



Contrôle des pare-feu

StorageGRID 11.9

NetApp
November 08, 2024

Sommaire

- Contrôle des pare-feu 1
 - Contrôler l'accès au niveau du pare-feu externe 1
 - Gérer les contrôles de pare-feu internes 2
 - Configurer le pare-feu interne 4

Contrôle des pare-feu

Contrôler l'accès au niveau du pare-feu externe

Vous pouvez ouvrir ou fermer des ports spécifiques au niveau du pare-feu externe.

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

Si vous souhaitez configurer le pare-feu interne StorageGRID, reportez-vous à la section "[Configurer le pare-feu interne](#)".

| Port | Description | Si le port est ouvert... |
|------|---|---|
| 443 | Port HTTPS par défaut pour les nœuds d'administration | Les navigateurs Web et les clients d'API de gestion peuvent accéder à Grid Manager, à l'API de gestion du grid, au gestionnaire des locataires et à l'API de gestion des locataires. Remarque : le port 443 est également utilisé pour un trafic interne. |
| 8443 | Port restreint de Grid Manager sur les nœuds d'administration | <ul style="list-style-type: none">• 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 | <ul style="list-style-type: none">• Les navigateurs Web et les clients d'API de gestion peuvent accéder au Gestionnaire de locataires et à l'API de gestion des locataires via HTTPS.• Les navigateurs Web et les clients API de gestion ne peuvent pas accéder à Grid Manager ou à l'API Grid Management.• Les demandes de contenu interne seront rejetées. |



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

Informations associées

- ["Connectez-vous au Grid Manager"](#)
- ["Créer un compte de locataire"](#)
- ["Communications externes"](#)

Gérer les contrôles de pare-feu internes

StorageGRID comprend un pare-feu interne sur chaque nœud qui améliore la sécurité de votre grille en vous permettant de contrôler l'accès réseau au nœud. Utilisez le pare-feu pour empêcher l'accès au réseau sur tous les ports, à l'exception de ceux nécessaires à votre déploiement de grille spécifique. Les modifications de configuration effectuées sur la page de contrôle du pare-feu sont déployées sur chaque nœud.

Utilisez les trois onglets de la page de contrôle du pare-feu pour personnaliser l'accès dont vous avez besoin pour votre grille.

- **Liste d'adresses privilégiées** : utilisez cet onglet pour autoriser l'accès sélectionné aux ports fermés. Vous pouvez ajouter des adresses IP ou des sous-réseaux en notation CIDR qui peuvent accéder aux ports fermés à l'aide de l'onglet gérer l'accès externe.
- **Gérer l'accès externe** : utilisez cet onglet pour fermer les ports ouverts par défaut ou rouvrir les ports précédemment fermés.
- **Réseau client non approuvé** : utilisez cet onglet pour indiquer si un nœud approuve le trafic entrant provenant du réseau client.

Les paramètres de cet onglet remplacent les paramètres de l'onglet gérer l'accès externe.

- Un nœud avec un réseau client non approuvé accepte uniquement les connexions sur les ports de point final de l'équilibreur de charge configurés sur ce nœud (points finaux globaux, liés à l'interface de nœud et au type de nœud).
- Les ports de point final de l'équilibreur de charge sont les seuls ports ouverts_ sur les réseaux clients non approuvés, quels que soient les paramètres de l'onglet gérer les réseaux externes.
- Une fois approuvés, tous les ports ouverts sous l'onglet gérer l'accès externe sont accessibles, ainsi que tous les noeuds finaux d'équilibrage de charge ouverts sur le réseau client.



Les paramètres que vous effectuez sur un onglet peuvent affecter les modifications d'accès que vous effectuez sur un autre onglet. Vérifiez les paramètres de tous les onglets pour vous assurer que votre réseau se comporte comme vous le souhaitez.

Pour configurer les contrôles de pare-feu internes, reportez-vous à la section ["Configurer les contrôles de pare-feu"](#).

