



## **Gestire la sicurezza**

### StorageGRID software

NetApp  
January 14, 2026

# Sommario

Gestire la sicurezza .....	1
Gestire la sicurezza .....	1
Gestire la crittografia .....	1
Gestire i certificati .....	1
Configurare i server di gestione delle chiavi .....	1
Gestire le impostazioni del proxy .....	1
Firewall di controllo .....	1
Esaminare i metodi di crittografia StorageGRID .....	1
Utilizzare più metodi di crittografia .....	4
Gestire i certificati .....	4
Gestire i certificati di sicurezza .....	4
Tipi di certificato server supportati .....	16
Configurare i certificati dell'interfaccia di gestione .....	16
Configurare i certificati API S3 .....	22
Copiare il certificato Grid CA .....	27
Configurare i certificati StorageGRID per FabricPool .....	28
Configurare i certificati client .....	29
Configurare le impostazioni di sicurezza .....	37
Gestire i criteri TLS e SSH .....	37
Configurare la sicurezza della rete e degli oggetti .....	41
Modificare le impostazioni di sicurezza dell'interfaccia .....	42
Gestisci l'accesso SSH esterno .....	44
Configurare i server di gestione delle chiavi .....	44
Che cos'è un server di gestione delle chiavi (KMS)? .....	44
Configurazione dei KMS e dell'appliance .....	45
Considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi .....	46
Considerazioni per la modifica del KMS per un sito .....	49
Configurare StorageGRID come client nel KMS .....	52
Aggiunta di un server di gestione delle chiavi (KMS) .....	53
Gestire un KMS .....	55
Gestire le impostazioni del proxy .....	62
Configurare il proxy di archiviazione .....	62
Configurare le impostazioni del proxy amministratore .....	63
Firewall di controllo .....	64
Controllare l'accesso al firewall esterno .....	64
Gestire i controlli firewall interni .....	65
Configurare il firewall interno .....	68

# Gestire la sicurezza

## Gestire la sicurezza

È possibile configurare diverse impostazioni di sicurezza da Gestione griglia per proteggere il sistema StorageGRID.

### Gestire la crittografia

StorageGRID offre diverse opzioni per la crittografia dei dati. Devi ["esaminare i metodi di crittografia disponibili"](#) determinare quali soddisfano i tuoi requisiti di protezione dei dati.

### Gestire i certificati

È possibile ["configurare e gestire i certificati del server"](#) utilizzare per le connessioni HTTP o i certificati client utilizzati per autenticare un'identità client o utente sul server.

### Configurare i server di gestione delle chiavi

Utilizzando un ["server di gestione delle chiavi"](#) possibile proteggere i dati StorageGRID anche se un'appliance viene rimossa dal data center. Una volta crittografati i volumi dell'appliance, non è possibile accedere ai dati dell'appliance a meno che il nodo non sia in grado di comunicare con il KMS.



Per utilizzare la gestione delle chiavi di crittografia, è necessario attivare l'impostazione **Node Encryption** per ogni appliance durante l'installazione, prima di aggiungere l'appliance alla griglia.

### Gestire le impostazioni del proxy

Se utilizzi servizi di piattaforma S3 o pool di cloud storage, puoi configurare un ["server proxy di archiviazione"](#) tra i nodi storage e gli endpoint S3 esterni. Se si inviano pacchetti AutoSupport utilizzando HTTPS o HTTP, è possibile configurare un ["admin proxy server \(server proxy amministratore\)"](#) tra i nodi Admin e il supporto tecnico.

### Firewall di controllo

Per migliorare la protezione del sistema, è possibile controllare l'accesso ai nodi amministrativi di StorageGRID aprendo o chiudendo porte specifiche su ["firewall esterno"](#). È inoltre possibile controllare l'accesso alla rete per ciascun nodo configurandone ["firewall interno"](#). È possibile impedire l'accesso a tutte le porte, ad eccezione di quelle necessarie per l'implementazione.

## Esaminare i metodi di crittografia StorageGRID

StorageGRID offre diverse opzioni per la crittografia dei dati. È necessario esaminare i metodi disponibili per determinare quali metodi soddisfano i requisiti di protezione dei dati.

La tabella fornisce un riepilogo generale dei metodi di crittografia disponibili in StorageGRID.

Opzione di crittografia	Come funziona	Valido per
Server di gestione delle chiavi (KMS) in Grid Manager	" <a href="#">configurare un server di gestione delle chiavi</a> " Per il sito StorageGRID e " <a href="#">abilitare la crittografia dei nodi per l'appliance</a> ". Quindi, un nodo appliance si connette al KMS per richiedere una chiave di crittografia a chiave (KEK). Questa chiave crittografa e decrta la chiave di crittografia dei dati (DEK) su ciascun volume.	Nodi appliance con <b>Node Encryption</b> attivato durante l'installazione. Tutti i dati dell'appliance sono protetti da perdite fisiche o rimozione dal data center.  <b>Nota:</b> La gestione delle chiavi di crittografia con un KMS è supportata solo per i nodi di archiviazione e le appliance di servizi.
Pagina crittografia unità nel programma di installazione dell'appliance StorageGRID	Se l'appliance contiene unità che supportano la crittografia hardware, è possibile impostare una passphrase dell'unità durante l'installazione. Quando si imposta una passphrase di unità, è impossibile per chiunque recuperare dati validi dalle unità rimosse dal sistema, a meno che non conoscano la passphrase. Prima di iniziare l'installazione, andare a <b>Configure hardware &gt; Drive Encryption</b> per impostare una passphrase di unità che si applica a tutte le unità gestite da StorageGRID con crittografia automatica in un nodo.	Appliance che contengono dischi con crittografia automatica. Tutti i dati presenti sulle unità protette sono protetti da perdita fisica o rimozione dal data center.  La crittografia dei dischi non si applica ai dischi gestiti da SANtricity. Se hai un'appliance storage con dischi a crittografia automatica e controller SANtricity, puoi abilitare la sicurezza dei dischi in SANtricity.
Protezione dei dischi in Gestione di sistema SANtricity	Se la funzione di protezione dell'unità è attivata per l'appliance StorageGRID, è possibile utilizzare " <a href="#">Gestore di sistema di SANtricity</a> " per creare e gestire la chiave di protezione. La chiave è necessaria per accedere ai dati sui dischi protetti.	Appliance storage con dischi FDE (Full Disk Encryption) o dischi a crittografia automatica. Tutti i dati presenti sulle unità protette sono protetti da perdita fisica o rimozione dal data center. Non è utilizzabile con alcune appliance di storage o con alcuna appliance di servizi.
Crittografia degli oggetti memorizzati	L'opzione viene attivata " <a href="#">Crittografia degli oggetti memorizzati</a> " in Grid Manager. Quando questa opzione è attivata, tutti i nuovi oggetti che non sono crittografati a livello di bucket o a livello di oggetto vengono crittografati durante l'acquisizione.	Nuovi dati oggetto S3 acquisiti.  Gli oggetti memorizzati esistenti non vengono crittografati. I metadati degli oggetti e altri dati sensibili non vengono crittografati.

