Renforcement du système pour StorageGRID

StorageGRID software

NetApp
July 23, 2026

Sommaire

Renforcement du système pour StorageGRID

Découvrez le renforcement du système pour StorageGRID

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

Lors de l'installation et de la configuration de 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 appliquer les meilleures pratiques du secteur en matière de renforcement de la sécurité des systèmes. Par exemple, vous utilisez des mots de passe robustes pour StorageGRID, utilisez HTTPS au lieu de HTTP et activez l'authentification basée sur des certificats lorsque cela est possible. Ces meilleures pratiques doivent inclure des mesures de sécurité physique et environnementale qui limitent l'accès physique ainsi que la protection du centre de données physique et de l'infrastructure de support. Vous devez également vous référer à toute norme et recommandation réglementaire applicable à votre entreprise et à votre zone géographique.

StorageGRID suit la procédure "Politique de gestion des vulnérabilités NetApp". Les vulnérabilités signalées sont vérifiées et traitées conformément au processus de réponse aux incidents de sécurité des produits.

Lors du renforcement de la sécurité d'un système StorageGRID, tenez compte des points 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 Admin, le réseau Client, ou les deux. Chaque réseau présente des considérations de sécurité différentes.
- **Le type de plateformes** que vous utilisez pour les différents nœuds de votre système StorageGRID. Les nœuds StorageGRID peuvent être déployés sur des machines virtuelles VMware, dans un moteur de conteneurs sur des hôtes Linux, ou sous forme d'appliances matérielles dédiées. Chaque type de plateforme possède ses propres bonnes pratiques de sécurisation.
- **Degré de confiance des comptes locataires**. Si vous êtes un fournisseur de services utilisant des comptes locataires non fiables, vos préoccupations en matière de sécurité différeront de celles liées à l'utilisation exclusive de comptes locataires internes de confiance.
- **Quelles exigences et conventions de sécurité** votre organisation suit. Vous pourriez devoir respecter des exigences réglementaires ou internes spécifiques.

Recommandations de renforcement pour les mises à niveau logicielles StorageGRID

Vous devez maintenir votre système StorageGRID et les services associés à jour afin de 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 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 de réduire la surface globale d'attaque. 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 antérieures.

Consultez l' "Outil NetApp Interoperability Matrix Tool"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, rendez-vous sur "NetApp Téléchargements : StorageGRID".
- Pour mettre à niveau le logiciel StorageGRID, consultez le "instructions de mise à niveau".
- Pour appliquer un correctif, consultez le "Procédure de correctif StorageGRID".

Mises à niveau 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, consultez la "Outil NetApp Interoperability Matrix Tool".

Mises à niveau des hyperviseurs

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

Pour obtenir la liste des versions prises en charge, consultez la "Outil NetApp Interoperability Matrix Tool".

Mises à niveau des nœuds Linux

Si vos nœuds StorageGRID utilisent des plateformes 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 firmware au matériel vulnérable dès que ces mises à jour sont disponibles.

Pour obtenir la liste des versions prises en charge, consultez la "Outil NetApp Interoperability Matrix Tool".

Recommandations de renforcement pour les réseaux StorageGRID

Le système StorageGRID prend en charge jusqu'à trois interfaces réseau par nœud de grille, ce qui vous permet de configurer le réseau de chaque nœud de grille individuellement 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 Grid

Vous devez configurer un réseau Grid pour tout le trafic interne de StorageGRID. Tous les nœuds du réseau Grid sont sur le réseau Grid 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 protégé contre les clients non fiables, tels que ceux présents sur l'internet ouvert.

- Dans la mesure du possible, utilisez le réseau Grid exclusivement pour le trafic interne. Les réseaux Admin et Client disposent 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 un équivalent sur le réseau Grid pour assurer une protection supplémentaire du 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 du grid. 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 (par des employés autorisés 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'impose pas cette utilisation en interne.

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

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

Lignes directrices pour le réseau client

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

Si vous utilisez le réseau client, suivez ces directives :

- Bloquez tous les ports de trafic interne sur le réseau client. Voir le "liste des ports internes".
- N'acceptez le trafic client entrant que sur les points de terminaison explicitement configurés. Consultez les informations à propos de "gestion des contrôles de pare-feu".

