Contrôlez les pare-feu

StorageGRID software

NetApp
July 23, 2026

Sommaire

Contrôlez les pare-feu

Contrôlez l'accès à StorageGRID à un pare-feu externe

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

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

Si vous souhaitez configurer le pare-feu interne de StorageGRID, consultez "Configurer le pare-feu interne".

Port	Description	Si le port est ouvert…
443	Port HTTPS par défaut pour les nœuds d'administration	Les navigateurs Web et les clients API de gestion peuvent accéder au Grid Manager, à l'API de gestion du Grid, au Tenant Manager et à l'API de gestion du Tenant. **Remarque :** Le port 443 est également utilisé pour une partie du trafic interne.
8443	Port restreint du Grid Manager sur les nœuds d'administration	• Les navigateurs Web et les clients API de gestion peuvent accéder au Grid Manager et à l'API de gestion du Grid à l'aide de HTTPS. • Les navigateurs Web et les clients API de gestion ne peuvent pas accéder au Tenant Manager ni à l'API de gestion des locataires. • Les demandes de contenu interne seront rejetées.
9443	Port restreint du gestionnaire de locataires sur les nœuds d'administration	• Les navigateurs Web et les clients API de gestion peuvent accéder au Tenant Manager et à l'API de gestion des locataires via HTTPS. • Les navigateurs Web et les clients de l'API de gestion ne peuvent pas accéder au Grid Manager ni à l'API de gestion du Grid. • Les demandes de contenu interne seront rejetées.

L'authentification unique (SSO) n'est pas disponible sur les ports restreints de Grid Manager ou de Tenant Manager. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec l'authentification unique.

Informations connexes

- "Connectez-vous au Grid Manager"
- "Créer un compte locataire"

- "Communications externes"

Gérez les contrôles de pare-feu internes dans StorageGRID

StorageGRID intègre un pare-feu interne sur chaque nœud, renforçant ainsi la sécurité de votre grid en vous permettant de contrôler l'accès réseau au nœud. Utilisez le pare-feu pour empêcher l'accès réseau sur tous les ports, sauf ceux nécessaires au déploiement spécifique de votre grid. Les modifications de configuration que vous effectuez sur la page de contrôle du pare-feu sont déployées sur chaque nœud.

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

- **Liste d'adresses privilégiées** : utilisez cet onglet pour autoriser l'accès à des ports fermés sélectionnés. Vous pouvez ajouter des adresses IP ou des sous-réseaux au format CIDR qui peuvent accéder aux ports fermés à l'aide de l'onglet Gérer l'accès externe.
- **Gérer l'accès externe** : Utilisez cet onglet pour fermer les ports ouverts par défaut ou rouvrir les ports précédemment fermés.
- **Réseau client non approuvé** : Utilisez cet onglet pour spécifier si un nœud fait confiance au trafic entrant provenant du réseau client.

  Les paramètres de cet onglet prévalent sur ceux de l'onglet Gérer l'accès externe.

  - Un nœud doté d'un Client Network non fiable n'acceptera que les connexions sur les ports de point de terminaison de l'équilibreur de charge configurés sur ce nœud (points de terminaison globaux, d'interface de nœud et liés au type de nœud).
  - Les ports des points de terminaison de l'équilibreur de charge *sont les seuls ports ouverts* sur les réseaux clients non approuvés, quels que soient les paramètres de l'onglet Manage external networks.
  - Une fois approuvés, tous les ports ouverts sous l'onglet Gérer l'accès externe sont accessibles, ainsi que tous les points de terminaison d'équilibrage de charge ouverts sur le réseau client.

> Les paramètres que vous définissez dans un onglet peuvent affecter les modifications d'accès que vous effectuez dans un autre onglet. Assurez-vous de vérifier les paramètres de tous les onglets pour que votre réseau se comporte comme vous l'attendez.

Pour configurer les contrôles du pare-feu interne, consultez "Configurer les contrôles du pare-feu".

Pour plus d'informations sur les pare-feu externes et la sécurité réseau, consultez "Contrôler l'accès au niveau du pare-feu externe".

