Gestion des réseaux et des connexions StorageGRID

StorageGRID 11.5

NetApp
April 11, 2024

Sommaire

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.

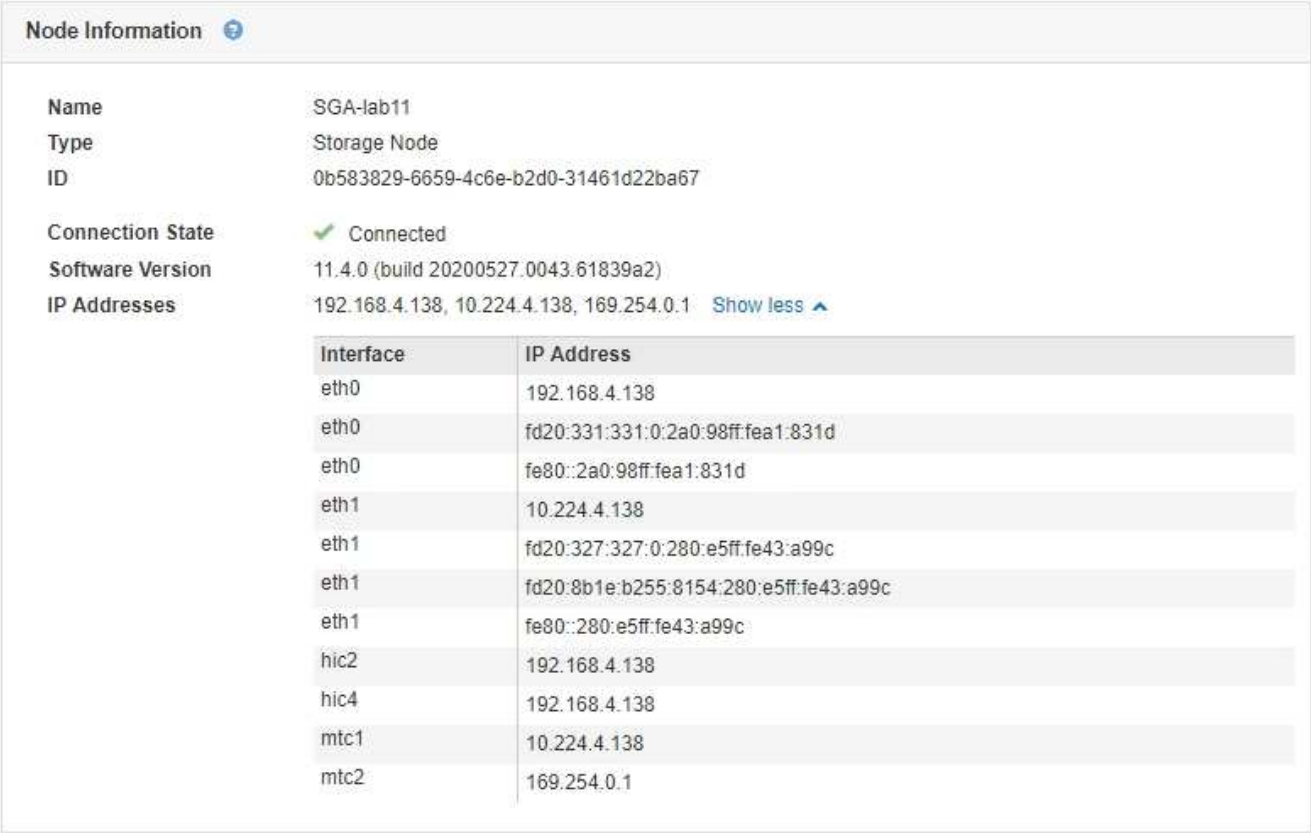
Description de la tâche

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.

