Hardening del sistema per StorageGRID

StorageGRID software

NetApp
February 12, 2026

Sommario

Hardening del sistema per StorageGRID

Scopri il rafforzamento del sistema per StorageGRID

La protezione avanzata del sistema è il processo che consente di eliminare il maggior numero possibile di rischi per la sicurezza da un sistema StorageGRID.

Durante l'installazione e la configurazione di StorageGRID, è possibile utilizzare queste linee guida per raggiungere gli obiettivi di protezione prescritti in termini di riservatezza, integrità e disponibilità.

Dovresti già utilizzare le best practice standard del settore per il rafforzamento del sistema. Ad esempio, si utilizzano password complesse per StorageGRID, si utilizza HTTPS anziché HTTP e si abilita l'autenticazione basata su certificato, ove disponibile. Tali best practice devono includere la sicurezza fisica e ambientale che limiti l'accesso fisico e protegga il data center fisico e l'infrastruttura di supporto. È inoltre necessario fare riferimento a tutti gli standard normativi e alle raccomandazioni applicabili alla propria attività e area geografica.

StorageGRID segue la "Policy di gestione delle vulnerabilità di NetApp". Le vulnerabilità segnalate vengono verificate e risolte in base al processo di risposta agli incidenti di sicurezza del prodotto.

Per la protezione avanzata di un sistema StorageGRID, tenere presente quanto segue:

- **Quale delle tre reti StorageGRID** è stata implementata. Tutti i sistemi StorageGRID devono utilizzare la rete griglia, ma è possibile utilizzare anche la rete di amministrazione, la rete client o entrambi. Ogni rete ha considerazioni di sicurezza diverse.
- **Il tipo di piattaforme** utilizzato per i singoli nodi nel sistema StorageGRID. I nodi StorageGRID possono essere implementati su macchine virtuali VMware, all'interno di un motore di container su host Linux o come appliance hardware dedicate. Ogni tipo di piattaforma dispone di un proprio set di Best practice per la protezione avanzata.
- **Quanto sono attendibili gli account tenant**. Se sei un provider di servizi con account tenant non attendibili, avrai problemi di sicurezza diversi rispetto all'utilizzo di tenant interni affidabili.
- **Quali sono i requisiti e le convenzioni di protezione** che la vostra organizzazione segue. Potrebbe essere necessario rispettare requisiti normativi o aziendali specifici.

Linee guida per il rafforzamento della sicurezza per gli aggiornamenti software StorageGRID

Per difenderti dagli attacchi, devi tenere aggiornato il tuo sistema StorageGRID e i servizi correlati.

Aggiornamenti al software StorageGRID

Se possibile, è necessario aggiornare il software StorageGRID alla versione principale più recente o alla versione principale precedente. Mantenere aggiornato StorageGRID aiuta a ridurre il tempo di attivazione delle vulnerabilità note e l'area complessiva della superficie di attacco. Inoltre, le versioni più recenti di StorageGRID contengono spesso funzionalità di protezione avanzata che non sono incluse nelle versioni precedenti.

Consultare "Tool di matrice di interoperabilità NetApp" (IMT) per determinare quale versione del software StorageGRID si deve utilizzare. Quando è necessaria una correzione rapida, NetApp assegna la priorità alla creazione di aggiornamenti per le release più recenti. Alcune patch potrebbero non essere compatibili con le

release precedenti.

- Per scaricare le versioni più recenti di StorageGRID e le correzioni rapide, visitare il sito Web all'indirizzo "Download NetApp: StorageGRID".
- Per aggiornare il software StorageGRID, vedere "istruzioni per l'aggiornamento".
- Per applicare una correzione rapida, vedere la "Procedura di hotfix StorageGRID".

Aggiornamenti a servizi esterni

I servizi esterni possono presentare vulnerabilità che influiscono indirettamente StorageGRID . Assicurarsi che i servizi da cui dipende StorageGRID siano sempre aggiornati. Questi servizi includono LDAP, KMS (o server KMIP), DNS e NTP.

Per un elenco delle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp" .

