Renforcement du système

StorageGRID software

NetApp
December 03, 2025

Sommaire

Renforcement du système

Considérations générales pour le renforcement du système

Le renforcement du système est le processus consistant à éliminer autant de risques de sécurité que possible d'un système StorageGRID .

Lorsque vous installez et configurez StorageGRID, utilisez ces instructions pour vous aider à atteindre les objectifs de sécurité prescrits en matière de confidentialité, d'intégrité et de disponibilité.

Vous devriez déjà utiliser les meilleures pratiques standard de l'industrie pour le renforcement du système. Par exemple, vous utilisez des mots de passe forts pour StorageGRID, utilisez HTTPS au lieu de HTTP et activez l'authentification basée sur les certificats lorsqu'elle est disponible.

StorageGRID suit le "Politique de gestion des vulnérabilités NetApp" . Les vulnérabilités signalées sont vérifiées et traitées conformément au processus de réponse aux incidents de sécurité du produit.

Lors du renforcement d'un système StorageGRID , tenez compte des éléments suivants :

- *Lequel des trois réseaux StorageGRID * avez-vous implémenté ? Tous les systèmes StorageGRID doivent utiliser le réseau Grid, mais vous pouvez également utiliser le réseau administrateur, le réseau client ou les deux. Chaque réseau a des considérations de sécurité différentes.
- **Le type de plates-formes** que vous utilisez pour les nœuds individuels de votre système StorageGRID . Les nœuds StorageGRID peuvent être déployés sur des machines virtuelles VMware, au sein d'un moteur de conteneur sur des hôtes Linux ou en tant qu'appliances matérielles dédiées. Chaque type de plateforme possède son propre ensemble de bonnes pratiques de renforcement.
- **Dans quelle mesure les comptes des locataires sont-ils fiables**. Si vous êtes un fournisseur de services avec des comptes locataires non approuvés, vous aurez des problèmes de sécurité différents de ceux que vous rencontreriez si vous utilisiez uniquement des locataires internes approuvés.
- **Quelles exigences et conventions de sécurité** votre organisation suit. Vous devrez peut-être vous conformer à des exigences réglementaires ou d'entreprise spécifiques.

Directives de renforcement pour les mises à niveau logicielles

Vous devez maintenir votre système StorageGRID et les services associés à jour pour vous défendre 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 majeure la plus récente ou vers la version majeure précédente. Maintenir StorageGRID à jour permet de réduire la durée pendant laquelle les vulnérabilités connues sont actives et réduit la surface d'attaque globale. De plus, les versions les plus récentes de StorageGRID contiennent souvent des fonctionnalités de renforcement de la sécurité qui ne sont pas incluses dans les versions précédentes.

Consultez le "Outil de matrice d'interopérabilité NetApp" (IMT) pour déterminer quelle version du logiciel StorageGRID vous devez utiliser. Lorsqu'un correctif est requis, NetApp donne la priorité à la création de mises à jour pour les versions les plus récentes. Certains correctifs peuvent ne pas être compatibles avec les versions antérieures.

- Pour télécharger les versions et correctifs les plus récents de StorageGRID , accédez à "Téléchargements NetApp : StorageGRID" .
- Pour mettre à niveau le logiciel StorageGRID , consultez le"instructions de mise à niveau" .
- Pour appliquer un correctif, consultez le"Procédure de correctif logiciel StorageGRID" .

Mises à niveau des services externes

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

Pour une liste des versions prises en charge, consultez le "Outil de matrice d'interopérabilité NetApp" .

Mises à niveau des hyperviseurs

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

Pour une liste des versions prises en charge, consultez le "Outil de matrice d'interopérabilité NetApp" .

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 les mises à jour du noyau sont appliquées au système d'exploitation hôte. De plus, vous devez appliquer les mises à jour du micrologiciel au matériel vulnérable lorsque ces mises à jour sont disponibles.

Pour une liste des versions prises en charge, consultez le "Outil de matrice d'interopérabilité NetApp" .

Directives de renforcement pour les réseaux StorageGRID

Le système StorageGRID prend en charge jusqu'à trois interfaces réseau par nœud de grille, vous permettant de configurer la mise en réseau de chaque nœud de grille individuel afin de répondre à vos exigences de sécurité et d'accès.