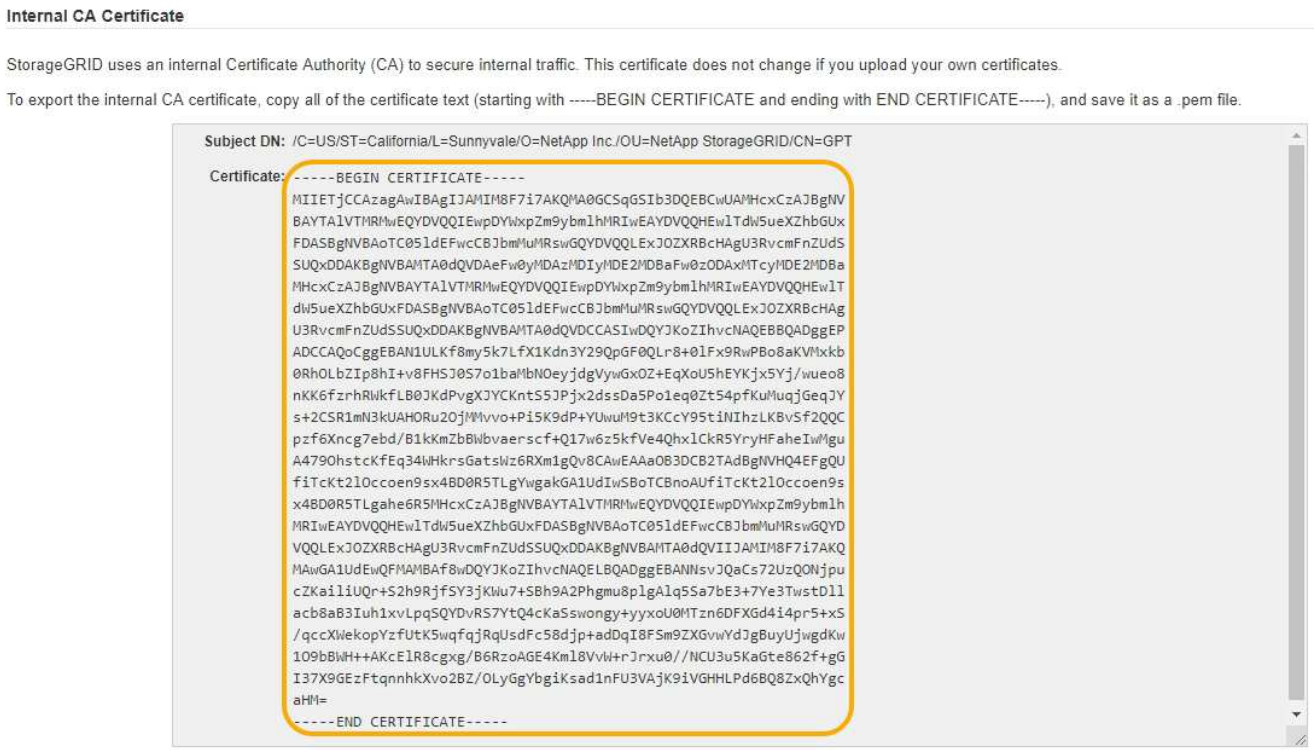
Description de la tâche

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.

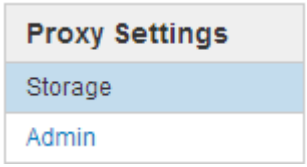
Description de la tâche

Vous pouvez configurer les paramètres d'un proxy de stockage unique.

Étapes

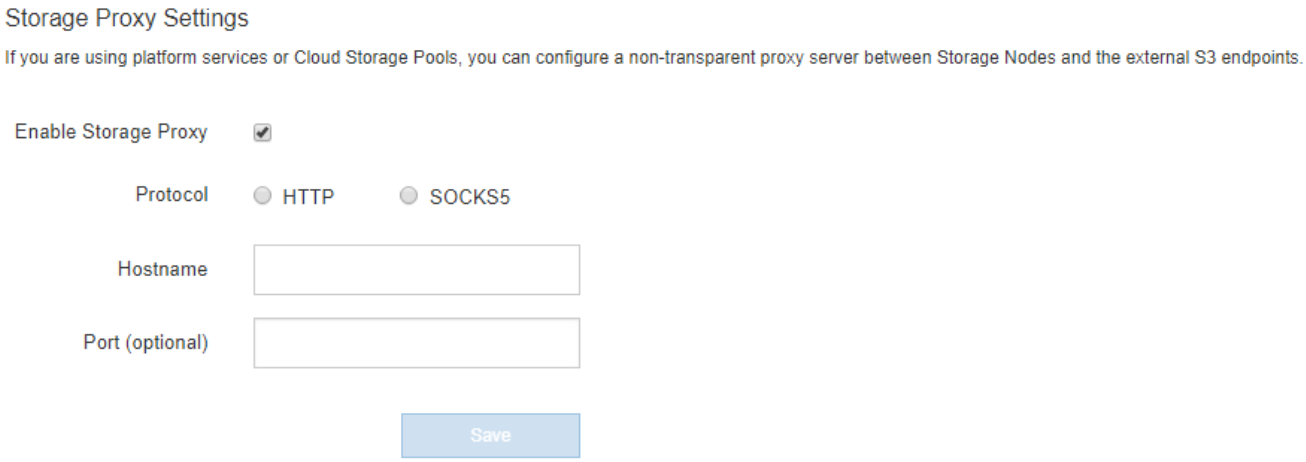
1. Sélectionnez **Configuration** > **Paramètres réseau** > **Paramètres proxy**.

   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

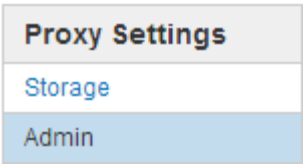
Vous pouvez configurer les paramètres d'un proxy d'administration unique.

Étapes

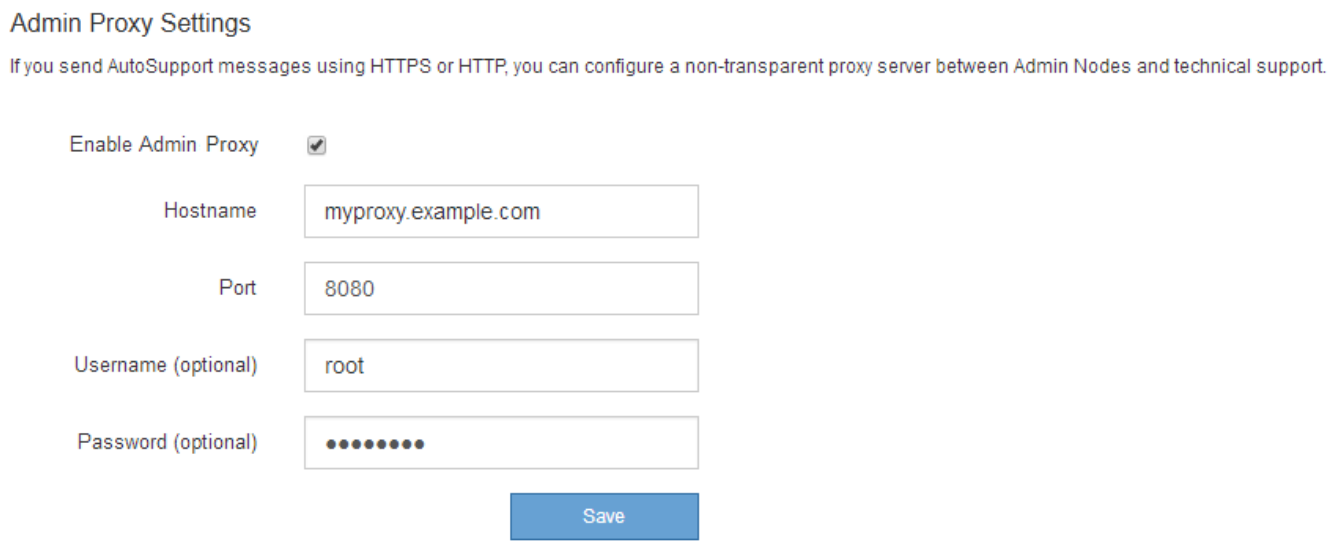
1. Sélectionnez **Configuration** > **Paramètres réseau** > **Paramètres proxy**.