Opzione di crittografia	Come funziona	Valido per
Crittografia bucket S3	Viene inviata una richiesta PutBucketEncryption per abilitare la crittografia per il bucket. Tutti i nuovi oggetti che non sono crittografati a livello di oggetto vengono crittografati durante l'acquisizione.	<p>Solo i dati S3 degli oggetti acquisiti di recente.</p> <p>È necessario specificare la crittografia per il bucket. Gli oggetti bucket esistenti non vengono crittografati. I metadati degli oggetti e altri dati sensibili non vengono crittografati.</p> <p><a href="#">"Operazioni sui bucket"</a></p>
Crittografia a oggetti lato server (SSE) S3	Viene inviata una richiesta S3 per memorizzare un oggetto e includere l' `x-amz-server-side-encryption` intestazione della richiesta.	<p>Solo i dati S3 degli oggetti acquisiti di recente.</p> <p>È necessario specificare la crittografia per l'oggetto. I metadati degli oggetti e altri dati sensibili non vengono crittografati.</p> <p>StorageGRID gestisce le chiavi.</p> <p><a href="#">"Utilizzare la crittografia lato server"</a></p>
Crittografia a oggetti S3 lato server con chiavi fornite dal cliente (SSE-C)	<p>Viene inviata una richiesta S3 per memorizzare un oggetto e includere tre intestazioni di richiesta.</p> <ul style="list-style-type: none"> <li>• x-amz-server-side-encryption-customer-algorithm</li> <li>• x-amz-server-side-encryption-customer-key</li> <li>• x-amz-server-side-encryption-customer-key-MD5</li> </ul>	<p>Solo i dati S3 degli oggetti acquisiti di recente.</p> <p>È necessario specificare la crittografia per l'oggetto. I metadati degli oggetti e altri dati sensibili non vengono crittografati.</p> <p>Le chiavi vengono gestite al di fuori di StorageGRID.</p> <p><a href="#">"Utilizzare la crittografia lato server"</a></p>
Crittografia di un volume esterno o di un datastore	Se la piattaforma di implementazione lo supporta, si utilizza un metodo di crittografia esterno a StorageGRID per crittografare un intero volume o datastore.	<p>Tutti i dati degli oggetti, i metadati e i dati di configurazione del sistema, presupponendo che ogni volume o datastore sia crittografato.</p> <p>Un metodo di crittografia esterno offre un controllo più rigoroso sugli algoritmi e sulle chiavi di crittografia. Può essere combinato con gli altri metodi elencati.</p>

Opzione di crittografia	Come funziona	Valido per
Crittografia degli oggetti al di fuori di StorageGRID	Si utilizza un metodo di crittografia esterno a StorageGRID per crittografare i dati degli oggetti e i metadati prima che vengano acquisiti in StorageGRID.	<p>Solo dati a oggetti e metadati (i dati di configurazione del sistema non sono crittografati).</p> <p>Un metodo di crittografia esterno offre un controllo più rigoroso sugli algoritmi e sulle chiavi di crittografia. Può essere combinato con gli altri metodi elencati.</p> <p><a href="#">"Amazon Simple Storage Service - Guida utente: Protezione dei dati mediante crittografia lato client"</a></p>

## Utilizzare più metodi di crittografia

A seconda dei requisiti, è possibile utilizzare più metodi di crittografia alla volta. Ad esempio:

- È possibile utilizzare un KMS per proteggere i nodi dell'appliance e utilizzare la funzionalità di sicurezza del disco in Gestione sistema di SANtricity per "crittografare due volte" i dati sui dischi con crittografia automatica delle stesse appliance.
- È possibile utilizzare un KMS per proteggere i dati sui nodi dell'appliance e utilizzare l'opzione di crittografia degli oggetti memorizzati per crittografare tutti gli oggetti quando vengono acquisiti.

Se solo una piccola parte degli oggetti richiede la crittografia, prendere in considerazione il controllo della crittografia a livello di bucket o di singolo oggetto. L'abilitazione di più livelli di crittografia comporta un costo aggiuntivo per le performance.

### Informazioni correlate

["Scopri le opzioni di crittografia certificate FIPS"](#)

## Gestire i certificati

### Gestire i certificati di sicurezza

I certificati di sicurezza sono piccoli file di dati utilizzati per creare connessioni sicure e affidabili tra i componenti di StorageGRID e tra i componenti di StorageGRID e i sistemi esterni.

StorageGRID utilizza due tipi di certificati di sicurezza:

- **I certificati server** sono richiesti quando si utilizzano connessioni HTTPS. I certificati del server vengono utilizzati per stabilire connessioni sicure tra client e server, autenticando l'identità di un server nei suoi client e fornendo un percorso di comunicazione sicuro per i dati. Il server e il client dispongono di una copia del certificato.
- **Certificati client** autenticano un'identità del client o dell'utente sul server, fornendo un'autenticazione più sicura rispetto alle sole password. I certificati client non crittografano i dati.

Quando un client si connette al server tramite HTTPS, il server risponde con il certificato del server, che

contiene una chiave pubblica. Il client confronta la firma del server con la firma presente sulla propria copia del certificato. Se le firme corrispondono, il client avvia una sessione con il server utilizzando la stessa chiave pubblica.

StorageGRID funziona come server per alcune connessioni (come l'endpoint del bilanciamento del carico) o come client per altre connessioni (come il servizio di replica di CloudMirror).

### Certificato Grid CA predefinito

StorageGRID dispone di un'autorità di certificazione (CA) integrata che genera un certificato CA Grid interno durante l'installazione del sistema. Per impostazione predefinita, il certificato Grid CA viene utilizzato per proteggere il traffico StorageGRID interno. Un'autorità di certificazione (CA) esterna può rilasciare certificati personalizzati pienamente conformi alle policy di sicurezza delle informazioni della tua organizzazione.

Utilizzare il certificato Grid CA per gli ambienti non di produzione. Per la produzione, utilizzare certificati personalizzati firmati da un'autorità di certificazione esterna. Le connessioni non protette senza certificato sono supportate ma non consigliate.

- I certificati CA personalizzati non rimuovono i certificati interni; tuttavia, i certificati personalizzati devono essere quelli specificati per la verifica delle connessioni al server.
- Tutti i certificati personalizzati devono soddisfare la ["linee guida per la protezione avanzata del sistema per i certificati server"](#).
- StorageGRID supporta il raggruppamento di certificati da una CA in un singolo file (noto come bundle di certificati CA).



StorageGRID include anche certificati CA del sistema operativo che sono gli stessi su tutte le griglie. Negli ambienti di produzione, assicurarsi di specificare un certificato personalizzato firmato da un'autorità di certificazione esterna al posto del certificato CA del sistema operativo.

Le varianti dei tipi di certificato server e client vengono implementate in diversi modi. Prima di configurare il sistema, è necessario disporre di tutti i certificati necessari per la configurazione specifica di StorageGRID.

