Tr-4645 : fonctions de sécurité

How to enable StorageGRID in your environment

NetApp
July 05, 2024

Sommaire

Tr-4645 : fonctions de sécurité

Sécurisation des données et des métadonnées StorageGRID dans un magasin d'objets

Découvrez les fonctions de sécurité intégrées à la solution de stockage objet StorageGRID.

Il s'agit d'une présentation des nombreuses fonctionnalités de sécurité de NetApp® StorageGRID®, couvrant l'accès aux données, les objets et les métadonnées, l'accès administratif et la sécurité de la plate-forme. Il a été mis à jour pour inclure les nouvelles fonctionnalités de StorageGRID 11.8.

La sécurité fait partie intégrante de la solution de stockage objet NetApp StorageGRID. La sécurité est particulièrement importante, car de nombreux types de données riches bien adaptées au stockage objet sont également sensibles, soumises aux réglementations et à la conformité. À mesure que les fonctionnalités StorageGRID continuent d'évoluer, le logiciel met à disposition de nombreuses fonctionnalités de sécurité précieuses pour protéger la stratégie de sécurité de l'entreprise et aider l'entreprise à respecter les bonnes pratiques du secteur.

Ce document présente les nombreuses fonctionnalités de sécurité d'StorageGRID 11.8, réparties en cinq catégories :

- Sécurité de l'accès aux données
- Fonctionnalités de sécurité des objets et des métadonnées
- Fonctions de sécurité de l'administration
- Fonctions de sécurité de la plate-forme
- Intégration au cloud

Ce document est destiné à être une fiche technique de sécurité. Il ne détaille pas comment configurer le système pour prendre en charge les fonctions de sécurité énumérées dans qui ne sont pas configurées par défaut. Le "Guide de renforcement de la StorageGRID" est disponible sur la page officielle "Documentation StorageGRID" .

Outre les fonctionnalités décrites dans ce rapport, StorageGRID suit le "Politique de notification et de réponse aux vulnérabilités de sécurité des produits NetApp". Les vulnérabilités signalées sont vérifiées et une réponse est apportée conformément au processus de réponse aux incidents de sécurité du produit.

NetApp StorageGRID fournit des fonctionnalités de sécurité avancées pour les cas d'utilisation très exigeants du stockage objet.

Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- NetApp StorageGRID : évaluation de la conformité SEC 17a-4(f), FINRA 4511(c) et CFTC 1.31(c)-(d) https://www.netapp.com/media/9041-ar-cohasset-netapp-storagegrid-sec-assessment.pdf
- Page de documentation StorageGRID 11.8 https://docs.netapp.com/us-en/storagegrid-118/
- Ressources de documentation StorageGRID https://www.netapp.com/data-storage/storagegrid/documentation/

- Documentation des produits NetApp https://www.netapp.com/support-and-training/documentation/

Termes et acronymes

Cette section fournit des définitions de la terminologie utilisée dans le document.

Terme ou acronyme	Définition
S3	Simple Storage Service.
Client	Application pouvant interagir avec StorageGRID via le protocole S3 d'accès aux données ou le protocole HTTP de gestion.
Administrateur des locataires	Administrateur du compte locataire StorageGRID
Utilisateur locataire	Utilisateur d'un compte de locataire StorageGRID
TLS	Sécurité de la couche de transport
ILM	Gestion du cycle de vie des informations
RÉSEAU LOCAL	Réseau local
Administrateur du grid	Administrateur du système StorageGRID
Grille	Le système StorageGRID
Godet	Un conteneur pour les objets stockés dans S3
LDAP	Protocole d'accès à l'annuaire simplifié
SEC	Securities and Exchange Commission; réglemente les membres de change, les courtiers ou les courtiers
FINRA	Autorité de réglementation du secteur financier ; diffère des exigences de format et de support de la règle SEC 17a-4(f)
CFTC	Commissions sur les opérations à terme sur les matières premières; réglemente les opérations à terme sur les matières premières
NIST	Institut national des normes et de la technologie

Sécurité de l'accès aux données

Découvrez les fonctionnalités de sécurité d'accès aux données de StorageGRID.