   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.

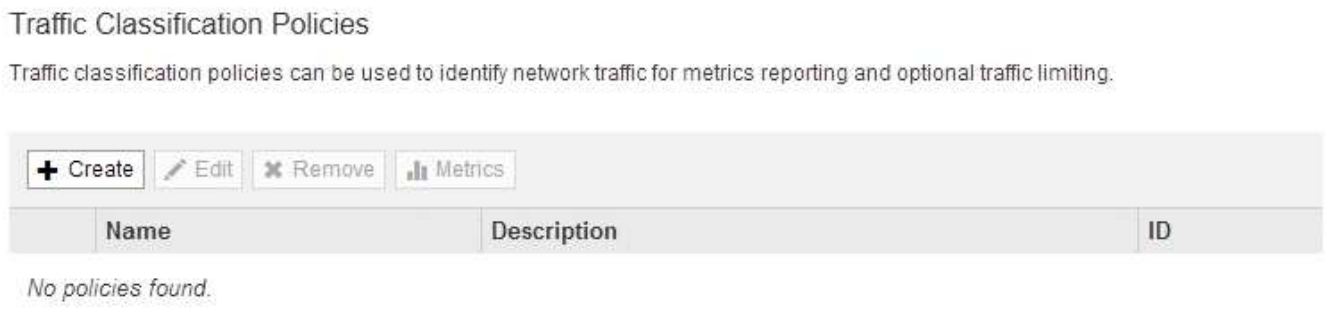
Ce dont vous avez besoin

- 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

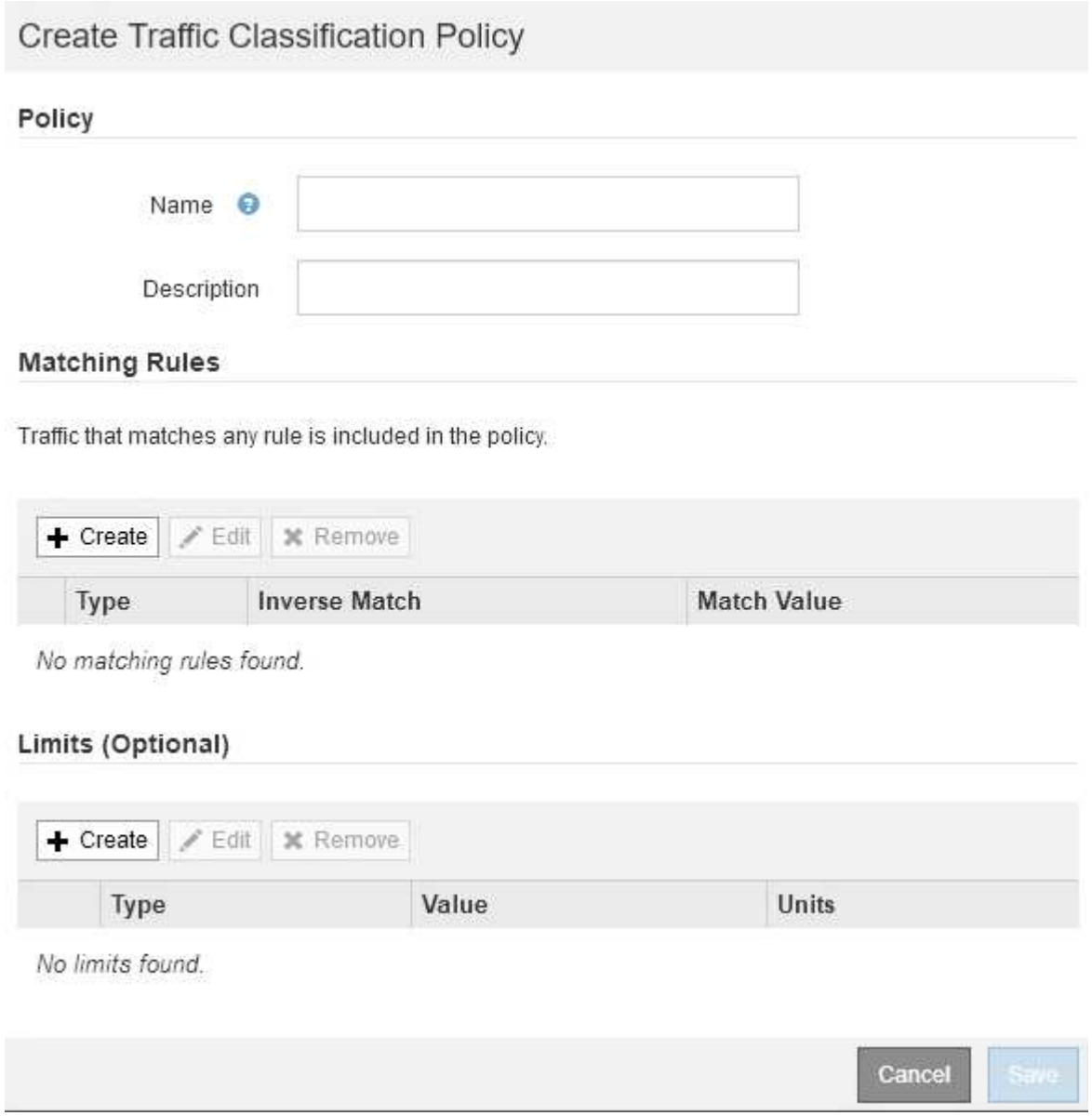
1. Sélectionnez **Configuration** > **Paramètres réseau** > **Classification du trafic**.

   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**.

