TR-4645: Sicherheitsfunktionen

How to enable StorageGRID in your environment

NetApp
August 19, 2024

Inhalt

TR-4645: Sicherheitsfunktionen

Sichern von StorageGRID-Daten und -Metadaten in einem Objektspeicher

Entdecken Sie die integrierten Sicherheitsfunktionen der StorageGRID Objekt-Storage-Lösung.

Dies ist ein Überblick über die vielen Sicherheitsfunktionen in NetApp® StorageGRID®, die Datenzugriff, Objekte und Metadaten, administrativen Zugriff und Plattformsicherheit abdecken. Es wurde aktualisiert und enthält nun die neuesten Funktionen, die mit StorageGRID 11.8 veröffentlicht wurden.

Sicherheit ist ein integraler Bestandteil der NetApp StorageGRID Objekt-Storage-Lösung. Die Sicherheit ist besonders wichtig, da viele Arten von umfangreichen Datenmengen, die gut für Objekt-Storage geeignet sind, ebenfalls sehr sensibel sind und gesetzlichen Vorschriften und Compliance unterliegen. Während sich die Funktionen von StorageGRID weiterentwickeln, stellt die Software viele Sicherheitsfunktionen zur Verfügung, die von unschätzbarem Wert sind, um die Sicherheit eines Unternehmens zu schützen und dem Unternehmen dabei zu helfen, die Best Practices der Branche einzuhalten.

Dieses Dokument bietet einen Überblick über die zahlreichen Sicherheitsfunktionen in StorageGRID 11.8, die in fünf Kategorien unterteilt sind:

- Sicherheitsfunktionen für den Datenzugriff
- Sicherheitsfunktionen für Objekte und Metadaten
- Sicherheitsfunktionen für die Administration
- Plattformsicherheitsfunktionen
- Cloud-Integration

Dieses Dokument ist als Sicherheitsdatenblatt gedacht. Es enthält keine Angaben dazu, wie das System so konfiguriert wird, dass es die in aufgeführten Sicherheitsfunktionen unterstützt, die nicht standardmäßig konfiguriert sind. Das "Leitfaden zum StorageGRID Hardening" ist auf der offiziellen Seite verfügbar "StorageGRID-Dokumentation" .

Zusätzlich zu den in diesem Bericht beschriebenen Funktionen folgt StorageGRID den "NetApp Richtlinie zur Reaktion auf und Benachrichtigung bei Produktsicherheitsschwachstellen". Gemeldete Schwachstellen werden überprüft und entsprechend dem Reaktionsprozess für Produktsicherheitsvorfälle reagiert.

NetApp StorageGRID bietet erweiterte Sicherheitsfunktionen für äußerst anspruchsvolle Enterprise-Objekt-Storage-Anwendungsfälle.

Wo Sie weitere Informationen finden

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- NetApp StorageGRID: Bewertung DER Compliance-Anforderungen gemäß SEC 17a-4(f), FINRA 4511(c) und CFTC 1.31(c)-(d) https://www.netapp.com/media/9041-ar-cohasset-netapp-storagegrid-sec-assessment.pdf
- StorageGRID 11.8 Dokumentationsseite https://docs.netapp.com/us-en/storagegrid-118/

- StorageGRID Dokumentations-Ressourcen https://www.netapp.com/data-storage/storagegrid/documentation/
- NetApp Produktdokumentation https://www.netapp.com/support-and-training/documentation/

Begriffe und Akronyme

Dieser Abschnitt enthält Definitionen für die im Dokument verwendete Terminologie.

Begriff oder Akronym	Definition
S3	Simple Storage Service.
Client	Eine Applikation, die eine Schnittstelle zu StorageGRID entweder über das S3-Protokoll für den Datenzugriff oder das HTTP-Protokoll für das Management bietet.
Mandantenadministrator	Der Administrator des StorageGRID-Mandantenkontos
Mandantenbenutzer	Ein Benutzer in einem StorageGRID-Mandantenkonto
TLS	Sicherheit In Transportschicht
ILM	Information Lifecycle Management
LAN	Lokales Netzwerk
Grid-Administrator	Der Administrator des StorageGRID-Systems
Raster	Dem StorageGRID-System
Eimer	Ein Container für in S3 gespeicherte Objekte
LDAP	Lightweight Directory Access Protocol
SEK.	Securities and Exchange Commission; regelt Börsenmitglieder, Makler oder Händler
FINRA	Aufsichtsbehörde für die Finanzindustrie; entspricht den Format- und Medienanforderungen der SEC Rule 17a-4(f)
CFTC	Commodities Futures Trading Commissions; regelt den Handel mit Rohstofftermingeschäften
NIST	National Institute of Standards and Technology

Sicherheitsfunktionen für den Datenzugriff

Erfahren Sie mehr über die Sicherheitsfunktionen für den Datenzugriff in StorageGRID.