Onglets Liste d'adresses privilégiées et Gérer l'accès externe

L'onglet « Liste des adresses privilégiées » vous permet d'enregistrer une ou plusieurs adresses IP autorisées à accéder à des ports de la grille fermés. L'onglet « Gérer l'accès externe » vous permet de fermer l'accès externe à certains ports externes ou à tous les ports externes ouverts (les ports externes sont des ports accessibles par défaut aux nœuds non-grille). Ces deux onglets peuvent souvent être utilisés conjointement pour personnaliser précisément l'accès réseau dont vous avez besoin pour votre grille.

> Les adresses IP privilégiées n'ont pas accès par défaut aux ports internes de la grille.

Exemple 1 : Utilisez un serveur de rebond pour les tâches de maintenance

Supposons que vous souhaitiez utiliser un serveur de rebond (un hôte sécurisé) pour l'administration du réseau. Vous pouvez suivre les étapes générales suivantes :

1. Utilisez l'onglet Liste des adresses privilégiées pour ajouter l'adresse IP de l'hôte de rebond.
2. Utilisez l'onglet Gérer l'accès externe pour bloquer tous les ports.

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

Une fois votre configuration enregistrée, tous les ports externes du nœud d'administration de votre grille seront bloqués pour tous les hôtes, à l'exception du jump host. Vous pouvez alors utiliser le jump host pour effectuer des tâches de maintenance sur votre grille de manière plus sécurisée.

Exemple 2 : Verrouillez les ports sensibles

Supposons que vous souhaitiez verrouiller les ports sensibles et le service sur ce port. Vous pouvez suivre les étapes générales suivantes :

1. Utilisez l'onglet Liste d'adresses privilégiées pour n'accorder l'accès qu'aux hôtes qui ont besoin d'accéder au service.
2. Utilisez l'onglet Gérer l'accès externe pour bloquer tous les ports.

> Ajoutez l'adresse IP privilégiée avant de bloquer l'accès à tout port attribué à l'accès à Grid Manager et Tenant Manager (les ports prédéfinis sont 443 et 8443). Tout utilisateur actuellement connecté à un port bloqué, y compris vous, perdra l'accès à Grid Manager à moins que son adresse IP n'ait été ajoutée à la liste des adresses privilégiées.

Une fois votre configuration enregistrée, le port sensible et le service associé sont accessibles aux hôtes figurant dans la liste d'adresses privilégiées. L'accès au service est refusé à tous les autres hôtes, quelle que soit l'interface d'où provient la requête.

Exemple 3 : Désactivez l'accès aux services inutilisés

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

Onglet Réseaux clients non approuvés

Si vous utilisez un réseau client, vous pouvez contribuer à sécuriser StorageGRID contre les attaques hostiles en n'acceptant le trafic client entrant que sur les points de terminaison explicitement configurés.

Par défaut, le réseau client de chaque nœud de la grille est *de confiance*. Autrement dit, par défaut, StorageGRID fait confiance aux connexions entrantes vers chaque nœud de la grille sur tous les "ports externes disponibles".

Vous pouvez réduire le risque d'attaques hostiles sur votre système StorageGRID en spécifiant que le réseau client de chaque nœud soit *non fiable*. Si le réseau client d'un nœud est non fiable, le nœud n'accepte les connexions entrantes que sur les ports explicitement configurés comme points de terminaison d'équilibrage de charge. Voir "Configurer les points de terminaison de l'équilibreur de charge" et "Configurer les contrôles du

pare-feu".

Exemple 1 : Le nœud passerelle accepte uniquement les requêtes HTTPS S3

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

1. À partir de la page "points de terminaison de l'équilibreur de charge", configurez un point de terminaison d'équilibrage de charge pour S3 via HTTPS sur le port 443.
2. Sur la page de contrôle du pare-feu, sélectionnez Non approuvé pour indiquer que le réseau client sur le nœud de passerelle n'est pas approuvé.

Après avoir enregistré votre configuration, tout le trafic entrant sur le réseau client du nœud de passerelle est bloqué, à l'exception des requêtes HTTPS S3 sur le port 443 et des requêtes d'écho ICMP (ping).

Exemple 2 : Un nœud de stockage envoie des requêtes de services de plateforme S3

Supposons que vous souhaitiez autoriser le trafic sortant des services de la plateforme S3 depuis un nœud de stockage, mais empêcher toute connexion entrante vers ce nœud de stockage sur le réseau client. Vous effectueriez l'étape générale suivante :

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

Une fois votre configuration enregistrée, le nœud de stockage n'accepte plus aucun trafic entrant sur le réseau client, mais il continue d'autoriser les requêtes sortantes vers les destinations des services de plateforme configurés.