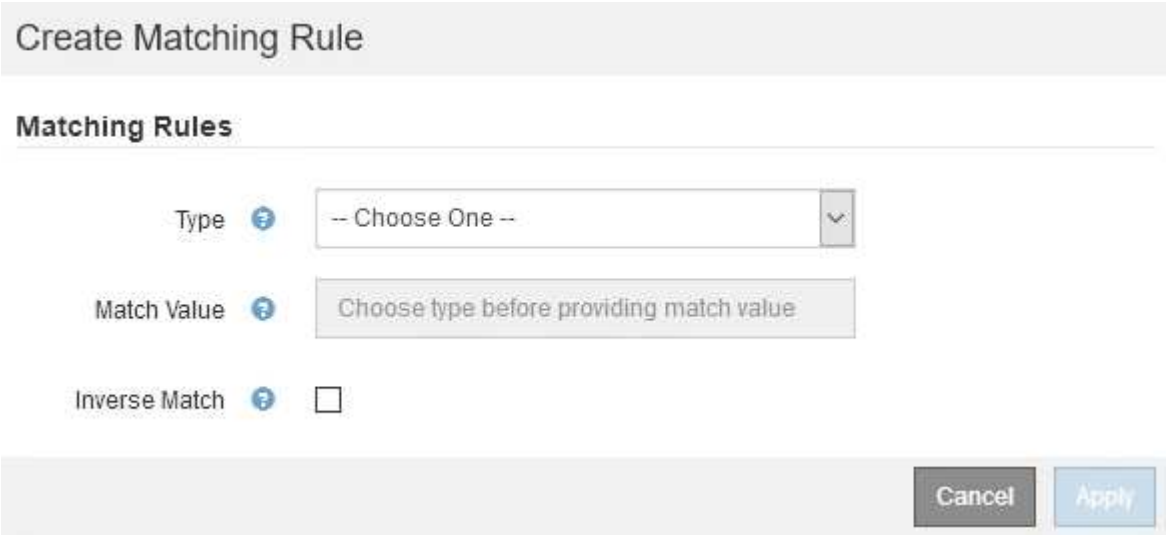
   Par exemple, décrivez à quoi s'applique cette politique de classification de trafic et à quoi elle limite.

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.

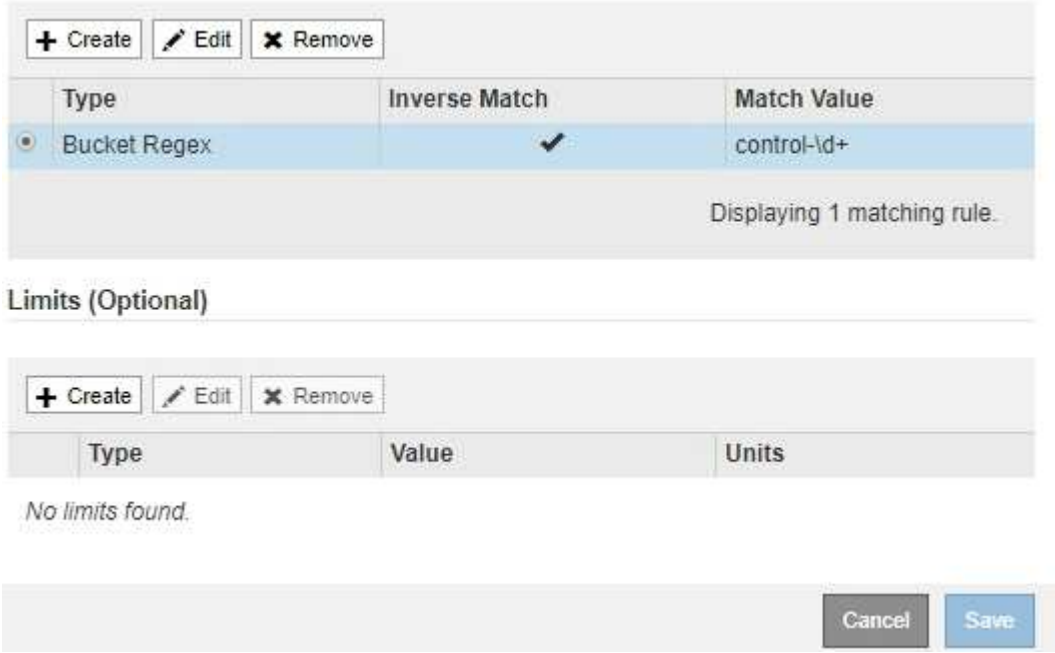
      - CIDR : saisissez un sous-réseau IPv4, en notation CIDR, qui correspond au sous-réseau souhaité.
      - Noeud final : sélectionnez un noeud final dans la liste des noeuds finaux existants. Il s'agit des noeuds finaux de l'équilibreur de charge que vous avez définis sur la page noeuds finaux de l'équilibreur 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.

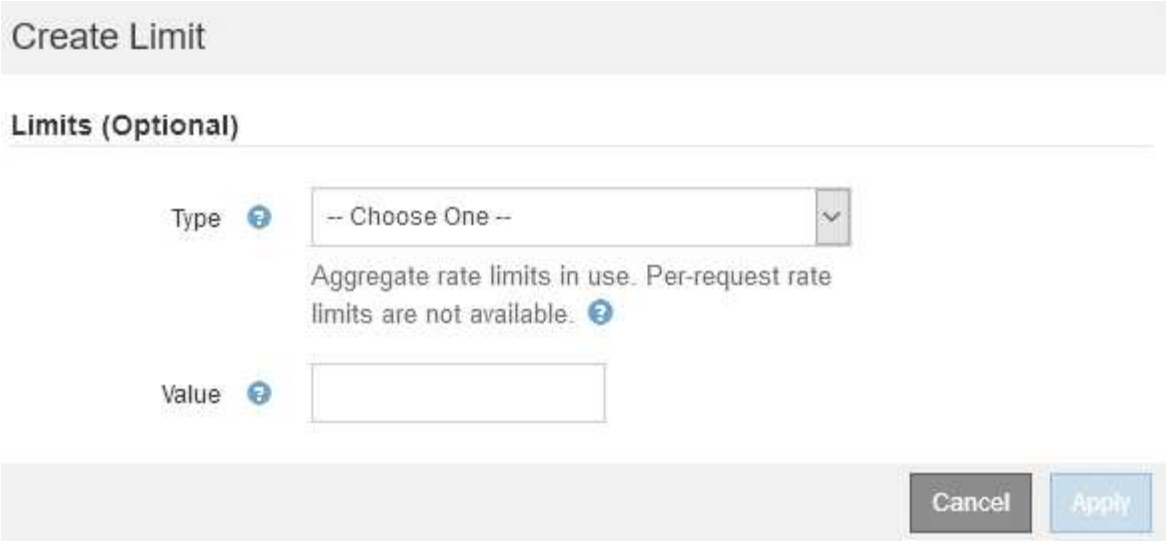
> Le trafic correspondant à n'importe quelle règle est géré par la règle.

