Durcissement du système

StorageGRID

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/storagegrid-117/harden/index.html on November 04, 2025. Always check docs.netapp.com for the latest.

Sommaire

Durcissement du système . . . 1
Durcissement du système : vue d'ensemble . . . 1
Considérations générales relatives au renforcement des systèmes StorageGRID . . . 1
Directives de renforcement des mises à niveau logicielles . . . 1
Mises à niveau du logiciel StorageGRID . . . 1
Mises à niveau vers des services externes . . . 2
Mises à niveau vers les hyperviseurs . . . 2
Mises à niveau vers les nœuds Linux . . . 2
Instructions de renforcement des réseaux StorageGRID . . . 2
Instructions relatives au réseau Grid . . . 2
Instructions pour le réseau d'administration . . . 3
Directives pour le réseau client . . . 3
Instructions de renforcement pour les nœuds StorageGRID . . . 3
Configuration du pare-feu . . . 3
Désactiver les services inutilisés . . . 4
Virtualisation, conteneurs et matériel partagé . . . 4
Protéger les nœuds pendant l'installation . . . 4
Instructions pour les nœuds d'administration . . . 4
Consignes relatives aux nœuds de stockage . . . 5
Instructions pour les nœuds de passerelle . . . 5
Consignes pour les nœuds d'appliances matérielles . . . 6
Instructions de renforcement pour TLS et SSH . . . 6
Directives de renforcement des certificats . . . 6
Directives de renforcement pour les règles TLS et SSH . . . 7
Autres directives de durcissement . . . 7
Journaux et messages d'audit . . . 8
NetApp AutoSupport . . . 8
Partage des ressources d'origine croisée (CORS) . . . 8
Dispositifs de sécurité externes . . . 8
Réduction des ransomwares . . . 8

Durcissement du système

Durcissement du système : vue d'ensemble

Le renforcement des systèmes consiste à éliminer autant de risques que possible pour la sécurité d'un système StorageGRID.

Ce document présente les directives de renforcement propres à StorageGRID. Ces directives constituent un complément aux meilleures pratiques standard du secteur en matière de renforcement des systèmes. Par exemple, ces instructions partent du principe que vous utilisez des mots de passe forts pour StorageGRID, utilisez HTTPS au lieu de HTTP et activez l'authentification basée sur les certificats, le cas échéant.

Lors de l'installation et de la configuration de StorageGRID, ces instructions vous aideront à répondre aux objectifs de sécurité que vous avez définis pour la confidentialité, l'intégrité et la disponibilité des systèmes d'information.

StorageGRID suit le "Politique de gestion des vulnérabilités de NetApp". Toutes les vulnérabilités signalées sont vérifiées et traitées selon le processus de réponse aux incidents de sécurité.

Considérations générales relatives au renforcement des systèmes StorageGRID

Lors du renforcement d'un système StorageGRID, vous devez prendre en compte les éléments suivants :

- Parmi les trois réseaux StorageGRID que vous avez mis en place, lesquels ? Tous les systèmes StorageGRID doivent utiliser le réseau Grid, mais vous pouvez également utiliser le réseau Admin, le réseau client ou les deux. Chaque réseau a des considérations de sécurité différentes.
- Type de plateforme utilisé pour les nœuds individuels du système StorageGRID. Les nœuds StorageGRID peuvent être déployés sur des machines virtuelles VMware, au sein d'un moteur de conteneurs sur des hôtes Linux, ou en tant qu'appliances matérielles dédiées. Chaque type de plateforme dispose de son propre ensemble de meilleures pratiques en matière de renforcement.
- Fiabilité des comptes locataires. Si vous êtes un fournisseur de services avec des comptes de locataires non fiables, vous vous interrogez différemment que si vous utilisez uniquement des locataires internes fiables.
- Les exigences et conventions de sécurité sont respectées par votre entreprise. Vous devrez peut-être vous conformer à des exigences réglementaires ou d'entreprise spécifiques.

Directives de renforcement des mises à niveau logicielles

Vous devez maintenir votre système StorageGRID et les services associés à jour pour vous protéger contre les attaques.

Mises à niveau du logiciel StorageGRID

Dans la mesure du possible, vous devez mettre à niveau le logiciel StorageGRID vers la version principale la plus récente ou vers la version majeure précédente. Maintenir StorageGRID à jour permet de réduire le temps d'activation des vulnérabilités connues et de réduire la surface d'attaque globale. En outre, les versions les plus récentes de StorageGRID comprennent souvent des fonctionnalités de renforcement de la sécurité qui ne sont pas incluses dans les versions précédentes.