Fonction	Fonction	Impact	Conformité réglementaire
TLS (transport Layer Security) configurable	TLS établit un protocole de liaison pour la communication entre un client et un nœud de passerelle StorageGRID, un nœud de stockage ou un point d'extrémité d'équilibreur de charge. StorageGRID prend en charge les suites de chiffrement suivantes pour TLS : • TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • TLS_AES_256_GCM_SHA384 • DHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • AES128-GCM-SHA256 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-CHACHA20-POLY1305 • ECDHE-RSA-CHACHA20-POLY1305 TLS v1.2 et 1.3 pris en charge. SSLv3, TLS v1.1 et versions antérieures ne sont plus pris en charge.	Permet à un client et à StorageGRID de s'identifier et de s'authentifier mutuellement et de communiquer avec confidentialité et intégrité des données. Garantit l'utilisation d'une version TLS récente. Les chiffrements sont désormais configurables sous les paramètres de configuration/sécurité	—

Fonction	Fonction	Impact	Conformité réglementaire
Certificat de serveur configurable (noeud final Load Balancer)	Les administrateurs du grid peuvent configurer les noeuds finaux Load Balancer pour générer ou utiliser un certificat de serveur.	Permet l'utilisation de certificats numériques signés par leur autorité de certification approuvée standard pour authentifier les opérations d'API d'objet entre la grille et le client par point final Load Balancer.	—
Certificat de serveur configurable (terminal API)	Les administrateurs du grid peuvent configurer de manière centralisée tous les terminaux de l'API StorageGRID pour qu'ils utilisent un certificat de serveur signé par l'autorité de certification de confiance de leur entreprise.	Permet l'utilisation de certificats numériques signés par leur autorité de certification standard de confiance pour authentifier les opérations de l'API objet entre un client et la grille.	—

Fonction	Fonction	Impact	Conformité réglementaire
Colocation	StorageGRID prend en charge plusieurs locataires par grille ; chaque locataire dispose de son propre espace de noms. Un locataire utilise le protocole S3. Par défaut, l'accès aux compartiments/conteneurs et aux objets est limité aux utilisateurs au sein du compte. Les locataires peuvent avoir un utilisateur (par exemple, un déploiement d'entreprise, dans lequel chaque utilisateur a son propre compte) ou plusieurs utilisateurs (par exemple, un déploiement de fournisseur de services, dans lequel chaque compte est une entreprise et un client du fournisseur de services). Les utilisateurs peuvent être locaux ou fédérés. Les utilisateurs fédérés sont définis par Active Directory ou LDAP (Lightweight Directory Access Protocol). StorageGRID fournit un tableau de bord par locataire, dans lequel les utilisateurs se connectent à l'aide de leurs informations d'identification de compte locales ou fédérées. Les utilisateurs peuvent accéder à des rapports visualisés sur l'utilisation des locataires par rapport au quota attribué par l'administrateur de la grille, y compris des informations d'utilisation dans les données et objets stockés par compartiments. Les utilisateurs disposant d'autorisations administratives peuvent effectuer des tâches d'administration système au niveau du locataire, telles que la gestion des utilisateurs et des groupes et des clés d'accès.	Permet aux administrateurs StorageGRID d'héberger les données de plusieurs locataires tout en isolant l'accès des locataires et d'établir l'identité des utilisateurs en fédérant les utilisateurs avec un fournisseur d'identité externe, tel qu'Active Directory ou LDAP.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)

Fonction	Fonction	Impact	Conformité réglementaire
Non-répudiation des identifiants d'accès	Chaque opération S3 est identifiée et consignée à l'aide d'un compte de locataire, d'un utilisateur et d'une clé d'accès uniques.	Permet aux administrateurs du grid d'établir les actions d'API exécutées par des individus.	—
Accès anonyme désactivé	Par défaut, l'accès anonyme est désactivé pour les comptes S3. Un demandeur doit disposer d'un droit d'accès valide pour qu'un utilisateur valide du compte de tenant puisse accéder aux compartiments, conteneurs ou objets du compte. L'accès anonyme aux compartiments ou objets S3 peut être activé avec une règle IAM explicite.	Permet aux administrateurs de Grid de désactiver ou de contrôler l'accès anonyme aux compartiments/conteneurs et objets.	—
Conformité WORM	Conçu pour répondre aux exigences de la règle SEC 17a-4(f) et validé par Cohasset. Les clients peuvent assurer la conformité au niveau du compartiment. La conservation peut être étendue, mais jamais réduite. Les règles de gestion du cycle de vie des informations (ILM) appliquent des niveaux minimaux de protection des données.	Permet aux locataires qui ont des exigences réglementaires en matière de conservation des données d'activer la protection WORM sur les objets stockés et les métadonnées d'objet.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)