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

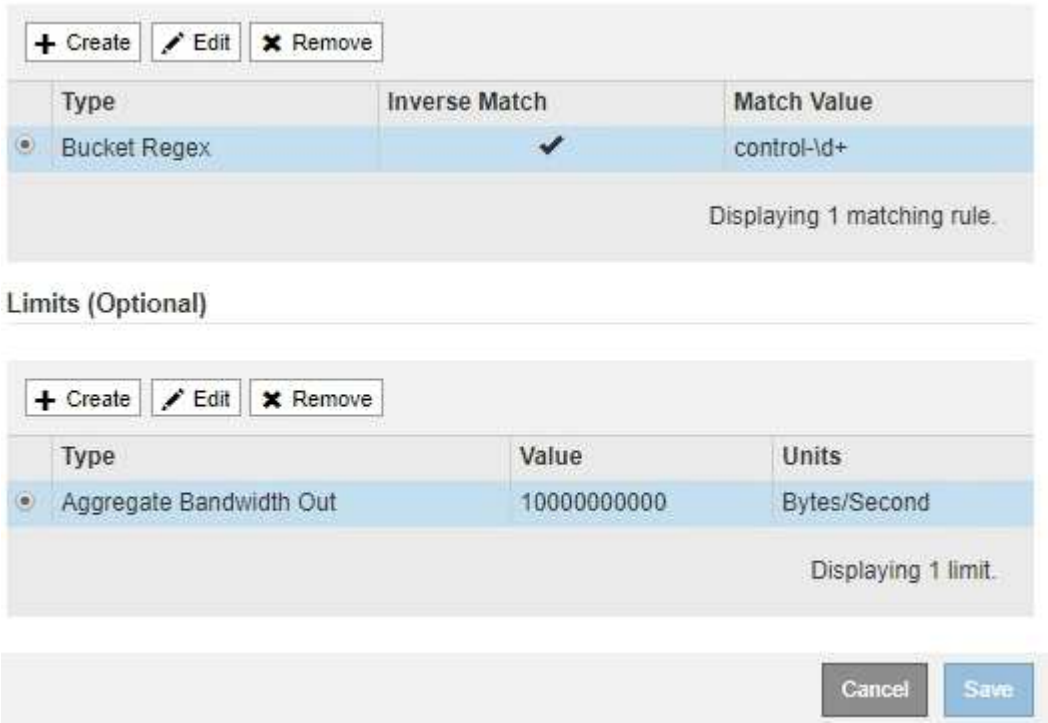
- Point final
- Correspondances CIDR non exactes (pas /32)
- Correspondances inverses

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.



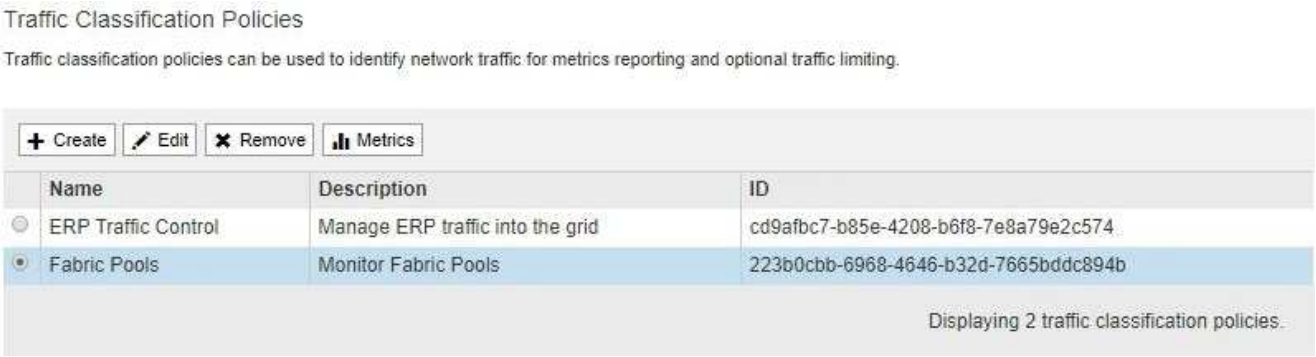
e. Répétez ces étapes pour chaque limite que vous souhaitez ajouter à la stratégie.

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.