Aggiornamenti agli hypervisor

Se i nodi StorageGRID sono in esecuzione su VMware o su un altro hypervisor, è necessario assicurarsi che il software e il firmware dell'hypervisor siano aggiornati.

Per un elenco delle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp" .

Upgrade ai nodi Linux

Se i nodi StorageGRID utilizzano piattaforme host Linux, è necessario assicurarsi che gli aggiornamenti di sicurezza e del kernel siano applicati al sistema operativo host. Inoltre, è necessario applicare gli aggiornamenti del firmware all'hardware vulnerabile quando questi aggiornamenti diventano disponibili.

Per un elenco delle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp" .

Linee guida per la protezione avanzata delle reti StorageGRID

Il sistema StorageGRID supporta fino a tre interfacce di rete per nodo di rete, consentendo di configurare la rete per ogni singolo nodo di rete in modo che corrisponda ai requisiti di sicurezza e accesso.

Per informazioni dettagliate sulle reti StorageGRID, consultare "Tipi di rete StorageGRID".

Linee guida per Grid Network

È necessario configurare una rete griglia per tutto il traffico StorageGRID interno. Tutti i nodi Grid si trovano sulla rete Grid e devono essere in grado di comunicare con tutti gli altri nodi.

Durante la configurazione della rete Grid, attenersi alle seguenti linee guida:

- Assicurarsi che la rete sia protetta da client non attendibili, ad esempio quelli su Internet aperto.
- Se possibile, utilizzare Grid Network esclusivamente per il traffico interno. Sia la rete di amministrazione che la rete client presentano ulteriori restrizioni firewall che bloccano il traffico esterno verso i servizi interni. È supportato l'utilizzo di Grid Network per il traffico client esterno, ma questo tipo di utilizzo offre meno livelli di protezione.

- Se l'implementazione di StorageGRID si estende su più data center, utilizzare una rete privata virtuale (VPN) o equivalente sulla rete grid per fornire una protezione aggiuntiva per il traffico interno.
- Alcune procedure di manutenzione richiedono l'accesso Secure shell (SSH) sulla porta 22 tra il nodo di amministrazione primario e tutti gli altri nodi della griglia. Utilizzare un firewall esterno per limitare l'accesso SSH ai client attendibili.

Linee guida per la rete amministrativa

La rete di amministrazione viene generalmente utilizzata per le attività amministrative (dipendenti attendibili che utilizzano Grid Manager o SSH) e per la comunicazione con altri servizi attendibili come LDAP, DNS, NTP o KMS (o server KMIP). Tuttavia, StorageGRID non applica questo utilizzo internamente.

Se si utilizza la rete di amministrazione, attenersi alle seguenti linee guida:

- Bloccare tutte le porte di traffico interne sulla rete di amministrazione. Consultare la "elenco delle porte interne".
- Se i client non attendibili possono accedere alla rete di amministrazione, bloccare l'accesso a StorageGRID sulla rete di amministrazione con un firewall esterno.

Linee guida per la rete client

La rete client viene generalmente utilizzata per i tenant e per le comunicazioni con servizi esterni, come il servizio di replica CloudMirror o un altro servizio della piattaforma. Tuttavia, StorageGRID non applica questo utilizzo internamente.

Se si utilizza la rete client, attenersi alle seguenti linee guida:

- Bloccare tutte le porte di traffico interne sulla rete client. Consultare la "elenco delle porte interne".
- Accettare il traffico client in entrata solo su endpoint configurati esplicitamente. Vedere le informazioni su "gestione dei controlli firewall".

Linee guida per la protezione avanzata dei nodi StorageGRID

I nodi StorageGRID possono essere implementati su macchine virtuali VMware, all'interno di un motore di container su host Linux o come appliance hardware dedicate. Ogni tipo di piattaforma e ogni tipo di nodo dispone di un proprio set di Best practice per la protezione avanzata.

Controlla l'accesso IPMI remoto a BMC

È possibile attivare o disattivare l'accesso IPMI remoto per tutti i dispositivi che contengono un BMC. L'interfaccia IPMI remota consente l'accesso hardware di basso livello alle apparecchiature StorageGRID da parte di chiunque disponga di un account BMC e di una password. Se non è necessario l'accesso IPMI remoto al BMC, disattivare questa opzione.

