Channel qui comporte deux entrées d'une bibliothèque de bandes, vous pouvez définir un lecteur pour chaque entrée.)

4. Définissez un chemin entre le serveur et le lecteur que vous avez défini.

   ```
   define path servername drivename srctype=server desttype=drive
   library=tapelibrary device=drive-dname
   ```

   - *drive-dname* est le nom du périphérique du lecteur
   - *tapelibrary* est le nom de bibliothèque de bandes que vous avez défini

     Répétez l'opération pour chaque lecteur que vous avez défini pour la bibliothèque de bandes à l'aide d'un lecteur distinct *drivename* et *drive-dname* pour chaque lecteur.

5. Définir une classe de périphérique pour les lecteurs.

   ```
   define devclass DeviceClassName devtype=lto library=tapelibrary
   format=tapetype
   ```

   - *DeviceClassName* est le nom de la classe de périphérique
   - *lto* est le type de lecteur connecté au serveur
   - *tapelibrary* est le nom de bibliothèque de bandes que vous avez défini
   - *tapetype* est le type de bande ; par exemple, ultrium3

6. Ajoutez des volumes de bande à l'inventaire de la bibliothèque.

   ```
   checkin libvolume tapelibrary
   ```

   tapelibrary est le nom de bibliothèque de bandes que vous avez défini.

7. Créez le pool de stockage sur bande primaire.

   ```
   define stgpool SGWSTapePool DeviceClassName description=description
   collocate=filespace maxscratch=XX
   ```

   - *SGWSTapePool* Est le nom du pool de stockage de bandes du nœud d'archivage. Vous pouvez sélectionner n'importe quel nom pour le pool de stockage de bandes (tant que le nom utilise les conventions de syntaxe attendues par le serveur TSM).
   - *DeviceClassName* est le nom de la classe de périphérique pour la bibliothèque de bandes.

- *description* Est une description du pool de stockage qui peut être affichée sur le serveur TSM à l'aide de `query stgpool` commande. Par exemple : « pool de stockage sur bande pour le nœud d'archivage ».
- *collocate=filespace* Spécifie que le serveur TSM doit écrire des objets à partir du même espace de fichiers dans une seule bande.
- `XX` est l'une des suivantes :
  - Nombre de bandes vides dans la bibliothèque de bandes (dans le cas où le nœud d'archivage est la seule application utilisant la bibliothèque).
  - Nombre de bandes allouées pour l'utilisation par le système StorageGRID (dans les cas où la bibliothèque de bandes est partagée).

8. Sur un serveur TSM, créez un pool de stockage sur disque. Sur la console d'administration du serveur TSM, entrez

   ```
   define stgpool SGWSDiskPool disk description=description
   maxsize=maximum_file_size nextstgpool=SGWSTapePool highmig=percent_high
   lowmig=percent_low
   ```

   - *SGWSDiskPool* Est le nom du pool de disques du nœud d'archivage. Vous pouvez sélectionner n'importe quel nom pour le pool de stockage sur disque (tant que le nom utilise les conventions de syntaxe attendues par le TSM).
   - *description* Est une description du pool de stockage qui peut être affichée sur le serveur TSM à l'aide de `query stgpool` commande. Par exemple, "disque de stockage pool pour le noeud d'archivage".
   - *maximum_file_size* force les objets de plus grande taille à être écrits directement sur bande, au lieu d'être mis en cache dans le pool de disques. Il est recommandé de le régler *maximum_file_size* À 10 Go.
   - *nextstgpool=SGWSTapePool* Désigne le pool de stockage sur disque au pool de stockage sur bandes défini pour le nœud d'archivage.
   - *percent_high* définit la valeur à laquelle le pool de disques commence à migrer son contenu vers le pool de bandes. Il est recommandé de le régler *percent_high* sur 0, pour que la migration des données commence immédiatement
   - *percent_low* définit la valeur à laquelle la migration vers le pool de bandes s'arrête. Il est recommandé de le régler *percent_low* à 0 pour effacer le pool de disques.

9. Sur un serveur TSM, créez un ou plusieurs volumes de disque et affectez-les au pool de disques.

   ```
   define volume SGWSDiskPool volume_name formatsize=size
   ```

   - *SGWSDiskPool* est le nom du pool de disques.
   - *volume_name* est le chemin complet vers l'emplacement du volume (par exemple, `/var/local/arc/stage6.dsm`) Sur le serveur TSM où il écrit le contenu du pool de disques en préparation du transfert sur bande.
   - *size* Est la taille, en Mo, du volume de disque.