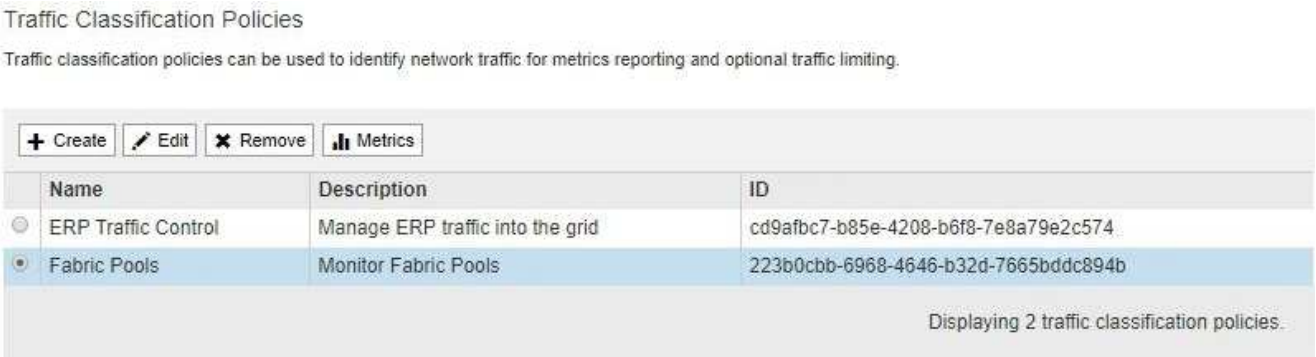
Ce dont vous avez besoin

- 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

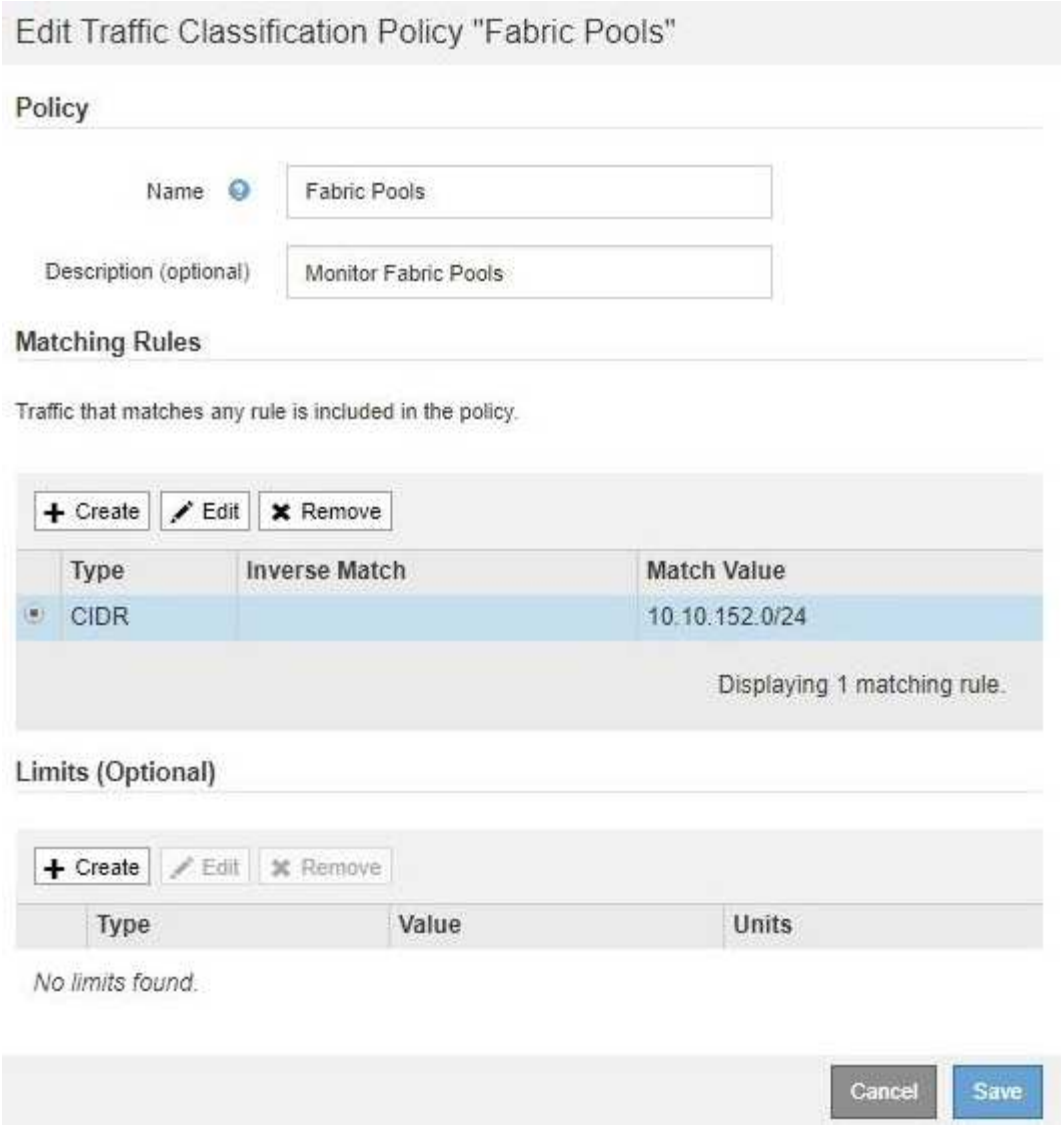
1. Sélectionnez **Configuration** > **Paramètres réseau** > **Classification du trafic**.

   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.

