# Hardening del sistema per StorageGRID

StorageGRID software

NetApp
July 23, 2026

# Sommario

# Hardening del sistema per StorageGRID

## Scopri il rafforzamento del sistema per StorageGRID

L'hardening del sistema è il processo di eliminazione del maggior numero possibile di rischi per la sicurezza da un sistema StorageGRID.

Durante l'installazione e la configurazione di StorageGRID, usa queste linee guida per raggiungere qualsiasi obiettivo di sicurezza prescritto in termini di riservatezza, integrità e disponibilità.

Dovresti già adottare le best practice standard del settore per la protezione dei sistemi. Ad esempio, usi password complesse per StorageGRID, usi HTTPS invece di HTTP e abiliti l'autenticazione basata su certificati dove disponibile. Queste best practice devono includere la sicurezza fisica e ambientale che limita l'accesso fisico e protegge il data center fisico e l'infrastruttura di supporto. Devi anche fare riferimento a tutti gli standard e le raccomandazioni normative applicabili alla tua attività e alla tua area geografica.

StorageGRID segue le "Policy di gestione delle vulnerabilità NetApp". Le vulnerabilità segnalate vengono verificate e risolte secondo il processo di risposta agli incidenti di sicurezza del prodotto.

Quando rafforzi la sicurezza di un sistema StorageGRID, considera quanto segue:

- **Quale delle tre reti StorageGRID** hai implementato. Tutti i sistemi StorageGRID devono utilizzare la Grid Network, ma potresti anche utilizzare la Admin Network, la Client Network o entrambe. Ogni rete presenta diverse considerazioni di sicurezza.
- **Il tipo di piattaforme** che usi per i singoli nodi nel tuo sistema StorageGRID. I nodi StorageGRID possono essere distribuiti su macchine virtuali VMware, all'interno di un engine di container su host Linux o come appliance hardware dedicate. Ogni tipo di piattaforma ha il proprio set di best practice per la protezione.
- **Quanto sono affidabili gli account dei tenant**. Se sei un service provider con account dei tenant non affidabili, avrai problematiche di sicurezza diverse rispetto a quando utilizzi solo tenant interni affidabili.
- **Quali requisiti e convenzioni di sicurezza** segue la tua organizzazione. Potresti dover rispettare specifici requisiti normativi o aziendali.

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

Devi mantenere il tuo sistema StorageGRID e i servizi correlati aggiornati per difenderti dagli attacchi.

### Aggiornamenti al software StorageGRID

Quando possibile, dovresti aggiornare il software StorageGRID alla versione principale più recente o a quella precedente. Mantenere StorageGRID aggiornato aiuta a ridurre il tempo in cui le vulnerabilità note rimangono attive e riduce la superficie di attacco complessiva. Inoltre, le versioni più recenti di StorageGRID spesso includono funzionalità di rafforzamento della sicurezza che non sono incluse nelle versioni precedenti.

Consulta l' "Tool NetApp Interoperability Matrix"IMT per determinare quale versione del software StorageGRID dovresti utilizzare. Quando è necessario un hotfix, NetApp dà priorità alla creazione di aggiornamenti per le versioni più recenti. Alcune patch potrebbero non essere compatibili con le versioni precedenti.

- Per scaricare le versioni più recenti di StorageGRID e gli hotfix, vai su "Download NetApp: StorageGRID".
- Per aggiornare il software StorageGRID, consulta la "istruzioni di aggiornamento".
- Per applicare una hotfix, vedi "Procedura di hotfix per StorageGRID".

### Aggiornamenti ai servizi esterni

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

Per un elenco delle versioni supportate, vedi il "Tool NetApp Interoperability Matrix".

### Aggiornamenti agli hypervisor

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

Per un elenco delle versioni supportate, vedi il "Tool NetApp Interoperability Matrix".

### Aggiornamenti ai nodi Linux

Se i nodi StorageGRID utilizzano piattaforme host Linux, devi assicurarti che gli aggiornamenti di sicurezza e gli aggiornamenti del kernel vengano applicati al sistema operativo host. Inoltre, devi applicare gli aggiornamenti del firmware all'hardware vulnerabile non appena questi aggiornamenti diventano disponibili.