     Par exemple, pour créer un volume de disque unique de sorte que le contenu d'un pool de disques remplisse une seule bande, définissez la valeur de la taille sur 200000 lorsque le volume de bande a une capacité de 200 Go.

Cependant, il est préférable de créer plusieurs volumes de disque de taille inférieure, car le serveur TSM peut écrire sur chaque volume du pool de disques. Par exemple, si la taille de la bande est de 250 Go, créez 25 volumes de disque d'une taille de 10 Go (10000) chacun.

Le serveur TSM préalloue de l'espace dans le répertoire du volume de disque. Cette opération peut prendre un certain temps (plus de trois heures pour un volume de disque de 200 Go).

Définition d'une stratégie de domaine et enregistrement d'un nœud

Vous devez définir une stratégie de domaine qui utilise la classe de gestion TSM pour les données enregistrées à partir du nœud d'archivage, puis enregistrer un nœud pour utiliser cette stratégie de domaine.

> Les processus du nœud d'archivage peuvent fuir de mémoire si le mot de passe client du nœud d'archivage dans Tivoli Storage Manager (TSM) expire. Assurez-vous que le serveur TSM est configuré de sorte que le nom d'utilisateur/mot de passe du client pour le nœud d'archivage n'expire jamais.

Lors de l'enregistrement d'un noeud sur le serveur TSM pour l'utilisation du noeud d'archivage (ou la mise à jour d'un noeud existant), vous devez spécifier le nombre de points de montage que le noeud peut utiliser pour les opérations d'écriture en spécifiant le paramètre MAXNUMMP à la commande ENREGISTRER NOEUD. Le nombre de points de montage est généralement équivalent au nombre de têtes de lecteur de bande attribuées au nœud d'archivage. Le numéro spécifié pour MAXNUMMP sur le serveur TSM doit être au moins aussi grand que la valeur définie pour **ARC** > **Target** > **Configuration** > **main** > **maximum Store sessions** pour le nœud d'archivage, Qui est défini sur 0 ou 1, car les sessions de stockage simultanées ne sont pas prises en charge par le nœud d'archivage.

La valeur MAXSESSIONS définie pour le serveur TSM contrôle le nombre maximal de sessions qui peuvent être ouvertes sur le serveur TSM par toutes les applications clientes. La valeur de MAXSESSIONS spécifiée sur TSM doit être au moins aussi grande que la valeur spécifiée pour **ARC** > **Target** > **Configuration** > **main** > **nombre de sessions** dans le gestionnaire de grille pour le noeud d'archives. Le nœud d'archivage crée simultanément au plus une session par point de montage et un petit nombre (< 5) de sessions supplémentaires.

Le nœud TSM affecté au nœud d'archivage utilise une stratégie de domaine personnalisée `tsm-domain`. Le `tsm-domain` La politique de domaine est une version modifiée de la politique de domaine « standard », configurée pour écrire sur bande et avec la destination d'archivage définie comme pool de stockage du système StorageGRID (*`SGWSDiskPool`*).

> Vous devez vous connecter au serveur TSM avec des privilèges d'administration et utiliser l'outil dsmadmc pour créer et activer la stratégie de domaine.

Création et activation de la stratégie de domaine

Vous devez créer une stratégie de domaine, puis l'activer pour configurer le serveur TSM afin d'enregistrer les données envoyées à partir du noeud d'archivage.

Étapes

1. Créer une stratégie de domaine.

```
copy domain standard tsm-domain
```

2. Si vous n'utilisez pas de classe de gestion existante, entrez l'une des options suivantes :

   ```
   define policyset tsm-domain standard
   ```

   ```
   define mgmtclass tsm-domain standard default
   ```

   default est la classe de gestion par défaut pour le déploiement.

3. Créez un groupe de copie dans le pool de stockage approprié. Entrer (sur une ligne) :

   ```
   define copygroup tsm-domain standard default type=archive
   destination=SGWSDiskPool retinit=event retmin=0 retver=0
   ```

   default Est la classe de gestion par défaut du nœud d'archivage. Les valeurs de `retinit`, `retmin`, et `retver` Ont été choisis pour refléter le comportement de rétention actuellement utilisé par le noeud d'archivage

   > Ne pas régler `retinit` à `retinit=create`. Réglage `retinit=create` Bloque le nœud d'archivage de supprimer du contenu car les événements de rétention sont utilisés pour supprimer du contenu du serveur TSM.

4. Attribuez la classe de gestion à la valeur par défaut.

   ```
   assign defmgmtclass tsm-domain standard default
   ```

5. Définissez la nouvelle règle sur active.

   ```
   activate policyset tsm-domain standard
   ```

   Ignorez l'avertissement « aucun groupe de copie de sauvegarde » qui s'affiche lorsque vous entrez la commande Activer.

