TR-4645: Funzionalità di sicurezza

How to enable StorageGRID in your environment

NetApp
July 05, 2024

Sommario

TR-4645: Funzionalità di sicurezza

Proteggi dati e metadati StorageGRID in un archivio di oggetti

Scopri le funzionalità di sicurezza integrate della soluzione di storage a oggetti StorageGRID.

Questa è una panoramica delle numerose funzionalità di protezione di NetApp® StorageGRID®, che includono l'accesso ai dati, gli oggetti e i metadati, l'accesso amministrativo e la protezione della piattaforma. È stato aggiornato per includere le funzioni più recenti rilasciate con StorageGRID 11,8.

La sicurezza è parte integrante della soluzione di storage a oggetti NetApp StorageGRID. La sicurezza è particolarmente importante, in quanto molti tipi di dati rich content adatti allo storage a oggetti sono anche sensibili, soggetti a normative e conformità. Con la continua evoluzione delle funzionalità di StorageGRID, il software rende disponibili molte funzionalità di sicurezza preziose per proteggere il livello di sicurezza di un'organizzazione e aiutare l'organizzazione a soddisfare le Best practice del settore.

In questo documento viene fornita una panoramica delle numerose funzioni di protezione di StorageGRID 11,8, suddivise in cinque categorie:

- Funzioni di sicurezza per l'accesso ai dati
- Funzionalità di sicurezza di oggetti e metadati
- Funzioni di protezione di amministrazione
- Funzioni di sicurezza della piattaforma
- Integrazione del cloud

Questo documento è destinato a essere una scheda tecnica di protezione, non descrive in dettaglio come configurare il sistema in modo che supporti le funzioni di protezione enumerate all'interno delle quali non sono configurate per impostazione predefinita. La "Guida alla tempra StorageGRID" è disponibile nella pagina ufficiale "Documentazione StorageGRID" .

Oltre alle funzionalità descritte in questo rapporto, StorageGRID segue la "Criteri di notifica e risposta alle vulnerabilità di protezione dei prodotti NetApp". Le vulnerabilità segnalate vengono verificate e risolte in base al processo di risposta agli incidenti di sicurezza del prodotto.

NetApp StorageGRID offre funzionalità di sicurezza avanzate per casi di utilizzo dello storage a oggetti aziendale molto esigenti.

Dove trovare ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti e/o siti Web:

- NetApp StorageGRID: Valutazione della conformità SEC 17a-4(f), FINRA 4511(c) e CFTC 1,31(c)-(d) https://www.netapp.com/media/9041-ar-cohasset-netapp-storagegrid-sec-assessment.pdf
- Pagina della documentazione di StorageGRID 11,8 https://docs.netapp.com/us-en/storagegrid-118/
- Pagina risorse documentazione StorageGRID https://www.netapp.com/data-storage/storagegrid/documentation/

- Documentazione dei prodotti NetApp https://www.netapp.com/support-and-training/documentation/

Termini e acronimi

In questa sezione vengono fornite le definizioni della terminologia utilizzata nel documento.

Termine o acronimo	Definizione
S3	Simple Storage Service.
Client	Applicazione in grado di interfacciarsi con StorageGRID tramite il protocollo S3 per l'accesso ai dati o il protocollo HTTP per la gestione.
Amministratore tenant	L'amministratore dell'account tenant StorageGRID
Utente tenant	Un utente all'interno di un account tenant StorageGRID
TLS	Transport Layer Security
ILM	Gestione del ciclo di vita delle informazioni
LAN	Local Area Network (rete locale)
Amministratore di grid	L'amministratore del sistema StorageGRID
Griglia	Il sistema StorageGRID
Bucket	Un contenitore per gli oggetti memorizzati in S3
LDAP	Lightweight Directory Access Protocol
SEC.	Securities and Exchange Commission; regola i membri di Exchange, i broker o i dealer
FINRA	Autorità di regolamentazione del settore finanziario; difende i requisiti di formato e media della norma SEC 17a-4(f)
CFTC	Commodity Futures Trading Commission; regola il commodity futures trading
NIST	Istituto Nazionale di Standard e tecnologia

Funzioni di sicurezza per l'accesso ai dati

Scopri le funzionalità di sicurezza dell'accesso ai dati di StorageGRID.