Per un elenco delle versioni supportate, vedi il "Tool NetApp Interoperability Matrix".

# Linee guida per la protezione delle reti StorageGRID

Il sistema StorageGRID supporta fino a tre interfacce di rete per nodo della griglia, permettendoti di configurare la rete per ogni singolo nodo della griglia in base ai tuoi requisiti di sicurezza e accesso.

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

### Linee guida per la rete Grid

Devi configurare una rete Grid per tutto il traffico interno di StorageGRID. Tutti i nodi Grid sono sulla rete Grid e devono poter comunicare con tutti gli altri nodi.

Durante la configurazione della rete Grid, segui queste linee guida:

- Assicurati che la rete sia protetta da client non attendibili, come quelli presenti su Internet.
- Quando possibile, usa la rete Grid esclusivamente per il traffico interno. Sia la rete Admin che la rete Client hanno ulteriori restrizioni firewall che bloccano il traffico esterno verso i servizi interni. L'uso della rete Grid per il traffico client esterno è supportato, ma offre meno livelli di protezione.
- Se l'implementazione di StorageGRID si estende su più data center, usa una rete privata virtuale (VPN) o equivalente sulla Grid Network per offrire una protezione aggiuntiva al traffico interno.
- Alcune procedure di manutenzione richiedono l'accesso Secure Shell (SSH) sulla porta 22 tra il nodo Admin primario e tutti gli altri nodi della griglia. Usa un firewall esterno per limitare l'accesso SSH ai client

attendibili.

### Linee guida per la rete Admin

La rete di amministrazione viene in genere utilizzata per attività amministrative (dipendenti fidati che utilizzano Grid Manager o SSH) e per comunicare con altri servizi fidati come LDAP, DNS, NTP o KMS (o server KMIP). Tuttavia, StorageGRID non impone internamente questo utilizzo.

Se usi la rete di amministrazione, segui queste linee guida:

- Blocca tutte le porte del traffico interno sulla rete di amministrazione. Vedi il "elenco delle porte interne".
- Se client non attendibili possono accedere alla rete di amministrazione, blocca l'accesso a StorageGRID sulla rete di amministrazione con un firewall esterno.

### Linee guida per la rete client

La rete client viene in genere utilizzata dai tenant e per comunicare con servizi esterni, come il servizio di replica CloudMirror o altri servizi della piattaforma. Tuttavia, StorageGRID non impone internamente questo utilizzo.

Se usi la rete client, segui queste linee guida:

- Blocca tutte le porte di traffico interne sulla Client Network. Vedi il "elenco delle porte interne".
- Accetta il traffico client in entrata solo sugli endpoint configurati esplicitamente. Vedi le informazioni su "gestire i controlli del firewall".

# Linee guida per il rafforzamento dei nodi StorageGRID

I nodi StorageGRID possono essere distribuiti 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 ha il proprio set di best practice per la protezione.

## Controlla l'accesso IPMI remoto al BMC

Puoi abilitare o disabilitare l'accesso IPMI remoto per tutti gli appliance che contengono un BMC. L'interfaccia IPMI remota consente l'accesso hardware di basso livello ai tuoi appliance StorageGRID a chiunque abbia un account BMC e una password. Se non ti serve l'accesso IPMI remoto al BMC, disabilita questa opzione.

- Per controllare l'accesso IPMI remoto al BMC in Grid Manager, vai a **Configurazione** > **Sicurezza** > **Impostazioni di sicurezza** > **Apparecchiature**:
  - Deseleziona la casella di controllo **Abilita accesso IPMI remoto** per disabilitare l'accesso IPMI al BMC.
  - Seleziona la casella di controllo **Abilita accesso IPMI remoto** per abilitare l'accesso IPMI al BMC.

Per ulteriori informazioni sull'hardening della BMC, consulta la "Rinforza i Baseboard Management Controller"scheda informativa sulla cybersecurity di "National Security Agency (NSA)"e "Cybersecurity and Infrastructure Security Agency (CISA)".

