Contrôler les pare-feu

StorageGRID software

NetApp
December 03, 2025

Sommaire

Contrôler les pare-feu . . . 1
- Contrôler l’accès au pare-feu externe . . . 1
- Gérer les contrôles du pare-feu interne . . . 2
  - Liste d’adresses privilégiées et onglets Gérer les accès externes . . . 2
  - Onglet Réseaux de clients non approuvés . . . 3
- Configurer le pare-feu interne . . . 4
  - Contrôles du pare-feu d’accès . . . 5
  - Liste d’adresses privilégiées . . . 5
  - Gérer les accès externes . . . 6
  - Réseau de clients non fiables . . . 7

Contrôler les pare-feu

Contrôler l’accès au 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 souhaiterez peut-être 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 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 de l’API de gestion peuvent accéder au gestionnaire de grille, à l’API de gestion de grille, au gestionnaire de locataires et à l’API de gestion de locataires. **Remarque :** le port 443 est également utilisé pour certains trafics internes.
8443	Port Grid Manager restreint sur les nœuds d’administration	• Les navigateurs Web et les clients de l’API de gestion peuvent accéder au Grid Manager et à l’API de gestion de grille à l’aide de HTTPS. • Les navigateurs Web et les clients de l’API de gestion ne peuvent pas accéder au gestionnaire de locataires ni à l’API de gestion des locataires. • Les demandes de contenu interne seront rejetées.
9443	Port du gestionnaire de locataires restreint sur les nœuds d’administration	• Les navigateurs Web et les clients de l’API de gestion peuvent accéder au gestionnaire de locataires et à l’API de gestion des locataires à l’aide de HTTPS. • Les navigateurs Web et les clients de l’API de gestion ne peuvent pas accéder au gestionnaire de grille ou à l’API de gestion de grille. • Les demandes de contenu interne seront rejetées.

L’authentification unique (SSO) n’est pas disponible sur les ports restreints Grid Manager ou 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

- "Sign in au gestionnaire de grille"

- "Créer un compte locataire"
- "Communications externes"

Gérer les contrôles du pare-feu interne

StorageGRID inclut 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 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 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 spécifier 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 acceptera uniquement 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 de type de nœud).
  - Les ports de point 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 Gérer les réseaux externes.
  - Lorsqu'ils sont 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 sur un onglet peuvent affecter les modifications d'accès que vous effectuez sur un autre onglet. Assurez-vous de vérifier les paramètres de tous les onglets pour vous assurer que votre réseau se comporte comme vous l'attendez.

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

Pour plus d'informations sur les pare-feu externes et la sécurité du réseau, consultez"Contrôler l'accès au 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 auxquelles l'accès aux ports de grille fermés est accordé. 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-grille). Ces deux onglets peuvent souvent être utilisés ensemble pour personnaliser l'accès réseau exact dont vous avez besoin pour autoriser votre grille.

Les adresses IP privilégiées n’ont pas d’accès au port de grille interne par défaut.

Exemple 1 : Utiliser un hôte de saut pour les tâches de maintenance

Supposons que vous souhaitiez utiliser un hôte de saut (un hôte renforcé en termes de sécurité) pour l’administration du réseau. Vous pouvez utiliser ces étapes générales :

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, sauf si leur adresse IP a 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 saut pour effectuer des tâches de maintenance sur votre réseau de manière plus sécurisée.

Exemple 2 : Verrouiller les ports sensibles

Supposons que vous souhaitiez 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 à tous les ports attribués pour accéder à Grid Manager et Tenant Manager (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, sauf si leur adresse IP a 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’où provient 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 utiliseriez le bouton 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 contribuer à sécuriser StorageGRID contre les attaques hostiles en acceptant le trafic client entrant uniquement sur les points de terminaison explicitement configurés.

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

Vous pouvez réduire la menace d’attaques hostiles sur votre système StorageGRID en spécifiant que le réseau client sur chaque nœud doit être *non fiable*. Si le réseau client d’un nœud n’est pas approuvé, le nœud accepte uniquement les connexions entrantes 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 de passerelle accepte uniquement les requêtes HTTPS S3

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

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

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

Exemple 2 : Le nœud de stockage envoie des demandes de services de la 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 vers ce nœud de stockage sur le réseau client. Vous effectueriez cette étape générale :

- 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 demandes sortantes vers les destinations des 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 de Grid Manager uniquement sur un sous-réseau spécifique. Vous effectuerez les étapes suivantes :

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 approuvé.
3. Lorsque vous créez un point de terminaison d'équilibrage de charge d'interface de gestion, entrez le port et sélectionnez l'interface de gestion à laquelle le port accédera.
4. Sélectionnez **Oui** pour le 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 en dehors de ce sous-réseau).