- Per controllare l'accesso IPMI remoto al BMC in Grid Manager, andare su **Configurazione** > **Sicurezza** > **Impostazioni di sicurezza** > **Appliance**:
  - Deselezionare la casella di controllo **Abilita accesso IPMI remoto** per disattivare l'accesso IPMI al BMC.

- Selezionare la casella di controllo **Abilita accesso IPMI remoto** per abilitare l'accesso IPMI al BMC.

Per ulteriori informazioni sull'indurimento BMC , vedere "Controller di gestione del battiscopa Harden" scheda informativa sulla sicurezza informatica dal "Agenzia per la sicurezza nazionale (NSA)" E "Agenzia per la sicurezza informatica e delle infrastrutture (CISA)" .

Configurazione del firewall

Nell'ambito del processo di protezione avanzata del sistema, è necessario rivedere le configurazioni dei firewall esterni e modificarle in modo che il traffico venga accettato solo dagli indirizzi IP e dalle porte da cui è strettamente necessario.

StorageGRID include un firewall interno su ciascun nodo che migliora la sicurezza della rete consentendo di controllare l'accesso alla rete. È necessario "gestire i controlli firewall interni"impedire l'accesso alla rete su tutte le porte, ad eccezione di quelle necessarie per la distribuzione specifica della griglia. Le modifiche apportate alla configurazione nella pagina di controllo Firewall vengono distribuite a ciascun nodo.

In particolare, è possibile gestire queste aree:

- **Privileged addresses** (indirizzi con privilegi): È possibile consentire agli indirizzi IP o alle subnet selezionate di accedere alle porte chiuse dalle impostazioni nella scheda Manage external access (Gestisci accesso esterno).
- **Manage external access** (Gestisci accesso esterno): È possibile chiudere le porte aperte per impostazione predefinita o riaprire le porte chiuse in precedenza.
- **Untrusted Client Network**: È possibile specificare se un nodo considera attendibile il traffico in entrata dalla rete client e le porte aggiuntive che si desidera aprire quando è configurata una rete client non attendibile.

Sebbene questo firewall interno offra un ulteriore livello di protezione contro alcune minacce comuni, non elimina la necessità di un firewall esterno.

Per un elenco di tutte le porte interne ed esterne utilizzate da StorageGRID, vedere"Porte interne StorageGRID" E"Porte utilizzate per le comunicazioni esterne" .

Disattivare i servizi inutilizzati

Per tutti i nodi StorageGRID , è necessario disabilitare o bloccare l'accesso ai servizi non utilizzati. Ad esempio, se non si prevede di utilizzare DHCP, utilizzare Grid Manager per chiudere la porta 68. Selezionare **Configurazione** > **Controllo firewall** > **Gestisci accesso esterno**. Quindi modifica l'interruttore di stato per la porta 68 da **Aperto** a **Chiuso**.

Virtualizzazione, container e hardware condiviso

Per tutti i nodi StorageGRID, evitare di eseguire StorageGRID sullo stesso hardware fisico del software non attendibile. Non presupporre che le protezioni dell'hypervisor impediscano al malware di accedere ai dati protetti da StorageGRID se StorageGRID e il malware esistono sullo stesso hardware fisico. Ad esempio, gli attacchi Meltdown e Spectre sfruttano le vulnerabilità critiche dei processori moderni e consentono ai programmi di rubare dati in memoria sullo stesso computer.

Proteggere i nodi durante l'installazione

Non consentire agli utenti non attendibili di accedere ai nodi StorageGRID sulla rete durante l'installazione dei nodi. I nodi non sono completamente sicuri fino a quando non si sono Uniti alla griglia.

Limitare l’accesso fisico all’hardware

È necessario limitare l’accesso fisico ai nodi dell’appliance hardware StorageGRID , nonché agli host delle macchine virtuali VMware e agli host Linux che eseguono StorageGRID , solo agli amministratori autorizzati. Alcuni esempi di controlli di accesso fisico includono serrature, guardie, barriere fisiche e videosorveglianza.