## Configurazione del firewall

Nell'ambito del processo di rafforzamento della sicurezza del sistema, devi rivedere le configurazioni dei firewall esterni e modificarle in modo che il traffico sia accettato solo dagli indirizzi IP e sulle porte da cui è strettamente necessario.

StorageGRID include un firewall interno su ciascun nodo che migliora la sicurezza della tua griglia permettendoti di controllare l'accesso di rete al nodo. Dovresti "gestire i controlli del firewall interno" per impedire l'accesso di rete su tutte le porte tranne quelle necessarie per la tua specifica implementazione della griglia. Le modifiche di configurazione che apporti nella pagina di controllo del firewall vengono applicate a ciascun nodo.

Nello specifico, puoi gestire queste aree:

- **Indirizzi privilegiati**: Puoi consentire a indirizzi IP o sottoreti selezionati di accedere alle porte chiuse dalle impostazioni nella scheda Gestisci accesso esterno.
- **Gestisci l'accesso esterno**: Puoi chiudere le porte aperte per impostazione predefinita o riaprire le porte che avevi chiuso in precedenza.
- **Rete client non attendibile**: Puoi specificare se un nodo considera attendibile il traffico in entrata dalla rete client, oltre alle porte aggiuntive che vuoi aprire quando è configurata la rete client non attendibile.

Sebbene questo firewall interno fornisca 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, vedi "Porte interne di StorageGRID" e "Porte utilizzate per le comunicazioni esterne".

## Disabilita i servizi non utilizzati

Per tutti i nodi StorageGRID, dovresti disabilitare o bloccare l'accesso ai servizi non utilizzati. Ad esempio, se non hai intenzione di usare DHCP, usa Grid Manager per chiudere la porta 68. Seleziona **Configuration** > **Firewall control** > **Manage external access**. Poi cambia lo stato della porta 68 da **Open** a **Closed**.

## Virtualizzazione, container e hardware condiviso

Per tutti i nodi StorageGRID, evita di eseguire StorageGRID sullo stesso hardware fisico di software non attendibile. Non dare per scontato che le protezioni dell'hypervisor impediscano al malware di accedere ai dati protetti da StorageGRID se sia StorageGRID che il malware si trovano sullo stesso hardware fisico. Ad esempio, gli attacchi Meltdown e Spectre sfruttano vulnerabilità critiche nei processori moderni e permettono ai programmi di rubare dati dalla memoria dello stesso computer.

## Proteggi i nodi durante l'installazione

Non permettere agli utenti non attendibili di accedere ai nodi StorageGRID tramite la rete durante l'installazione. I nodi non sono completamente sicuri finché non hanno effettuato il join della grid.

## Limita l'accesso fisico all'hardware

Devi limitare l'accesso fisico ai nodi dell'appliance hardware StorageGRID, così come agli host di 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 gestiti solo da amministratori autorizzati.

Non permettere ad amministratori non autorizzati di accedere ai nodi degli appliance hardware.

## Linee guida per i nodi Admin

I nodi di amministrazione forniscono servizi di gestione come la configurazione del sistema, il monitoraggio e la registrazione. Quando accedi al Grid Manager o al Tenant Manager, ti connetti a un nodo di amministrazione.

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

- Proteggi tutti i nodi di amministrazione da client non attendibili, come quelli presenti su Internet aperta. Assicurati che nessun client non attendibile possa accedere a nessun nodo di amministrazione sulla Grid Network, sulla Admin Network o sulla Client Network.
- I gruppi di StorageGRID controllano l'accesso alle funzionalità di Grid Manager e Tenant Manager. Assegna a ciascun gruppo di utenti le autorizzazioni minime necessarie per il loro ruolo e utilizza la modalità di accesso di sola lettura per impedire agli utenti di modificare la configurazione.
- Quando usi gli endpoint del bilanciatore di carico StorageGRID, usa i nodi gateway invece dei nodi di amministrazione per il traffico client non attendibile.
- Se hai tenant non affidabili, non permettere loro di accedere direttamente al Tenant Manager o alla Tenant Management API. Invece, fai in modo che questi tenant utilizzino un tenant portal o un sistema esterno di gestione tenant che interagisce con la Tenant Management API.
- Facoltativamente, puoi usare un proxy admin per avere più controllo sulla comunicazione AutoSupport dai nodi Admin al supporto NetApp. Vedi i passaggi per "creare un proxy admin".
- Facoltativamente, usa le porte 8443 e 9443 riservate per separare le comunicazioni tra Grid Manager e Tenant Manager. Blocca la porta condivisa 443 e limita le richieste dei tenant alla porta 9443 per una protezione aggiuntiva.
- Facoltativamente, usa nodi di amministrazione separati per gli amministratori della griglia e nodi tenant per gli utenti tenant.