### Accesso ai certificati di sicurezza

È possibile accedere alle informazioni su tutti i certificati StorageGRID in una singola posizione, insieme ai collegamenti al flusso di lavoro di configurazione per ciascun certificato.

#### Fasi

1. Da Grid Manager, seleziona **Configurazione > Sicurezza > Certificati**.

# Certificates

View and manage the certificates that secure HTTPS connections between StorageGRID and external clients, such as S3 or Swift, and external servers, such as a key management server (KMS).

Global

Grid CA

Client

Load balancer endpoints

Tenants

Other

The StorageGRID certificate authority ("grid CA") generates and signs two global certificates during installation. The management interface certificate on Admin Nodes secures the management interface. The S3 and Swift API certificate on Storage and Gateway Nodes secures client access. You should replace each default certificate with your own custom certificate signed by an external certificate authority.

Name	Description	Type ⓘ	Expiration date ⓘ ⌵
<a href="#">Management interface certificate</a>	Secures the connection between client web browsers and the Grid Manager, Tenant Manager, Grid Management API, and Tenant Management API.	Custom	Jun 4th, 2022
<a href="#">S3 and Swift API certificate</a>	Secures the connections between S3 and Swift clients and Storage Nodes or between clients and the deprecated CLB service on Gateway Nodes. You can optionally use this certificate for a load balancer endpoint as well.	Custom	Jun 4th, 2022

2. Selezionare una scheda nella pagina certificati per informazioni su ciascuna categoria di certificati e per accedere alle impostazioni del certificato. È possibile accedere a una scheda se si dispone di ["autorizzazione appropriata"](#).
- **Globale:** Protegge l'accesso a StorageGRID da browser Web e client API esterni.
  - **Grid CA:** Protegge il traffico StorageGRID interno.
  - **Client:** Protegge le connessioni tra client esterni e il database StorageGRID Prometheus.
  - **Endpoints del bilanciamento del carico:** Protegge le connessioni tra i client S3 e il bilanciamento del carico StorageGRID.
  - **Tenant:** Protegge le connessioni ai server di federazione delle identità o dagli endpoint dei servizi della piattaforma alle risorse di storage S3.
  - **Altro:** Protegge le connessioni StorageGRID che richiedono certificati specifici.

Ciascuna scheda viene descritta di seguito con collegamenti a dettagli aggiuntivi del certificato.



## Globale

I certificati globali proteggono l'accesso StorageGRID dai browser Web e dai client API S3 esterni. Durante l'installazione, l'autorità di certificazione StorageGRID genera inizialmente due certificati globali. La procedura consigliata per un ambiente di produzione consiste nell'utilizzare certificati personalizzati firmati da un'autorità di certificazione esterna.

- [Certificato dell'interfaccia di gestione](#): Protegge le connessioni del browser Web del client alle interfacce di gestione StorageGRID.
- [Certificato API S3](#): Protegge le connessioni API client ai nodi di archiviazione, ai nodi amministrativi e ai nodi gateway, che le applicazioni client S3 utilizzano per caricare e scaricare i dati oggetto.

Le informazioni sui certificati globali installati includono:

- **Nome**: Nome del certificato con collegamento alla gestione del certificato.
- **Descrizione**
- **Type**: Personalizzato o predefinito. + per una maggiore sicurezza della griglia, è necessario utilizzare sempre un certificato personalizzato.
- **Data di scadenza**: Se si utilizza il certificato predefinito, non viene visualizzata alcuna data di scadenza.

È possibile:

- Sostituire i certificati predefiniti con certificati personalizzati firmati da un'autorità di certificazione esterna per una maggiore sicurezza della griglia:
  - ["Sostituire il certificato predefinito dell'interfaccia di gestione generata da StorageGRID"](#) Utilizzato per le connessioni di Grid Manager e Tenant Manager.
  - ["Sostituire il certificato API S3"](#) Utilizzato per connessioni endpoint nodo storage e bilanciamento del carico (opzionali).
- ["Ripristinare il certificato dell'interfaccia di gestione predefinita"](#).
- ["Ripristinare il certificato API S3 predefinito"](#).
- ["Utilizzare uno script per generare un nuovo certificato autofirmato dell'interfaccia di gestione"](#).
- Copiare o scaricare ["certificato dell'interfaccia di gestione"](#) o ["Certificato API S3"](#).

## CA griglia

Il [Certificato Grid CA](#), generato dall'autorità di certificazione StorageGRID durante l'installazione di StorageGRID, protegge tutto il traffico StorageGRID interno.

Le informazioni sul certificato includono la data di scadenza del certificato e il contenuto del certificato.

È possibile ["Copia o scarica il certificato Grid CA"](#), ma non è possibile modificarlo.

## Client

[Certificati client](#), Generato da un'autorità di certificazione esterna, proteggere le connessioni tra gli strumenti di monitoraggio esterni e il database di StorageGRID Prometheus.

La tabella dei certificati contiene una riga per ciascun certificato client configurato e indica se il certificato può essere utilizzato per l'accesso al database Prometheus, insieme alla data di scadenza

del certificato.

È possibile:

- ["Caricare o generare un nuovo certificato client."](#)
- Selezionare il nome di un certificato per visualizzare i dettagli del certificato in cui è possibile:
  - ["Modificare il nome del certificato client."](#)
  - ["Impostare l'autorizzazione di accesso Prometheus."](#)
  - ["Caricare e sostituire il certificato del client."](#)
  - ["Copiare o scaricare il certificato client."](#)
  - ["Rimuovere il certificato client."](#)
- Selezionare **azioni** per rapidamente ["modifica"](#), ["allega"](#) o ["rimuovere"](#) un certificato client. È possibile selezionare fino a 10 certificati client e rimuoverli contemporaneamente utilizzando **azioni > Rimuovi**.

### Endpoint del bilanciamento del carico

[Certificati endpoint per il bilanciamento del carico](#) Proteggere le connessioni tra i client S3 e il servizio di bilanciamento del carico StorageGRID su nodi gateway e nodi amministrativi.

La tabella degli endpoint del bilanciamento del carico contiene una riga per ogni endpoint del bilanciamento del carico configurato e indica se per l'endpoint viene utilizzato il certificato API S3 globale o un certificato endpoint del bilanciamento del carico personalizzato. Viene visualizzata anche la data di scadenza di ciascun certificato.



Le modifiche a un certificato endpoint possono richiedere fino a 15 minuti per essere applicate a tutti i nodi.

È possibile:

- ["Visualizzare un endpoint di bilanciamento del carico"](#), inclusi i dettagli del certificato.
- ["Specificare un certificato endpoint per il bilanciamento del carico per FabricPool."](#)
- ["Utilizzare il certificato API S3 globale"](#) invece di generare un nuovo certificato endpoint per il bilanciamento del carico.

### Tenant

I locatari possono utilizzare [certificati del server di federazione delle identità](#) o [certificati endpoint del servizio di piattaforma](#) assicurare le loro connessioni con StorageGRID.