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Konfigurierbare TLS (Transport Layer Security)	TLS erstellt ein Handshake-Protokoll für die Kommunikation zwischen einem Client und einem StorageGRID-Gateway-Node, Speicher-Node oder Load Balancer-Endpunkt. StorageGRID unterstützt die folgenden Verschlüsselungssuites für 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 und 1.3 unterstützt. SSLv3, TLS v1.1 und frühere Versionen werden nicht mehr unterstützt.	Ein Client und ein StorageGRID können sich gegenseitig identifizieren und authentifizieren und mit Vertraulichkeit und Datenintegrität kommunizieren. Stellt die Verwendung einer aktuellen TLS-Version sicher. Die Chiffren können jetzt unter den Konfigurations-/Sicherheitseinstellungen konfiguriert werden	—

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Konfigurierbares Serverzertifikat (Load Balancer Endpoint)	Grid-Administratoren können Load-Balancer-Endpunkte konfigurieren, um ein Serverzertifikat zu erstellen oder zu verwenden.	Ermöglicht die Verwendung von digitalen Zertifikaten, die von ihrer standardmäßigen vertrauenswürdigen Zertifizierungsstelle (CA) signiert wurden, um Objekt-API-Vorgänge zwischen Grid und Client pro Load Balancer-Endpunkt zu authentifizieren.	—
Konfigurierbares Serverzertifikat (API-Endpunkt)	Grid-Administratoren können alle StorageGRID-API-Endpunkte zentral so konfigurieren, dass ein von der vertrauenswürdigen CA ihres Unternehmens signiertes Serverzertifikat verwendet wird.	Ermöglicht die Verwendung von digitalen Zertifikaten, die von ihrer standardmäßigen vertrauenswürdigen Zertifizierungsstelle signiert wurden, um Objekt-API-Vorgänge zwischen einem Client und dem Grid zu authentifizieren.	—