Funzione	Funzione	Impatto	Conformità normativa
TLS (Transport Layer Security) configurabile	TLS stabilisce un protocollo di handshake per la comunicazione tra un client e un nodo di gateway StorageGRID, un nodo storage o un endpoint del bilanciamento del carico. StorageGRID supporta le seguenti suite di crittografia per 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 Supporto di TLS v1,2 e 1,3. SSLv3, TLS v1,1 e versioni precedenti non sono più supportati.	Consente a un client e a StorageGRID di identificarsi e autenticarsi reciprocamente e comunicare con riservatezza e integrità dei dati. Garantisce l'uso di una versione TLS recente. Le crittografie sono ora configurabili nelle impostazioni di configurazione/protezione	—

Funzione	Funzione	Impatto	Conformità normativa
Certificato server configurabile (endpoint bilanciamento del carico)	Gli amministratori di grid possono configurare gli endpoint di Load Balancer in modo da generare o utilizzare un certificato server.	Consente l'utilizzo di certificati digitali firmati dalla propria autorità di certificazione (CA) standard per autenticare le operazioni API degli oggetti tra la griglia e il client per ogni endpoint di bilanciamento del carico.	—
Certificato server configurabile (endpoint API)	Gli amministratori della griglia possono configurare centralmente tutti gli endpoint delle API StorageGRID in modo che utilizzino un certificato server firmato dalla CA attendibile dell'organizzazione.	Consente l'utilizzo di certificati digitali firmati dalla CA standard e attendibile per autenticare le operazioni API degli oggetti tra un client e la griglia.	—

Funzione	Funzione	Impatto	Conformità normativa
Multi-tenancy	StorageGRID supporta tenant multipli per grid e ogni tenant ha il proprio namespace. Un tenant offre un protocollo S3:1; per impostazione predefinita, l'accesso a bucket/container e oggetti è limitato agli utenti all'interno dell'account. I tenant possono avere un utente (ad esempio, un'implementazione aziendale, in cui ogni utente ha un proprio account) o più utenti (ad esempio, un'implementazione di un provider di servizi, in cui ogni account è un'azienda e un cliente del provider di servizi). Gli utenti possono essere locali o federati; gli utenti federati sono definiti da Active Directory o LDAP (Lightweight Directory Access Protocol). StorageGRID fornisce una dashboard per tenant, in cui gli utenti accedono utilizzando le credenziali dell'account locale o federato. Gli utenti possono accedere ai report visualizzati sull'utilizzo del tenant rispetto alla quota assegnata dall'amministratore del grid, incluse le informazioni sull'utilizzo nei dati e negli oggetti archiviati dai bucket. Gli utenti con autorizzazioni amministrative possono eseguire attività di amministrazione del sistema a livello di tenant, come la gestione di utenti, gruppi e chiavi di accesso.	Consente agli amministratori di StorageGRID di ospitare i dati da più tenant isolando al contempo l'accesso al tenant e di stabilire l'identità dell'utente federando gli utenti con un provider di identità esterno, come Active Directory o LDAP.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Mancata pubblicazione delle credenziali di accesso	Ogni operazione S3 viene identificata e registrata con un account tenant, un utente e una chiave di accesso univoci.	Consente agli amministratori Grid di stabilire quali azioni API vengono eseguite da ciascun utente.	—

Funzione	Funzione	Impatto	Conformità normativa
Accesso anonimo disattivato	Per impostazione predefinita, l'accesso anonimo è disattivato per gli account S3. Un richiedente deve disporre di una credenziale di accesso valida per un utente valido nell'account tenant per accedere a bucket, contenitori o oggetti all'interno dell'account. L'accesso anonimo a bucket o oggetti S3 può essere abilitato con un criterio IAM esplicito.	Consente agli amministratori Grid di disabilitare o controllare l'accesso anonimo a bucket/container e oggetti.	—
WORM di conformità	Progettato per soddisfare i requisiti della norma SEC 17a-4(f) e convalidato da Cohasset. I clienti possono garantire la conformità a livello della benna. La ritenzione può essere estesa ma mai ridotta. Le regole di Information Lifecycle management (ILM) applicano livelli minimi di protezione dei dati.	Consente ai tenant con requisiti di data retention normativi per consentire protezione WORM su oggetti memorizzati e metadati di oggetti.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
WORM	Gli amministratori di grid possono abilitare IL WORM a livello di griglia attivando l'opzione Disattiva modifica client, che impedisce ai client di sovrascrivere o eliminare oggetti o metadati di oggetti in tutti gli account tenant. Gli amministratori dei tenant S3 possono inoltre abilitare il WORM in base al tenant, bucket o prefisso dell'oggetto specificando il criterio IAM, che include l'autorizzazione personalizzata S3: PutOverwriteObject per la sovrascrittura di oggetti e metadati.	Permette agli amministratori di Grid e agli amministratori dei tenant di controllare la protezione WORM su oggetti archiviati e metadati di oggetti.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)