Fonction	Fonction	Impact	Conformité réglementaire
VER	Les administrateurs du grid peuvent activer le mode WORM au niveau de la grille en activant l'option Désactiver la modification du client, qui empêche les clients d'écraser ou de supprimer des objets ou des métadonnées d'objet dans tous les comptes de locataires. Les administrateurs de locataires S3 peuvent également activer le mode WORM par locataire, compartiment ou préfixe d'objet en spécifiant une règle IAM qui inclut l'autorisation S3 : PutOverwriteObject personnalisée pour le remplacement d'objets et de métadonnées.	Permet aux administrateurs du grid et aux locataires de contrôler la protection WORM sur les objets stockés et les métadonnées d'objet.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
Gestion des clés de cryptage du serveur hôte KM	Les administrateurs du grid peuvent configurer un ou plusieurs serveurs de gestion externe des clés (KMS) dans Grid Manager afin que les clés de chiffrement soient attribuées aux services StorageGRID et aux appliances de stockage. Chaque serveur hôte KMS ou cluster de serveurs hôtes KMS utilise le protocole KMIP (Key Management Interoperability Protocol) pour fournir une clé de chiffrement aux nœuds de l'appliance sur le site StorageGRID associé.	Vous pouvez chiffrer les données au repos. Une fois les volumes de l'appliance chiffrés, vous ne pouvez pas accéder aux données de l'appliance sauf si le nœud peut communiquer avec le serveur hôte KMS.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)

Fonction	Fonction	Impact	Conformité réglementaire
Basculement automatique	StorageGRID fournit une redondance intégrée et un basculement automatisé. L'accès aux comptes de locataires, aux compartiments et aux objets peut continuer même en cas de pannes multiples, depuis des disques ou des nœuds jusqu'à des sites entiers. StorageGRID est conscient des ressources et redirige automatiquement les requêtes vers les nœuds disponibles et les emplacements de données. Les sites StorageGRID peuvent même fonctionner en mode iskattered. En cas de panne de réseau étendu, un site est déconnecté du reste du système, les lectures et écritures peuvent continuer avec les ressources locales, et la réplication reprend automatiquement lorsque le réseau WAN est restauré.	Permet aux administrateurs du grid de répondre aux exigences de disponibilité, aux contrats de niveau de service et aux autres obligations contractuelles et de mettre en œuvre des plans de continuité de l'activité.	—
Fonctions de sécurité d'accès aux données spécifiques à S3	Signature AWS version 2 et version 4	La signature des requêtes d'API permet d'authentifier les opérations de l'API S3. Amazon prend en charge deux versions de Signature version 2 et version 4. Le processus de signature vérifie l'identité du demandeur, protège les données en transit et les protège contre les attaques de relecture potentielles.	S'aligne sur la recommandation AWS pour Signature version 4 et permet une rétrocompatibilité avec les anciennes applications avec Signature version 2.

Fonction	Fonction	Impact	Conformité réglementaire
—	Verrouillage d'objet S3	La fonctionnalité de verrouillage objet S3 d'StorageGRID est une solution de protection objet équivalente au verrouillage objet S3 dans Amazon S3.	Permet aux locataires de créer des compartiments avec S3 Object Lock activé pour se conformer aux réglementations exigeant la conservation de certains objets pendant une durée fixe ou indéfiniment.
Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)	Stockage sécurisé des identifiants S3	Les clés d'accès S3 sont stockées dans un format protégé par une fonction de hachage des mots de passe (SHA-2).	Permet le stockage sécurisé des clés d'accès par une combinaison de longueur de clé (un nombre généré de manière aléatoire de 10^{31}) et d'un algorithme de hachage de mot de passe.
—	Clés d'accès S3 limitées dans le temps	Lorsque vous créez une clé d'accès S3 pour un utilisateur, les clients peuvent définir une date et une heure d'expiration sur la clé d'accès.	Permet aux administrateurs du grid de provisionner des clés d'accès S3 temporaires.
—	Plusieurs clés d'accès par compte d'utilisateur	StorageGRID permet de créer plusieurs clés d'accès et de les activer simultanément pour un compte utilisateur. Chaque action d'API étant consignée avec un compte utilisateur de locataire et une clé d'accès, la non-répudiation est préservée même si plusieurs clés sont actives.	Permet aux clients de faire pivoter les clés d'accès sans interruption et à chaque client d'avoir sa propre clé, décourageant ainsi le partage des clés entre les clients.