La tabella tenant ha una riga per ciascun tenant e indica se ciascun tenant dispone dell'autorizzazione per utilizzare la propria origine di identità o i propri servizi di piattaforma.

È possibile:

- ["Selezionare il nome di un tenant per accedere al tenant manager"](#)
- ["Selezionare un nome tenant per visualizzare i dettagli della federazione delle identità del tenant"](#)
- ["Selezionare un nome tenant per visualizzare i dettagli dei servizi della piattaforma tenant"](#)
- ["Specificare un certificato endpoint del servizio di piattaforma durante la creazione dell'endpoint"](#)

### Altro

StorageGRID utilizza altri certificati di sicurezza per scopi specifici. Questi certificati sono elencati in base al nome funzionale. Altri certificati di sicurezza includono:

- [Certificati Cloud Storage Pool](#)
- [Certificati di notifica degli avvisi via email](#)
- [Certificati server syslog esterni](#)
- [Certificati di connessione Grid Federation](#)
- [Certificati di federazione delle identità](#)
- [Certificati KMS \(Key Management Server\)](#)
- [Certificati Single Sign-on](#)

Le informazioni indicano il tipo di certificato utilizzato da una funzione e le relative date di scadenza del certificato server e client, a seconda dei casi. Selezionando il nome di una funzione si apre una scheda del browser in cui è possibile visualizzare e modificare i dettagli del certificato.



È possibile visualizzare e accedere alle informazioni relative ad altri certificati solo se si dispone di ["autorizzazione appropriata"](#).

È possibile:

- ["Specificare un certificato Cloud Storage Pool per S3, C2S S3 o Azure"](#)
- ["Specificare un certificato per le notifiche e-mail di avviso"](#)
- ["Utilizzare un certificato per un server syslog esterno"](#)
- ["Ruotare i certificati di connessione Grid Federation"](#)
- ["Visualizzare e modificare un certificato di federazione delle identità"](#)
- ["Caricare i certificati del server e del client del server di gestione delle chiavi \(KMS\)"](#)
- ["Specificare manualmente un certificato SSO per un trust della parte che si basa"](#)

## Dettagli del certificato di sicurezza

Di seguito sono descritti i tipi di certificato di protezione, con collegamenti alle istruzioni di implementazione.

### Certificato dell'interfaccia di gestione

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	<p>Autentica la connessione tra i browser Web client e l'interfaccia di gestione di StorageGRID, consentendo agli utenti di accedere a Grid Manager e Tenant Manager senza avvisi di sicurezza.</p> <p>Questo certificato autentica anche le connessioni API Grid Management e API Tenant Management.</p> <p>È possibile utilizzare il certificato predefinito creato durante l'installazione o caricare un certificato personalizzato.</p>	<b>Configurazione &gt; Sicurezza &gt; Certificati</b> , seleziona la scheda <b>Globale</b> , quindi seleziona <b>Certificato dell'interfaccia di gestione</b>	<a href="#">"Configurare i certificati dell'interfaccia di gestione"</a>

#### Certificato API S3

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica le connessioni client S3 sicure a un nodo di storage e agli endpoint del bilanciamento del carico (opzionale).	<b>Configurazione &gt; Sicurezza &gt; Certificati</b> , seleziona la scheda <b>Globale</b> , quindi seleziona <b>Certificato API S3</b>	<a href="#">"Configurare i certificati API S3"</a>

#### Certificato Grid CA

Consultare la [Descrizione del certificato Grid CA predefinito](#).

#### Certificato del client di amministratore

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Client	<p>Installato su ciascun client, consentendo a StorageGRID di autenticare l'accesso client esterno.</p> <ul style="list-style-type: none"> <li>• Consente ai client esterni autorizzati di accedere al database StorageGRID Prometheus.</li> <li>• Consente il monitoraggio sicuro di StorageGRID utilizzando strumenti esterni.</li> </ul>	<p><b>Configurazione &gt; Sicurezza &gt; Certificati e</b> quindi selezionare la scheda <b>Client</b></p>	<p><a href="#">"Configurare i certificati client"</a></p>

**Certificato endpoint per il bilanciamento del carico**

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	<p>Autentica la connessione tra i client S3 e il servizio di bilanciamento del carico StorageGRID sui nodi gateway e i nodi amministrativi. È possibile caricare o generare un certificato di bilanciamento del carico quando si configura un endpoint di bilanciamento del carico. Le applicazioni client utilizzano il certificato di bilanciamento del carico durante la connessione a StorageGRID per salvare e recuperare i dati degli oggetti.</p> <p>È inoltre possibile utilizzare una versione personalizzata del certificato globale <a href="#">Certificato API S3</a> per autenticare le connessioni al servizio Load Balancer. Se il certificato globale viene utilizzato per autenticare le connessioni del bilanciamento del carico, non è necessario caricare o generare un certificato separato per ciascun endpoint del bilanciamento del carico.</p> <p><b>Nota:</b> il certificato utilizzato per l'autenticazione del bilanciamento del carico è il certificato più utilizzato durante il normale funzionamento StorageGRID.</p>	<b>Configurazione &gt; Rete &gt; Endpoint del bilanciatore del carico</b>	<ul style="list-style-type: none"> <li>• <a href="#">"Configurare gli endpoint del bilanciamento del carico"</a></li> <li>• <a href="#">"Creare un endpoint di bilanciamento del carico per FabricPool"</a></li> </ul>

#### Certificato endpoint Cloud Storage Pool

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione da un pool di storage cloud StorageGRID a una posizione di storage esterna, ad esempio lo storage S3 Glacier o Microsoft Azure Blob. Per ogni tipo di cloud provider è necessario un certificato diverso.	<b>ILM &gt; Storage Pools</b>	<a href="#">"Creare un pool di storage cloud"</a>

#### Certificato di notifica degli avvisi via email

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	<p>Autentica la connessione tra un server e-mail SMTP e StorageGRID utilizzato per le notifiche degli avvisi.</p> <ul style="list-style-type: none"> <li>• Se le comunicazioni con il server SMTP richiedono TLS (Transport Layer Security), è necessario specificare il certificato CA del server di posta elettronica.</li> <li>• Specificare un certificato client solo se il server di posta SMTP richiede certificati client per l'autenticazione.</li> </ul>	<b>Avvisi &gt; Configurazione e-mail</b>	<a href="#">"Imposta le notifiche via email per gli avvisi"</a>

#### Certificato server syslog esterno

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	<p>Autentica la connessione TLS o RELP/TLS tra un server syslog esterno che registra gli eventi in StorageGRID.</p> <p><b>Nota:</b> non è richiesto un certificato server syslog esterno per le connessioni TCP, RELP/TCP e UDP a un server syslog esterno.</p>	<b>Configurazione &gt; Monitoraggio &gt; Server di audit e syslog</b>	"Utilizzare un server syslog esterno"