Funzione	Funzione	Impatto	Conformità normativa
Gestione della chiave di crittografia del server host KMS	Gli amministratori di grid possono configurare uno o più server KMS (External Key Management Server) in Grid Manager in modo da fornire chiavi di crittografia ai servizi StorageGRID e alle appliance di storage. Ogni server host KMS o cluster di server host KMS utilizza il Key Management Interoperability Protocol (KMIP) per fornire una chiave di crittografia ai nodi di appliance nel sito StorageGRID associato.	Crittografia dei dati a riposo attivata. Una volta crittografati i volumi dell'appliance, non è possibile accedere ai dati sull'appliance a meno che il nodo non sia in grado di comunicare con il server host KMS.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Failover automatico	StorageGRID offre ridondanza integrata e failover automatizzato. L'accesso ad account, bucket e oggetti tenant può continuare anche in caso di guasti multipli, da dischi o nodi a interi siti. StorageGRID è consapevole delle risorse e reindirizza automaticamente le richieste ai nodi disponibili e alle posizioni dei dati. I siti StorageGRID possono persino funzionare in modalità island; se un'interruzione della WAN disconnette un sito dal resto del sistema, le letture e le scritture possono continuare con le risorse locali e la replica riprende automaticamente quando la WAN viene ripristinata.	Consente agli amministratori Grid di gestire i tempi di attività, gli SLA e altri obblighi contrattuali e di implementare i piani di business continuity.	—
Funzionalità di protezione dell'accesso ai dati specifiche per S3	Firma AWS versione 2 e versione 4	La firma delle richieste API fornisce l'autenticazione per le operazioni API S3. Amazon supporta due versioni di Signature versione 2 e 4. Il processo di firma verifica l'identità del richiedente, protegge i dati in transito e protegge da potenziali attacchi di riproduzione.	Si allinea al suggerimento AWS per la versione Signature 4 e consente la compatibilità con le versioni precedenti delle applicazioni con la versione Signature 2.

Funzione	Funzione	Impatto	Conformità normativa
—	Blocco oggetti S3	La funzionalità blocco oggetti S3 in StorageGRID è una soluzione di protezione degli oggetti equivalente a blocco oggetti S3 in Amazon S3.	Consente ai tenant di creare bucket con blocco oggetti S3 abilitato per la conformità alle normative che richiedono la conservazione di determinati oggetti per un periodo di tempo fisso o indefinitamente.
Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)	Archiviazione protetta di credenziali S3	Le chiavi di accesso S3 sono memorizzate in un formato protetto da una funzione di hashing di password (SHA-2).	Consente l'archiviazione protetta delle chiavi di accesso mediante una combinazione di lunghezza della chiave (un numero generato casualmente da 10^{31}) e un algoritmo di hash delle password.
—	S3 tasti di accesso con limite di tempo	Quando si crea una chiave di accesso S3 per un utente, i clienti possono impostare una data e un'ora di scadenza sulla chiave di accesso.	Offre agli amministratori Grid la possibilità di fornire chiavi di accesso S3 temporanee.
—	Più chiavi di accesso per account utente	StorageGRID consente di creare più chiavi di accesso e contemporaneamente di attivarle per un account utente. Poiché ogni azione API viene registrata con un account utente tenant e una chiave di accesso, la non ripubblicazione viene mantenuta nonostante siano attive più chiavi.	Consente ai client di ruotare le chiavi di accesso senza interruzioni e consente a ciascun client di disporre della propria chiave, scoraggiando la condivisione delle chiavi tra i client.