I nodi degli appliance hardware sono progettati per essere installati e utilizzati solo da amministratori autorizzati. Non consentire agli amministratori non autorizzati di accedere ai nodi degli apparecchi hardware.

Linee guida per i nodi di amministrazione

I nodi di amministrazione forniscono servizi di gestione quali configurazione, monitoraggio e registrazione del sistema. Quando si accede a Grid Manager o al tenant Manager, si sta effettuando la connessione a un nodo amministratore.

Seguire queste linee guida per proteggere i nodi di amministrazione nel sistema StorageGRID:

- Proteggere tutti i nodi di amministrazione da client non attendibili, ad esempio quelli su Internet aperto. Assicurarsi che nessun client non attendibile possa accedere a qualsiasi nodo Admin sulla rete Grid, sulla rete amministrativa o sulla rete client.
- I gruppi StorageGRID controllano l’accesso alle funzioni di gestione griglia e di gestione tenant. Concedere a ciascun gruppo di utenti le autorizzazioni minime richieste per il proprio ruolo e utilizzare la modalità di accesso in sola lettura per impedire agli utenti di modificare la configurazione.
- Quando si utilizzano gli endpoint del bilanciamento del carico StorageGRID, utilizzare i nodi gateway invece dei nodi di amministrazione per il traffico client non attendibile.
- Se si dispone di tenant non attendibili, non consentire loro di accedere direttamente al tenant Manager o all’API di gestione tenant. I tenant non attendibili devono invece utilizzare un portale tenant o un sistema di gestione tenant esterno, che interagisce con l’API di gestione tenant.
- In alternativa, utilizzare un proxy amministratore per un maggiore controllo sulle comunicazioni AutoSupport dai nodi amministrativi al supporto NetApp. Vedere la procedura per "creazione di un proxy amministratore".
- Facoltativamente, utilizzare le porte limitate 8443 e 9443 per separare le comunicazioni di Grid Manager e Tenant Manager. Bloccare la porta condivisa 443 e limitare le richieste del tenant alla porta 9443 per una protezione aggiuntiva.
- Facoltativamente, utilizzare nodi di amministrazione separati per gli amministratori di grid e gli utenti del tenant.

Per ulteriori informazioni, vedere le istruzioni di "Amministrazione di StorageGRID".

Linee guida per i nodi di storage

I nodi di storage gestiscono e memorizzano i dati e i metadati degli oggetti. Seguire queste linee guida per proteggere i nodi di storage nel sistema StorageGRID.

- Non consentire ai client non attendibili di connettersi direttamente ai nodi di storage. Utilizzare un endpoint di bilanciamento del carico servito da un nodo gateway o da un bilanciamento del carico di terze parti.
- Non abilitare i servizi in uscita per tenant non attendibili. Ad esempio, quando si crea l’account per un tenant non attendibile, non consentire al tenant di utilizzare la propria origine di identità e non consentire l’utilizzo dei servizi della piattaforma. Vedere la procedura per "creazione di un account tenant".
- Utilizzare un bilanciamento del carico di terze parti per il traffico client non attendibile. Il bilanciamento del carico di terze parti offre un maggiore controllo e ulteriori livelli di protezione dagli attacchi.

- In alternativa, puoi utilizzare un proxy storage per un maggiore controllo sui pool di cloud storage e sulle comunicazioni dei servizi della piattaforma dai nodi storage ai servizi esterni. Vedere la procedura per "creazione di un proxy di archiviazione".
- Facoltativamente, è possibile connettersi ai servizi esterni tramite la rete client. Quindi, seleziona **Configurazione** > **Sicurezza** > **Controllo firewall** > **Reti client non attendibili** e indica che la rete client sul nodo di archiviazione non è attendibile. Il nodo di archiviazione non accetta più traffico in entrata sulla rete client, ma continua a consentire richieste in uscita per i servizi della piattaforma.