Consulter le "Matrice d'interopérabilité NetApp" (IMT) pour déterminer quelle version du logiciel StorageGRID

vous devez utiliser. Lorsqu'un correctif est requis, NetApp privilégie la création de mises à jour pour les dernières versions. Certains correctifs peuvent ne pas être compatibles avec les versions antérieures.

- Pour télécharger les versions et correctifs StorageGRID les plus récents, rendez-vous sur le site "Téléchargement NetApp : StorageGRID".
- Pour mettre à niveau le logiciel StorageGRID, reportez-vous au "instructions de mise à niveau".
- Pour appliquer un correctif, reportez-vous au "Procédure de correctif StorageGRID".

Mises à niveau vers des services externes

Les services externes peuvent comporter des vulnérabilités qui affectent indirectement StorageGRID. Vous devez vous assurer que les services dont dépend StorageGRID sont tenus à jour. Ces services incluent : LDAP, KMS (ou serveur KMIP), DNS et NTP.

Utilisez le "Matrice d'interopérabilité NetApp" pour obtenir une liste des versions prises en charge.

Mises à niveau vers les hyperviseurs

Si vos nœuds StorageGRID s'exécutent sur VMware ou sur un autre hyperviseur, vous devez vous assurer que le logiciel et le firmware de l'hyperviseur sont à jour.

Utilisez le "Matrice d'interopérabilité NetApp" pour obtenir une liste des versions prises en charge.

Mises à niveau vers les nœuds Linux

Si vos nœuds StorageGRID utilisent des plates-formes hôtes Linux, vous devez vous assurer que les mises à jour de sécurité et de noyau sont appliquées au système d'exploitation hôte. En outre, vous devez appliquer des mises à jour de micrologiciel au matériel vulnérable lorsque ces mises à jour sont disponibles.

Utilisez le "Matrice d'interopérabilité NetApp" pour obtenir une liste des versions prises en charge.

Instructions de renforcement des réseaux StorageGRID

Le système StorageGRID prend en charge jusqu'à trois interfaces réseau par nœud grid, ce qui vous permet de configurer le réseau pour chaque nœud grid en fonction de vos besoins de sécurité et d'accès.

Pour plus d'informations sur les réseaux StorageGRID, reportez-vous au "Types de réseau StorageGRID".

Instructions relatives au réseau Grid

Vous devez configurer un réseau Grid pour tout le trafic StorageGRID interne. Tous les nœuds de la grille se trouvent sur le réseau Grid et ils doivent pouvoir communiquer avec tous les autres nœuds.

Lors de la configuration du réseau Grid, suivez les instructions suivantes :

- Assurez-vous que le réseau est sécurisé par des clients non approuvés, tels que ceux qui se trouvent sur Internet ouvert.
- Si possible, utilisez le réseau Grid exclusivement pour le trafic interne. Le réseau d'administration et le réseau client disposent d'autres restrictions de pare-feu qui bloquent le trafic externe vers les services internes. L'utilisation du réseau Grid pour le trafic client externe est prise en charge, mais cette utilisation

offre moins de couches de protection.

- Si le déploiement StorageGRID s'étend sur plusieurs data centers, utilisez un réseau privé virtuel (VPN) ou un équivalent sur le réseau Grid afin de protéger le trafic interne.
- Certaines procédures de maintenance exigent un accès SSH (Secure Shell) sur le port 22 entre le nœud d'administration principal et tous les autres nœuds de la grille. Utilisez un pare-feu externe pour restreindre l'accès SSH aux clients approuvés.

Instructions pour le réseau d'administration

Le réseau Admin est généralement utilisé pour les tâches d'administration (employés de confiance utilisant Grid Manager ou SSH) et pour la communication avec d'autres services de confiance tels que LDAP, DNS, NTP, KMS (ou serveur KMIP). Cependant, StorageGRID n'applique pas cette utilisation en interne.

Si vous utilisez le réseau Admin, suivez les instructions suivantes :

- Bloquez tous les ports de trafic internes sur le réseau d'administration. Voir la "liste des ports internes".
- Si des clients non approuvés peuvent accéder au réseau d'administration, bloquez l'accès à StorageGRID sur le réseau d'administration avec un pare-feu externe.