Per ulteriori informazioni, consulta le istruzioni per "gestire StorageGRID".

## Linee guida per i nodi di archiviazione

I nodi di archiviazione gestiscono e memorizzano i dati oggetto e i metadati. Segui queste linee guida per proteggere i nodi di archiviazione nel tuo sistema StorageGRID.

- Non consentire ai client non attendibili di connettersi direttamente ai Storage Node. Usa un endpoint di bilanciamento del carico servito da un Gateway Node o da un load balancer di terze parti.
- Non abilitare i servizi outbound per i tenant non attendibili. Ad esempio, quando crei l'account per un tenant non attendibile, non permettere al tenant di usare la propria fonte di identità e non permettere l'uso dei servizi della piattaforma. Vedi i passaggi per "creare un account tenant".
- Utilizza un bilanciatore di carico di terze parti per il traffico client non attendibile. Il bilanciamento del carico di terze parti offre maggiore controllo e ulteriori livelli di protezione contro gli attacchi.
- Facoltativamente, puoi usare un proxy di storage per avere più controllo sui Cloud Storage Pools e sulla comunicazione dei servizi della piattaforma dai Storage Nodes ai servizi esterni. Vedi i passaggi per "creare un proxy di storage".
- Facoltativamente, puoi connetterti a servizi esterni utilizzando la Client Network. Quindi, seleziona **Configuration** > **Security** > **Firewall control** > **Untrusted Client Networks** e indica che la Client Network sullo Storage Node non è attendibile. Lo Storage Node non accetta più alcun traffico in entrata sulla Client Network, ma continua a consentire le richieste outbound per i Platform Services.

## Linee guida per i nodi gateway

I nodi gateway forniscono un'interfaccia di bilanciamento del carico opzionale che le applicazioni client possono utilizzare per connettersi a StorageGRID. Segui queste linee guida per proteggere qualsiasi nodo gateway nel tuo sistema StorageGRID:

- Configura e usa gli endpoint del bilanciamento del carico. Vedi "Considerazioni sul bilanciamento del carico".
- Usa un bilanciatore di carico di terze parti tra il client e il Gateway Node o gli Storage Node per il traffico client non attendibile. Il bilanciamento del carico di terze parti offre maggiore controllo e ulteriori livelli di protezione contro gli attacchi. Se usi un bilanciatore di carico di terze parti, il traffico di rete può comunque essere configurato, facoltativamente, per passare attraverso un endpoint interno del bilanciatore di carico o essere inviato direttamente agli Storage Node.
- Se usi endpoint di bilanciamento del carico, puoi far connettere i client tramite la Client Network. Poi seleziona **Configuration** > **Security** > **Firewall control** > **Untrusted Client Networks** e indica che la Client Network sul Gateway Node non è attendibile. Il Gateway Node accetta traffico in entrata solo sulle porte configurate esplicitamente come endpoint di bilanciamento del carico.

## Linee guida per i nodi delle appliance hardware

Gli appliance hardware StorageGRID sono progettati specificamente per l'utilizzo in un sistema StorageGRID. Alcuni appliance possono essere utilizzati come Storage Nodes. Altri appliance possono essere utilizzati come Admin Nodes o Gateway Nodes. Puoi combinare nodi appliance con nodi basati su software oppure implementare griglie completamente ingegnerizzate, composte solo da appliance.