Linee guida per i nodi gateway

I nodi gateway forniscono un'interfaccia opzionale per il bilanciamento del carico che le applicazioni client possono utilizzare per connettersi a StorageGRID. Attenersi alle seguenti linee guida per proteggere i nodi gateway nel sistema StorageGRID:

- Configurare e utilizzare gli endpoint del bilanciamento del carico. Vedere "Considerazioni per il bilanciamento del carico".
- Utilizzare un bilanciamento del carico di terze parti tra il client e il nodo gateway o i nodi di storage per il traffico client non attendibile. Il bilanciamento del carico di terze parti offre un maggiore controllo e ulteriori livelli di protezione dagli attacchi. Se si utilizza un bilanciamento del carico di terze parti, il traffico di rete può comunque essere configurato in modo opzionale per passare attraverso un endpoint interno di bilanciamento del carico o essere inviato direttamente ai nodi di storage.
- Se si utilizzano endpoint di bilanciamento del carico, è possibile fare in modo che i client si connettano tramite la rete client. Quindi, seleziona **Configurazione** > **Sicurezza** > **Controllo firewall** > **Reti client non attendibili** e indica che la rete client sul nodo gateway non è attendibile. Il nodo gateway accetta solo il traffico in entrata sulle porte configurate esplicitamente come endpoint del bilanciatore del carico.

Linee guida per i nodi dell'appliance hardware

Le appliance hardware StorageGRID sono progettate appositamente per l'utilizzo in un sistema StorageGRID. Alcune appliance possono essere utilizzate come nodi di storage. Altri appliance possono essere utilizzati come nodi di amministrazione o nodi gateway. È possibile combinare nodi appliance con nodi basati su software o implementare grid all-appliance completamente progettati.

Segui queste linee guida per proteggere i nodi dell'appliance hardware nel tuo sistema StorageGRID:

- Se l'appliance utilizza Gestione di sistema di SANtricity per la gestione del controller di storage, impedire ai client non attendibili di accedere a Gestione di sistema di SANtricity tramite la rete.
- Se l'appliance è dotata di un controller di gestione della scheda base (BMC), tenere presente che la porta di gestione BMC consente l'accesso hardware di basso livello. Collegare la porta di gestione BMC solo a una rete di gestione interna sicura e affidabile.

  È possibile stabilire una VLAN per isolare le connessioni di rete BMC e limitare l'accesso a Internet BMC alle reti attendibili. Per ulteriori informazioni sull'applicazione della separazione VLAN, vedere "Controller di gestione del battiscopa Harden" scheda informativa sulla sicurezza informatica dal "Agenzia per la sicurezza nazionale (NSA)" E "Agenzia per la sicurezza informatica e delle infrastrutture (CISA)" .

  Se non è disponibile una rete di gestione interna sicura e affidabile, lasciare la porta di gestione BMC scollegata o bloccata. Durante un caso di supporto, il supporto tecnico potrebbe richiedere un accesso temporaneo.

- Se l'appliance supporta la gestione remota dell'hardware del controller su Ethernet utilizzando lo standard IPMI (Intelligent Platform Management Interface), bloccare il traffico non attendibile sulla porta 623.

È possibile abilitare o disabilitare l'accesso IPMI remoto per tutti gli apparecchi che contengono un BMC. L'interfaccia IPMI remota consente l'accesso hardware di basso livello ai dispositivi StorageGRID a chiunque disponga di un account e di una password BMC . Se non è necessario l'accesso IPMI remoto al BMC, disabilitare questa opzione utilizzando uno dei seguenti metodi: + In Grid Manager, andare su **Configurazione** > **Sicurezza** > **Impostazioni di sicurezza** > **Appliance** e deselezionare la casella di controllo **Abilita accesso IPMI remoto**. + Nell'API di gestione della griglia, utilizzare l'endpoint privato: `PUT /private/bmc` .

+ Puoi anchedisabilitare l'accesso IPMI remoto .

- Per i modelli di appliance che contengono unità SED, FDE o NL-SAS FIPS gestite con SANtricity System Manager, "Abilitare e configurare la protezione dell'unità SANtricity".
- Per i modelli di appliance contenenti SSD SED o FIPS NVMe gestiti tramite StorageGRID Appliance Installer e Grid Manager, "Abilitare e configurare la crittografia dell'unità StorageGRID" .
- Per gli apparecchi senza unità SED, FDE o FIPS, utilizzare un server di gestione delle chiavi (KMS) per "abilitare e configurare la crittografia del nodo software StorageGRID" .