Fonction	Fonction	Impact	Conformité réglementaire
—	Règle d’accès IAM S3	StorageGRID prend en charge les règles IAM S3, ce qui permet aux administrateurs du grid de spécifier le contrôle d’accès granulaire par locataire, compartiment ou préfixe d’objet. StorageGRID prend également en charge les conditions et les variables des règles IAM, ce qui permet des règles de contrôle d’accès plus dynamiques.	Permet aux administrateurs de Grid de spécifier le contrôle d’accès par groupes d’utilisateurs pour l’ensemble du tenant ; permet également aux utilisateurs locataires de spécifier le contrôle d’accès pour leurs propres compartiments et objets.
—	Chiffrement côté serveur avec clés gérées par StorageGRID (SSE)	StorageGRID prend en charge SSE, ce qui permet une protection mutualisée des données au repos avec des clés de chiffrement gérées par StorageGRID.	Permet aux locataires de chiffrer les objets. Une clé de chiffrement est requise pour écrire et récupérer ces objets.
Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)	Chiffrement côté serveur avec clés de chiffrement fournies par le client (SSE-C)	StorageGRID prend en charge SSE-C, ce qui permet une protection mutualisée des données au repos avec des clés de chiffrement gérées par le client. Bien que StorageGRID gère toutes les opérations de chiffrement et de déchiffrement d’objets, avec SSE-C, le client doit gérer les clés de cryptage lui-même.	Permet aux clients de chiffrer les objets avec des clés qu’ils contrôlent. Une clé de chiffrement est requise pour écrire et récupérer ces objets.

Sécurité des objets et des métadonnées

Explorez les fonctionnalités de sécurité des objets et des métadonnées de StorageGRID.

Fonction	Fonction	Impact	Conformité réglementaire
Advanced Encryption Standard (AES) - chiffrement d'objets côté serveur	StorageGRID assure le chiffrement des objets côté serveur basé sur AES 128 et AES 256. Les administrateurs du grid peuvent activer le chiffrement comme paramètre global par défaut. StorageGRID prend également en charge l'en-tête de chiffrement S3 x-amz côté serveur pour activer ou désactiver le chiffrement par objet. Lorsque cette option est activée, les objets sont chiffrés lorsqu'ils sont stockés ou en transit entre des nœuds de grid.	Stockage et transmission sécurisés d'objets, indépendamment du matériel de stockage sous-jacent.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
Gestion intégrée des clés	Lorsque le chiffrement est activé, chaque objet est chiffré avec une clé symétrique unique générée de manière aléatoire, stockée dans StorageGRID sans accès externe.	Permet le chiffrement des objets sans gestion externe des clés.	
Disques de chiffrement conformes à la norme FIPS (Federal information Processing Standard) 140-2	Les appliances StorageGRID SG5712, SG5760, SG6060 et SGF6024 offrent la possibilité d'utiliser des disques de chiffrement conformes à la norme FIPS 140-2. Les clés de chiffrement des disques peuvent être gérées par un serveur KMIP externe.	Stockage sécurisé des données, métadonnées et objets du système. Le chiffrement logiciel des objets StorageGRID sécurise le stockage et la transmission des objets.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)

Fonction	Fonction	Impact	Conformité réglementaire
Analyse de l'intégrité en arrière-plan et auto-rétablissement	StorageGRID utilise un mécanisme d'interverrouillage de hachages, de checksums et de vérifications de la redondance cyclique (CRC) au niveau de l'objet et des sous-objets pour se protéger contre l'incohérence, la falsification ou la modification des données, aussi bien lorsque les objets sont en stockage qu'en transit. StorageGRID détecte automatiquement les objets corrompus et falsifiés et les remplace, tout en mettant en quarantaine les données modifiées et en alertant l'administrateur.	Permet aux administrateurs du grid de respecter les SLA, les réglementations et autres obligations en matière de durabilité des données. Aide les clients à détecter les ransomwares ou les virus qui tentent de chiffrer, d'altérer ou de modifier des données.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
Placement et conservation des objets basés sur des règles	StorageGRID permet aux administrateurs du grid de configurer des règles ILM, qui spécifient la conservation, le placement, la protection, la transition et l'expiration des objets. Les administrateurs du grid peuvent configurer StorageGRID pour filtrer les objets en fonction de leurs métadonnées et appliquer des règles à différents niveaux de granularité, notamment à l'échelle du grid, du locataire, du compartiment, du préfixe de clé et des paires clé-valeur de métadonnées définies par l'utilisateur. StorageGRID permet de s'assurer que les objets sont stockés conformément aux règles ILM tout au long de leur cycle de vie, à moins qu'ils ne soient explicitement supprimés par le client.	Renforce le placement, la protection et la conservation des données. Aide les clients à respecter les SLA en matière de durabilité, de disponibilité et de performance.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)