Segui queste linee guida per proteggere tutti i nodi hardware del tuo sistema StorageGRID:

- Se l'appliance utilizza SANtricity System Manager per la gestione dello storage controller, impedisci ai client non attendibili di accedere a SANtricity System Manager tramite la rete.
- Se l'appliance è dotata di un baseboard management controller (BMC), tieni presente che la porta di gestione del BMC consente l'accesso hardware di basso livello. Collega la porta di gestione del BMC solo a una rete di gestione interna sicura e affidabile.

  Puoi creare una VLAN per isolare le connessioni di rete BMC e limitare l'accesso a Internet di BMC alle sole reti attendibili. Per ulteriori informazioni sull'applicazione della separazione VLAN, consulta la "Rinforza i Baseboard Management Controller" scheda informativa sulla cybersecurity del "National Security Agency (NSA)" e "Cybersecurity and Infrastructure Security Agency (CISA)".

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

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

> Puoi abilitare o disabilitare l'accesso IPMI remoto per tutti gli appliance che contengono un BMC. L'interfaccia IPMI remota consente l'accesso hardware di basso livello ai tuoi StorageGRID appliance a chiunque abbia un account BMC e una password. Se non ti serve l'accesso IPMI remoto al BMC, disabilita questa opzione usando uno dei seguenti metodi: + In Grid Manager, vai su **Configuration** > **Security** > **Security settings** > **Appliances** e deseleziona la casella **Enable remote IPMI access**. + Nell'API di gestione Grid, usa l'endpoint privato: `PUT /private/bmc`.

+ Puoi anche disabilita l'accesso IPMI remoto.

- Per i modelli di appliance contenenti unità SED, FDE o FIPS NL-SAS che gestisci con SANtricity System Manager, "Abilita e configura SANtricity Drive Security".
- Per i modelli di appliance contenenti SSD NVMe SED o FIPS che gestisci tramite StorageGRID Appliance Installer e Grid Manager, "Abilita e configura la crittografia delle unità StorageGRID".
- Per gli apparati senza unità SED, FDE o FIPS, usa un Key Management Server (KMS) per "Abilita e configura la crittografia del nodo software StorageGRID".

**Informazioni correlate**

"Scopri la sicurezza delle unità disco 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 il rafforzamento dei certificati

Dovresti sostituire i certificati predefiniti creati durante l'installazione con i tuoi certificati personalizzati.

Per molte organizzazioni, il certificato digitale autofirmato per l'accesso web a StorageGRID non è conforme alle proprie politiche di sicurezza delle informazioni. Sui sistemi di produzione, dovresti installare un certificato digitale firmato da una CA da utilizzare per l'autenticazione di StorageGRID.

Nello specifico, dovresti utilizzare certificati server personalizzati invece di questi certificati predefiniti:

- **Certificato di interfaccia di gestione**: usato per proteggere l'accesso a Grid Manager, Tenant Manager, Grid Management API e Tenant Management API.
- **Certificato API S3**: Usato per proteggere l'accesso ai nodi di archiviazione e ai nodi gateway, che le applicazioni client S3 usano per caricare e scaricare i dati degli oggetti.

Vedi "Gestisci i certificati di sicurezza" per dettagli e istruzioni.

> StorageGRID gestisce separatamente i certificati utilizzati per gli endpoint del bilanciatore di carico. Per configurare i certificati del bilanciatore di carico, vedi "${post_edited_translations.segment}".

Quando usi certificati server personalizzati, segui queste linee guida:

- I certificati devono avere un `subjectAltName` che corrisponde alle voci DNS per StorageGRID. Per dettagli, vedi la sezione 4.2.1.6, "Subject Alternative Name", in "RFC 5280: Certificato PKIX e profilo CRL".
- Quando possibile, evita l'uso di certificati wildcard. Un'eccezione a questa best practice è il certificato per un endpoint S3 virtual hosted style, che richiede l'uso di un wildcard se i nomi dei bucket non sono noti in anticipo.
- Quando devi usare i caratteri jolly nei certificati, dovresti adottare ulteriori misure per ridurre i rischi. Usa un modello di caratteri jolly come `*.s3.example.com`, e non usare il suffisso `s3.example.com` per altre applicazioni. Questo modello funziona anche con l'accesso S3 in stile percorso, come `dc1-s1.s3.example.com/mybucket`.