Informazioni correlate

"Scopri di più sulla sicurezza delle unità in SANtricity System Manager"

Linee guida per l'hardening di TLS e SSH in StorageGRID

Dovresti controllare l'accesso SSH, sostituire i certificati TLS predefiniti e selezionare la policy di sicurezza appropriata per le connessioni TLS e SSH.

Linee guida per la protezione avanzata dei certificati

È necessario sostituire i certificati predefiniti creati durante l'installazione con certificati personalizzati.

Per molte organizzazioni, il certificato digitale autofirmato per l'accesso Web a StorageGRID non è conforme alle policy di sicurezza delle informazioni. Nei sistemi di produzione, è necessario installare un certificato digitale con firma CA da utilizzare per l'autenticazione di StorageGRID.

In particolare, è necessario utilizzare certificati server personalizzati anziché i seguenti certificati predefiniti:

- **Certificato dell'interfaccia di gestione**: Utilizzato per proteggere l'accesso a Grid Manager, Tenant Manager, Grid Management API e Tenant Management API.
- **Certificato API S3**: Utilizzato per proteggere l'accesso ai nodi di archiviazione e ai nodi gateway, che le applicazioni client S3 utilizzano per caricare e scaricare i dati oggetto.

Per ulteriori informazioni e istruzioni, vedere"Gestire i certificati di sicurezza".

StorageGRID gestisce separatamente i certificati utilizzati per gli endpoint del bilanciamento del carico. Per configurare i certificati di bilanciamento del carico, vedere "Configurare gli endpoint del bilanciamento del carico".

Quando si utilizzano certificati server personalizzati, attenersi alle seguenti linee guida:

- I certificati devono avere un *`subjectAltName`* che corrisponda alle voci DNS per StorageGRID. Per ulteriori informazioni, vedere la sezione 4,2.1,6, "Nome alternativo oggetto" in "RFC 5280: Certificato PKIX e profilo CRL".

- Se possibile, evitare l'utilizzo di certificati con caratteri jolly. Un'eccezione a questa linea guida è il certificato per un endpoint di stile host virtuale S3, che richiede l'utilizzo di un carattere jolly se i nomi dei bucket non sono noti in anticipo.
- Quando è necessario utilizzare i caratteri jolly nei certificati, è necessario adottare ulteriori misure per ridurre i rischi. Utilizzare un modello con caratteri jolly come `*.s3.example.com`, e non utilizzare il `s3.example.com` suffisso per altre applicazioni. Questo modello funziona anche con l'accesso S3 in stile percorso, ad esempio `dc1-s1.s3.example.com/mybucket` .
- Impostare i tempi di scadenza del certificato su brevi (ad esempio, 2 mesi) e utilizzare l'API Grid Management per automatizzare la rotazione del certificato. Ciò è particolarmente importante per i certificati con caratteri jolly.

Inoltre, i client devono utilizzare un rigoroso controllo del nome host quando comunicano con StorageGRID.

Linee guida per la protezione avanzata dei criteri TLS e SSH

È possibile selezionare un criterio di protezione per determinare quali protocolli e cifrature utilizzare per stabilire connessioni TLS sicure con applicazioni client e connessioni SSH sicure ai servizi StorageGRID interni.

La policy di sicurezza controlla il modo in cui TLS e SSH crittografano i dati in movimento. Come buona pratica, dovresti disabilitare le opzioni di crittografia non necessarie per la compatibilità dell'applicazione. Utilizzare la politica Modern predefinita, a meno che il sistema non debba essere conforme ai Common Criteria, conforme a FIPS 140-2 o non sia necessario utilizzare altri cifrari

Per ulteriori informazioni e istruzioni, vedere"Gestire i criteri TLS e SSH".

Gestisci l'accesso SSH esterno

Per migliorare la sicurezza del sistema, l'accesso SSH esterno è bloccato per impostazione predefinita. Abilitare l'accesso SSH solo quando è necessario eseguire attività che richiedono l'accesso SSH in ingresso, ad esempio la risoluzione dei problemi. Fare riferimento a"Gestisci l'accesso SSH esterno" per dettagli e istruzioni.