Directives pour le réseau client

Le réseau client est généralement utilisé pour les locataires et pour communiquer avec des services externes, tels que le service de réplication CloudMirror ou un autre service de plate-forme. Cependant, StorageGRID n'applique pas cette utilisation en interne.

Si vous utilisez le réseau client, suivez les instructions suivantes :

- Bloquer tous les ports de trafic interne sur le réseau client. Voir la "liste des ports internes".
- Acceptez le trafic client entrant uniquement sur les terminaux configurés explicitement. Voir les informations sur "gestion des contrôles de pare-feu".

Instructions de renforcement pour les nœuds StorageGRID

Les nœuds StorageGRID peuvent être déployés sur des machines virtuelles VMware, au sein d'un moteur de conteneurs sur des hôtes Linux, ou en tant qu'appliances matérielles dédiées. Chaque type de plateforme et chaque type de nœud dispose de ses propres pratiques de renforcement.

Configuration du pare-feu

Dans le cadre du processus de renforcement du système, vous devez examiner les configurations de pare-feu externes et les modifier afin que le trafic soit accepté uniquement à partir des adresses IP et sur les ports à partir desquels il est strictement nécessaire.

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. Vous devriez "gérer les contrôles de pare-feu internes" pour empêcher l'accès au réseau sur tous les ports, à l'exception de ceux nécessaires à votre déploiement de grid spécifique. Les modifications de configuration effectuées sur la page de contrôle du pare-feu sont déployées sur chaque nœud.

Plus précisément, vous pouvez gérer les domaines suivants :

- **Adresses privilégiées** : vous pouvez autoriser certaines adresses IP ou sous-réseaux à accéder aux ports fermés par les paramètres de l'onglet gérer l'accès externe.
- **Gérer l'accès externe** : vous pouvez fermer les ports ouverts par défaut ou rouvrir les ports précédemment fermés.
- **Réseau client non approuvé** : vous pouvez spécifier si un nœud approuve le trafic entrant provenant du réseau client ainsi que les ports supplémentaires que vous souhaitez ouvrir lorsque le réseau client non approuvé est configuré.

Bien que ce pare-feu interne offre une couche supplémentaire de protection contre certaines menaces courantes, il ne supprime pas la nécessité d'un pare-feu externe.

Pour obtenir la liste de tous les ports internes et externes utilisés par StorageGRID, reportez-vous à la section "Référence du port réseau".

Désactiver les services inutilisés

Pour tous les nœuds StorageGRID, désactivez ou bloquez l'accès aux services non utilisés. Par exemple, si vous n'envisagez pas de configurer l'accès client aux partages d'audit pour NFS, bloquez ou désactivez l'accès à ces services.

Virtualisation, conteneurs et matériel partagé

Pour tous les nœuds StorageGRID, évitez d'exécuter StorageGRID sur le même matériel physique que les logiciels non fiables. Ne supposez pas que les protections de l'hyperviseur empêchent les logiciels malveillants d'accéder aux données protégées par StorageGRID si StorageGRID et le logiciel malveillant existent sur le même matériel physique. Par exemple, les attaques Meltdown et Specter exploitent des vulnérabilités critiques dans les processeurs modernes et permettent aux programmes de voler des données en mémoire sur le même ordinateur.

Protéger les nœuds pendant l'installation

N'autorisez pas les utilisateurs non approuvés à accéder aux nœuds StorageGRID sur le réseau lors de l'installation des nœuds. Les nœuds ne sont pas entièrement sécurisés tant qu'ils n'ont pas rejoint la grille.

Instructions pour les nœuds d'administration

Des nœuds d'administration qui assurent les services de gestion tels que la configuration du système, la surveillance et la journalisation. Lorsque vous vous connectez à Grid Manager ou au Gestionnaire de locataires, vous vous connectez à un noeud d'administration.