Pour plus d'informations sur les pare-feu externes et la sécurité réseau, reportez-vous à la section ["Contrôler l'accès au niveau du pare-feu externe"](#).

Liste d'adresses privilégiées et onglets gérer les accès externes

L'onglet liste d'adresses privilégiées vous permet d'enregistrer une ou plusieurs adresses IP qui ont accès aux ports de la grille fermés. L'onglet gérer l'accès externe vous permet de fermer l'accès externe aux ports externes sélectionnés ou à tous les ports externes ouverts (les ports externes sont des ports accessibles par défaut par les nœuds non-grid). Ces deux onglets peuvent souvent être utilisés ensemble pour personnaliser

l'accès réseau exact dont vous avez besoin pour votre grille.



Par défaut, les adresses IP privilégiées n'ont pas d'accès au port de la grille interne.

Exemple 1 : utilisez un hôte de secours pour les tâches de maintenance

Supposons que vous souhaitiez utiliser un hôte de secours (un hôte renforcé par la sécurité) pour l'administration du réseau. Vous pouvez utiliser les étapes générales suivantes :

1. Utilisez l'onglet liste d'adresses privilégiées pour ajouter l'adresse IP de l'hôte de saut.
2. Utilisez l'onglet gérer l'accès externe pour bloquer tous les ports.



Ajoutez l'adresse IP privilégiée avant de bloquer les ports 443 et 8443. Tous les utilisateurs actuellement connectés sur un port bloqué, y compris vous, perdront l'accès à Grid Manager à moins que leur adresse IP n'ait été ajoutée à la liste d'adresses privilégiées.

Après avoir enregistré votre configuration, tous les ports externes du nœud d'administration de votre grille seront bloqués pour tous les hôtes, à l'exception de l'hôte de saut. Vous pouvez ensuite utiliser l'hôte de secours pour effectuer des tâches de maintenance sur votre grille de manière plus sécurisée.

Exemple 2 : verrouiller les ports sensibles

Supposons que vous souhaitez verrouiller les ports sensibles et le service sur ce port (par exemple, SSH sur le port 22). Vous pouvez utiliser les étapes générales suivantes :

1. Utilisez l'onglet liste d'adresses privilégiées pour accorder l'accès uniquement aux hôtes qui ont besoin d'accéder au service.
2. Utilisez l'onglet gérer l'accès externe pour bloquer tous les ports.



Ajoutez l'adresse IP privilégiée avant de bloquer l'accès aux ports affectés à Grid Manager et au gestionnaire de locataires (les ports prédéfinis sont 443 et 8443). Tous les utilisateurs actuellement connectés sur un port bloqué, y compris vous, perdront l'accès à Grid Manager à moins que leur adresse IP n'ait été ajoutée à la liste d'adresses privilégiées.

Après avoir enregistré votre configuration, le port 22 et le service SSH seront disponibles pour les hôtes de la liste d'adresses privilégiées. Tous les autres hôtes se verront refuser l'accès au service, quelle que soit l'interface d'origine de la demande.

Exemple 3 : désactiver l'accès aux services inutilisés

Au niveau du réseau, vous pouvez désactiver certains services que vous n'avez pas l'intention d'utiliser. Par exemple, pour bloquer le trafic client HTTP S3, vous pouvez utiliser la bascule de l'onglet gérer l'accès externe pour bloquer le port 18084.

Onglet réseaux de clients non approuvés

Si vous utilisez un réseau client, vous pouvez protéger StorageGRID des attaques hostiles en acceptant le trafic client entrant uniquement sur les nœuds finaux configurés explicitement.

Par défaut, le réseau client sur chaque nœud de la grille est *Trusted*. C'est-à-dire, par défaut, StorageGRID approuve les connexions entrantes à chaque nœud de grille sur tous "ports externes disponibles".

Vous pouvez réduire la menace d'attaques hostiles sur votre système StorageGRID en spécifiant que le réseau client sur chaque nœud est *non fiable*. Si le réseau client d'un nœud n'est pas fiable, le nœud accepte uniquement les connexions entrantes sur les ports explicitement configurés en tant que points finaux d'équilibreur de charge. Voir "[Configurer les terminaux de l'équilibreur de charge](#)" et "[Configurer les contrôles de pare-feu](#)".