Une fois votre configuration enregistrée, seuls les hôtes du sous-réseau que vous avez spécifié peuvent accéder au gestionnaire de grille. 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 Grid Manager à l'aide d'un"navigateur Web pris en charge" .
* Tu as"autorisations d'accès spécifiques" .
* Vous avez examiné les informations contenues 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 accepte le trafic entrant uniquement sur des 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 inclut un pare-feu interne sur chaque nœud qui vous permet d'ouvrir ou de fermer certains des ports sur les nœuds de votre grille. Vous pouvez utiliser les onglets de contrôle du pare-feu pour ouvrir ou fermer les ports ouverts par défaut sur le réseau de grille, le réseau d'administration et le réseau client. Vous pouvez également créer une liste d'adresses IP privilégiées pouvant accéder aux ports de grille fermés. Si vous utilisez un réseau client, vous pouvez spécifier si un nœud approuve le trafic entrant provenant du réseau client et vous pouvez configurer l'accès de ports spécifiques sur le réseau client.

Limiter le nombre de ports ouverts aux adresses IP en dehors de votre réseau à ceux qui sont absolument nécessaires améliore la sécurité de votre réseau. 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, y compris des exemples, consultez"Gérer les contrôles du pare-feu" .

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

Contrôles du pare-feu d'accès

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 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 que vous apportez 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 les paramètres de l'onglet Gérer l'accès externe.

Les adresses IP privilégiées et les sous-réseaux n'ont pas d'accès au réseau interne par défaut. De plus, les points de terminaison de l'équilibreur de charge et les ports supplémentaires ouverts dans l'onglet Liste d’adresses privilégiées sont accessibles même s’ils sont 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 auquel vous souhaitez accorder l’accès aux ports fermés.
2. Vous pouvez également sélectionner **Ajouter une autre adresse IP ou un autre sous-réseau en notation CIDR** pour ajouter des clients privilégiés supplémentaires.

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

3. Si vous le souhaitez, sélectionnez *Autoriser les adresses IP privilégiées à accéder aux ports internes de StorageGRID *. Voir "Ports internes StorageGRID" .

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

4. Sélectionnez **Enregistrer**.

Gérer les accès externes

Lorsqu’un port est fermé dans l’onglet Gérer l’accès externe, le port n’est pas accessible par une adresse IP non-grille, sauf si vous ajoutez 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 avec tous les ports externes (ports accessibles par défaut par les nœuds non-grille) pour les nœuds de votre grille.
2. Configurez les ports que vous souhaitez ouvrir et fermer à l’aide des options suivantes :
   - Utilisez le bouton bascule 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 répertoriés 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, sauf si leur adresse IP a été ajoutée à la liste d’adresses privilégiées.

Utilisez la barre de défilement sur le côté droit 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 entrez un **2**, tous les ports dont le nom contient la chaîne « 2 » sont affichés.

3. Sélectionnez **Enregistrer**

Réseau de clients non fiables

Si le réseau client d'un nœud n'est pas approuvé, le nœud accepte uniquement le trafic entrant sur les ports configurés comme points de terminaison d'équilibrage 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 des 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 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 du nouveau nœud, spécifiez le paramètre par défaut à utiliser lorsque de nouveaux nœuds sont ajoutés à la grille dans le cadre d'une procédure d'extension.
   - **Fiable** (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 dans 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 sélectionnés supplémentaires :
   - Sélectionnez **Ne pas faire confiance aux nœuds affichés** pour ajouter tous les nœuds affichés dans le tableau à la liste des réseaux clients non approuvés.
   - Sélectionnez **Faire confiance aux nœuds affichés** pour supprimer tous les nœuds affichés dans le tableau de la liste Réseau client non approuvé.
   - Utilisez le bouton bascule à côté de chaque nœud pour définir le réseau client comme approuvé ou non approuvé pour le nœud sélectionné.

     Par exemple, vous pouvez sélectionner **Ne pas faire confiance aux nœuds affichés** pour ajouter tous les nœuds à la liste des réseaux clients non approuvés, puis utiliser le bouton bascule à côté d'un nœud individuel pour ajouter ce nœud unique à la liste des réseaux clients approuvés.

Utilisez la barre de défilement sur le côté droit 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 entrez un **GW**, tous les nœuds dont le nom contient la chaîne « GW » sont affichés.

4. Sélectionnez **Enregistrer**.

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