Funzione	Funzione	Impatto	Conformità normativa
—	S3 criterio di accesso IAM	StorageGRID supporta policy IAM S3, consentendo agli amministratori Grid di specificare un controllo granulare degli accessi per tenant, bucket o prefisso oggetto. StorageGRID supporta inoltre le variabili e le condizioni dei criteri IAM, consentendo criteri di controllo degli accessi più dinamici.	Consente agli amministratori di Grid di specificare il controllo dell'accesso per gruppi di utenti per l'intero tenant; inoltre, permette agli utenti tenant di specificare il controllo dell'accesso per i propri bucket e oggetti.
—	Crittografia lato server con chiavi gestite da StorageGRID (SSE)	StorageGRID supporta SSE, consentendo una protezione multitenant dei dati a riposo con chiavi di crittografia gestite da StorageGRID.	Consente ai tenant di crittografare gli oggetti. La chiave di crittografia è necessaria per scrivere e recuperare questi oggetti.
Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)	Crittografia lato server con chiavi di crittografia fornite dal cliente (SSE-C)	StorageGRID supporta SSE-C, abilitando la protezione multitenant dei dati a riposo con chiavi di crittografia gestite dal client. Sebbene StorageGRID gestisca tutte le operazioni di crittografia e decrittografia degli oggetti, con SSE-C, il client deve gestire autonomamente le chiavi di crittografia.	Consente ai client di crittografare gli oggetti con le chiavi controllate dall'utente. La chiave di crittografia è necessaria per scrivere e recuperare questi oggetti.

Sicurezza di oggetti e metadati

Esplora le funzionalità di sicurezza degli oggetti e dei metadati in StorageGRID.

Funzione	Funzione	Impatto	Conformità normativa
Crittografia degli oggetti lato server AES (Advanced Encryption Standard)	StorageGRID fornisce la crittografia degli oggetti sul lato server basata su AES 128 e AES 256. Gli amministratori della griglia possono abilitare la crittografia come impostazione predefinita globale. StorageGRID supporta inoltre l'intestazione di crittografia S3 x-amz-lato server per consentire l'attivazione o la disattivazione della crittografia in base all'oggetto. Se abilitato, gli oggetti vengono crittografati quando vengono archiviati o in transito tra i nodi della griglia.	Aiuta a proteggere lo storage e la trasmissione degli oggetti, indipendentemente dall'hardware per lo storage sottostante.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Gestione delle chiavi integrata	Quando la crittografia è attivata, ogni oggetto viene crittografato con una chiave simmetrica univoca generata in modo casuale, memorizzata all'interno di StorageGRID senza accesso esterno.	Consente la crittografia degli oggetti senza richiedere una gestione esterna delle chiavi.	
Dischi di crittografia conformi a Federal Information Processing Standard (FIPS) 140-2-2	Le appliance SG5712, SG5760, SG6060 e SGF6024 StorageGRID offrono l'opzione di dischi di crittografia conformi FIPS 140-2-2. Le chiavi di crittografia dei dischi possono essere facoltativamente gestite da un server KMIP esterno.	Abilita lo storage sicuro di dati, metadati e oggetti di sistema. Fornisce inoltre una crittografia degli oggetti basata su software StorageGRID, che protegge storage e trasmissione di oggetti.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Scansione di integrità in background e autoriparazione	StorageGRID utilizza un meccanismo di interblocco costituito da hash, checksum e controlli di ridondanza ciclici (CRC) a livello di oggetto e sottooggetto per proteggere da incoerenza, manomissioni o modifiche dei dati, sia quando gli oggetti sono in storage che in transito. StorageGRID rileva automaticamente gli oggetti corrotti e manomessi e li sostituisce, mettendo in quarantena i dati modificati e avvisando l'amministratore.	Permette agli amministratori di grid di soddisfare SLA, normative e altri obblighi in termini di conservazione dei dati. Aiuta i clienti a rilevare ransomware o virus che tentano di crittografare, manomettere o modificare i dati.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)