Exemple 1 : le nœud de passerelle n'accepte que les requêtes HTTPS S3

Supposons que vous souhaitiez qu'un nœud de passerelle refuse tout trafic entrant sur le réseau client, à l'exception des requêtes HTTPS S3. Vous devez effectuer les étapes générales suivantes :

1. À partir de la "[Terminaux d'équilibrage de charge](#)" page, configurez un terminal d'équilibreur de charge pour S3 sur HTTPS sur le port 443.
2. Sur la page de contrôle du pare-feu, sélectionnez non approuvé pour indiquer que le réseau client sur le nœud passerelle n'est pas fiable.

Après avoir enregistré votre configuration, tout le trafic entrant sur le réseau client du nœud passerelle est supprimé, sauf pour les requêtes HTTPS S3 sur le port 443 et les requêtes ICMP Echo (ping).

Exemple 2 : le nœud de stockage envoie des demandes de services de plateforme S3

Supposons que vous souhaitiez activer le trafic sortant des services de la plateforme S3 à partir d'un nœud de stockage, mais que vous souhaitiez empêcher toute connexion entrante à ce nœud de stockage sur le réseau client. Vous devez effectuer cette étape générale :

- Dans l'onglet réseaux de clients non approuvés de la page de contrôle du pare-feu, indiquez que le réseau client sur le nœud de stockage n'est pas fiable.

Une fois la configuration enregistrée, le nœud de stockage n'accepte plus le trafic entrant sur le réseau client, mais continue à autoriser les requêtes sortantes vers les destinations de services de plate-forme configurées.

Exemple 3 : limitation de l'accès à Grid Manager à un sous-réseau

Supposons que vous souhaitiez autoriser l'accès à Grid Manager uniquement sur un sous-réseau spécifique. Procédez comme suit :

1. Connectez le réseau client de vos nœuds d'administration au sous-réseau.
2. Utilisez l'onglet réseau client non approuvé pour configurer le réseau client comme non fiable.
3. Lorsque vous créez un nœud final d'équilibreur de charge dans l'interface de gestion, entrez le port et sélectionnez l'interface de gestion à laquelle le port accèrera.
4. Sélectionnez **Oui** pour réseau client non sécurisé.
5. Utilisez l'onglet gérer l'accès externe pour bloquer tous les ports externes (avec ou sans adresses IP privilégiées définies pour les hôtes situés en dehors de ce sous-réseau).

Après avoir enregistré votre configuration, seuls les hôtes du sous-réseau que vous avez spécifié peuvent accéder à Grid Manager. Tous les autres hôtes sont bloqués.

Configurer le pare-feu interne

Vous pouvez configurer le pare-feu StorageGRID pour contrôler l'accès réseau à des ports spécifiques sur vos nœuds StorageGRID.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un ["navigateur web pris en charge"](#).
- Vous avez ["autorisations d'accès spécifiques"](#).
- Vous avez examiné les informations dans ["Gérer les contrôles de pare-feu"](#) et ["Instructions de mise en réseau"](#).
- Si vous souhaitez qu'un nœud d'administration ou un nœud de passerelle accepte le trafic entrant uniquement sur des nœuds finaux configurés explicitement, vous avez défini les nœuds finaux de l'équilibreur de charge.



Lors de la modification de la configuration du réseau client, les connexions client existantes peuvent échouer si les nœuds finaux de l'équilibreur de charge n'ont pas été configurés.

Description de la tâche

StorageGRID comprend un pare-feu interne sur chaque nœud qui vous permet d'ouvrir ou de fermer certains ports sur les nœuds de votre grille. Vous pouvez utiliser les onglets de contrôle du pare-feu pour ouvrir ou fermer des ports ouverts par défaut sur le réseau Grid, le réseau Admin et le réseau client. Vous pouvez également créer une liste d'adresses IP privilégiées pouvant accéder aux ports de la grille fermés. Si vous utilisez un réseau client, vous pouvez spécifier si un nœud approuve le trafic entrant à partir du réseau client et configurer l'accès à des ports spécifiques sur le réseau client.