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Mandantenfähigkeit	StorageGRID unterstützt mehrere Mandanten pro Grid, wobei jeder Mandant einen eigenen Namespace besitzt. Ein Mandant stellt ein S3-Protokoll bereit. Standardmäßig ist der Zugriff auf Buckets/Container und Objekte auf Benutzer in dem Konto beschränkt. Mandanten können einen Benutzer (z. B. eine Unternehmensimplementierung , bei der jeder Benutzer ein eigenes Konto hat) oder mehrere Benutzer (z. B. eine Service-Provider-Implementierung, bei der jedes Konto ein Unternehmen und ein Kunde des Service-Providers ist) aufweisen. Benutzer können lokal oder föderiert sein; föderierte Benutzer werden durch Active Directory oder Lightweight Directory Access Protocol (LDAP) definiert. StorageGRID bietet ein mandantenfähiges Dashboard, in dem sich Benutzer mit ihren lokalen oder föderierten Kontoinformationen anmelden können. Benutzer können auf visualisierte Berichte zur Mandantennutzung anhand des vom Grid-Administrator zugewiesenen Kontingents zugreifen, einschließlich Nutzungsinformationen in Daten und Objekten, die von Buckets gespeichert sind. Benutzer mit Administratorrechten können Systemadministrationsaufgaben auf Mandantenebene durchführen, wie zum Beispiel Benutzer und Gruppen und Zugriffsschlüssel managen.	StorageGRID-Administratoren können Daten von mehreren Mandanten hosten, dabei den Mandantenzugriff isolieren und die Benutzeridentität festlegen, indem Benutzer mit einem externen Identitätsanbieter wie Active Directory oder LDAP verknüpft werden.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Nichtabstreitbarkeit der Zugangsdaten	Jeder S3-Vorgang wird mit einem eindeutigen Mandantenkonto, einem eindeutigen Benutzer und einem Zugriffsschlüssel identifiziert und protokolliert.	Ermöglicht Grid-Administratoren festzulegen, welche API-Aktionen von welchen Personen ausgeführt werden.	—
Anonymer Zugriff deaktiviert	Standardmäßig ist der anonyme Zugriff für S3-Konten deaktiviert. Ein Anforderer muss über gültige Zugangsdaten für einen gültigen Benutzer im Mandantenkonto verfügen, um auf Buckets, Container oder Objekte innerhalb des Kontos zugreifen zu können. Anonymer Zugriff auf S3-Buckets oder -Objekte kann mit einer expliziten IAM-Richtlinie aktiviert werden.	Ermöglicht Grid-Administratoren, den anonymen Zugriff auf Buckets/Container und Objekte zu deaktivieren oder zu steuern.	—
Compliance-WORM	Entwickelt, um die Anforderungen der SEC Rule 17a-4(f) zu erfüllen und von Cohasset validiert. Kunden können Compliance auf Bucket-Ebene aktivieren. Die Aufbewahrung kann erweitert, aber nie reduziert werden. Regeln für Information Lifecycle Management (ILM) setzen minimale Datensicherungsstufen fest.	Mandanten mit gesetzlichen Datenaufbewahrungsanforderungen ermöglichen WORM-Schutz bei gespeicherten Objekten und Objektmetadaten.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
WORM	Grid-Administratoren können den WORM für das gesamte Grid aktivieren, indem sie die Option Client-Änderung deaktivieren aktivieren, die verhindert, dass Clients Objekte oder Objektmetadaten in allen Mandantenkonten überschreiben oder löschen. S3-Mandantenadministratoren können WORM auch nach Mandant, Bucket oder Objektpräfix durch Angabe der IAM-Richtlinie aktivieren, die die benutzerdefinierte S3: PutOverwriteObject-Berechtigung für Objekt- und Metadatenüberschreibungen umfasst.	Grid-Administratoren und Mandantenadministratoren können die WORM-Sicherung von gespeicherten Objekten und Objektmetadaten steuern.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)
KMS-Host-Server-Verschlüsselungsschlüsselverwaltung	Grid-Administratoren können einen oder mehrere externe KMS (Key Management Server) im Grid Manager konfigurieren, um Verschlüsselungen für StorageGRID Services und Storage Appliances bereitzustellen. Jeder KMS-Hostserver oder KMS-Hostserver-Cluster verwendet das Key Management Interoperability Protocol (KMIP), um einen Verschlüsselungsschlüssel für die Appliance-Nodes am zugehörigen StorageGRID-Standort bereitzustellen.	Die Verschlüsselung ruhender Daten wird erreicht. Nachdem die Appliance-Volumes verschlüsselt wurden, können Sie nur auf Daten auf der Appliance zugreifen, wenn der Node mit dem KMS-Hostserver kommunizieren kann.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Automatisiertes Failover	StorageGRID bietet integrierte Redundanz und automatisiertes Failover. Der Zugriff auf Mandantenkonten, Buckets und Objekte kann auch bei diversen Ausfällen – von Festplatten oder Nodes bis hin zu ganzen Standorten – fortgesetzt werden. StorageGRID erkennt Ressourcen und leitet Anfragen automatisch an verfügbare Nodes und Datenspeicherorte um. StorageGRID Standorte können sogar im Inselmodus betrieben werden. Wenn ein WAN-Ausfall die Verbindung eines Standorts zum restlichen System trennt, können Lese- und Schreibvorgänge mit den lokalen Ressourcen fortgesetzt werden, und die Replizierung wird automatisch wieder aufgenommen, sobald das WAN wiederhergestellt ist.	Ermöglicht Grid-Administratoren, Uptime, SLA und andere vertragliche Verpflichtungen zu erfüllen und Business-Continuity-Pläne zu implementieren.	—
S3-spezifische Datenzugriffssicherheitsfunktionen	AWS Signature Version 2 und Version 4	Das Signieren von API-Anforderungen bietet eine Authentifizierung für S3-API-Vorgänge. Amazon unterstützt zwei Versionen von Signature Version 2 und Version 4. Beim Signaturprozess wird die Identität des Anforderers überprüft, die Daten während der Übertragung geschützt und vor potenziellen Replay-Angriffen geschützt.	Entspricht der AWS-Empfehlung für Signature Version 4 und ermöglicht Abwärtskompatibilität mit älteren Anwendungen mit Signature Version 2.

