Durcissement du système

StorageGRID 11.5

NetApp
April 11, 2024

Sommaire

Durcissement du système

Découvrez les paramètres du système, les meilleures pratiques et les recommandations pour protéger un système StorageGRID contre les menaces de sécurité.

- "Renforcement d'un système StorageGRID"
- "Directives de renforcement des mises à niveau logicielles"
- "Instructions de renforcement des réseaux StorageGRID"
- "Instructions de renforcement pour les nœuds StorageGRID"
- "Consignes de renforcement des certificats de serveur"
- "Autres directives de durcissement"]

Renforcement d'un système StorageGRID

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 la 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 concernant le renforcement du système 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, dans un container Docker 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.

Informations associées

"Stratégie de gestion des vulnérabilités"

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. Les dernières versions d'StorageGRID incluent en outre souvent des fonctionnalités de renforcement de la sécurité qui ne sont pas incluses dans les versions précédentes.

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 la page de téléchargement du logiciel StorageGRID. Pour obtenir des instructions détaillées sur la mise à niveau du logiciel StorageGRID, reportez-vous aux instructions de mise à niveau de StorageGRID. Pour obtenir des instructions sur l'application d'un correctif, reportez-vous aux instructions de récupération et de maintenance.

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 la matrice d'interopérabilité NetApp pour obtenir la 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 la matrice d'interopérabilité NetApp pour obtenir la liste des versions prises en charge.

Mise à niveau vers des 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 la matrice d'interopérabilité NetApp pour obtenir la liste des versions prises en charge.

Informations associées

"Téléchargement NetApp : StorageGRID"

"Mise à niveau du logiciel"

"Maintenance et récupération"

"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.

Instructions pour le 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. Consultez la liste des ports internes dans le guide d'installation de votre plate-forme.
- 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. Consultez la liste des ports internes dans le guide d'installation de votre plate-forme.
- Acceptez le trafic client entrant uniquement sur les terminaux configurés explicitement. Pour plus d'informations sur la gestion des réseaux clients non approuvés, reportez-vous aux instructions d'administration de StorageGRID.

Informations associées

"Instructions réseau"

"Primaire de grille"

"Administrer StorageGRID"

"Installez Red Hat Enterprise Linux ou CentOS"

"Installez Ubuntu ou Debian"

"Installez VMware"

Instructions de renforcement pour les nœuds StorageGRID

Les nœuds StorageGRID peuvent être déployés sur des machines virtuelles VMware, dans un container Docker 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.

Les nœuds qui s'exécutent sur les plateformes VMware et les appliances StorageGRID utilisent un pare-feu interne géré automatiquement. 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 au guide d'installation de votre plate-forme.

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 partez pas du principe de protection de l'hyperviseur pour empêcher les programmes malveillants d'accéder aux données protégées par StorageGRID si StorageGRID et le programme malveillant existent tous deux 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.

Désactiver les services inutilisés

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

Protéger les nœuds pendant l'installation

N'autorisez pas les utilisateurs non approuvés à accéder aux nœuds StorageGRID via 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 disposez de locataires non approuvés, ne leur autorisez pas à accéder directement 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 plus de contrôle sur les communications AutoSupport depuis les nœuds d'administration vers la prise en charge de NetApp. Reportez-vous aux étapes de création d'un proxy d'administration dans les instructions d'administration de StorageGRID.
- 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 d'administration de 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.

- N'activez pas les services sortants pour les locataires non fiables. 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'autorise pas l'utilisation des services de plateforme. Reportez-vous aux étapes de création d'un compte de locataire dans les instructions d'administration de StorageGRID.
- 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. Reportez-vous aux étapes de création d'un proxy de stockage dans les instructions d'administration de StorageGRID.
- Vous pouvez également vous connecter à des services externes à l'aide du réseau client. Sélectionnez ensuite **Configuration** > **Paramètres réseau** > **réseau client non fiable** et indiquez que le réseau client sur le nœud 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 au lieu d'utiliser le service CLB sur les nœuds de passerelle. Voir les étapes de gestion de l'équilibrage de charge dans les instructions d'administration de StorageGRID.

  Le service CLB est obsolète.

- 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** > **Paramètres réseau** > **réseau client non fiable** 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.
- 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.
- Pour les appliances sans disques FDE ou FIPS, activez le chiffrement de nœud à l'aide d'un serveur de gestion des clés (KMS).

Consultez les instructions d'installation et de maintenance de votre appliance matérielle StorageGRID.

Informations associées

"Installez Red Hat Enterprise Linux ou CentOS"

"Installez Ubuntu ou Debian"

"Installez VMware"

"Administrer StorageGRID"

"Utilisez un compte de locataire"

"SG100 etamp ; appareils de services SG1000"

"Appliances de stockage SG5600"

"Appliances de stockage SG5700"

"Dispositifs de stockage SG6000"

Consignes de renforcement des certificats de serveur

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 de serveur d'interface de gestion** : utilisé pour sécuriser l'accès à Grid Manager, au Gestionnaire de locataires, à l'API de gestion de grille et à l'API de gestion des locataires.
- **Object Storage API Service Endpoints Server Certificate** : 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 les données d'objet.

> StorageGRID gère séparément les certificats utilisés pour les terminaux de l'équilibreur de charge. Pour configurer les certificats d'équilibreur de charge, reportez-vous aux étapes de configuration des noeuds finaux d'équilibreur de charge dans les instructions d'administration de StorageGRID.

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. Une exception à cette directive est le certificat d'un terminal de type hébergé virtuel S3. Il requiert 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.

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.

Pour plus d'informations sur les journaux StorageGRID, reportez-vous aux instructions de surveillance et de dépannage. Pour plus d'informations sur les messages d'audit StorageGRID, reportez-vous aux instructions relatives aux messages d'audit.

NetApp AutoSupport

La fonction AutoSupport de StorageGRID vous permet de surveiller 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 des nature sensibles des messages AutoSupport, NetApp recommande fortement d'utiliser HTTPS comme protocole de transport par défaut pour l'envoi des messages AutoSupport au support NetApp.

Vous pouvez également configurer un proxy d'administration pour plus de contrôle sur les communications AutoSupport depuis les nœuds d'administration vers le support technique de NetApp. Reportez-vous aux étapes de création d'un proxy d'administration dans les instructions d'administration de StorageGRID.

Partage de ressources interorigine (CORS)

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

Consultez les étapes de configuration du partage de ressources d'origine croisée (CORS) dans les instructions d'utilisation des comptes de tenant.

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.

Informations associées

"Moniteur et amp ; dépannage"

"Examiner les journaux d'audit"

"Utilisez un compte de locataire"

"Administrer StorageGRID"