Limiter le nombre de ports ouverts aux adresses IP en dehors de votre grille à ceux qui sont absolument nécessaires améliore la sécurité de votre grille. Vous utilisez les paramètres de chacun des trois onglets de contrôle du pare-feu pour vous assurer que seuls les ports nécessaires sont ouverts.

Pour plus d'informations sur l'utilisation des contrôles de pare-feu, notamment des exemples, reportez-vous à la section ["Gérer les contrôles de pare-feu"](#).

Pour plus d'informations sur les pare-feu externes et la sécurité réseau, reportez-vous à la section ["Contrôler l'accès au niveau du pare-feu externe"](#).

Accès aux contrôles de pare-feu

Étapes

1. Sélectionnez **CONFIGURATION > sécurité > contrôle du pare-feu**.

Les trois onglets de cette page sont décrits dans ["Gérer les contrôles de pare-feu"](#).

2. Sélectionnez n'importe quel onglet pour configurer les contrôles du pare-feu.

Vous pouvez utiliser ces onglets dans n'importe quel ordre. Les configurations que vous définissez sur un onglet ne limitent pas ce que vous pouvez faire sur les autres onglets. Cependant, les modifications de configuration effectuées sur un onglet peuvent modifier le comportement des ports configurés sur d'autres onglets.

Liste d'adresses privilégiées

Vous utilisez l'onglet liste d'adresses privilégiées pour accorder aux hôtes l'accès aux ports fermés par défaut ou fermés par des paramètres de l'onglet gérer l'accès externe.

Par défaut, les adresses IP privilégiées et les sous-réseaux ne disposent pas d'un accès au grid interne. En outre, les nœuds finaux d'équilibrage de charge et les ports supplémentaires ouverts dans l'onglet liste

d'adresses privilégiées sont accessibles même si bloqués dans l'onglet gérer l'accès externe.



Les paramètres de l'onglet liste d'adresses privilégiées ne peuvent pas remplacer les paramètres de l'onglet réseau client non approuvé.

Étapes

1. Dans l'onglet liste d'adresses privilégiées, entrez l'adresse ou le sous-réseau IP que vous souhaitez accorder à l'accès aux ports fermés.
2. Si vous le souhaitez, sélectionnez **Ajouter une autre adresse IP ou un autre sous-réseau en notation CIDR** pour ajouter des clients privilégiés supplémentaires.



Ajoutez autant d'adresses que possible à la liste privilégiée.

3. Vous pouvez également sélectionner **Autoriser les adresses IP privilégiées à accéder aux ports internes StorageGRID**. Voir "[Ports internes StorageGRID](#)".



Cette option supprime certaines protections pour les services internes. Laissez-le désactivé si possible.

4. Sélectionnez **Enregistrer**.

Gérer l'accès externe

Lorsqu'un port est fermé dans l'onglet gérer l'accès externe, il est impossible d'accéder au port par une adresse IP non grille à moins que vous n'ajoutiez l'adresse IP à la liste d'adresses privilégiées. Vous ne pouvez fermer que les ports ouverts par défaut et vous ne pouvez ouvrir que les ports que vous avez fermés.



Les paramètres de l'onglet gérer l'accès externe ne peuvent pas remplacer les paramètres de l'onglet réseau client non approuvé. Par exemple, si un nœud n'est pas approuvé, le port SSH/22 est bloqué sur le réseau client même s'il est ouvert dans l'onglet gérer l'accès externe. Les paramètres de l'onglet réseau client non approuvé remplacent les ports fermés (tels que 443, 8443, 9443) sur le réseau client.