Recommandations 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 sous forme d'appliances matérielles dédiées. Chaque type de plateforme et chaque type de nœud possède ses propres bonnes pratiques de sécurisation.

Contrôlez l'accès IPMI distant au BMC

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

- Pour contrôler l'accès IPMI à distance au BMC dans Grid Manager, allez dans **Configuration** > **Sécurité** > **Paramètres de sécurité** > **Appareils** :
  - Décochez la case **Activer l'accès IPMI à distance** pour désactiver l'accès IPMI au BMC.
  - Sélectionnez la case à cocher **Activer l'accès IPMI à distance** pour activer l'accès IPMI au BMC.

Pour plus d'informations sur le renforcement de la sécurité de BMC, consultez la "Renforcez les Baseboard Management Controllers" fiche d'information sur la cybersécurité de la "National Security Agency (NSA)" et la "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 des pare-feu externes et les modifier afin que le trafic ne soit accepté qu'à partir des adresses IP et sur les ports à partir desquels il est strictement nécessaire.

StorageGRID intègre un pare-feu interne sur chaque nœud, renforçant ainsi la sécurité de votre grille en vous permettant de contrôler l'accès réseau au nœud. Vous devez "gérer les contrôles du pare-feu interne" pour empêcher l'accès réseau sur tous les ports, à l'exception de ceux nécessaires au déploiement spécifique de votre grille. 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 les domaines suivants :

- **Adresses privilégiées** : Vous pouvez autoriser certaines adresses IP ou certains sous-réseaux à accéder à des ports fermés par les paramètres de l'onglet Manage external access.
- **Gérer l'accès externe** : Vous pouvez fermer les ports ouverts par défaut ou rouvrir les ports précédemment fermés.
- **Réseau client non fiable** : Vous pouvez spécifier si un nœud fait confiance au trafic entrant provenant du réseau client, ainsi que les ports supplémentaires que vous souhaitez ouvrir lorsque le réseau client non fiable est configuré.

Bien que ce pare-feu interne offre une couche de protection supplémentaire 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, consultez "Ports internes de StorageGRID" et "Ports utilisés pour les communications externes".

Désactivez 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 Grid Manager pour fermer le port 68. Sélectionnez **Configuration** > **Contrôle du pare-feu** > **Gérer l'accès externe**. Ensuite, modifiez 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 fiables. Ne supposez 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 des vulnérabilités critiques dans les processeurs modernes et permettent à des programmes de voler des données en mémoire sur le même ordinateur.

Protégez les nœuds pendant l'installation

N'autorisez pas les utilisateurs non approuvés à accéder aux nœuds StorageGRID via le réseau pendant leur installation. 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 des appliances matérielles StorageGRID, ainsi qu'aux hôtes de machines virtuelles VMware et aux hôtes Linux exécutant StorageGRID, aux seuls administrateurs autorisés. Quelques exemples de contrôles d'accès physique incluent les serrures, les agents de sécurité, les barrières physiques et la vidéosurveillance.

Les nœuds matériels sont conçus pour être installés et utilisés uniquement par des administrateurs autorisés. N'autorisez pas les administrateurs non autorisés à accéder aux nœuds matériels.

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 Grid Manager ou au Tenant Manager, 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, notamment ceux situés sur Internet. Assurez-vous qu'aucun client non fiable ne puisse 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. Attribuez 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 de nœuds d'administration pour le trafic client non fiable.
- Si vous avez des locataires non fiables, ne leur accordez pas d'accès direct au Tenant Manager ni à l'API de gestion des locataires. À la place, demandez à ces locataires non fiables d'utiliser un portail locataire ou un système de gestion des locataires externe, qui interagit avec l'API de gestion des locataires.
- Vous pouvez également utiliser un proxy d'administration pour un meilleur contrôle des communications AutoSupport des nœuds d'administration vers le support NetApp. Consultez la procédure pour "création d'un proxy d'administration".
- Vous pouvez utiliser les ports restreints 8443 et 9443 pour séparer les communications entre Grid Manager et Tenant Manager. Bloquez le port partagé 443 et limitez les requêtes 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 "administration de StorageGRID".