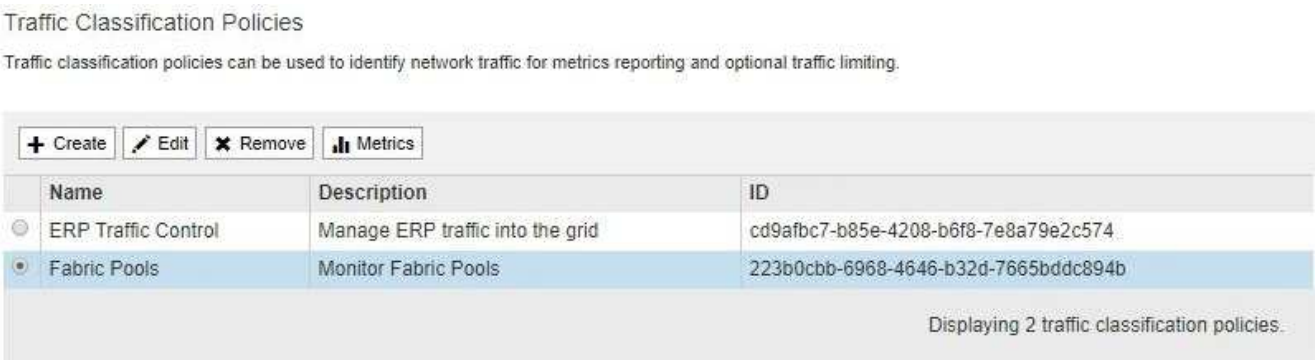
Ce dont vous avez besoin

- 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

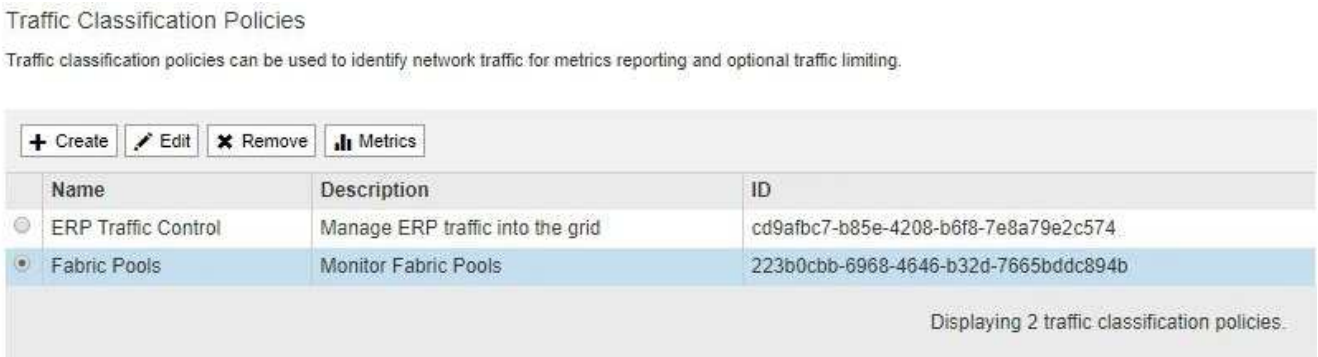
Pour toute règle de classification de trafic existante, vous pouvez afficher les mesures du service Load Balancer afin de déterminer si la stratégie limite le trafic sur le réseau. Les données des graphiques peuvent vous aider à déterminer si vous devez ajuster la stratégie.

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**.

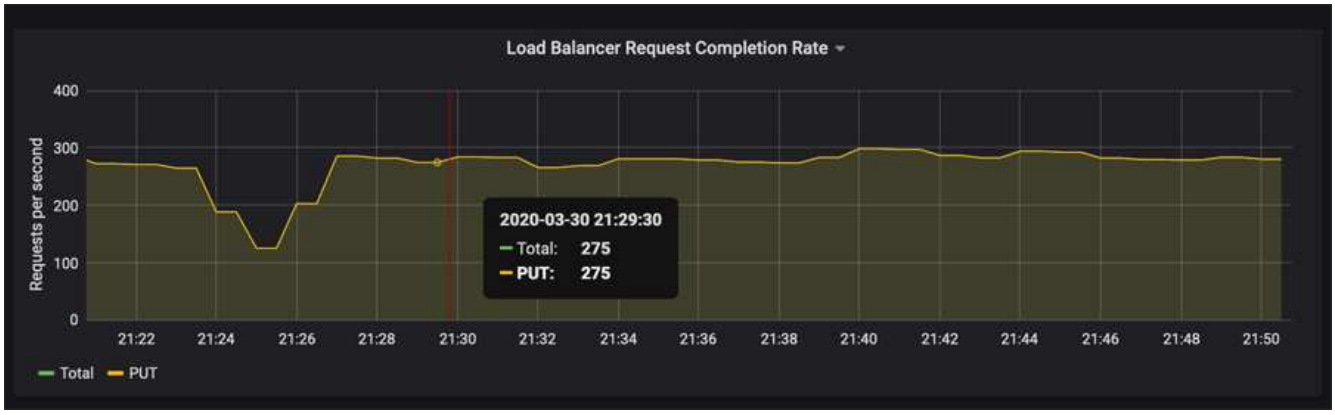
   Une nouvelle fenêtre de navigateur s'ouvre et les graphiques de la politique de classification du trafic s'affichent. Les graphiques affichent des mesures uniquement pour le trafic correspondant à la stratégie sélectionnée.

   Vous pouvez sélectionner d'autres stratégies à afficher à l'aide de la liste déroulante **policy**.

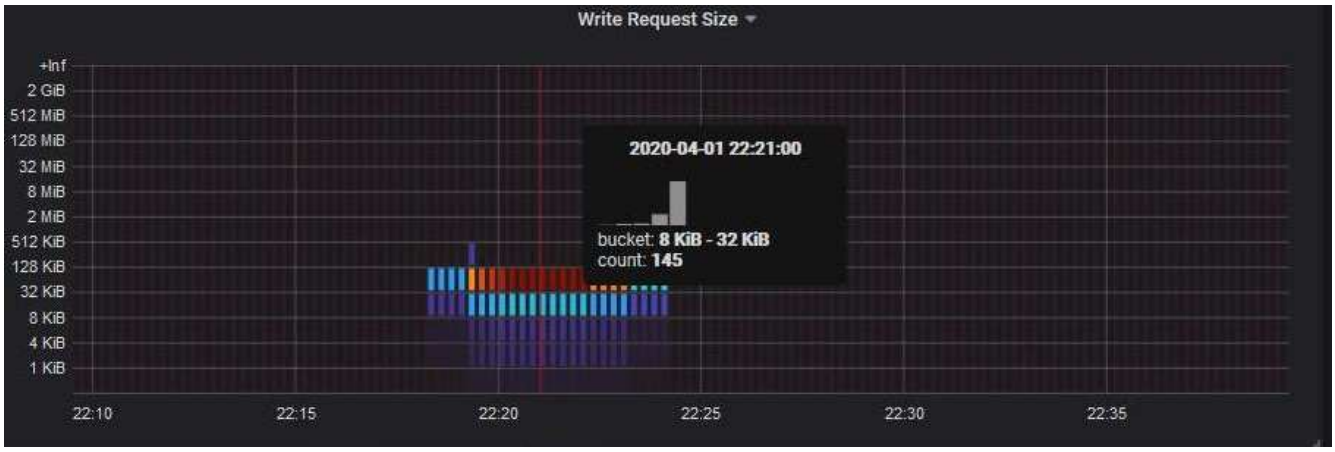
Les graphiques suivants sont inclus sur la page Web.