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
—	S3-Objektsperre	Die S3-Objektsperrfunktion in StorageGRID ist eine Objektschutzlösung, die S3-Objektsperrung in Amazon S3 entspricht.	Ermöglicht Mandanten, Buckets mit aktivierter S3 Object Lock zu erstellen, um Vorschriften zu erfüllen, für die bestimmte Objekte für einen festgelegten Zeitraum oder auf unbestimmte Zeit aufbewahrt werden müssen.
SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)	Sichere Speicherung der S3 Zugangsdaten	S3-Zugriffsschlüssel werden in einem Format gespeichert, das durch eine Passwort-Hashing-Funktion (SHA-2) geschützt ist.	Ermöglicht die sichere Speicherung von Zugriffsschlüsseln durch eine Kombination aus Schlüssellänge (10^{31} zufällig generierte Nummer) und einem Passwort-Hashing-Algorithmus.
—	Zeitgebundene S3-Zugriffsschlüssel	Beim Erstellen eines S3 Zugriffsschlüssels für einen Benutzer können Kunden ein Ablaufdatum und eine Uhrzeit für den Zugriffsschlüssel festlegen.	Bietet Grid-Administratoren die Möglichkeit, temporäre S3-Zugriffsschlüssel bereitzustellen.
—	Mehrere Zugriffsschlüssel pro Benutzerkonto	Mit StorageGRID können mehrere Zugriffsschlüssel erstellt und gleichzeitig für ein Benutzerkonto aktiv werden. Da jede API-Aktion mit einem Mandanten-Benutzerkonto und einem Zugriffsschlüssel protokolliert wird, bleibt die Nichtabstreitbarkeit erhalten, obwohl mehrere Schlüssel aktiv sind.	Ermöglicht Clients das unterbrechungsfreie Drehen von Zugriffsschlüsseln und ermöglicht jedem Client einen eigenen Schlüssel, wodurch die gemeinsame Nutzung von Schlüsseln über Clients hinweg vermieden wird.

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
—	S3 IAM-Zugriffsrichtlinie	StorageGRID unterstützt S3 IAM-Richtlinien, sodass Grid-Administratoren granulare Zugriffssteuerung nach Mandanten, Bucket oder Objektpräfix angeben können. StorageGRID unterstützt außerdem IAM-Richtlinienbedingungen und -Variablen, wodurch dynamischere Zugriffssteuerungsrichtlinien ermöglicht werden.	Ermöglicht Grid-Administratoren, die Zugriffssteuerung nach Benutzergruppen für den gesamten Mandanten festzulegen; ermöglicht es den Mandantenbenutzern auch, die Zugriffssteuerung für ihre eigenen Buckets und Objekte festzulegen.
—	Serverseitige Verschlüsselung mit über StorageGRID gemanagten Schlüsseln (SSE)	StorageGRID unterstützt SSE und ermöglicht mandantenfähigen Schutz von Daten im Ruhezustand mit von StorageGRID gemanagten Verschlüsselungen.	Ermöglicht Mandanten die Verschlüsselung von Objekten. Zum Schreiben und Abrufen dieser Objekte ist ein Verschlüsselungsschlüssel erforderlich.
SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)	Serverseitige Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln (SSE-C)	StorageGRID unterstützt SSE-C und ermöglicht damit mandantenfähigen Schutz von Daten im Ruhezustand mit vom Client gemanagten Verschlüsselungsschlüsseln. Obwohl StorageGRID alle Objektverschlüsselung und -Entschlüsselung managt, muss der Client bei SSE-C die Schlüssel selbst managen.	Ermöglicht Clients die Verschlüsselung von Objekten mit den Schlüsseln, die sie steuern. Zum Schreiben und Abrufen dieser Objekte ist ein Verschlüsselungsschlüssel erforderlich.

Sicherheit von Objekten und Metadaten

Entdecken Sie die Sicherheitsfunktionen für Objekte und Metadaten in StorageGRID.