Directives relatives aux nœuds de stockage

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

- N'autorisez pas les clients non fiables à se connecter directement aux nœuds de stockage. Utilisez un

point de terminaison d'équilibrage de charge fourni 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 sa propre source d'identité et n'autorisez pas l'utilisation des services de la plateforme. Consultez la procédure pour "création d'un compte locataire".
- Utilisez un répartiteur de charge tiers pour le trafic des clients non fiables. L'équilibrage de charge tiers offre un meilleur contrôle et des niveaux de protection supplémentaires contre les attaques.
- Vous pouvez également utiliser un proxy de stockage pour un contrôle accru des Cloud Storage Pools et des communications des services de plateforme des nœuds de stockage vers les services externes. Consultez les étapes pour "création d'un proxy de stockage".
- Vous pouvez éventuellement vous connecter à des services externes via le Client Network. Ensuite, sélectionnez **Configuration** > **Security** > **Firewall control** > **Untrusted Client Networks** et indiquez que le Client Network sur le Storage Node n'est pas approuvé. Le Storage Node n'accepte plus aucun trafic entrant sur le Client Network, mais continue d'autoriser les requêtes sortantes pour les Platform Services.

Directives pour les nœuds de passerelle

Les nœuds de passerelle offrent une interface d'équilibrage de charge optionnelle permettant aux applications clientes de se connecter à StorageGRID. Suivez ces instructions pour sécuriser les nœuds de passerelle de votre système StorageGRID :

- Configurez et utilisez 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 fiable. L'équilibrage de charge tiers offre un meilleur contrôle et une protection renforcée contre les attaques. Si vous utilisez un équilibreur de charge tiers, le trafic réseau peut toujours être configuré pour transiter par un point de terminaison d'équilibrage 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 faire en sorte que les clients se connectent 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 passerelle n'est pas approuvé. Le nœud passerelle n'accepte le trafic entrant que sur les ports explicitement configurés comme points de terminaison d'équilibrage de charge.

Directives relatives aux nœuds d'appliances matérielles

Les appliances matérielles StorageGRID sont spécialement conçues pour être utilisées dans un système StorageGRID. Certaines appliances peuvent être utilisées comme nœuds de stockage. D'autres appliances peuvent être utilisées comme nœuds d'administration ou nœuds passerelle. Vous pouvez combiner des nœuds appliances avec des nœuds logiciels ou déployer des grilles entièrement composées d'appliances.

Suivez ces instructions pour sécuriser les nœuds matériels de votre système StorageGRID :

- 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 via le réseau.
- Si l'appareil est équipé d'un contrôleur de gestion de carte mère (BMC), sachez que le port de gestion du BMC permet un accès matériel de bas niveau. Connectez le port de gestion du BMC uniquement à un réseau de gestion interne sécurisé et de confiance.

  Vous pouvez établir un VLAN pour isoler les connexions réseau BMC et restreindre l'accès Internet du

BMC aux réseaux de confiance. Pour plus d'informations sur l'application de la séparation par VLAN, consultez la "Renforcez les Baseboard Management Controllers" fiche d'information sur la cybersécurité de la "National Security Agency (NSA)" et de la "Agence de cybersécurité et de sécurité des infrastructures (CISA)".

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

- Si l'appareil prend en charge la gestion à distance du matériel du contrôleur via Ethernet à l'aide de la norme Intelligent Platform Management Interface (IPMI), bloquez le trafic non fiable sur le port 623.

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

+ Vous pouvez aussi désactiver l'accès IPMI à distance.

- Pour les modèles d'appliances 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'appliances contenant des SSD NVMe SED ou FIPS que vous gérez à l'aide de StorageGRID Appliance Installer et de Grid Manager, "activer et configurer le chiffrement des disques StorageGRID".
- Pour les appareils sans disques SED, FDE ou FIPS, utilisez un serveur de gestion de clés (KMS) pour "activer et configurer le chiffrement du nœud logiciel StorageGRID".