Fonction	Fonction	Impact	Conformité réglementaire
Analyse des métadonnées en arrière-plan	StorageGRID analyse régulièrement les métadonnées d'objet en arrière-plan pour appliquer des modifications au placement ou à la protection des données d'objet, comme spécifié par la règle ILM.	Permet de détecter les objets corrompus.	
Cohérence ajustable	Les locataires peuvent sélectionner des niveaux de cohérence au niveau du compartiment pour s'assurer que les ressources, telles que la connectivité multisite, sont disponibles.	Offre la possibilité d'effectuer des écritures dans la grille uniquement lorsqu'un nombre requis de sites ou de ressources est disponible.	

Fonctions de sécurité de l'administration

Découvrez les fonctions de sécurité d'administration de StorageGRID.

Fonction	Fonction	Impact	Conformité réglementaire
Certificat de serveur (interface de gestion Grid)	Les administrateurs du grid peuvent configurer l'interface de gestion Grid pour utiliser un certificat de serveur signé par l'autorité de certification approuvée de leur organisation.	Permet l'utilisation de certificats numériques signés par leur autorité de certification standard et approuvée pour authentifier l'accès à l'interface utilisateur de gestion et à l'API entre un client de gestion et la grille.	—
Authentification utilisateur administrative	Les utilisateurs administratifs sont authentifiés à l'aide du nom d'utilisateur et du mot de passe. Les utilisateurs et groupes administratifs peuvent être locaux ou fédérés, importés depuis Active Directory ou LDAP du client. Les mots de passe des comptes locaux sont stockés dans un format protégé par bcrypt ; les mots de passe de ligne de commande sont stockés dans un format protégé par SHA-2.	Authentifie l'accès administratif à l'interface utilisateur de gestion et aux API.	—

Fonction	Fonction	Impact	Conformité réglementaire
Prise en charge SAML	StorageGRID prend en charge l'authentification unique (SSO) à l'aide de la norme SAML 2.0 (Security assertion Markup Language 2.0). Lorsque l'authentification SSO est activée, tous les utilisateurs doivent être authentifiés par un fournisseur d'identités externe avant d'accéder au Grid Manager, au tenant Manager, à l'API Grid Management ou à l'API de gestion des locataires. Les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.	Niveaux de sécurité supplémentaires pour les administrateurs du grid et des locataires tels que SSO et l'authentification multifacteur (MFA)	NIST SP800-63
Contrôle granulaire des autorisations	Les administrateurs du grid peuvent attribuer des autorisations aux rôles et attribuer des rôles à des groupes d'utilisateurs administratifs, ce qui permet d'appliquer les tâches que les clients administratifs sont autorisés à effectuer à l'aide de l'interface utilisateur de gestion et des API.	Permet aux administrateurs de Grid de gérer le contrôle d'accès pour les utilisateurs et les groupes d'administration.	—

Fonction	Fonction	Impact	Conformité réglementaire
Journalisation des audits distribués	StorageGRID offre une infrastructure intégrée de journalisation des audits distribuée et évolutive pour des centaines de nœuds répartis sur un maximum de 16 sites. Les nœuds logiciels StorageGRID génèrent des messages d'audit, qui sont transmis via un système de relais d'audit redondant et finalement capturés dans un ou plusieurs référentiels de journaux d'audit. Les messages d'audit capturent les événements au niveau objet, tels que les opérations de l'API S3 initiées par le client, les événements de cycle de vie des objets par ILM, les vérifications de l'état des objets en arrière-plan et les modifications de configuration effectuées à partir de l'interface utilisateur de gestion ou des API. Les journaux d'audit peuvent être exportés depuis les nœuds d'administration via CIFS ou NFS, ce qui permet d'extraire les messages d'audit par des outils tels que Splunk et ELK. Il existe quatre types de messages d'audit : • Messages d'audit système • Messages d'audit du stockage objet • Messages d'audit du protocole HTTP • Messages d'audit de gestion	Fournit aux administrateurs du grid un service d'audit évolutif et éprouvé qui leur permet d'exploiter les données d'audit pour divers objectifs. Tels que la résolution de problèmes, l'audit des performances des SLA, les opérations d'API d'accès aux données du client et les modifications de la configuration de la gestion.	—