6. Enregistrez un nœud pour utiliser le nouvel ensemble de règles sur le serveur TSM. Sur le serveur TSM, entrez (sur une ligne) :

   ```
   register node arc-user arc-password passexp=0 domain=tsm-domain
   MAXNUMMP=number-of-sessions
   ```

   Arc-user et arc-mot-de-passe sont les mêmes nom de noeud client et mot de passe que ceux définis sur le noeud d'archivage, et la valeur MAXNUMMP est définie sur le nombre de lecteurs de bande réservés pour les sessions de magasin de noeud d'archivage.

   > Par défaut, l'enregistrement d'un nœud crée un ID utilisateur administratif avec l'autorité propriétaire du client, avec le mot de passe défini pour le nœud.

Migration des données vers StorageGRID

Vous pouvez migrer d'importants volumes de données vers le système StorageGRID tout en utilisant le système StorageGRID pour les opérations quotidiennes.

La section suivante est un guide pour comprendre et planifier la migration d'importants volumes de données

vers le système StorageGRID. Ce n'est pas un guide général de la migration des données et n'inclut pas des étapes détaillées pour effectuer une migration. Suivez les instructions de cette section pour assurer une migration efficace des données dans le système StorageGRID sans perturber les opérations quotidiennes et que les données migrées sont correctement gérées par le système StorageGRID.

- "Confirmation de la capacité du système StorageGRID"
- "Définition de la règle ILM pour les données migrées"
- "Impact de la migration sur les opérations"
- "Planification de la migration des données"
- "Surveillance de la migration des données"
- "Création de notifications personnalisées pour les alarmes de migration"

Confirmation de la capacité du système StorageGRID

Avant de migrer d'importants volumes de données vers le système StorageGRID, vérifiez que le système StorageGRID dispose des capacités de disque nécessaires pour gérer le volume prévu.

Si le système StorageGRID inclut un nœud d'archivage et qu'une copie d'objets migrés a été enregistrée dans le stockage nearline (par exemple une bande), assurez-vous que la capacité de stockage du nœud d'archivage est suffisante pour le volume prévu de données migrées.

Dans le cadre de l'évaluation de la capacité, examinez le profil de données des objets que vous prévoyez de migrer et calculez la capacité de disque requise. Pour plus d'informations sur la surveillance de la capacité des disques de votre système StorageGRID, reportez-vous aux instructions de contrôle et de dépannage de StorageGRID.

Informations associées

"Moniteur et amp ; dépannage"

"Gestion des nœuds de stockage"

Définition de la règle ILM pour les données migrées

La règle ILM du système StorageGRID détermine le nombre de copies effectuées, l'emplacement des copies stockées et la durée de conservation de ces copies. Une règle ILM comprend un ensemble de règles ILM décrit la procédure de filtrage des objets et de gestion des données d'objet au fil du temps.

Selon l'utilisation des données migrées et vos exigences concernant les données migrées, vous pouvez définir des règles ILM uniques pour les données migrées qui ne sont pas les règles ILM utilisées pour les opérations quotidiennes. Par exemple, si la gestion quotidienne des données implique différentes exigences réglementaires que les données incluses dans la migration, il est possible de vouloir créer un nombre différent de copies des données migrées sur un niveau de stockage différent.

Vous pouvez configurer des règles qui s'appliquent exclusivement aux données migrées si une distinction unique entre les données migrées et les données objet enregistrées au quotidien.

Si vous faites la distinction de manière fiable entre les types de données en utilisant l'un des critères de métadonnées, ce critère vous permet de définir une règle ILM qui ne s'applique qu'aux données migrées.

Avant de commencer la migration des données, veillez à bien comprendre la règle ILM du système StorageGRID et la manière dont elle s'applique aux données migrées, et à effectuer et tester toutes les modifications apportées à la règle ILM.

> Une règle ILM incorrecte peut entraîner une perte de données irrécupérable. Examinez attentivement toutes les modifications apportées à une stratégie ILM avant de l'activer pour vous assurer que celle-ci fonctionne comme prévu.

Informations associées

"Gestion des objets avec ILM"

Impact de la migration sur les opérations

Le système StorageGRID permet un fonctionnement efficace du stockage objet et de la récupération. Il offre une excellente protection contre la perte de données grâce à la création transparente de copies redondantes des données d'objet et des métadonnées.

Toutefois, la migration des données doit être gérée avec soin conformément aux instructions de ce chapitre pour éviter tout impact sur les opérations quotidiennes des systèmes ou, dans des cas extrêmes, placer les données en cas de perte en cas de défaillance du système StorageGRID.