Suivez les instructions suivantes pour sécuriser les nœuds d'administration dans votre système StorageGRID :

- Sécurisez tous les nœuds d'administration des clients non fiables, tels que ceux qui sont sur Internet ouvert. Assurez-vous qu'aucun client non approuvé ne peut accéder à un nœud d'administration sur le réseau Grid, le réseau d'administration ou le réseau client.
- Les groupes StorageGRID contrôlent l'accès aux fonctionnalités de Grid Manager et de tenant Manager. Accordez à chaque groupe d'utilisateurs les autorisations minimales requises pour leur rôle et utilisez le mode d'accès en lecture seule pour empêcher les utilisateurs de modifier la configuration.
- Lorsque vous utilisez des terminaux d'équilibrage de charge StorageGRID, utilisez des nœuds de passerelle au lieu des nœuds d'administration pour le trafic client non fiable.
- Si vous avez des locataires non approuvés, ne les autorisez pas à avoir un accès direct au gestionnaire de

locataires ou à l'API de gestion des locataires. Certains locataires non fiables utilisent un portail de locataires ou un système de gestion externe des locataires qui interagit avec l'API de gestion des locataires.

- Vous pouvez également utiliser un proxy d'administration pour mieux contrôler la communication AutoSupport entre les nœuds d'administration et le support NetApp. Voir les étapes pour "Création d'un proxy Admin".
- Utilisez éventuellement les ports 8443 et 9443 restreints pour séparer les communications Grid Manager et tenant Manager. Bloquez le port partagé 443 et limitez les demandes des locataires au port 9443 pour une protection supplémentaire.
- La possibilité d'utiliser des nœuds d'administration distincts pour les administrateurs du grid et les utilisateurs des locataires.

Pour plus d'informations, reportez-vous aux instructions de "Administration d'StorageGRID".

Consignes relatives aux nœuds de stockage

Des nœuds de stockage gèrent et stockent les données et les métadonnées d'objets. Suivez ces instructions pour sécuriser les nœuds de stockage dans votre système StorageGRID.

- Ne permettez pas aux clients non approuvés de se connecter directement aux nœuds de stockage. Utilisez un terminal d'équilibrage de charge desservi par un nœud de passerelle ou un équilibreur de charge tiers.
- N'activez pas les services sortants pour les locataires non approuvés. Par exemple, lors de la création du compte pour un locataire non approuvé, n'autorisez pas le locataire à utiliser son propre référentiel d'identité et n'autorisez pas l'utilisation des services de plate-forme. Voir les étapes pour "création d'un compte de locataire".
- Utilisez un équilibreur de charge tiers pour le trafic client non fiable. L'équilibrage de la charge fourni par des tiers offre un meilleur contrôle et des couches de protection supplémentaires contre les attaques.
- Vous pouvez également utiliser un proxy de stockage pour plus de contrôle sur les pools de stockage cloud et les communications des services de plateforme depuis les nœuds de stockage vers les services externes. Voir les étapes pour "Création d'un proxy de stockage".
- Vous pouvez également vous connecter à des services externes à l'aide du réseau client. Sélectionnez ensuite **CONFIGURATION** > **sécurité** > **contrôle du pare-feu** > **réseaux clients non approuvés** et indiquez que le réseau client sur le noeud de stockage n'est pas fiable. Le nœud de stockage n'accepte plus de trafic entrant sur le réseau client, mais il continue à autoriser les requêtes sortantes pour les services de plate-forme.

Instructions pour les nœuds de passerelle

Les nœuds de passerelle fournissent une interface d'équilibrage de la charge facultative que les applications client peuvent utiliser pour se connecter à StorageGRID. Pour sécuriser tous les nœuds de passerelle de votre système StorageGRID, procédez comme suit :

- Configurez et utilisez des terminaux d'équilibrage de charge. Voir "Considérations relatives à l'équilibrage de charge".
- Utilisez un équilibreur de charge tiers entre le client et le nœud de passerelle ou les nœuds de stockage pour le trafic client non fiable. L'équilibrage de la charge fourni par des tiers offre un meilleur contrôle et des couches de protection supplémentaires contre les attaques. Si vous utilisez un équilibreur de charge tiers, le trafic réseau peut, éventuellement, être configuré de manière à passer par un terminal interne d'équilibrage de la charge ou être directement envoyé aux nœuds de stockage.

- Si vous utilisez des points de terminaison d'équilibrage de charge, les clients peuvent éventuellement se connecter via le réseau client. Sélectionnez ensuite **CONFIGURATION** > **sécurité** > **contrôle du pare-feu** > **réseaux clients non approuvés** et indiquez que le réseau client sur le nœud passerelle n'est pas fiable. Le nœud passerelle accepte uniquement le trafic entrant sur les ports explicitement configurés en tant que points finaux d'équilibreur de charge.