Fonction	Fonction	Impact	Conformité réglementaire
Audit du système	Les messages d'audit du système capturent les événements liés au système, tels que l'état des nœuds de grid, la détection d'objets corrompus, les objets validés à tous les emplacements spécifiés conformément à la règle ILM et la progression des tâches de maintenance à l'échelle du système (tâches de grid).	Aide les clients à résoudre les problèmes liés aux systèmes et apporte une preuve que les objets sont stockés conformément à leur SLA. Les SLA sont implémentés par les règles ILM de StorageGRID et sont protégés contre l'intégrité.	—
Audit du stockage objet	Les messages d'audit du stockage objet capturent les transactions de l'API objet et les événements liés au cycle de vie. Ces événements incluent le stockage objet et la récupération, les transferts de nœuds grid à nœud grid et les vérifications.	Aide les clients à vérifier la progression des données dans le système et si les SLA, spécifiés dans la ILM de StorageGRID, sont livrés.	—
Audit du protocole HTTP	Les messages d'audit du protocole HTTP capturent les interactions du protocole HTTP liées aux applications clientes et aux nœuds StorageGRID. En outre, les clients peuvent capturer des en-têtes de requête HTTP spécifiques (tels que X-retransmis-for et les métadonnées utilisateur [x-amz-meta-*]) dans l'audit.	Aide les clients à auditer les opérations d'API d'accès aux données entre les clients et StorageGRID et à tracer une action sur un compte utilisateur individuel et une clé d'accès. Ils peuvent également connecter les métadonnées utilisateur à des fins d'audit et utiliser des outils de recherche de journaux, tels que Splunk ou ELK, pour rechercher des métadonnées objet.	—
Audit de gestion	Les messages d'audit de gestion consignent les demandes des utilisateurs administrateurs dans l'interface de gestion (Grid Management interface) ou les API. Chaque requête qui n'est pas une requête GET ou HEAD à l'API consigne une réponse avec le nom d'utilisateur, l'IP et le type de requête à l'API.	Aide les administrateurs Grid à établir un enregistrement des modifications de configuration système effectuées par l'utilisateur à partir de quelle adresse IP source et de quelle adresse IP de destination à quel moment.	—

Fonction	Fonction	Impact	Conformité réglementaire
Prise en charge de TLS 1.3 pour l'interface de gestion et l'accès aux API	TLS établit un protocole de poignée de main pour la communication entre un client admin et un nœud admin StorageGRID.	Permet à un client administratif et à StorageGRID de s'identifier et de s'authentifier mutuellement et de communiquer avec confidentialité et intégrité des données.	—
SNMPv3 pour surveillance StorageGRID	SNMPv3 fournit la sécurité en offrant à la fois une authentification forte et un cryptage des données pour la confidentialité. Avec v3, les unités de données de protocole sont chiffrées à l'aide de CBC-DES pour son protocole de chiffrement. L'authentification utilisateur de la personne qui a envoyé l'unité de données de protocole est fournie par le protocole d'authentification HMAC-SHA ou HMAC-MD5. SNMPv2 et v1 sont toujours pris en charge.	Permet aux administrateurs de la grille de surveiller le système StorageGRID en activant un agent SNMP sur le nœud d'administration.	—
Certificats client pour l'exportation des metrics Prometheus	Les administrateurs du grid peuvent télécharger ou générer des certificats clients qui peuvent être utilisés pour fournir un accès sécurisé et authentifié à la base de données StorageGRID Prometheus.	Les administrateurs du grid peuvent utiliser des certificats client pour surveiller StorageGRID en externe à l'aide d'applications telles que Grafana.	—

Fonctions de sécurité de la plate-forme

Découvrez les fonctionnalités de sécurité de la plate-forme dans StorageGRID.