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Advanced Encryption Standard (AES) Server-seitige Objektverschlüsselung	StorageGRID bietet serverseitige Objektverschlüsselung nach AES 128 und AES 256. Grid-Administratoren können die Verschlüsselung als globale Standardeinstellung aktivieren. StorageGRID unterstützt außerdem den S3 x-amz-Server-seitigen Verschlüsselungsheader, um die Verschlüsselung für einzelne Objekte zu aktivieren oder zu deaktivieren. Wenn diese Option aktiviert ist, werden die Objekte bei der Speicherung bzw. Übertragung zwischen den Grid-Nodes verschlüsselt.	Unterstützt die sichere Speicherung und Übertragung von Objekten, unabhängig von der zugrunde liegenden Storage-Hardware.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)
Integriertes Verschlüsselungsmanagement	Bei aktivierter Verschlüsselung wird jedes Objekt mit einem zufällig generierten eindeutigen symmetrischen Schlüssel verschlüsselt, der ohne externen Zugriff in StorageGRID gespeichert wird.	Ermöglicht die Verschlüsselung von Objekten ohne externes Verschlüsselungsmanagement	
FIPS 140-2-2-konforme Verschlüsselungsfestplatten (Federal Information Processing Standard	Die StorageGRID Appliances SG5712, SG5760, SG6060 und SGF6024 bieten die Möglichkeit, FIPS 140-2-2-konforme Verschlüsselungsfestplatten anzubieten. Die Schlüssel für die Festplatten können optional von einem externen KMIP-Server gemanagt werden.	Ermöglicht sichere Speicherung von Systemdaten, Metadaten und Objekten StorageGRID bietet außerdem softwarebasierte Objektverschlüsselung, die die Storage und die Übertragung von Objekten sichert.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Hintergrundintegrität sprüfung und Selbstheilung	StorageGRID nutzt einen Verriegelungsmechanismus aus Hashes, Prüfsummen und zyklischen Redundanzprüfungen (Cyclic Redundancy Checks, CRCs) auf Objekt- und Unterobjektebene, um sich sowohl im Storage- als auch auf der Übertragungsstrecke vor Dateninkonsistenz, Manipulation oder Änderung zu schützen. StorageGRID erkennt beschädigte und manipulierte Objekte automatisch und ersetzt sie. Gleichzeitig werden die geänderten Daten in Quarantäne verschoben und der Administrator benachrichtigt.	Grid-Administratoren können SLAs, Vorschriften und andere Verpflichtungen hinsichtlich der Datenaufbewahrung erfüllen. Unterstützt Kunden dabei, Ransomware oder Viren zu erkennen, die versuchen, Daten zu verschlüsseln, zu manipulieren oder zu ändern.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)
Richtlinienbasierte Objektplatzierung und -Aufbewahrung	Mit StorageGRID können Grid-Administratoren ILM-Regeln konfigurieren, die die Objektaufbewahrung, -Platzierung, -Sicherung, -Übertragung und -Verfallsdaten festlegen. Grid-Administratoren können StorageGRID konfigurieren, um Objekte nach Metadaten zu filtern und Regeln auf verschiedenen Granularitätsebenen anzuwenden, einschließlich Grid-weiter, Mandant, Bucket, Schlüsselpräfix, und benutzerdefinierte Metadaten-Schlüssel-Wert-Paare. StorageGRID hilft sicherzustellen, dass Objekte während ihrer gesamten Lebenszyklen gemäß den ILM-Regeln gespeichert werden, es sei denn, sie werden vom Client ausdrücklich gelöscht.	Hilft bei der Durchsetzung von Datenablage, Datensicherheit und Datenhaltung. Unterstützt Kunden bei der Einhaltung von SLAs für Langlebigkeit, Verfügbarkeit und Performance.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Metadaten werden im Hintergrund gescannt	StorageGRID scannt regelmäßig Objektmetadaten im Hintergrund, um Änderungen an der Platzierung oder Sicherung von Objektdaten gemäß ILM anzuwenden.	Hilft bei der Erkennung beschädigter Objekte.	
Abstimmbare Konsistenz	Mandanten können Konsistenzstufen auf Bucket-Ebene auswählen, um sicherzustellen, dass Ressourcen wie standortübergreifende Konnektivität verfügbar sind.	Bietet die Möglichkeit, Schreibvorgänge nur dann in das Grid zu übertragen, wenn eine erforderliche Anzahl von Standorten oder Ressourcen verfügbar ist.	

Sicherheitsfunktionen für die Administration

Entdecken Sie die Sicherheitsfunktionen für die Administration in StorageGRID.