- Imposta tempi di scadenza brevi per i certificati (ad esempio, 2 mesi) e usa l'API Grid Management per automatizzare la rotazione dei certificati. Questo è particolarmente importante per i certificati wildcard.

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

### Linee guida per il rafforzamento delle policy TLS e SSH

Puoi selezionare una policy di sicurezza per determinare quali protocolli e algoritmi di crittografia vengono utilizzati per stabilire connessioni TLS sicure con le applicazioni client e connessioni SSH sicure ai servizi interni di StorageGRID.

La policy di sicurezza controlla il modo in cui TLS e SSH crittografano i dati in transito. Come best practice, dovresti disabilitare le opzioni di crittografia che non sono necessarie per la compatibilità delle applicazioni. Usa la policy Modern predefinita, a meno che il tuo sistema non debba essere conforme ai Common Criteria, a FIPS 140-2 o tu abbia bisogno di usare altri algoritmi di crittografia.

Vedi "Gestisci le policy TLS e SSH" per dettagli e istruzioni.

### Gestisci l'accesso SSH esterno

Per migliorare la sicurezza del sistema, l'accesso SSH esterno è bloccato per impostazione predefinita. Abilita l'accesso SSH solo quando devi eseguire attività che richiedono l'accesso SSH in entrata, come la risoluzione dei problemi. Consulta "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 delle reti e dei nodi StorageGRID, dovresti seguire le linee guida per le altre aree del sistema StorageGRID.

### password di installazione temporanea

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

Per ulteriori informazioni, consulta:

- "Installa StorageGRID sui nodi basati su software"
- "Installa l'appliance StorageGRID"

### Registri e messaggi di audit

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

Configura StorageGRID per inviare gli eventi di sicurezza a un server syslog esterno. Se utilizzi l'esportazione syslog, seleziona TLS e RELP/TLS come protocolli di trasporto.

Consulta "Riferimento ai file di registro" per ulteriori informazioni sui log di StorageGRID. Consulta "Messaggi di audit" per ulteriori informazioni sui messaggi di audit di StorageGRID.

## NetApp AutoSupport

La funzionalità AutoSupport di StorageGRID ti permette di monitorare in modo proattivo lo stato di salute del tuo sistema e di inviare automaticamente i pacchetti al sito di supporto NetApp, al team di supporto interno della tua organizzazione o a un partner di supporto. Per impostazione predefinita, l'invio dei pacchetti AutoSupport a NetApp è abilitato quando StorageGRID viene configurato per la prima volta.

La funzione AutoSupport può essere disabilitata. Tuttavia, NetApp consiglia di abilitarla perché AutoSupport aiuta ad accelerare l'identificazione e la risoluzione dei problemi qualora si presentassero sul tuo sistema StorageGRID.

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

## Condivisione delle risorse tra origini diverse (CORS)

Puoi configurare la condivisione delle risorse tra origini diverse (CORS) per un bucket S3 se vuoi che quel bucket e gli oggetti in esso siano accessibili alle applicazioni web di altri domini. In generale, non abilitare CORS a meno che non sia necessario. Se CORS è necessario, limitane l'uso alle origini attendibili.

Vedi i passaggi per "Configurare CORS per bucket e oggetti".

## Dispositivi di sicurezza esterni

Una soluzione di hardening completa deve affrontare i meccanismi di sicurezza esterni a StorageGRID. Usare dispositivi infrastrutturali aggiuntivi per filtrare e limitare l'accesso a StorageGRID è un modo efficace per stabilire e mantenere una rigorosa postura di sicurezza. Questi dispositivi di sicurezza esterni includono firewall, sistemi di prevenzione delle intrusioni (IPS) e altri dispositivi di sicurezza.

Per il traffico client non attendibile, è consigliato un bilanciatore di carico di terze parti. Il bilanciamento del carico di terze parti offre più controllo e ulteriori livelli di protezione contro gli attacchi.

## Mitigazione del ransomware

Contribuisci a proteggere i dati dei tuoi oggetti dagli attacchi ransomware seguendo le raccomandazioni in "Difesa dai ransomware con StorageGRID".