Consignes pour les nœuds d'appliances matérielles

Les appliances matérielles StorageGRID sont spécialement conçues pour une utilisation dans un système StorageGRID. Certaines appliances peuvent être utilisées comme nœuds de stockage. Les autres appliances peuvent être utilisées comme nœuds d'administration ou nœuds de passerelle. Vous pouvez associer des nœuds d'appliance à des nœuds basés sur logiciel ou déployer des grilles 100 % appliance entièrement conçues.

Pour sécuriser les nœuds d'appliance matérielle de votre système StorageGRID, procédez comme suit :

- Si l'appliance utilise SANtricity System Manager pour la gestion du contrôleur de stockage, empêchez les clients non fiables d'accéder à SANtricity System Manager sur le réseau.
- Si l'appliance est équipée d'un contrôleur de gestion de la carte mère (BMC), notez que le port de gestion du BMC permet un accès matériel de faible niveau. Connectez le port de gestion BMC uniquement à un réseau de gestion interne sécurisé, fiable et. Si aucun réseau de ce type n'est disponible, laissez le port de gestion BMC déconnecté ou bloqué, à moins qu'une connexion BMC ne soit demandée par le support technique.
- Si l'appliance prend en charge la gestion à distance du matériel du contrôleur via Ethernet à l'aide de la norme IPMI (Intelligent Platform Management interface), bloquez le trafic non fiable sur le port 623.

> Vous pouvez activer ou désactiver l'accès IPMI à distance pour tous les dispositifs contenant un contrôleur BMC en utilisant le point de terminaison privé de l'API de gestion, PUT /private/bmc.

- Si le contrôleur de stockage de l'appliance inclut des disques FDE ou FIPS et que la fonction de sécurité des disques est activée, utilisez SANtricity pour configurer les clés de sécurité des disques. Voir "Configuration de SANtricity System Manager (SG6000 et SG5700)".
- Pour les appliances sans disques FDE ou FIPS, activez le chiffrement de nœud à l'aide d'un serveur de gestion des clés (KMS). Voir "Facultatif : activez le chiffrement de nœud".

Instructions de renforcement pour TLS et SSH

Vous devez remplacer les certificats par défaut créés lors de l'installation et sélectionner la stratégie de sécurité appropriée pour les connexions TLS et SSH.

Directives de renforcement des certificats

Vous devez remplacer les certificats par défaut créés lors de l'installation par vos propres certificats personnalisés.

Pour de nombreuses organisations, le certificat numérique auto-signé pour l'accès au Web StorageGRID n'est pas conforme à leurs politiques de sécurité de l'information. Sur les systèmes de production, vous devez installer un certificat numérique signé par une autorité de certification pour l'authentification de StorageGRID.

Plus précisément, vous devez utiliser des certificats de serveur personnalisés au lieu de ces certificats par défaut :

- **Certificat d'interface de gestion** : utilisé pour sécuriser l'accès au Grid Manager, au tenant Manager, à l'API Grid Management et à l'API tenant Management.
- **Certificat API S3 et Swift** : utilisé pour sécuriser l'accès aux nœuds de stockage et aux nœuds de passerelle, que les applications client S3 et Swift utilisent pour charger et télécharger des données d'objet.

Voir "Gérer les certificats de sécurité" pour plus de détails et d'instructions.

> StorageGRID gère séparément les certificats utilisés pour les terminaux de l'équilibreur de charge. Pour configurer les certificats d'équilibreur de charge, reportez-vous à la section "Configurer les terminaux de l'équilibreur de charge".

Lorsque vous utilisez des certificats de serveur personnalisés, suivez les instructions suivantes :

- Les certificats doivent avoir un `subjectAltName` Correspondant aux entrées DNS de StorageGRID. Pour plus de détails, reportez-vous à la section 4.2.1.6, «sous-objet autre nom», dans "RFC 5280 : certificat PKIX et profil CRL".
- Si possible, évitez d'utiliser des certificats génériques. À l'exception de cette règle, le certificat d'un terminal de type hébergement virtuel S3 nécessite l'utilisation d'un caractère générique si les noms de compartiment ne sont pas connus à l'avance.
- Lorsque vous devez utiliser des caractères génériques dans les certificats, vous devez prendre des mesures supplémentaires pour réduire les risques. Utilisez un motif générique comme `*.s3.example.com`, et n'utilisez pas le `s3.example.com` suffixe pour les autres applications. Ce modèle fonctionne également avec l'accès S3 de type chemin d'accès, comme `dc1-s1.s3.example.com/mybucket`.
- Définissez les délais d'expiration du certificat sur court (par exemple, 2 mois) et utilisez l'API Grid Management pour automatiser la rotation des certificats. Ceci est particulièrement important pour les certificats génériques.