Funzione	Funzione	Impatto	Conformità normativa
Conservazione e posizionamento degli oggetti basati su policy	StorageGRID consente agli amministratori di grid di configurare regole ILM che specificano conservazione, posizionamento, protezione, transizione e scadenza degli oggetti. Gli amministratori del grid possono configurare StorageGRID per filtrare gli oggetti in base ai propri metadati e applicare regole a vari livelli di granularità, tra cui Grid-wide, tenant, bucket, key prefix, coppie di valori chiave e metadati definiti dall'utente. StorageGRID contribuisce a garantire che gli oggetti vengano memorizzati in base alle regole ILM durante il loro ciclo di vita, a meno che non vengano esplicitamente eliminati dal client.	Aiuta ad applicare il posizionamento, la protezione e la conservazione dei dati. Aiuta i clienti a raggiungere gli SLA relativi a durata, disponibilità e performance.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Scansione dei metadati in background	StorageGRID esegue periodicamente la scansione dei metadati degli oggetti in background per applicare modifiche al posizionamento o alla protezione dei dati degli oggetti come specificato da ILM.	Aiuta a rilevare gli oggetti danneggiati.	
Uniformità regolabile	I tenant possono selezionare livelli di coerenza a livello del bucket per garantire che siano disponibili risorse come la connettività multisito.	Offre l'opzione per eseguire il commit delle scritture sulla griglia solo quando è disponibile un numero richiesto di siti o risorse.	

Funzioni di protezione di amministrazione

Scoprite le funzioni di protezione dell'amministrazione in StorageGRID.

Funzione	Funzione	Impatto	Conformità normativa
Certificato server (Grid Management Interface)	Gli amministratori di rete possono configurare Grid Management Interface in modo che utilizzi un certificato server firmato dalla CA attendibile dell'organizzazione.	Consente l'utilizzo di certificati digitali firmati dalla CA standard e attendibile per autenticare l'accesso all'interfaccia utente di gestione e all'API tra un client di gestione e la griglia.	—
Autenticazione utente amministrativo	Gli utenti amministrativi vengono autenticati utilizzando il nome utente e la password. Gli utenti e i gruppi amministrativi possono essere locali o federati, importati da Active Directory o LDAP del cliente. Le password degli account locali sono memorizzate in un formato protetto da bcrypt; le password della riga di comando sono memorizzate in un formato protetto da SHA-2.	Autentica l'accesso amministrativo alla UI di gestione e alle API.	—
Supporto SAML	StorageGRID supporta il single sign-on (SSO) utilizzando lo standard SAML 2,0 (Security Assertion Markup Language 2,0). Quando SSO è attivato, tutti gli utenti devono essere autenticati da un provider di identità esterno prima di poter accedere a Grid Manager, Tenant Manager, Grid Management API o Tenant Management API. Gli utenti locali non possono accedere a StorageGRID.	Offre livelli aggiuntivi di sicurezza per gli amministratori di tenant e grid come SSO e Multifactor Authentication (MFA).	NIST SP800-63
Controllo granulare delle autorizzazioni	Gli amministratori Grid possono assegnare autorizzazioni ai ruoli e assegnare ruoli a gruppi di utenti amministrativi, in base alle attività a cui i client amministrativi possono eseguire utilizzando sia l'interfaccia utente di gestione che le API.	Consente agli amministratori Grid di gestire il controllo degli accessi per gli utenti e i gruppi amministrativi.	—

Funzione	Funzione	Impatto	Conformità normativa
Registrazione di controllo distribuita	StorageGRID fornisce un'infrastruttura integrata di registrazione degli audit distribuita, scalabile fino a centinaia di nodi in un massimo di 16 siti. I nodi software StorageGRID generano messaggi di audit, che vengono trasmessi attraverso un sistema di inoltro di audit ridondante e infine acquisiti in uno o più repository di audit log. I messaggi di audit acquisiscono eventi a livello di granularità degli oggetti, come operazioni API S3 avviate dal client, eventi del ciclo di vita degli oggetti da ILM, controlli dello stato di salute degli oggetti in background e modifiche della configurazione effettuate dall'interfaccia utente di gestione o dalle API. È possibile esportare gli audit log dai nodi amministrativi tramite CIFS o NFS, consentendo il mining dei messaggi di audit da parte di tool come Splunk ed ELK. Esistono quattro tipi di messaggi di controllo: • Messaggi di audit del sistema • Messaggi di audit dello storage a oggetti • Messaggi di controllo del protocollo HTTP • Gestione dei messaggi di controllo	Fornisce agli amministratori Grid un servizio di controllo collaudato e scalabile e consente loro di estrarre i dati di controllo per vari obiettivi. Tali obiettivi includono la risoluzione dei problemi, il controllo delle prestazioni dello SLA, le operazioni API di accesso ai dati dei client e le modifiche alla configurazione di gestione.	—