Pour des informations détaillées sur les réseaux StorageGRID , consultez le"Types de réseaux StorageGRID" .

Lignes directrices pour le réseau de grille

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

Lors de la configuration du réseau Grid, suivez ces instructions :

- Assurez-vous que le réseau est sécurisé contre les clients non fiables, tels que ceux présents sur Internet ouvert.
- Dans la mesure du possible, utilisez le réseau Grid exclusivement pour le trafic interne. Le réseau d'administration et le réseau client disposent tous deux de restrictions de pare-feu supplémentaires 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 centres de données, utilisez un réseau privé virtuel (VPN) ou équivalent sur le réseau Grid pour fournir une protection supplémentaire au trafic interne.
- Certaines procédures de maintenance nécessitent un accès Secure Shell (SSH) sur le port 22 entre le nœud d'administration principal et tous les autres nœuds de grille. Utilisez un pare-feu externe pour restreindre l'accès SSH aux clients de confiance.

Directives pour le réseau d'administration

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

Si vous utilisez le réseau d'administration, suivez ces instructions :

- Bloquez tous les ports de trafic internes sur le réseau d'administration. Voir le"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.

Lignes directrices pour le réseau de clients

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 plateforme. Cependant, StorageGRID n'applique pas cette utilisation en interne.

Si vous utilisez le réseau client, suivez ces directives :

- Bloquez tous les ports de trafic internes sur le réseau client. Voir le"liste des ports internes" .
- Acceptez le trafic client entrant uniquement sur les points de terminaison explicitement configurés. Voir les informations sur"gestion des contrôles du pare-feu" .

Directives de renforcement pour les nœuds StorageGRID

Les nœuds StorageGRID peuvent être déployés sur des machines virtuelles VMware, au sein d'un moteur de conteneur sur des hôtes Linux ou en tant qu'appliances matérielles dédiées. Chaque type de plateforme et chaque type de nœud possède son propre ensemble de bonnes pratiques de renforcement.

Contrôler l'accès IPMI à distance au BMC

Vous pouvez activer ou désactiver l'accès IPMI à distance pour tous les appareils contenant un BMC. L'interface IPMI distante permet l'accès matériel de bas niveau à vos appliances StorageGRID par toute personne disposant d'un compte BMC et d'un mot de passe. Si vous n'avez pas besoin d'un accès IPMI à distance au BMC, désactivez cette option.

- Pour contrôler l'accès IPMI à distance au BMC dans Grid Manager, accédez à **CONFIGURATION** > **Sécurité** > **Paramètres de sécurité** > **Appliances** :
  - Décochez la case **Activer l'accès IPMI à distance** pour désactiver l'accès IPMI au BMC.
  - Cochez la case **Activer l'accès IPMI à distance** pour activer l'accès IPMI au BMC.

Configuration du pare-feu

Dans le cadre du processus de renforcement du système, vous devez vérifier les configurations du pare-feu externe 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 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. Tu devrais"gérer les contrôles du pare-feu interne" 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.

Plus précisément, vous pouvez gérer ces domaines :

- **Adresses privilégiées** : Vous pouvez autoriser les adresses IP ou les sous-réseaux sélectionnés 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 de protection supplémentaire contre certaines menaces courantes, il ne supprime pas le besoin d'un pare-feu externe.

Pour une liste de tous les ports internes et externes utilisés par StorageGRID, voir"Référence du port réseau" .

Désactiver les services inutilisés

Pour tous les nœuds StorageGRID , vous devez désactiver ou bloquer l'accès aux services inutilisés. Par exemple, si vous ne prévoyez pas d'utiliser DHCP, utilisez le gestionnaire de grille pour fermer le port 68. Sélectionnez **CONFIGURATION** > **Contrôle du pare-feu** > **Gérer l'accès externe**. Modifiez ensuite le statut du port 68 de **Ouvert** à **Fermé**.