Informations connexes

"Découvrez la sécurité des disques 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 pour les 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 à StorageGRID n'est pas conforme à leurs politiques de sécurité informatique. 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 devriez 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 de gestion du Grid et à l'API de gestion du Tenant.
- **Certificat API S3** : Utilisé pour sécuriser l'accès aux nœuds de stockage et aux nœuds de passerelle, que les applications clientes S3 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 points de terminaison de l'équilibreur de charge. Pour configurer les certificats de l'équilibreur de charge, consultez "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` correspondant aux entrées DNS de StorageGRID. Pour plus de détails, consultez la section 4.2.1.6, « Subject Alternative Name », dans "RFC 5280 : Profil de certificat et de liste de révocation de certificats PKIX".
- Dans la mesure du possible, évitez l'utilisation de certificats génériques. Une exception à cette règle concerne le certificat d'un endpoint S3 de type hébergement virtuel, qui requiert l'utilisation d'un caractère générique si les noms de buckets 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 de caractère 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 par chemin, tel que `dc1-s1.s3.example.com/mybucket`.
- Définissez des durées d'expiration courtes pour les certificats (par exemple, 2 mois) et utilisez l'API de gestion de la grille 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 pour la politique TLS et SSH

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

La politique de sécurité contrôle la façon dont TLS et SSH chiffrent les données en transit. En tant que bonne pratique, vous devez désactiver les options de chiffrement qui ne sont pas requises pour la compatibilité des applications. Utilisez la politique Moderne par défaut, sauf si votre système doit être conforme aux Common Criteria, à la norme FIPS 140-2, ou si vous devez utiliser d'autres algorithmes de chiffrement.

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

Gérer l'accès SSH externe

Pour renforcer la sécurité du système, l'accès SSH externe est bloqué par défaut. N'activez l'accès SSH que lorsque vous devez effectuer des tâches nécessitant un accès SSH entrant, comme le dépannage. Consultez "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

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

Mot de passe d'installation temporaire

Pour sécuriser le système StorageGRID lors de l'installation, définissez un mot de passe sur la page de mot de passe temporaire de l'installateur 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 le script `configure-storagegrid.py`.

Pour plus d'informations, consultez :

- "Installer StorageGRID sur des nœuds logiciels"
- "Installer l'appliance StorageGRID"

Journaux et messages d'audit

Protégez toujours les journaux et la sortie des messages d'audit StorageGRID de manière sécurisée. Les journaux et les messages d'audit StorageGRID fournissent des informations inestimables du point de vue du support et de la disponibilité du système. De plus, les informations et les détails contenus dans les journaux et la sortie des messages d'audit StorageGRID sont généralement de nature sensible.

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

Consultez la "Référence aux fichiers journaux" pour plus d'informations sur les journaux StorageGRID. Consultez "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 paquets 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 paquets AutoSupport à NetApp est activé lors de la première configuration de StorageGRID.

La fonctionnalité AutoSupport peut être désactivée. Cependant, NetApp recommande de l'activer, car AutoSupport aide à accélérer l'identification et la résolution des problèmes si un incident survient sur votre système StorageGRID.

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

Partage de ressources entre origines (CORS)

Vous pouvez configurer le partage de ressources entre origines (CORS) pour un compartiment S3 si vous souhaitez que ce compartiment et les objets qu'il contient soient accessibles aux applications web d'autres domaines. En règle générale, n'activez pas CORS sauf si cela est requis. Si CORS est requis, limitez-le aux

origines de confiance.

Consultez les étapes pour "Configuration de CORS pour les compartiments et les objets".

Dispositifs de sécurité externes

Une solution de renforcement de sécurité complète doit prendre en compte les mécanismes de sécurité externes à StorageGRID. L'utilisation de dispositifs 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 les pare-feu, les systèmes de prévention des intrusions (IPS) et d'autres dispositifs de sécurité.

Il est recommandé d'utiliser un répartiteur de charge tiers pour le trafic des clients non fiables. Le répartition de charge tiers offre un meilleur contrôle et des couches de protection supplémentaires contre les attaques.

Atténuation des ransomwares

Aidez à protéger vos données objets contre les attaques de ransomware en suivant les recommandations dans "Défense contre les ransomwares avec StorageGRID".