Funzione	Funzione	Impatto	Conformità normativa
Audit del sistema	I messaggi di controllo del sistema acquisiscono gli eventi correlati al sistema, come gli stati dei nodi della griglia, il rilevamento degli oggetti corrotti, gli oggetti sottoposti a commit in tutte le posizioni specificate per la regola ILM e l'avanzamento delle attività di manutenzione a livello di sistema (attività griglia).	Aiuta i clienti a risolvere i problemi del sistema e fornisce la prova che gli oggetti vengono memorizzati in base al loro SLA. Gli SLA sono implementati dalle regole ILM di StorageGRID e protetti dall'integrità.	—
Verifica dello storage a oggetti	I messaggi di audit dello storage a oggetti acquisiscono la transazione di API a oggetti e gli eventi relativi al ciclo di vita. Questi eventi includono storage e recupero di oggetti, trasferimenti da grid-node a grid-node e verifiche.	Aiuta i clienti a controllare lo stato di avanzamento dei dati nel sistema e se gli SLA, specificati come StorageGRID ILM, vengono erogati.	—
Controllo del protocollo HTTP	I messaggi di controllo del protocollo HTTP acquisiscono le interazioni del protocollo HTTP correlate alle applicazioni client e ai nodi StorageGRID. Inoltre, i clienti possono acquisire intestazioni specifiche delle richieste HTTP (ad esempio, X-Forwarding-for e metadati utente [x-amz-meta-*]) nella verifica.	Aiuta i clienti a controllare le operazioni API di accesso ai dati tra client e StorageGRID e a tracciare un'azione per un account utente e una chiave di accesso individuali. I clienti possono anche registrare i metadati degli utenti nelle verifiche e utilizzare strumenti di log mining come Splunk o ELK, per cercare i metadati degli oggetti.	—
Audit di gestione	I messaggi di controllo di gestione registrano le richieste degli utenti amministrativi all'interfaccia utente di gestione (Grid Management Interface) o alle API. Ogni richiesta che non è UNA richiesta GET o HEAD all'API registra una risposta con il nome utente, l'IP e il tipo di richiesta all'API.	Aiuta gli amministratori Grid a stabilire un record delle modifiche alla configurazione del sistema apportate dall'utente da quale IP di origine e quale IP di destinazione in quale momento.	—

Funzione	Funzione	Impatto	Conformità normativa
Supporto TLS 1,3 per l'interfaccia utente di gestione e l'accesso API	TLS stabilisce un protocollo handshake per la comunicazione tra un client admin e un nodo admin StorageGRID.	Consente a un client amministrativo e a StorageGRID di identificarsi e autenticarsi reciprocamente e comunicare con riservatezza e integrità dei dati.	—
SNMPv3 per il monitoraggio StorageGRID	SNMPv3 garantisce la sicurezza offrendo autenticazione avanzata e crittografia dei dati per la privacy. Con v3, le unità dei dati del protocollo vengono crittografate utilizzando CBC-DES per il protocollo di crittografia. L'autenticazione dell'utente di chi ha inviato l'unità dati del protocollo è fornita dal protocollo di autenticazione HMAC-SHA o HMAC-MD5. SNMPv2 e v1 sono ancora supportati.	Aiuta gli amministratori di rete a monitorare il sistema StorageGRID abilitando un agente SNMP sul nodo Admin.	—
Certificati client per l'esportazione delle metriche Prometheus	Gli amministratori di rete possono caricare o generare certificati client che possono essere utilizzati per fornire un accesso sicuro e autenticato al database StorageGRID Prometheus.	Gli amministratori di rete possono utilizzare i certificati client per monitorare StorageGRID esternamente utilizzando applicazioni come Grafana.	—

Funzioni di sicurezza della piattaforma

Informazioni sulle funzionalità di sicurezza della piattaforma in StorageGRID.