#### certificato di connessione Grid Federation

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	Autenticare e crittografare le informazioni inviate tra il sistema StorageGRID corrente e un'altra griglia in una connessione a federazione di griglie.	<b>Configurazione &gt; Sistema &gt; Federazione di griglia</b>	<ul style="list-style-type: none"> <li>• "Creare connessioni di federazione di griglie"</li> <li>• "Ruotare i certificati di connessione"</li> </ul>

#### Certificato di federazione delle identità

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	<p>Autentica la connessione tra StorageGRID e un provider di identità esterno, ad esempio Active Directory, OpenLDAP o Oracle Directory Server.</p> <p>Utilizzato per la federazione delle identità, che consente ai gruppi di amministrazione e agli utenti di essere gestiti da un sistema esterno.</p>	<b>Configurazione &gt; Controllo accessi &gt; Federazione identità</b>	"USA la federazione delle identità"

#### Certificato del Key Management Server (KMS)



Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	Autentica la connessione tra StorageGRID e un KMS (Key Management Server) esterno, che fornisce chiavi di crittografia ai nodi appliance StorageGRID.	<b>Configurazione &gt; Sicurezza &gt; Server di gestione delle chiavi</b>	" <a href="#">Aggiunta del server di gestione delle chiavi (KMS)</a> "

#### Certificato endpoint dei servizi di piattaforma

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione dal servizio della piattaforma StorageGRID a una risorsa di storage S3.	<b>Tenant Manager &gt; STORAGE (S3) &gt; endpoint dei servizi della piattaforma</b>	" <a href="#">Creare endpoint di servizi di piattaforma</a> "  " <a href="#">Modifica dell'endpoint dei servizi della piattaforma</a> "

#### Certificato SSO (Single Sign-on)

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra i servizi di federazione delle identità, come ad FS (Active Directory Federation Services) e StorageGRID, utilizzati per le richieste SSO (Single Sign-on).	<b>Configurazione &gt; Controllo accessi &gt; Single sign-on</b>	" <a href="#">Configurare il single sign-on</a> "

### Esempi di certificati

#### Esempio 1: Servizio di bilanciamento del carico

In questo esempio, StorageGRID agisce come server.

1. È possibile configurare un endpoint di bilanciamento del carico e caricare o generare un certificato server in StorageGRID.
2. Si configura una connessione client S3 all'endpoint del bilanciamento del carico e si carica lo stesso certificato sul client.
3. Quando il client desidera salvare o recuperare i dati, si connette all'endpoint del bilanciamento del carico utilizzando HTTPS.
4. StorageGRID risponde con il certificato del server, che contiene una chiave pubblica, e con una firma basata sulla chiave privata.

5. Il client confronta la firma del server con la firma presente sulla propria copia del certificato. Se le firme corrispondono, il client avvia una sessione utilizzando la stessa chiave pubblica.
6. Il client invia i dati dell'oggetto a StorageGRID.

### Esempio 2: Server KMS (Key Management Server) esterno

In questo esempio, StorageGRID agisce come client.

1. Utilizzando il software del server di gestione delle chiavi esterno, è possibile configurare StorageGRID come client KMS e ottenere un certificato server con firma CA, un certificato client pubblico e la chiave privata per il certificato client.
2. Utilizzando Grid Manager, è possibile configurare un server KMS e caricare i certificati server e client e la chiave privata del client.
3. Quando un nodo StorageGRID necessita di una chiave di crittografia, effettua una richiesta al server KMS che include i dati del certificato e una firma basata sulla chiave privata.
4. Il server KMS convalida la firma del certificato e decide che può fidarsi di StorageGRID.
5. Il server KMS risponde utilizzando la connessione validata.

## Tipi di certificato server supportati

Il sistema StorageGRID supporta certificati personalizzati crittografati con RSA o ECDSA (algoritmo di firma digitale a curva ellittica).



Il tipo di crittografia per il criterio di protezione deve corrispondere al tipo di certificato del server. Ad esempio, le crittografia RSA richiedono certificati RSA e le crittografia ECDSA richiedono certificati ECDSA. Vedere ["Gestire i certificati di sicurezza"](#). Se si configura un criterio di protezione personalizzato non compatibile con il certificato del server, è possibile ["ripristinare temporaneamente il criterio di protezione predefinito"](#).

Per ulteriori informazioni su come StorageGRID protegge le connessioni client, vedere ["Sicurezza per S3 client"](#).

## Configurare i certificati dell'interfaccia di gestione

È possibile sostituire il certificato dell'interfaccia di gestione predefinita con un singolo certificato personalizzato che consente agli utenti di accedere a Grid Manager e a Tenant Manager senza incontrare avvisi di sicurezza. È inoltre possibile ripristinare il certificato dell'interfaccia di gestione predefinita o generarne uno nuovo.

### A proposito di questa attività

Per impostazione predefinita, ogni nodo amministrativo riceve un certificato firmato dalla CA della griglia. Questi certificati firmati dalla CA possono essere sostituiti da un singolo certificato dell'interfaccia di gestione personalizzata comune e dalla chiave privata corrispondente.

Poiché per tutti i nodi di amministrazione viene utilizzato un singolo certificato di interfaccia di gestione personalizzata, è necessario specificare il certificato come carattere jolly o certificato multidominio se i client devono verificare il nome host durante la connessione a Grid Manager e Tenant Manager. Definire il certificato personalizzato in modo che corrisponda a tutti i nodi Admin nella griglia.

È necessario completare la configurazione sul server e, a seconda dell'autorità di certificazione principale (CA)

utilizzata, gli utenti potrebbero dover installare il certificato Grid CA nel browser Web che utilizzeranno per accedere a Grid Manager e a Tenant Manager.



Per garantire che le operazioni non vengano interrotte da un certificato server non riuscito, l'avviso **Scadenza del certificato server per l'interfaccia di gestione** viene attivato quando il certificato server sta per scadere. Se necessario, è possibile visualizzare la data di scadenza del certificato corrente selezionando **Configurazione > Sicurezza > Certificati** e controllando la data di scadenza del certificato dell'interfaccia di gestione nella scheda Globale.



Se si accede a Grid Manager o Tenant Manager utilizzando un nome di dominio invece di un indirizzo IP, il browser mostra un errore di certificato senza l'opzione di ignorare se si verifica una delle seguenti condizioni:

- Il certificato dell'interfaccia di gestione personalizzata scade.
- Voi [ripristinare da un certificato dell'interfaccia di gestione personalizzata al certificato server predefinito](#).

### Aggiungere un certificato di interfaccia di gestione personalizzata

Per aggiungere un certificato di interfaccia di gestione personalizzato, è possibile fornire un certificato personalizzato o generarne uno utilizzando Grid Manager.

#### Fasi

1. Selezionare **Configurazione > Sicurezza > Certificati**.
2. Nella scheda **Global**, selezionare **Management interface certificate**.
3. Selezionare **Usa certificato personalizzato**.
4. Caricare o generare il certificato.

