Renforcement du système pour StorageGRID

StorageGRID software

NetApp
February 12, 2026

Sommaire

Renforcement du système pour StorageGRID

Découvrez le renforcement du système pour StorageGRID

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

Lors de l'installation et de la configuration de StorageGRID, suivez 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. Ces meilleures pratiques doivent inclure la sécurité physique et environnementale qui limite l'accès physique et protège le centre de données physique et l'infrastructure de support. Vous devez également vous référer à toutes les normes et recommandations réglementaires applicables à votre entreprise et à votre zone géographique.

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.

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

- **Lequel des trois réseaux StorageGRID** que vous avez mis en œuvre. 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.
- **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 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.
- **Comment les comptes de locataires sont approuvés**. 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** que votre organisation suit. Vous devrez peut-être vous conformer à des exigences réglementaires ou d'entreprise spécifiques.

Recommandations de renforcement pour les mises à niveau logicielles StorageGRID

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.

Consultez 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 "Téléchargement NetApp : StorageGRID".
- Pour mettre à niveau le logiciel StorageGRID, reportez-vous au "instructions de mise à niveau".
- Pour appliquer un correctif, consultez le "Procédure de correctif StorageGRID".

Mises à niveau vers des services externes

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

Pour obtenir la liste des versions prises en charge, reportez-vous au "Matrice d'interopérabilité NetApp" .

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.

Pour obtenir la liste des versions prises en charge, reportez-vous au "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 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.

Pour obtenir la liste des versions prises en charge, reportez-vous au "Matrice d'interopérabilité NetApp" .

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.

Contrôler l'accès IPMI à distance au BMC

Vous pouvez activer ou désactiver l'accès IPMI à distance pour tous les dispositifs contenant un contrôleur BMC. L'interface IPMI distante permet à toute personne disposant d'un compte BMC et d'un mot de passe d'accéder à votre matériel de bas niveau à vos appliances StorageGRID. Si vous n'avez pas besoin d'un accès IPMI à distance au contrôleur 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 distant** pour désactiver l'accès IPMI au contrôleur BMC.
  - Cochez la case **Activer l'accès IPMI distant** pour activer l'accès IPMI au contrôleur BMC.

Pour plus d'informations sur le renforcement du BMC , consultez le "Contrôleurs de gestion de la carte mère Harden" fiche d'information sur la cybersécurité du "Agence de sécurité nationale (NSA)" et "Agence de cybersécurité et de sécurité des infrastructures (CISA)" .

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 devez "gérer les contrôles de pare-feu internes"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 une liste de tous les ports internes et externes utilisés par StorageGRID, voir"Ports internes StorageGRID" et"Ports utilisés pour les communications externes" .

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 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.

Limiter l’accès physique au matériel

Vous devez limiter l’accès physique aux nœuds de l’appliance matérielle StorageGRID ainsi qu’aux hôtes de machines virtuelles VMware et aux hôtes Linux exécutant StorageGRID aux seuls administrateurs autorisés. Certains exemples de contrôles d’accès physiques comprennent les serrures, les gardes, les barrières physiques et la vidéosurveillance.

Les nœuds d’appareils matériels sont conçus pour être installés et exploités uniquement par des administrateurs autorisés. N’autorisez pas les administrateurs non autorisés à accéder aux nœuds de l’appliance matérielle.

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 davantage de contrôle sur la communication AutoSupport entre les nœuds d’administration et le support NetApp. Voir les étapes pour "création d’un proxy d’administration".
- 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 "Administration d’StorageGRID"de .

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 davantage de contrôle sur les pools de stockage cloud et la communication des services de plateforme depuis les 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.

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, 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.

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'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.

  Vous pouvez établir un VLAN pour isoler les connexions réseau BMC et restreindre l'accès Internet BMC aux réseaux approuvés. Pour plus d'informations sur l'application de la séparation VLAN, consultez le "Contrôleurs de gestion de la carte mère Harden" fiche d'information sur la cybersécurité du "Agence de

sécurité nationale (NSA)" et "Agence de cybersécurité et de sécurité des infrastructures (CISA)" .

Si un réseau de gestion interne sécurisé et fiable n'est pas disponible, laissez le port de gestion BMC déconnecté ou bloqué. Le support technique peut demander un accès temporaire pendant une demande d'assistance.

- 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 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` .

+ Vous pouvez égalementdésactiver l'accès IPMI à distance .

- Pour les modèles d'appliance contenant des disques SED, FDE ou NL-SAS FIPS que vous gérez avec SANtricity System Manager "Activez et configurez la sécurité des lecteurs SANtricity".
- 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, "Activez et configurez le chiffrement de lecteur StorageGRID" .
- Pour les appareils sans lecteurs SED, FDE ou FIPS, utilisez un serveur de gestion de clés (KMS) pour "activer et configurer le chiffrement du nœud logiciel StorageGRID" .

Informations associées

"En savoir plus sur la sécurité des lecteurs dans SANtricity System Manager"

Recommandations de renforcement pour TLS et SSH dans StorageGRID

Vous devez contrôler l'accès SSH, remplacer les certificats TLS par défaut 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 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** : utilisé pour sécuriser l'accès aux nœuds de stockage et aux nœuds de passerelle, que

les applications clientes S3 utilisent pour télécharger 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 "Configurer les terminaux de l'équilibreur de charge"la section .

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

- Les certificats doivent avoir un *`subjectAltName`* qui correspond aux entrées DNS pour StorageGRID. Pour plus de détails, reportez-vous à la section 4.2.1.6, « Nom alternatif du sujet », 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 modèle générique tel que `*.s3.example.com`, et n'utilisez pas le `s3.example.com` suffixe pour d'autres applications. Ce schéma fonctionne également avec l'accès S3 de style chemin d'accès, tel que `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 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, à la norme FIPS 140-2 ou si vous devez utiliser d'autres chiffrements.

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

Gérer l'accès SSH externe

Pour améliorer la sécurité du système, l'accès SSH externe est bloqué par défaut. Activez l'accès SSH uniquement lorsque vous devez effectuer des tâches nécessitant un accès SSH entrant, comme le dépannage. Se référer à"Gérer l'accès SSH externe" pour plus de détails et d'instructions.

Recommandations de renforcement pour les journaux, les mots de passe et les messages d'audit dans StorageGRID

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.

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 temporaire du programme d'installation dans l'interface utilisateur d'installation de StorageGRID ou dans l'API d'installation. Lorsqu'il est 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` le script.

Pour plus d'informations, se reporter à :

- "Installer StorageGRID sur des nœuds logiciels"
- "Installez 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. 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.

Pour plus d'informations sur les journaux StorageGRID, reportez-vous à la section"Référence des fichiers journaux". Pour plus d'informations sur les messages d'audit StorageGRID, reportez-vous à la section"Messages d'audit".

NetApp AutoSupport

La fonctionnalité AutoSupport de StorageGRID vous permet de contrôler de manière proactive l'état de votre système et d'envoyer automatiquement des packages sur le site de support NetApp, l'équipe de support interne de votre entreprise ou 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 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 de la nature sensible des packages AutoSupport, NetApp recommande vivement d'utiliser HTTPS comme protocole de transport par défaut pour l'envoi des packages AutoSupport à 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 de CORS pour les buckets et les objets" .

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 de la section "Protégez vos données contre les ransomwares avec StorageGRID".