Linee guida per il rafforzamento della sicurezza per log, password e messaggi di audit in StorageGRID

Oltre a seguire le linee guida per la protezione avanzata per reti e nodi StorageGRID, è necessario seguire le linee guida per la protezione avanzata per altre aree del sistema StorageGRID.

Password di installazione temporanea

Per proteggere il sistema StorageGRID durante l'installazione, impostare una password nella pagina della password del programma di installazione temporanea nell'interfaccia utente di installazione di StorageGRID o nell'API di installazione. Una volta impostata, questa password viene applicata a tutti i metodi di installazione di StorageGRID, inclusi l'interfaccia utente, l'API di installazione e `configure-storagegrid.py` lo script.

Per ulteriori informazioni, fare riferimento a:

- "Installa StorageGRID sui nodi basati su software"

- "Installare l'appliance StorageGRID"

Registri e messaggi di audit

Proteggere sempre i log StorageGRID e l'output dei messaggi di controllo in modo sicuro. I registri e i messaggi di audit di StorageGRID forniscono informazioni preziose dal punto di vista del supporto e della disponibilità del sistema. Inoltre, le informazioni e i dettagli contenuti nei registri StorageGRID e nell'output dei messaggi di audit sono generalmente di natura sensibile.

Configurare StorageGRID per inviare eventi di sicurezza a un server syslog esterno. Se si utilizza l'esportazione syslog, selezionare TLS e RELP/TLS per i protocolli di trasporto.

Per ulteriori informazioni sui registri StorageGRID, vedere la "Riferimenti ai file di log". Per ulteriori informazioni sui messaggi di controllo StorageGRID, vedere "Messaggi di audit".

NetApp AutoSupport

La funzione AutoSupport di StorageGRID consente di monitorare in modo proattivo lo stato del sistema e di inviare automaticamente i pacchetti al sito di supporto NetApp, al team di supporto interno dell'organizzazione o a un partner di supporto. Per impostazione predefinita, l'invio di pacchetti AutoSupport a NetApp è attivato quando StorageGRID viene configurato per la prima volta.

La funzione AutoSupport può essere disattivata. Tuttavia, NetApp consiglia di abilitare l'IT perché AutoSupport aiuta a velocizzare l'identificazione e la risoluzione dei problemi in caso di problemi nel sistema StorageGRID.

AutoSupport supporta HTTPS, HTTP e SMTP per i protocolli di trasporto. Data la natura sensibile dei pacchetti AutoSupport, NetApp consiglia vivamente di utilizzare HTTPS come protocollo di trasporto predefinito per l'invio di pacchetti AutoSupport a NetApp.

Condivisione delle risorse tra origini (CORS)

È possibile configurare la condivisione delle risorse cross-origin (CORS) per un bucket S3 se si desidera che quel bucket e gli oggetti in quel bucket siano accessibili alle applicazioni web in altri domini. In generale, non abilitare il CORS a meno che non sia necessario. Se è richiesto un CORS, limitarlo alle origini attendibili.

Vedi i passaggi per"configurazione di CORS per bucket e oggetti" .

Dispositivi di sicurezza esterni

Una soluzione di protezione avanzata completa deve affrontare i meccanismi di sicurezza esterni a StorageGRID. L'utilizzo di ulteriori dispositivi di infrastruttura per il filtraggio e la limitazione dell'accesso a StorageGRID è un metodo efficace per stabilire e mantenere una posizione di sicurezza rigorosa. Questi dispositivi di sicurezza esterni includono firewall, sistemi di prevenzione delle intrusioni (IPS) e altri dispositivi di sicurezza.

Per il traffico client non attendibile, si consiglia un bilanciamento del carico di terze parti. Il bilanciamento del carico di terze parti offre un maggiore controllo e ulteriori livelli di protezione dagli attacchi.

Mitigazione ransomware

Aiuta a proteggere i dati degli oggetti dagli attacchi ransomware seguendo i consigli descritti in "Difesa ransomware con StorageGRID".