Virtualisation, conteneurs et matériel partagé

Pour tous les nœuds StorageGRID , évitez d'exécuter StorageGRID sur le même matériel physique que des logiciels non approuvés. Ne présumez pas que les protections de l'hyperviseur empêcheront 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 Spectre exploitent les vulnérabilités critiques des 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 via le réseau lorsque les nœuds sont en cours d'installation. Les nœuds ne sont pas totalement sécurisés tant qu'ils n'ont pas rejoint le réseau.

Directives pour les nœuds d'administration

Les nœuds d'administration fournissent des services de gestion tels que la configuration du système, la surveillance et la journalisation. Lorsque vous vous connectez au gestionnaire de grille ou au gestionnaire de

locataires, vous vous connectez à un nœud d'administration.

Suivez ces instructions pour sécuriser les nœuds d'administration de votre système StorageGRID :

- Sécurisez tous les nœuds d'administration contre les clients non fiables, tels que ceux présents sur Internet ouvert. Assurez-vous qu'aucun client non approuvé ne peut accéder à un nœud d'administration sur le réseau de grille, 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 points de terminaison d'équilibrage de charge StorageGRID , utilisez des nœuds de passerelle au lieu des nœuds d'administration pour le trafic client non approuvé.
- Si vous avez des locataires non approuvés, ne leur permettez pas d'avoir un accès direct au gestionnaire de locataires ou à l'API de gestion des locataires. Au lieu de cela, demandez à tous les locataires non approuvés d'utiliser un portail de locataires ou un système de gestion de locataires externe, qui interagit avec l'API de gestion des locataires.
- Vous pouvez également utiliser un proxy d'administration pour un meilleur contrôle sur la communication AutoSupport des nœuds d'administration vers le support NetApp . Voir les étapes pour"création d'un proxy d'administration" .
- Vous pouvez également utiliser les ports restreints 8443 et 9443 pour séparer les communications de Grid Manager et de Tenant Manager. Bloquez le port partagé 443 et limitez les demandes des locataires au port 9443 pour une protection supplémentaire.
- Vous pouvez également utiliser des nœuds d'administration distincts pour les administrateurs de grille et les utilisateurs locataires.

Pour plus d'informations, consultez les instructions pour"administrer StorageGRID" .

Directives pour les nœuds de stockage

Les nœuds de stockage gèrent et stockent les données et les métadonnées des objets. Suivez ces directives pour sécuriser les nœuds de stockage dans votre système StorageGRID .

- N'autorisez pas les clients non approuvés à se connecter directement aux nœuds de stockage. Utilisez un point de terminaison d'équilibrage de charge servi 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 d'un compte pour un locataire non approuvé, n'autorisez pas le locataire à utiliser sa propre source d'identité et n'autorisez pas l'utilisation des services de la plateforme. Voir les étapes pour"créer un compte locataire" .
- Utilisez un équilibreur de charge tiers pour le trafic client non fiable. L'équilibrage de charge tiers offre davantage de contrôle et des couches de protection supplémentaires contre les attaques.
- Vous pouvez également utiliser un proxy de stockage pour un meilleur contrôle sur les pools de stockage Cloud et la communication des services de plateforme des nœuds de stockage vers les services externes. Voir les étapes pour"création d'un proxy de stockage" .
- En option, connectez-vous à des services externes à l'aide du réseau client. Ensuite, sélectionnez **CONFIGURATION** > **Sécurité** > **Contrôle du pare-feu** > **Réseaux clients non approuvés** et indiquez que le réseau client sur le nœud de stockage n'est pas approuvé. Le nœud de stockage n'accepte plus aucun trafic entrant sur le réseau client, mais il continue d'autoriser les demandes sortantes pour les services de plate-forme.

Directives pour les nœuds de passerelle

Les nœuds de passerelle fournissent une interface d'équilibrage de charge facultative que les applications clientes peuvent utiliser pour se connecter à StorageGRID. Suivez ces directives pour sécuriser tous les nœuds de passerelle de votre système StorageGRID :

- Configurer et utiliser les points de terminaison de l'équilibreur 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 approuvé. L'équilibrage de charge tiers offre davantage de contrôle et des couches de protection supplémentaires contre les attaques. Si vous utilisez un équilibreur de charge tiers, le trafic réseau peut toujours être configuré pour passer par un point de terminaison d'équilibreur de charge interne ou être envoyé directement aux nœuds de stockage.
- Si vous utilisez des points de terminaison d'équilibrage de charge, vous pouvez éventuellement demander aux clients de se connecter via le réseau client. Ensuite, sélectionnez **CONFIGURATION** > **Sécurité** > **Contrôle du pare-feu** > **Réseaux clients non approuvés** et indiquez que le réseau client sur le nœud de passerelle n'est pas approuvé. Le nœud de passerelle accepte uniquement le trafic entrant sur les ports explicitement configurés comme points de terminaison d'équilibrage de charge.