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Serverzertifikat (Grid-Managementoberfläche)	Grid-Administratoren können die Grid-Managementoberfläche so konfigurieren, dass ein von der vertrauenswürdigen CA ihres Unternehmens signiertes Serverzertifikat verwendet wird.	Ermöglicht die Verwendung von digitalen Zertifikaten, die von ihrer standardmäßigen vertrauenswürdigen Zertifizierungsstelle signiert sind, um die Management-UI und den API-Zugriff zwischen einem Management-Client und dem Grid zu authentifizieren.	—

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Administrative Benutzerauthentifizierung	Administratorbenutzer werden mit Benutzername und Passwort authentifiziert. Administrative Benutzer und Gruppen können lokal oder föderiert sein und aus dem Active Directory oder LDAP des Kunden importiert werden. Lokale Kontokennwörter werden in einem durch bcrypt geschützten Format gespeichert; Kommandozeilen-Passwörter werden in einem durch SHA-2 geschützten Format gespeichert.	Authentifiziert den administrativen Zugriff auf die Management-UI und -APIs.	—
SAML Support	StorageGRID unterstützt Single Sign-On (SSO) unter Verwendung des SAML 2.0-Standards (Security Assertion Markup Language 2.0). Wenn SSO aktiviert ist, müssen alle Benutzer von einem externen Identitäts-Provider authentifiziert werden, bevor sie auf den Grid Manager, den Mandanten-Manager, die Grid-Management-API oder die Mandantenmanagement-API zugreifen können. Lokale Benutzer können sich nicht bei StorageGRID anmelden.	Zusätzliche Sicherheitsstufen für Grid- und Mandantenadministratoren wie SSO und Multi-Faktor-Authentifizierung (MFA)	NIST SP800-63
Granulare Berechtigungskontrolle	Grid-Administratoren können Rollen Berechtigungen zuweisen und administrativen Benutzergruppen Rollen zuweisen. Dadurch werden die Aufgaben erzwungen, die administrative Clients sowohl über die Management-UI als auch über APIs ausführen dürfen.	Ermöglicht Grid-Administratoren das Management der Zugriffssteuerung für Admin-Benutzer und -Gruppen.	—

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Verteilte Audit-Protokollierung	StorageGRID bietet eine integrierte, verteilte Audit-Protokollierungs-Infrastruktur, die auf Hunderte Nodes an bis zu 16 Standorten skalierbar ist. Die StorageGRID-Software-Knoten erzeugen Audit-Meldungen, die über ein redundantes Audit-Relay-System übertragen und schließlich in einem oder mehreren Audit-Log-Repositorys erfasst werden. Audit-Meldungen erfassen Ereignisse auf Objektebene, z. B. Client-initiierte S3-API-Operationen, Objekt-Lebenszyklus-Ereignisse durch ILM, Zustandsprüfungen von Objekten im Hintergrund sowie Konfigurationsänderungen, die über die Management-UI oder -APIs vorgenommen werden. Audit-Protokolle können über CIFS oder NFS von Admin-Nodes exportiert werden, sodass Audit-Meldungen durch Tools wie Splunk und ELK abgebaut werden. Es gibt vier Arten von Überwachungsmeldungen: • Systemaudits Meldungen • Audit-Meldungen zu Objekt-Storage • HTTP-Protokollauditmeldungen • Meldungen von Management-Audits	Bietet Grid-Administratoren einen bewährten und skalierbaren Audit-Service und ermöglicht es ihnen, Audit-Daten für verschiedene Ziele zu extrahieren. Zu diesen Zielen gehören Fehlerbehebung, Revision der SLA-Performance, Client-Datenzugriffs-API-Operationen und Änderungen der Managementkonfiguration.	—