Fonction	Fonction	Impact	Conformité réglementaire
Infrastructure de clé publique (PKI) interne, certificats de nœud et TLS	StorageGRID utilise une PKI interne et des certificats de nœud pour authentifier et crypter les communications internœuds. La communication internœud est sécurisée par TLS.	Permet de sécuriser le trafic système sur le LAN ou le WAN, en particulier dans un déploiement multisite.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
Pare-feu de nœud	StorageGRID configure automatiquement les tables IP et les règles de pare-feu pour contrôler le trafic réseau entrant et sortant, ainsi que pour fermer les ports inutilisés.	Protection du système StorageGRID, des données et des métadonnées contre le trafic réseau non sollicité.	—
Durcicement du système d'exploitation	Le système d'exploitation de base des appliances physiques et des nœuds virtuels StorageGRID est renforcé ; les logiciels non liés sont supprimés.	Permet de minimiser les surfaces d'attaque potentielles.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
Mises à jour périodiques de la plate-forme et des logiciels	StorageGRID fournit régulièrement des versions logicielles, notamment des systèmes d'exploitation, des binaires d'applications et des mises à jour logicielles.	Ils permettent de maintenir le système StorageGRID à jour avec les logiciels et les binaires d'applications les plus récents.	—
Connexion racine désactivée via SSH (Secure Shell)	La connexion root via SSH est désactivée sur tous les nœuds StorageGRID. L'accès SSH utilise l'authentification par certificat.	Aide les clients à se protéger contre les éventuels problèmes de piratage à distance des mots de passe de la connexion racine.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
Synchronisation temporelle automatisée	StorageGRID synchronise automatiquement les horloges système de chaque nœud avec plusieurs serveurs NTP (External Time Network Time Protocol). Au moins quatre serveurs NTP de Stratum 3 ou version ultérieure sont requis.	Garantit la même référence de temps sur tous les nœuds.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)

Fonction	Fonction	Impact	Conformité réglementaire
Réseaux séparés pour le trafic client, administrateur et grid interne	Les nœuds logiciels et les appliances matérielles StorageGRID prennent en charge plusieurs interfaces réseau physiques et virtuelles, de sorte que les clients peuvent séparer le trafic client, d'administration et le trafic réseau interne sur différents réseaux.	Permettez aux administrateurs du grid de séparer le trafic réseau interne et externe et de fournir le trafic sur les réseaux avec différents SLA.	—
Plusieurs interfaces VLAN (Virtual LAN)	StorageGRID prend en charge la configuration des interfaces VLAN sur vos réseaux client et grid StorageGRID.	Permettez aux administrateurs de Grid de partitionner et d'isoler le trafic des applications pour plus de sécurité, de flexibilité et de performances.	
Réseau client non fiable	L'interface réseau client non fiable accepte les connexions entrantes uniquement sur les ports qui ont été explicitement configurés comme des noeuds finaux d'équilibrage de charge.	Garantit que les interfaces exposées à des réseaux non fiables sont sécurisées.	—
Pare-feu configurable	Gérez les ports ouverts et fermés pour les réseaux Admin, Grid et client.	Autoriser les administrateurs du grid à contrôler l'accès aux ports et à gérer l'accès aux périphériques approuvés aux ports.	
Comportement SSH amélioré	De nouveaux certificats d'hôte SSH et clés d'hôte sont générés lors de la mise à niveau d'un nœud vers StorageGRID 11.5.	Améliore la protection contre les attaques de l'homme du milieu.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)
Chiffrement de nœud	Dans le cadre de la nouvelle fonction de chiffrement du serveur hôte KMS, un nouveau paramètre de chiffrement de nœud est ajouté au programme d'installation de l'appliance StorageGRID.	Ce paramètre doit être activé pendant la phase de configuration matérielle de l'installation de l'appliance.	Règle SEC 17a-4(f) CTFC 1.31(c)-(d) (FINRA) règle 4511(c)

Intégration au cloud

Découvrez comment StorageGRID s'intègre aux services cloud.

Fonction	Fonction	Impact
Analyse antivirus basée sur les notifications	Notifications d'événements de support des services de plateforme StorageGRID. Les notifications d'événements peuvent être utilisées avec des services de cloud computing externes pour déclencher des flux de travail d'analyse antivirus sur les données.	Permet aux administrateurs de locataires de déclencher l'analyse antivirus des données à l'aide de services de cloud computing externes.

Informations sur le copyright

Informations sur les marques commerciales