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

Supposons que vous souhaitiez autoriser l'accès à Grid Manager uniquement sur un sous-réseau spécifique. Vous effectueriez les étapes suivantes :

1. Connectez le réseau client de vos nœuds d'administration au sous-réseau.
2. Utilisez l'onglet Untrusted Client Network pour configurer le réseau client comme non approuvé.
3. Lorsque vous créez un point de terminaison d'équilibreur de charge d'interface de gestion, saisissez le port et sélectionnez l'interface de gestion à laquelle le port accédera.
4. Sélectionnez **Oui** pour Réseau client non approuvé.
5. Utilisez l'onglet Gérer l'accès externe pour bloquer tous les ports externes (avec ou sans adresses IP privilégiées définies pour les hôtes situés en dehors de ce sous-réseau).

Une fois votre configuration enregistrée, seuls les hôtes du sous-réseau que vous avez spécifié peuvent accéder au Grid Manager. Tous les autres hôtes sont bloqués.

Configurer le pare-feu interne de StorageGRID

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

Avant de commencer

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

- Vous avez "autorisations d'accès spécifiques".
- Vous avez examiné les informations dans "Gérer les contrôles du pare-feu" et "Directives de mise en réseau".
- Si vous souhaitez qu'un nœud d'administration ou un nœud de passerelle n'accepte le trafic entrant que sur les points de terminaison explicitement configurés, vous avez défini les points de terminaison de l'équilibreur de charge.

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

À propos de cette tâche

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

Limiter le nombre de ports ouverts aux adresses IP extérieures à votre grid aux seuls ports strictement nécessaires renforce la sécurité de votre grid. Vous utilisez les paramètres de chacun des trois onglets de contrôle du pare-feu pour vous assurer que seuls les ports nécessaires sont ouverts.

Pour plus d'informations sur l'utilisation des contrôles du pare-feu, y compris des exemples, consultez "Gérer les contrôles du pare-feu".

Pour plus d'informations sur les pare-feu externes et la sécurité réseau, consultez "Contrôler l'accès au niveau du pare-feu externe".

Contrôler l'accès au pare-feu

Étapes

1. Sélectionnez **Configuration** > **Sécurité** > **Contrôle du pare-feu**.

   Les trois onglets de cette page sont décrits dans "Gérer les contrôles du pare-feu".

2. Sélectionnez un onglet pour configurer les contrôles du pare-feu.

   Vous pouvez utiliser ces onglets dans n'importe quel ordre. Les configurations que vous définissez dans un onglet n'empêchent pas ce que vous pouvez faire dans les autres onglets ; cependant, les modifications de configuration que vous effectuez dans un onglet peuvent modifier le comportement des ports configurés dans les autres onglets.

Liste d'adresses privilégiées

Vous utilisez l'onglet Liste d'adresses privilégiées pour accorder aux hôtes l'accès aux ports fermés par défaut ou fermés par les paramètres de l'onglet Gérer l'accès externe.

Les adresses IP et les sous-réseaux privilégiés n'ont pas accès au grid interne par défaut. De plus, les points de terminaison de l'équilibreur de charge et les ports supplémentaires ouverts dans l'onglet Liste des adresses privilégiées sont accessibles même s'ils sont bloqués dans l'onglet Gérer l'accès externe.

Les paramètres de l'onglet « Liste des adresses privilégiées » ne peuvent pas remplacer les paramètres de l'onglet « Réseau client non approuvé ».

Étapes

1. Dans l'onglet Liste des adresses privilégiées, saisissez l'adresse ou le sous-réseau IP auquel vous souhaitez accorder l'accès aux ports fermés.
2. Vous pouvez également sélectionner **Ajouter une autre adresse IP ou un sous-réseau au format CIDR** pour ajouter des clients privilégiés supplémentaires.

   Ajoutez le moins d'adresses possible à la liste privilégiée.

3. Vous pouvez également sélectionner **Autoriser les adresses IP privilégiées à accéder aux ports internes de StorageGRID**. Voir "Ports internes de StorageGRID".

   Cette option désactive certaines protections des services internes. Laissez-la désactivée si possible.