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Systemprüfung	Systemauditmeldungen erfassen systembezogene Ereignisse, wie Grid-Node-Status, Erkennung beschädigter Objekte, Objekte, die per ILM-Regel an allen angegebenen Standorten festgelegt wurden, und den Fortschritt systemweiter Wartungsaufgaben (Grid-Aufgaben).	Unterstützt Kunden bei der Behebung von Systemproblemen und liefert den Nachweis, dass Objekte gemäß SLA gespeichert werden. SLAs werden durch StorageGRID ILM-Regeln implementiert und sind integritätsgeschützt.	—
Objekt-Storage-Prüfung	Objekt-Storage-Audit-Nachrichten erfassen Objekt-API-Transaktionen und Lifecycle-bezogene Ereignisse. Zu diesen Ereignissen gehören Objekt-Storage und -Abruf, Grid-Node zu Grid-Node-Transfers und Überprüfungen.	Unterstützt Kunden bei der Prüfung des Fortschritts der Daten über das System und bei der Bereitstellung von SLAs mit dem Namen StorageGRID ILM.	—
HTTP-Protokollaudit	HTTP-Protokollauditmeldungen erfassen HTTP-Protokollinteraktionen im Zusammenhang mit Client-Anwendungen und StorageGRID-Knoten. Darüber hinaus können Kunden bestimmte HTTP-Anforderungsheader (z. B. X-Forwarded-for und Benutzer-Metadaten [x-amz-meta-*]) in einem Audit erfassen.	Unterstützt Kunden beim Prüfen von API-Operationen für den Datenzugriff zwischen Clients und StorageGRID und bei der Nachverfolgung einer Aktion auf ein einzelnes Benutzerkonto und einen Zugriffsschlüssel. Kunden können zudem Benutzermetadaten bei einem Audit protokollieren und mithilfe von Tools für das Mining wie Splunk oder ELK nach Objekt-Metadaten suchen.	—
Management-Prüfung	Management Audit-Nachrichten protokollieren Benutzeranforderungen von Administratoren an die Management-UI (Grid Management Interface) oder APIs. Jede Anfrage, die keine GET- oder HEAD-Anforderung an die API ist, protokolliert eine Antwort mit dem Benutzernamen, der IP und der Art der Anfrage an die API.	Hilft Grid-Administratoren, eine Aufzeichnung der Änderungen an der Systemkonfiguration zu erstellen, die von welchem Benutzer von welcher Quell-IP und welcher Ziel-IP zu welchem Zeitpunkt vorgenommen wurden.	—

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
TLS 1.3-Unterstützung für Management UI- und API-Zugriff	TLS erstellt ein Handshake-Protokoll für die Kommunikation zwischen einem Admin-Client und einem StorageGRID-Admin-Node.	Ein administrativer Client und ein StorageGRID können sich gegenseitig identifizieren und authentifizieren und kommunizieren mit Vertraulichkeit und Datenintegrität.	—
SNMPv3 für StorageGRID-Überwachung	SNMPv3 bietet Sicherheit durch eine starke Authentifizierung und Datenverschlüsselung zum Schutz der Privatsphäre. Mit v3 werden die Protokolldateneinheiten verschlüsselt, wobei CBC-DES für das Verschlüsselungsprotokoll verwendet wird. Die Benutzerauthentifizierung, wer die Protokolldateneinheit gesendet hat, wird entweder über das HMAC-SHA- oder das HMAC-MD5-Authentifizierungsprotokoll bereitgestellt. SNMPv2 und v1 werden weiterhin unterstützt.	Unterstützt Grid-Administratoren bei der Überwachung des StorageGRID-Systems durch Aktivieren eines SNMP-Agenten auf dem Admin-Knoten.	—
Client-Zertifikate für Prometheus Kennzahlenexport	Grid-Administratoren können Client-Zertifikate hochladen oder generieren, die für einen sicheren, authentifizierten Zugriff auf die StorageGRID Prometheus-Datenbank verwendet werden können.	Grid-Administratoren können StorageGRID mithilfe von Client-Zertifikaten extern mit Applikationen wie Grafana überwachen.	—

Plattformsicherheitsfunktionen

Erfahren Sie mehr über die Plattformsicherheitsfunktionen in StorageGRID.