Funzione	Funzione	Impatto	Conformità normativa
Infrastruttura a chiave pubblica (PKI) interna, certificati dei nodi e TLS	StorageGRID utilizza un'infrastruttura PKI interna e certificati di nodo per autenticare e crittografare la comunicazione internodale. La comunicazione internodale è protetta da TLS.	Contribuisce a proteggere il traffico del sistema su LAN o WAN, soprattutto in un'implementazione multisito.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)

Funzione	Funzione	Impatto	Conformità normativa
Firewall nodo	StorageGRID configura automaticamente le tabelle IP e le regole di firewall per controllare il traffico di rete in entrata e in uscita, oltre a chiudere le porte non utilizzate.	Consente di proteggere il sistema StorageGRID, i dati e i metadati dal traffico di rete non richiesto.	—
Protezione avanzata dei sistemi operativi	Il sistema operativo di base delle appliance fisiche e dei nodi virtuali StorageGRID è rafforzato; vengono rimossi i pacchetti software non correlati.	Contribuisce a ridurre al minimo le potenziali superfici di attacco.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Aggiornamenti periodici della piattaforma e del software	StorageGRID fornisce versioni software regolari che includono il sistema operativo, i file binari delle applicazioni e gli aggiornamenti software.	Aiuta a mantenere il sistema StorageGRID aggiornato con i software e i file binari delle applicazioni correnti.	—
Accesso root disabilitato su Secure Shell (SSH)	Il login root su SSH è disabilitato su tutti i nodi StorageGRID. L'accesso SSH utilizza l'autenticazione del certificato.	Aiuta i clienti a proteggersi da potenziali violazioni remote delle password del login root.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Sincronizzazione automatica dell'ora	StorageGRID sincronizza automaticamente gli orologi di sistema di ciascun nodo con più server NTP (Time Network Protocol) esterni. Sono necessari almeno quattro server NTP di strato 3 o successivo.	Garantisce lo stesso riferimento temporale in tutti i nodi.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Separare le reti per il traffico grid interno, amministrativo e client	I nodi software e le appliance hardware StorageGRID supportano più interfacce di rete virtuali e fisiche, in modo che i clienti possano separare il traffico di client, amministrazione e rete interna su reti diverse.	Consenti agli amministratori Grid di separare il traffico di rete interno ed esterno e di distribuire il traffico sulle reti con SLA diversi.	—
Interfacce VLAN (Virtual LAN) multiple	StorageGRID supporta la configurazione delle interfacce VLAN sul client StorageGRID e sulle reti grid.	Consenti agli amministratori Grid di partizionare e isolare il traffico delle applicazioni per garantire sicurezza, flessibilità e prestazioni.	

Funzione	Funzione	Impatto	Conformità normativa
Rete client non attendibile	L'interfaccia di rete client non attendibile accetta connessioni in entrata solo su porte che sono state esplicitamente configurate come endpoint di bilanciamento del carico.	Garantisce la protezione delle interfacce esposte a reti non attendibili.	—
Firewall configurabile	Gestire le porte aperte e chiuse per le reti Admin, Grid e client.	Consentire agli amministratori di rete di controllare l'accesso alle porte e di gestire l'accesso alle porte dei dispositivi approvati.	
Comportamento SSH avanzato	Nuovi certificati host SSH e chiavi host vengono generati quando si aggiorna un nodo a StorageGRID 11,5.	Migliora la protezione da attacchi "uomo in mezzo".	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)
Crittografia dei nodi	Come parte della nuova funzione di crittografia del server host KMS, viene aggiunta una nuova impostazione di crittografia dei nodi al programma di installazione dell'appliance StorageGRID.	Questa impostazione deve essere attivata durante la fase di configurazione hardware dell'installazione dell'appliance.	Regola SEC 17a-4(f) CTFC 1,31(c)-(d) (FINRA) regola 4511(c)

Integrazione del cloud

Scopri come StorageGRID si integra con i servizi cloud.

Funzione	Funzione	Impatto
Scansione antivirus basata su notifiche	I servizi della piattaforma StorageGRID supportano le notifiche degli eventi. Le notifiche degli eventi possono essere utilizzate con servizi di cloud computing esterni per attivare i flussi di lavoro di scansione antivirus sui dati.	Consente agli amministratori dei tenant di attivare la scansione dei dati tramite virus utilizzando servizi di cloud computing esterni.