Directives pour les nœuds d'appareils matériels

Les appareils matériels StorageGRID sont spécialement conçus pour être utilisés dans un système StorageGRID . Certains appareils peuvent être utilisés comme nœuds de stockage. D'autres appareils peuvent être utilisés comme nœuds d'administration ou nœuds de passerelle. Vous pouvez combiner des nœuds d'appareils avec des nœuds basés sur des logiciels ou déployer des grilles entièrement conçues et composées d'appareils.

Suivez ces instructions pour sécuriser tous les nœuds d'appareils matériels de votre système StorageGRID :

- Si l'appliance utilise SANtricity System Manager pour la gestion du contrôleur de stockage, empêchez les clients non approuvés d'accéder à SANtricity System Manager via le réseau.
- Si l'appareil dispose d'un contrôleur de gestion de la carte mère (BMC), sachez que le port de gestion BMC permet un accès matériel de bas niveau. Connectez le port de gestion BMC uniquement à un réseau de gestion interne sécurisé et fiable. Si aucun réseau de ce type n'est disponible, laissez le port de gestion BMC déconnecté ou bloqué, sauf si une connexion BMC est demandée par le support technique.
- Si l'appareil 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 approuvé sur le port 623.

> Vous pouvez activer ou désactiver l'accès IPMI à distance pour tous les appareils contenant un BMC. L'interface IPMI distante permet l'accès matériel de bas niveau à vos appliances StorageGRID par toute personne disposant d'un compte BMC et d'un mot de passe. Si vous n'avez pas besoin d'un accès IPMI à distance au BMC, désactivez cette option à l'aide de l'une des méthodes suivantes : + Dans Grid Manager, accédez à **CONFIGURATION** > **Sécurité** > **Paramètres de sécurité** > **Appliances** et décochez la case **Activer l'accès IPMI à distance**. + Dans l'API de gestion de grille, utilisez le point de terminaison privé : `PUT /private/bmc` .

- Pour les modèles d'appareils contenant des disques SED, FDE ou FIPS NL-SAS que vous gérez avec SANtricity System Manager, "activer et configurer SANtricity Drive Security" .
- Pour les modèles d'appareils contenant des SSD NVMe SED ou FIPS que vous gérez à l'aide du programme d'installation de l'appareil StorageGRID et du gestionnaire de grille, "activer et configurer le chiffrement du lecteur StorageGRID" .

- Pour les appareils sans lecteurs SED, FDE ou FIPS, activez et configurez le chiffrement des nœuds logiciels StorageGRID "en utilisant un serveur de gestion de clés (KMS)" .

Directives de renforcement pour TLS et SSH

Vous devez remplacer les certificats par défaut créés lors de l'installation et sélectionner la politique 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 Web StorageGRID n'est pas conforme à leurs politiques de sécurité des informations. 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** : utilisé pour sécuriser l'accès aux nœuds de stockage et aux nœuds de passerelle, que les applications clientes S3 utilisent pour télécharger et charger 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 points de terminaison de l'équilibreur de charge. Pour configurer les certificats d'équilibrage de charge, voir"Configurer les points de terminaison de l'équilibreur de charge" .

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

- Les certificats doivent avoir un `subjectAltName` qui correspond aux entrées DNS pour StorageGRID. Pour plus de détails, voir la section 4.2.1.6, « Nom alternatif du sujet », dans "RFC 5280 : Certificat PKIX et profil CRL" .
- Dans la mesure du possible, évitez l'utilisation de certificats génériques. Une exception à cette directive est le certificat d'un point de terminaison de style hébergé virtuel S3, qui 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 modèle générique tel que `*.s3.example.com` , et n'utilisez pas le `s3.example.com` suffixe pour d'autres applications. Ce modèle fonctionne également avec l'accès S3 de type chemin, tel que `dc1-s1.s3.example.com/mybucket` .
- Définissez les délais d'expiration des certificats sur une durée courte (par exemple, 2 mois) et utilisez l'API Grid Management pour automatiser la rotation des certificats. Ceci est particulièrement important pour les certificats génériques.