- 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

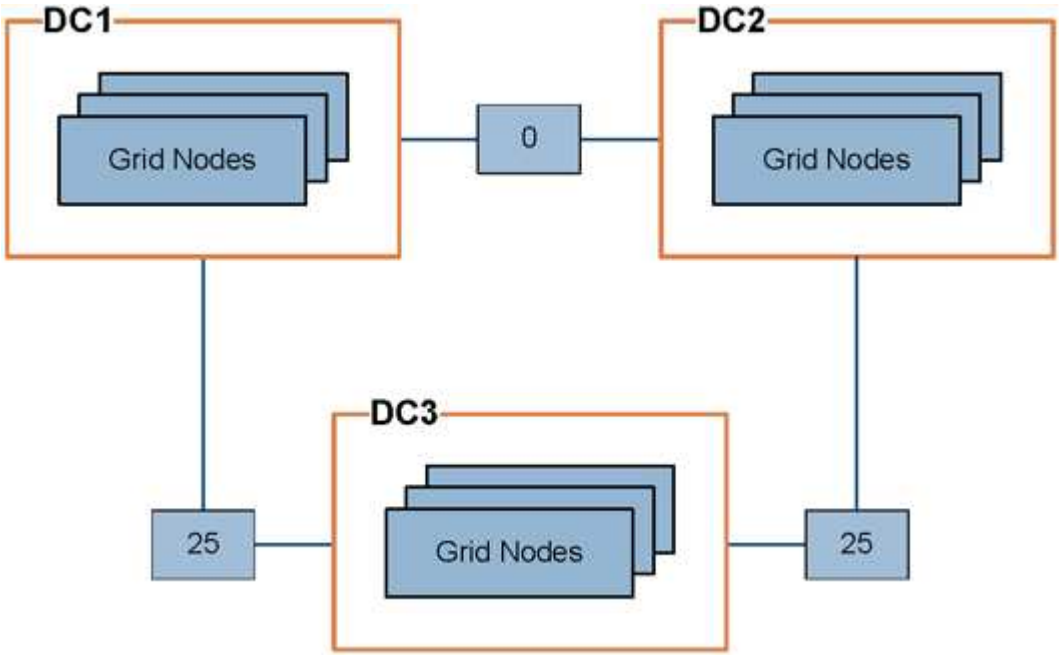
Les coûts de liaison vous permettent de définir la priorité du site de data Center qui fournit un service demandé lorsqu'au moins deux sites de data Center existent. Vous

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

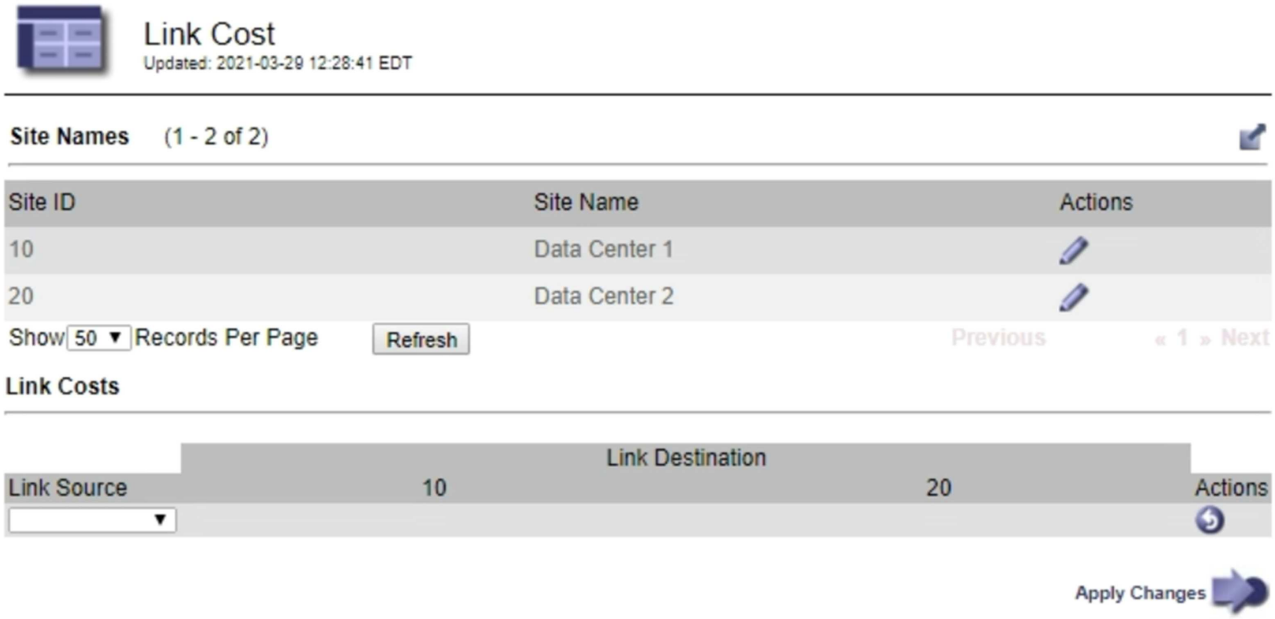
Vous pouvez mettre à jour les coûts de liaison entre les sites de data Center afin de refléter la latence entre les sites.

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**.