## Carica certificato

Caricare i file dei certificati del server richiesti.

a. Selezionare **carica certificato**.

b. Caricare i file dei certificati del server richiesti:

- **Server certificate**: Il file di certificato del server personalizzato (con codifica PEM).
- **Chiave privata del certificato**: Il file della chiave privata del certificato del server personalizzato (.key).



Le chiavi private EC devono essere di almeno 224 bit. Le chiavi private RSA devono essere di almeno 2048 bit.

- **Bundle CA**: Un singolo file opzionale contenente i certificati di ogni autorità di certificazione di emissione intermedia (CA). Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.

c. Espandere **Dettagli certificato** per visualizzare i metadati di ciascun certificato caricato. Se è stato caricato un bundle CA opzionale, ciascun certificato viene visualizzato nella propria scheda.

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato oppure selezionare **Download CA bundle** (Scarica pacchetto CA) per salvare il bundle del certificato.

Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione .pem.

Ad esempio: storagegrid\_certificate.pem

- Selezionare **Copy certificate PEM** or **Copy CA bundle PEM** per copiare il contenuto del certificato e incollarlo altrove.

d. Selezionare **Salva**. Il certificato dell'interfaccia di gestione personalizzata viene utilizzato per tutte le nuove connessioni successive a Grid Manager, Tenant Manager, Grid Manager API o tenant Manager API.

## Generare un certificato

Generare i file dei certificati del server.



La procedura consigliata per un ambiente di produzione consiste nell'utilizzare un certificato dell'interfaccia di gestione personalizzata firmato da un'autorità di certificazione esterna.

a. Selezionare **genera certificato**.

b. Specificare le informazioni del certificato:

Campo	Descrizione
Nome di dominio	Uno o più nomi di dominio completi da includere nel certificato. Utilizzare un * come carattere jolly per rappresentare più nomi di dominio.

Campo	Descrizione
IP	Uno o più indirizzi IP da includere nel certificato.
Soggetto (facoltativo)	<p>X.509 nome soggetto o nome distinto (DN) del proprietario del certificato.</p> <p>Se in questo campo non viene immesso alcun valore, il certificato generato utilizza il primo nome di dominio o indirizzo IP come nome comune (CN) del soggetto.</p>
Giorni di validità	Numero di giorni successivi alla creazione della scadenza del certificato.
Aggiungere estensioni di utilizzo chiave	<p>Se selezionata (impostazione predefinita e consigliata), l'utilizzo delle chiavi e le estensioni estese dell'utilizzo delle chiavi vengono aggiunte al certificato generato.</p> <p>Queste estensioni definiscono lo scopo della chiave contenuta nel certificato.</p> <p><b>Nota:</b> Lasciare questa casella di controllo selezionata a meno che non si verifichino problemi di connessione con client meno recenti quando i certificati includono queste estensioni.</p>

c. Selezionare **generate**.

d. Selezionare **Dettagli certificato** per visualizzare i metadati del certificato generato.

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.

e. Selezionare **Salva**. Il certificato dell'interfaccia di gestione personalizzata viene utilizzato per tutte le nuove connessioni successive a Grid Manager, Tenant Manager, Grid Manager API o tenant Manager API.

5. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.



Dopo aver caricato o generato un nuovo certificato, attendere fino a un giorno per la cancellazione degli avvisi relativi alla scadenza del certificato.

6. Dopo aver aggiunto un certificato dell'interfaccia di gestione personalizzata, la pagina del certificato dell'interfaccia di gestione visualizza informazioni dettagliate sul certificato per i certificati in uso. + è possibile scaricare o copiare il PEM del certificato secondo necessità.

## Ripristinare il certificato dell'interfaccia di gestione predefinita

È possibile ripristinare l'utilizzo del certificato dell'interfaccia di gestione predefinita per Grid Manager e Tenant Manager Connections.

### Fasi

1. Selezionare **Configurazione > Sicurezza > Certificati**.
2. Nella scheda **Global**, selezionare **Management interface certificate**.
3. Selezionare **Usa certificato predefinito**.

Quando si ripristina il certificato dell'interfaccia di gestione predefinita, i file di certificato del server personalizzati configurati vengono cancellati e non possono essere ripristinati dal sistema. Il certificato predefinito dell'interfaccia di gestione viene utilizzato per tutte le nuove connessioni client successive.

4. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

## Utilizzare uno script per generare un nuovo certificato autofirmato dell'interfaccia di gestione

Se è richiesta una convalida rigorosa del nome host, è possibile utilizzare uno script per generare il certificato dell'interfaccia di gestione.

### Prima di iniziare

- Si dispone di ["autorizzazioni di accesso specifiche"](#).
- Si dispone del `Passwords.txt` file.

### A proposito di questa attività

La procedura consigliata per un ambiente di produzione consiste nell'utilizzare un certificato firmato da un'autorità di certificazione esterna.

### Fasi

1. Ottenere il nome di dominio completo (FQDN) di ciascun nodo di amministrazione.
2. Accedere al nodo di amministrazione principale:
  - a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
  - b. Immettere la password elencata nel `Passwords.txt` file.
  - c. Immettere il seguente comando per passare alla directory principale: `su -`
  - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

3. Configurare StorageGRID con un nuovo certificato autofirmato.

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

- Per `--domains`, utilizzare i caratteri jolly per rappresentare i nomi di dominio completi di tutti i nodi Admin. Ad esempio, `*.ui.storagegrid.example.com` utilizza il carattere jolly `*` per rappresentare `admin1.ui.storagegrid.example.com` e `admin2.ui.storagegrid.example.com`.
- Impostare `--type` su `management` per configurare il certificato dell'interfaccia di gestione, utilizzato da Grid Manager e Tenant Manager.

- Per impostazione predefinita, i certificati generati sono validi per un anno (365 giorni) e devono essere ricreati prima della scadenza. È possibile utilizzare l' `--days` argomento per sovrascrivere il periodo di validità predefinito.