Étapes

1. Sélectionnez **gérer l'accès externe**. L'onglet affiche un tableau contenant tous les ports externes (ports accessibles par défaut par les nœuds non GRID) pour les nœuds de votre grille.
2. Configurez les ports que vous souhaitez ouvrir et fermer à l'aide des options suivantes :
 - Utilisez la bascule située en regard de chaque port pour ouvrir ou fermer le port sélectionné.
 - Sélectionnez **Ouvrir tous les ports affichés** pour ouvrir tous les ports répertoriés dans le tableau.
 - Sélectionnez **Fermer tous les ports affichés** pour fermer tous les ports répertoriés dans le tableau.



Si vous fermez les ports Grid Manager 443 ou 8443, tous les utilisateurs actuellement connectés sur un port bloqué, y compris vous, perdront l'accès à Grid Manager, sauf si leur adresse IP a été ajoutée à la liste d'adresses privilégiées.



Utilisez la barre de défilement située à droite du tableau pour vous assurer que vous avez affiché tous les ports disponibles. Utilisez le champ de recherche pour trouver les paramètres de n'importe quel port externe en entrant un numéro de port. Vous pouvez entrer un numéro de port partiel. Par exemple, si vous entrez un **2**, tous les ports dont le nom contient la chaîne "2" s'affichent.

3. Sélectionnez **Enregistrer**

Réseau client non fiable

Si le réseau client d'un nœud n'est pas approuvé, le nœud accepte uniquement le trafic entrant sur les ports configurés comme points finaux de l'équilibreur de charge et, éventuellement, les ports supplémentaires que vous sélectionnez dans cet onglet. Vous pouvez également utiliser cet onglet pour spécifier le paramètre par défaut pour les nouveaux nœuds ajoutés dans une extension.



Les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.

Les modifications de configuration effectuées dans l'onglet **réseau client non approuvé** remplacent les paramètres de l'onglet **gérer l'accès externe**.

Étapes

1. Sélectionnez **réseau client non approuvé**.
2. Dans la section définir les nouveaux nœuds par défaut, spécifiez le paramètre par défaut lorsque de nouveaux nœuds sont ajoutés à la grille dans une procédure d'extension.
 - **Approuvé** (par défaut) : lorsqu'un nœud est ajouté dans une extension, son réseau client est approuvé.
 - **Non fiable** : lorsqu'un nœud est ajouté dans une extension, son réseau client n'est pas fiable.

Si nécessaire, vous pouvez revenir à cet onglet pour modifier le paramètre d'un nouveau nœud spécifique.



Ce paramètre n'affecte pas les nœuds existants du système StorageGRID.

3. Utilisez les options suivantes pour sélectionner les nœuds qui doivent autoriser les connexions client uniquement sur les terminaux d'équilibrage de charge configurés explicitement ou sur les ports sélectionnés supplémentaires :
 - Sélectionnez **ne pas faire confiance aux nœuds affichés** pour ajouter tous les nœuds affichés dans le tableau à la liste réseau client non approuvé.
 - Sélectionnez **confiance sur les nœuds affichés** pour supprimer tous les nœuds affichés dans le tableau de la liste réseau client non approuvé.
 - Utilisez la bascule en regard de chaque nœud pour définir le réseau client comme approuvé ou non fiable pour le nœud sélectionné.

Par exemple, vous pouvez sélectionner **ne plus faire confiance aux nœuds affichés** pour ajouter tous les nœuds à la liste réseau client non approuvé, puis utiliser la bascule à côté d'un nœud individuel pour ajouter ce nœud à la liste réseau client approuvé.



Utilisez la barre de défilement située à droite du tableau pour vous assurer que vous avez affiché tous les nœuds disponibles. Utilisez le champ de recherche pour rechercher les paramètres d'un nœud en saisissant son nom. Vous pouvez entrer un nom partiel. Par exemple, si vous entrez un **GW**, tous les nœuds qui ont la chaîne "GW" comme partie de leur nom sont affichés.

4. Sélectionnez **Enregistrer**.

Les nouveaux paramètres de pare-feu sont immédiatement appliqués et appliqués. Les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.