En outre, les clients doivent utiliser un contrôle strict du nom d'hôte lors de la communication avec StorageGRID.

Directives de renforcement pour les règles TLS et SSH

Vous pouvez sélectionner une stratégie de sécurité pour déterminer quels protocoles et chiffrements sont utilisés pour établir des connexions TLS sécurisées avec les applications client et des connexions SSH sécurisées avec les services StorageGRID internes.

La règle de sécurité contrôle la façon dont TLS et SSH chiffrent les données en mouvement. Il est recommandé de désactiver les options de cryptage qui ne sont pas nécessaires pour assurer la compatibilité des applications. Utilisez la stratégie moderne par défaut, sauf si votre système doit être conforme aux critères communs ou si vous devez utiliser d'autres chiffrements.

Voir "Gestion des règles TLS et SSH" pour plus de détails et d'instructions.

Autres directives de durcissement

Outre les directives de renforcement des réseaux et nœuds StorageGRID, vous devez suivre les instructions de renforcement correspondant à d'autres domaines du système StorageGRID.

Journaux et messages d'audit

Protégez toujours les journaux StorageGRID et la sortie des messages d'audit de manière sécurisée. Les journaux et les messages d'audit StorageGRID fournissent des informations précieuses du point de vue du support et de la disponibilité du système. En outre, les informations figurant dans les journaux StorageGRID et dans les résultats des messages d'audit sont généralement sensibles.

Configurez StorageGRID pour envoyer des événements de sécurité à un serveur syslog externe. Si vous utilisez syslog export, sélectionnez TLS et RELP/TLS pour les protocoles de transport.

Voir la "Référence des fichiers journaux" Pour plus d'informations sur les journaux StorageGRID. Voir "Messages d'audit" Pour plus d'informations sur les messages d'audit StorageGRID.

NetApp AutoSupport

La fonction AutoSupport de StorageGRID vous permet de contrôler de manière proactive l'état de votre système et d'envoyer automatiquement des messages et des détails au support technique NetApp, à l'équipe de support interne de votre entreprise ou à un partenaire de support. Par défaut, les messages AutoSupport envoyés au support technique NetApp sont activés lorsque StorageGRID est configuré pour la première fois.

La fonction AutoSupport peut être désactivée. Cependant, NetApp recommande de l'activer, car AutoSupport accélère l'identification et la résolution des problèmes sur le système StorageGRID.

AutoSupport prend en charge les protocoles de transport HTTPS, HTTP et SMTP. En raison du caractère sensible des messages AutoSupport, NetApp recommande vivement d'utiliser le protocole de transport par défaut HTTPS pour l'envoi des messages AutoSupport au support NetApp.

Partage des ressources d'origine croisée (CORS)

Vous pouvez configurer le partage de ressources entre sources (CORS) pour un compartiment S3 si vous souhaitez que ce compartiment et ces objets soient accessibles aux applications web d'autres domaines. En général, n'activez pas les codes de commande à moins qu'ils ne soient requis. Si CORS est requis, limitez-le aux origines de confiance.

Voir les étapes pour "Configuration du partage des ressources d'origine croisée (CORS)".

Dispositifs de sécurité externes

Une solution de renforcement complète doit traiter des mécanismes de sécurité en dehors de StorageGRID. L'utilisation de dispositifs d'infrastructure supplémentaires pour filtrer et limiter l'accès à StorageGRID constitue un moyen efficace d'établir et de maintenir un niveau de sécurité strict. Ces systèmes de sécurité externes comprennent des pare-feu, des systèmes de prévention des intrusions (IDS) et d'autres dispositifs de sécurité.

Un équilibreur de charge tiers est recommandé pour le trafic client non fiable. L'équilibrage de la charge fourni par des tiers offre un meilleur contrôle et des couches de protection supplémentaires contre les attaques.

Réduction des ransomwares

Protégez vos données d'objet contre les attaques par ransomware en suivant les recommandations du "Protégez vos données contre les ransomwares avec StorageGRID".

Informations sur le copyright

Copyright © 2025 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 DÉLICTUELLE (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.