Il periodo di validità di un certificato inizia quando `make-certificate` viene eseguito. È necessario assicurarsi che il client di gestione sia sincronizzato con la stessa origine temporale di StorageGRID; in caso contrario, il client potrebbe rifiutare il certificato.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type  
management --days 720
```

L'output risultante contiene il certificato pubblico necessario al client API di gestione.

#### 4. Selezionare e copiare il certificato.

Includere i tag BEGIN e END nella selezione.

#### 5. Disconnettersi dalla shell dei comandi. `$ exit`

#### 6. Verificare che il certificato sia stato configurato:

- Accedere a Grid Manager.
- Selezionare **Configurazione > Sicurezza > Certificati**
- Nella scheda **Global**, selezionare **Management interface certificate**.

#### 7. Configurare il client di gestione in modo che utilizzi il certificato pubblico copiato. Includere i tag inizio e FINE.

### Scaricare o copiare il certificato dell'interfaccia di gestione

È possibile salvare o copiare il contenuto del certificato dell'interfaccia di gestione per utilizzarlo altrove.

#### Fasi

- Selezionare **Configurazione > Sicurezza > Certificati**.
- Nella scheda **Global**, selezionare **Management interface certificate**.
- Selezionare la scheda **Server** o **bundle CA**, quindi scaricare o copiare il certificato.

### Scaricare il file di certificato o il bundle CA

Scaricare il certificato o il file bundle CA .pem. Se si utilizza un bundle CA opzionale, ciascun certificato del bundle viene visualizzato nella propria sottoscheda.

a. Selezionare **Scarica certificato** o **Scarica bundle CA**.

Se si sta scaricando un bundle CA, tutti i certificati contenuti nelle schede secondarie del bundle CA vengono scaricati come un singolo file.

b. Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione .pem.

Ad esempio: `storagegrid_certificate.pem`

### Copia certificato o pacchetto CA PEM

Copiare il testo del certificato per incollarlo altrove. Se si utilizza un bundle CA opzionale, ciascun certificato del bundle viene visualizzato nella propria sottoscheda.

a. Selezionare **Copy certificate PEM** or **Copy CA bundle PEM**.

Se si copia un bundle CA, tutti i certificati contenuti nelle schede secondarie del bundle CA vengono copiati insieme.

b. Incollare il certificato copiato in un editor di testo.

c. Salvare il file di testo con l'estensione .pem.

Ad esempio: `storagegrid_certificate.pem`

## Configurare i certificati API S3

È possibile sostituire o ripristinare il certificato del server utilizzato per le connessioni client S3 ai nodi di storage o agli endpoint di bilanciamento del carico. Il certificato del server personalizzato sostitutivo è specifico dell'organizzazione.



I dettagli Swift sono stati rimossi da questa versione del sito della documentazione. Vedere ["StorageGRID 11,8: Configurazione dei certificati API S3 e Swift"](#).

### A proposito di questa attività

Per impostazione predefinita, ogni nodo di storage viene emesso un certificato server X.509 firmato dalla CA della griglia. Questi certificati firmati dalla CA possono essere sostituiti da un singolo certificato server personalizzato comune e dalla chiave privata corrispondente.

Per tutti i nodi di storage viene utilizzato un singolo certificato server personalizzato, pertanto è necessario specificare il certificato come certificato wildcard o multi-dominio se i client devono verificare il nome host durante la connessione all'endpoint di storage. Definire il certificato personalizzato in modo che corrisponda a tutti i nodi di storage nella griglia.

Dopo aver completato la configurazione sul server, potrebbe essere necessario installare anche il certificato CA Grid nel client API S3 da utilizzare per accedere al sistema, a seconda dell'autorità di certificazione



principale (CA) in uso.



Per garantire che le operazioni non vengano interrotte da un certificato server non riuscito, l'avviso **Scadenza del certificato server globale per l'API S3** viene attivato quando il certificato del server radice sta per scadere. Se necessario, è possibile visualizzare la data di scadenza del certificato corrente selezionando **Configurazione > Sicurezza > Certificati** e controllando la data di scadenza del certificato API S3 nella scheda Globale.

È possibile caricare o generare un certificato API S3 personalizzato.

### **Aggiungere un certificato API S3 personalizzato**

#### **Fasi**

1. Selezionare **Configurazione > Sicurezza > Certificati**.
2. Nella scheda **Globale**, selezionare **S3 certificato API**.
3. Selezionare **Usa certificato personalizzato**.
4. Caricare o generare il certificato.

## Carica certificato

Caricare i file dei certificati del server richiesti.

a. Selezionare **carica certificato**.

b. Caricare i file dei certificati del server richiesti:

- **Server certificate:** Il file di certificato del server personalizzato (con codifica PEM).
- **Chiave privata del certificato:** Il file della chiave privata del certificato del server personalizzato (.key).



Le chiavi private EC devono essere di almeno 224 bit. Le chiavi private RSA devono essere di almeno 2048 bit.

- **Bundle CA:** Un singolo file opzionale contenente i certificati di ciascuna autorità di certificazione di emissione intermedia. Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.

c. Selezionare i dettagli del certificato per visualizzare i metadati e PEM per ogni certificato API S3 personalizzato caricato. Se è stato caricato un bundle CA opzionale, ciascun certificato viene visualizzato nella propria scheda.

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato oppure selezionare **Download CA bundle** (Scarica pacchetto CA) per salvare il bundle del certificato.

Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione .pem.

Ad esempio: storagegrid\_certificate.pem

- Selezionare **Copy certificate PEM** or **Copy CA bundle PEM** per copiare il contenuto del certificato e incollarlo altrove.

d. Selezionare **Salva**.

Il certificato server personalizzato viene utilizzato per le nuove connessioni client S3 successive.

## Generare un certificato

Generare i file dei certificati del server.

a. Selezionare **genera certificato**.

b. Specificare le informazioni del certificato:

Campo	Descrizione
Nome di dominio	Uno o più nomi di dominio completi da includere nel certificato. Utilizzare un * come carattere jolly per rappresentare più nomi di dominio.
IP	Uno o più indirizzi IP da includere nel certificato.

Campo	Descrizione
Soggetto (facoltativo)	<p>X.509 nome soggetto o nome distinto (DN) del proprietario del certificato.</p> <p>Se in questo campo non viene immesso alcun valore, il certificato generato utilizza il primo nome di dominio o indirizzo IP come nome comune (CN) del soggetto.</p>
Giorni di validità	Numero di giorni successivi alla creazione della scadenza del certificato.
Aggiungere estensioni di utilizzo chiave	<p>Se selezionata (impostazione predefinita e consigliata), l'utilizzo delle chiavi e le estensioni estese dell'utilizzo delle chiavi vengono aggiunte al certificato generato.</p> <p>Queste estensioni definiscono lo scopo della chiave contenuta nel certificato.</p> <p><b>Nota:</b> Lasciare questa casella di controllo selezionata a meno che non si verifichino problemi di connessione con client meno recenti quando i certificati includono queste estensioni.</p>

c. Selezionare **generate**.

d. Selezionare **Dettagli certificato** per visualizzare i metadati e PEM per il certificato API S3 personalizzato generato.

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.

e. Selezionare **Salva**.

Il certificato server personalizzato viene utilizzato per le nuove connessioni client S3 successive.

5. Selezionare una scheda per visualizzare i metadati per il certificato del server StorageGRID predefinito, un certificato CA firmato caricato o un certificato personalizzato generato.