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Interne Public-Key-Infrastruktur (PKI), Node-Zertifikate und TLS	StorageGRID verwendet interne PKI- und Node-Zertifikate zur Authentifizierung und Verschlüsselung der Kommunikation zwischen den Knoten. Die Kommunikation zwischen den Knoten ist durch TLS gesichert.	Unterstützt den sicheren Systemdatenverkehr über LAN oder WAN, insbesondere bei standortübergreifenden Bereitstellungen.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)
Knoten-Firewall	StorageGRID konfiguriert automatisch IP-Tabellen und Firewallregeln zur Steuerung von eingehendem und ausgehendem Netzwerk-Traffic sowie zum Schließen nicht verwendeter Ports.	Der Schutz von StorageGRID-Systemen, Daten und Metadaten vor unaufgefordertem Netzwerkverkehr	—
OS-Sicherung	Das Basis-Betriebssystem der physischen Appliances und virtuellen Nodes von StorageGRID ist gehärtet; zugehörige Softwarepakete werden entfernt.	Minimiert mögliche Angriffsflächen.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)
Regelmäßige Plattform- und Software-Updates	StorageGRID veröffentlicht regelmäßige Software-Versionen, die das Betriebssystem, Binärdateien von Applikationen und Software Updates enthalten.	Hilft dabei, das StorageGRID System mit aktueller Software und Binärdateien zu aktualisieren.	—
Root-Anmeldung über Secure Shell (SSH) deaktiviert	Die Root-Anmeldung über SSH ist auf allen StorageGRID Nodes deaktiviert. SSH-Zugriff verwendet Zertifikatauthentifizierung.	Hilft Kunden, sich vor einem möglichen Remote-Passwort-Cracking der Root-Anmeldung zu schützen.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)
Automatisierte Zeitsynchronisierung	StorageGRID synchronisiert Systemuhren jedes Node automatisch mit mehreren externen NTP-Servern (Time Network Time Protocol). Mindestens vier NTP-Server von Stratum 3 oder höher sind erforderlich.	Stellt die gleiche Zeitreferenz für alle Knoten sicher.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)

Funktion	Funktion	Auswirkungen	Einhaltung gesetzlicher Vorschriften
Getrennte Netzwerke für Client-, Admin- und internen Grid-Traffic	StorageGRID Software Nodes und Hardware Appliances unterstützen mehrere virtuelle und physische Netzwerkschnittstellen, sodass die Kunden den Client-, Administrations- und internen Grid-Traffic über verschiedene Netzwerke trennen können.	Grid-Administratoren können internen und externen Netzwerkverkehr trennen und Datenverkehr über Netzwerke mit unterschiedlichen SLAs bereitstellen.	—
Mehrere virtuelle LAN-Schnittstellen (VLAN)	StorageGRID unterstützt die Konfiguration von VLAN-Schnittstellen auf Ihren StorageGRID-Client- und Grid-Netzwerken.	Grid-Administratoren können den Datenverkehr von Applikationen partitionieren und isolieren, um so Sicherheit, Flexibilität und Performance zu gewährleisten.	
Nicht Vertrauenswürdiges Client-Netzwerk	Die nicht vertrauenswürdige Client-Netzwerkschnittstelle akzeptiert eingehende Verbindungen nur an Ports, die explizit als Load-Balancer-Endpunkte konfiguriert wurden.	Stellt sicher, dass Schnittstellen geschützt sind, die nicht vertrauenswürdigen Netzwerken zugänglich sind.	—
Konfigurierbare Firewall	Verwaltung offener und geschlossener Ports für Admin-, Grid- und Client-Netzwerke.	Ermöglichen Sie Grid-Administratoren, den Zugriff auf Ports zu steuern und den genehmigten Gerätezugriff auf die Ports zu verwalten.	
Erweitertes SSH-Verhalten	Beim Upgrade eines Node auf StorageGRID 11.5 werden neue SSH-Hostzertifikate und Hostschlüssel generiert.	Verbessert den man-in-the-Middle-Angriffsschutz.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)
Node-Verschlüsselung	Als Teil der neuen KMS-Host-Server-Verschlüsselungsfunktion wird dem StorageGRID-Appliance-Installationsprogramm eine neue Einstellung für die Knotenverschlüsselung hinzugefügt.	Diese Einstellung muss während der Hardwarekonfigurationsphase der Appliance-Installation aktiviert werden.	SEC-Regel 17a-4(f) CTFC 1.31(c)-(d) (FINRA) Regel 4511(c)

Cloud-Integration

Integration von StorageGRID in Cloud-Services

Funktion	Funktion	Auswirkungen
Benachrichtigungs-basierte Virus-Scan	Die StorageGRID Plattform-Services unterstützen Ereignisbenachrichtigungen. Ereignisbenachrichtigungen können mit externen Cloud Computing Services verwendet werden, um Workflows zur Virenprüfung der Daten zu starten.	Mandantenadministratoren können einen Virus-Scan von Daten mithilfe von externen Cloud-Computing-Services auslösen.