4. Sélectionnez **Enregistrer**.

Gérer l'accès externe

Lorsqu'un port est fermé dans l'onglet Gérer l'accès externe, le port ne peut pas être accessible par une adresse IP non-grid, sauf si vous ajoutez l'adresse IP à la liste des adresses privilégiées. Vous pouvez uniquement fermer les ports ouverts par défaut et uniquement ouvrir les ports que vous avez fermés.

Les paramètres de l'onglet « Gérer l'accès externe » ne peuvent pas prévaloir sur ceux de l'onglet « Réseau client non fiable ». Par exemple, si un nœud est non fiable, le port SSH/22 est bloqué sur le réseau client, même s'il est ouvert dans l'onglet « Gérer l'accès externe ». Les paramètres de l'onglet « Réseau client non fiable » prévalent sur les ports fermés (tels que 443, 8443, 9443) sur le réseau client.

Étapes

1. Sélectionnez **Gérer l'accès externe**. L'onglet affiche un tableau répertoriant tous les ports externes (ports accessibles par défaut aux nœuds hors grille) des nœuds de votre grille.
2. Configurez les ports que vous souhaitez ouvrir et fermer à l'aide des options suivantes :
   - Utilisez le bouton à bascule situé à côté de chaque port pour ouvrir ou fermer le port sélectionné.
   - Sélectionnez **Ouvrir tous les ports affichés** pour ouvrir tous les ports répertoriés dans le tableau.
   - Sélectionnez **Fermer tous les ports affichés** pour fermer tous les ports listés dans le tableau.

   Si vous fermez les ports 443 ou 8443 de Grid Manager, tous les utilisateurs actuellement connectés sur un port bloqué, y compris vous, perdront l'accès à Grid Manager à moins que leur adresse IP n'ait été ajoutée à la liste des adresses privilégiées.

Utilisez la barre de défilement à droite du tableau pour vous assurer d'avoir visualisé tous les ports disponibles. Utilisez le champ de recherche pour trouver les paramètres de n'importe quel port externe en saisissant un numéro de port. Vous pouvez saisir un numéro de port partiel. Par exemple, si vous saisissez **2**, tous les ports dont le nom contient la chaîne « 2 » seront affichés.

3. Sélectionnez **Save**

Réseau de clients non fiables

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

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

Les modifications de configuration que vous effectuez dans l'onglet **Réseau client non approuvé** remplacent les paramètres de l'onglet **Gérer l'accès externe**.

Étapes

1. Sélectionnez **Réseau client non approuvé**.
2. Dans la section Définir la valeur par défaut des nouveaux nœuds, spécifiez le paramètre par défaut qui doit être appliqué lorsque de nouveaux nœuds sont ajoutés à la grille lors d'une procédure d'expansion.
   - **Fiable** (par défaut) : lorsqu'un nœud est ajouté dans une extension, son réseau client est fiable.
   - **Non fiable** : Lorsqu'un nœud est ajouté lors d'une extension, son réseau client est non fiable.

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

     Ce paramètre n'affecte pas les nœuds existants de votre système StorageGRID.
3. Utilisez les options suivantes pour sélectionner les nœuds qui doivent autoriser les connexions client uniquement sur les points de terminaison d'équilibrage de charge explicitement configurés ou sur des ports supplémentaires sélectionnés :
   - Sélectionnez **Ne pas faire confiance aux nœuds affichés** pour ajouter tous les nœuds affichés dans le tableau à la liste Untrusted Client Network.
   - Sélectionnez **Faire confiance aux nœuds affichés** pour supprimer tous les nœuds affichés dans le tableau de la liste Untrusted Client Network.
   - Utilisez le bouton bascule situé à côté de chaque nœud pour définir le réseau client comme étant de confiance ou non de confiance pour le nœud sélectionné.

     Par exemple, vous pouvez sélectionner **Ne pas faire confiance aux nœuds affichés** pour ajouter tous les nœuds à la liste Réseau client non fiable, puis utiliser le bouton bascule situé à côté d'un nœud individuel pour ajouter ce nœud à la liste Réseau client fiable.

Utilisez la barre de défilement à droite du tableau pour vous assurer d'avoir visualisé tous les nœuds disponibles. Utilisez le champ de recherche pour trouver les paramètres de n'importe quel nœud en saisissant le nom du nœud. Vous pouvez saisir un nom partiel. Par exemple, si vous saisissez **GW**, tous les nœuds dont le nom contient la chaîne "GW" seront affichés.

4. Sélectionnez **Enregistrer**.

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