De plus, les clients doivent utiliser une vérification stricte du nom d'hôte lors de la communication avec StorageGRID.

Directives de renforcement des politiques TLS et SSH

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

La politique de sécurité contrôle la manière dont TLS et SSH chiffrent les données en mouvement. En tant que bonne pratique, vous devez désactiver les options de chiffrement qui ne sont pas nécessaires à la compatibilité des applications. Utilisez la politique moderne par défaut, sauf si votre système doit être conforme aux critères communs ou si vous devez utiliser d'autres chiffrements.

Voir"Gérer la politique TLS et SSH" pour plus de détails et d'instructions.

Autres directives de durcissement

En plus de suivre les directives de renforcement pour les réseaux et les nœuds StorageGRID , vous devez suivre les directives de renforcement pour les autres zones du système StorageGRID .

Mot de passe d'installation temporaire

Pour sécuriser le système StorageGRID pendant l'installation, définissez un mot de passe sur la page de mot de passe du programme d'installation temporaire dans l'interface utilisateur d'installation de StorageGRID ou dans l'API d'installation. Une fois défini, ce mot de passe s'applique à toutes les méthodes d'installation de StorageGRID, y compris l'interface utilisateur, l'API d'installation et `configure-storagegrid.py` scénario.

Pour plus d'informations, reportez-vous à :

- "Installer StorageGRID sur Red Hat Enterprise Linux"
- "Installer StorageGRID sur Ubuntu ou Debian"
- "Installer StorageGRID sur VMware"
- "Installer l'appliance 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. De plus, les informations et les détails contenus dans les journaux StorageGRID et dans la sortie des messages d'audit sont généralement de nature sensible.

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

Voir le"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 fonctionnalité AutoSupport de StorageGRID vous permet de surveiller de manière proactive l'état de votre système et d'envoyer automatiquement des packages au site de support NetApp , à l'équipe de support interne de votre organisation ou à un partenaire de support. Par défaut, l'envoi de packages AutoSupport à

NetApp est activé lorsque StorageGRID est configuré pour la première fois.

La fonction AutoSupport peut être désactivée. Cependant, NetApp recommande de l'activer car AutoSupport permet d'accélérer l'identification et la résolution des problèmes en cas de problème sur votre système StorageGRID .

AutoSupport prend en charge HTTPS, HTTP et SMTP pour les protocoles de transport. En raison de la nature sensible des packages AutoSupport , NetApp recommande fortement d'utiliser HTTPS comme protocole de transport par défaut pour l'envoi de packages AutoSupport à NetApp.

Partage de ressources inter-origines (CORS)

Vous pouvez configurer le partage de ressources inter-origines (CORS) pour un bucket S3 si vous souhaitez que ce bucket et les objets qu'il contient soient accessibles aux applications Web d'autres domaines. En général, n'activez pas CORS à moins que cela ne soit nécessaire. Si CORS est requis, limitez-le aux origines fiables.

Voir les étapes pour"configuration du partage de ressources inter-origines (CORS)" .

Dispositifs de sécurité externes

Une solution de renforcement complète doit aborder les mécanismes de sécurité en dehors de StorageGRID. L'utilisation de périphériques d'infrastructure supplémentaires pour filtrer et limiter l'accès à StorageGRID est un moyen efficace d'établir et de maintenir une posture de sécurité stricte. Ces dispositifs de sécurité externes comprennent des pare-feu, des systèmes de prévention des intrusions (IPS) et d'autres dispositifs de sécurité.

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

Atténuation des risques de ransomware

Aidez à protéger vos données d'objet contre les attaques de ransomware en suivant les recommandations de "Défense contre les ransomwares avec StorageGRID" .

Informations sur le copyright

Informations sur les marques commerciales