La migration de volumes importants de données impose une charge supplémentaire au système. Lorsque le système StorageGRID est lourdement chargé, il répond plus lentement aux demandes de stockage et de récupération d'objets. Cela peut interférer avec les demandes de stockage et de récupération qui font partie intégrante des opérations quotidiennes. La migration peut également entraîner d'autres problèmes opérationnels. Par exemple, lorsqu'un nœud de stockage arrive à saturation de la capacité, la charge intermittente importante due à l'ingestion par lots peut faire basculer le nœud de stockage entre la lecture seule et la lecture-écriture, générant des notifications.

Si le chargement persiste, les files d'attente peuvent développer différentes opérations que le système StorageGRID doit exécuter pour assurer la redondance complète des données d'objet et des métadonnées.

La migration des données doit être gérée avec soin conformément aux directives présentées dans ce document afin de garantir un fonctionnement sûr et efficace du système StorageGRID pendant la migration. Lors de la migration des données, ingestion d'objets par lots ou ingestion continue. Ensuite, surveillez en continu le système StorageGRID pour vous assurer que les différentes valeurs d'attribut ne sont pas dépassées.

Planification de la migration des données

Évitez la migration des données pendant les heures de fonctionnement essentielles. Limitez la migration des données aux soirées, week-ends et autres fois que l'utilisation du système est faible.

Si possible, ne pas planifier de migration des données pendant les périodes d'activité élevée. Toutefois, s'il n'est pas pratique d'éviter complètement la période d'activité élevée, il est sûr de procéder aussi longtemps que vous surveillez attentivement les attributs pertinents et que vous prenez des mesures s'ils dépassent les valeurs acceptables.

Informations associées

"Surveillance de la migration des données"

Surveillance de la migration des données

La migration des données doit être contrôlée et ajustée selon les besoins, pour garantir le placement des données conformément à la politique ILM dans les délais impartis.

Ce tableau répertorie les attributs que vous devez contrôler lors de la migration des données, ainsi que les problèmes qu'ils représentent.

Si vous utilisez des stratégies de classification du trafic avec des limites de taux pour accélérer l'entrée, vous pouvez surveiller le taux observé en conjonction avec les statistiques décrites dans le tableau suivant et réduire les limites si nécessaire.

Superviser	Description
Nombre d'objets en attente de l'évaluation ILM	1. Sélectionnez **support** > **Outils** > **topologie de grille**. 2. Sélectionnez ***déploiement*** > **Présentation** > **main**. 3. Dans la section ILM Activity, surveillez le nombre d'objets affichés pour les attributs suivants : ◦ **Attente - tous (XQUZ)**: Le nombre total d'objets en attente d'évaluation ILM. ◦ **Attente - client (XCQZ)** : nombre total d'objets en attente d'évaluation ILM des opérations client (par exemple, transfert). 4. Si le nombre d'objets affichés pour l'un de ces attributs dépasse 100,000, réduisez la vitesse d'entrée des objets afin de réduire la charge sur le système StorageGRID.
Capacité de stockage des systèmes d'archivage ciblés	Si la règle ILM enregistre une copie des données migrées vers un système de stockage d'archives ciblé (bande ou cloud), surveillez la capacité du système de stockage d'archivage ciblé pour s'assurer que la capacité disponible est suffisante.
Archive Node > **ARC** > **Store**	Si une alarme pour l'attribut **Store Failures (ARVF)** est déclenchée, le système de stockage d'archives ciblé a peut-être atteint sa capacité. Vérifiez le système de stockage d'archives ciblé et résolvez tout problème ayant déclenché une alarme.

Création de notifications personnalisées pour les alarmes de migration

StorageGRID peut envoyer des notifications d'alerte ou des notifications d'alarme (système hérité) à l'administrateur système responsable de la surveillance de la migration si certaines valeurs dépassent les seuils recommandés.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir configuré les paramètres de messagerie pour les notifications d'alerte (ou d'alarme).

Étapes

1. Créez une règle d’alerte personnalisée ou une alarme personnalisée globale pour chaque metric Prometheus ou attribut StorageGRID que vous souhaitez surveiller pendant la migration des données.

   Les alertes sont déclenchées en fonction des valeurs de mesure Prometheus. Les alarmes sont déclenchées en fonction des valeurs d’attribut. Pour plus d’informations, reportez-vous aux instructions de surveillance et de dépannage de StorageGRID.

2. Désactivez la règle d’alerte personnalisée ou l’alarme personnalisée globale une fois la migration des données terminée.

   Notez que les alarmes personnalisées globales remplacent les alarmes par défaut.

Informations associées

"Moniteur et amp ; dépannage"