Dopo aver caricato o generato un nuovo certificato, attendere fino a un giorno per la cancellazione degli avvisi relativi alla scadenza del certificato.

6. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

7. Dopo aver aggiunto un certificato API S3 personalizzato, la pagina del certificato API S3 visualizza informazioni dettagliate sul certificato API S3 personalizzato in uso. + è possibile scaricare o copiare il PEM del certificato secondo necessità.

## Ripristinare il certificato API S3 predefinito

È possibile ripristinare l'utilizzo del certificato API S3 predefinito per le connessioni client S3 ai nodi di archiviazione. Tuttavia, non è possibile utilizzare il certificato API S3 predefinito per un endpoint di bilanciamento del carico.

### Fasi

1. Selezionare **Configurazione > Sicurezza > Certificati**.
2. Nella scheda **Globale**, selezionare **S3 certificato API**.
3. Selezionare **Usa certificato predefinito**.

Quando si ripristina la versione predefinita del certificato API S3 globale, i file di certificato del server personalizzato configurati vengono eliminati e non possono essere recuperati dal sistema. Il certificato API S3 predefinito verrà utilizzato per le successive nuove connessioni client S3 ai nodi storage.

4. Selezionare **OK** per confermare l'avviso e ripristinare il certificato API S3 predefinito.

Se si dispone dell'autorizzazione di accesso root e il certificato API S3 personalizzato è stato utilizzato per le connessioni endpoint del bilanciamento del carico, viene visualizzato un elenco degli endpoint del bilanciamento del carico che non saranno più accessibili utilizzando il certificato API S3 predefinito.

Accedere a ["Configurare gli endpoint del bilanciamento del carico"](#) per modificare o rimuovere gli endpoint interessati.

5. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

## Scaricare o copiare il certificato API S3

È possibile salvare o copiare il contenuto del certificato API S3 per utilizzarlo altrove.

### Fasi

1. Selezionare **Configurazione > Sicurezza > Certificati**.
2. Nella scheda **Globale**, selezionare **S3 certificato API**.
3. Selezionare la scheda **Server** o **bundle CA**, quindi scaricare o copiare il certificato.

### Scaricare il file di certificato o il bundle CA

Scaricare il certificato o il file bundle CA .pem. Se si utilizza un bundle CA opzionale, ciascun certificato del bundle viene visualizzato nella propria sottoscheda.

a. Selezionare **Scarica certificato o Scarica bundle CA**.

Se si sta scaricando un bundle CA, tutti i certificati contenuti nelle schede secondarie del bundle CA vengono scaricati come un singolo file.

b. Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione .pem.

Ad esempio: `storagegrid_certificate.pem`

### Copia certificato o pacchetto CA PEM

Copiare il testo del certificato per incollarlo altrove. Se si utilizza un bundle CA opzionale, ciascun certificato del bundle viene visualizzato nella propria sottoscheda.

a. Selezionare **Copy certificate PEM** or **Copy CA bundle PEM**.

Se si copia un bundle CA, tutti i certificati contenuti nelle schede secondarie del bundle CA vengono copiati insieme.

b. Incollare il certificato copiato in un editor di testo.

c. Salvare il file di testo con l'estensione .pem.

Ad esempio: `storagegrid_certificate.pem`

### Informazioni correlate

- ["UTILIZZARE L'API REST S3"](#)
- ["Configurare i nomi di dominio degli endpoint S3"](#)

## Copiare il certificato Grid CA

StorageGRID utilizza un'autorità di certificazione interna (CA) per proteggere il traffico interno. Questo certificato non cambia se si caricano i propri certificati.

### Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).

### A proposito di questa attività

Se è stato configurato un certificato server personalizzato, le applicazioni client devono verificare il server utilizzando il certificato server personalizzato. Non devono copiare il certificato CA dal sistema StorageGRID.

### Fasi

1. Selezionare **Configurazione > Sicurezza > Certificati** e quindi selezionare la scheda **CA griglia**.

2. Nella sezione **Certificate PEM**, scaricare o copiare il certificato.

#### Scaricare il file del certificato

Scaricare il file del certificato .pem.

- a. Selezionare **Scarica certificato**.
- b. Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione .pem.

Ad esempio: `storagegrid_certificate.pem`

#### Copia certificato PEM

Copiare il testo del certificato per incollarlo altrove.

- a. Selezionare **Copy certificate PEM** (Copia certificato PEM).
- b. Incollare il certificato copiato in un editor di testo.
- c. Salvare il file di testo con l'estensione .pem.

Ad esempio: `storagegrid_certificate.pem`

## Configurare i certificati StorageGRID per FabricPool

Per i client S3 che eseguono una convalida rigorosa del nome host e non supportano la disattivazione della convalida rigorosa del nome host, ad esempio i client ONTAP che utilizzano FabricPool, è possibile generare o caricare un certificato server quando si configura l'endpoint del bilanciamento del carico.

### Prima di iniziare

- Si dispone di ["autorizzazioni di accesso specifiche"](#).
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).

### A proposito di questa attività

Quando si crea un endpoint di bilanciamento del carico, è possibile generare un certificato server autofirmato o caricare un certificato firmato da un'autorità di certificazione (CA) nota. Negli ambienti di produzione, è necessario utilizzare un certificato firmato da una CA nota. I certificati firmati da una CA possono essere ruotati senza interruzioni. Sono inoltre più sicuri perché offrono una migliore protezione contro gli attacchi man-in-the-middle.

La procedura riportata di seguito fornisce linee guida generali per i client S3 che utilizzano FabricPool. Per informazioni e procedure più dettagliate, vedere ["Configurare StorageGRID per FabricPool"](#).

### Fasi

1. Facoltativamente, configurare un gruppo ad alta disponibilità (ha) da utilizzare per FabricPool.
2. Creare un endpoint di bilanciamento del carico S3 da utilizzare per FabricPool.

Quando si crea un endpoint di bilanciamento del carico HTTPS, viene richiesto di caricare il certificato del

server, la chiave privata del certificato e il bundle CA opzionale.

### 3. Collega StorageGRID come Tier cloud in ONTAP.

Specificare la porta endpoint del bilanciamento del carico e il nome di dominio completo utilizzato nel certificato CA caricato. Quindi, fornire il certificato CA.



Se una CA intermedia ha emesso il certificato StorageGRID, è necessario fornire il certificato CA intermedio. Se il certificato StorageGRID è stato emesso direttamente dalla CA principale, è necessario fornire il certificato della CA principale.

## Configurare i certificati client

I certificati client consentono ai client esterni autorizzati di accedere al database StorageGRID Prometheus, fornendo un modo sicuro per i tool esterni di monitorare StorageGRID.

Se si desidera accedere a StorageGRID utilizzando uno strumento di monitoraggio esterno, è necessario caricare o generare un certificato client utilizzando Grid Manager e copiare le informazioni del certificato nello strumento esterno.

Vedere ["Gestire i certificati di sicurezza"](#) e ["Configurare certificati server personalizzati"](#).



Per garantire che le operazioni non vengano interrotte da un certificato server non riuscito, l'avviso **Scadenza dei certificati client configurati nella pagina Certificati** viene attivato quando il certificato server sta per scadere. Se necessario, è possibile visualizzare la data di scadenza del certificato corrente selezionando **Configurazione > Sicurezza > Certificati** e controllando la data di scadenza del certificato client nella scheda Client.



Se si utilizza un server di gestione delle chiavi (KMS) per proteggere i dati su nodi di appliance appositamente configurati, vedere le informazioni specifiche su ["Caricamento di un certificato del client KMS"](#).

### Prima di iniziare

- Si dispone dell'autorizzazione di accesso root.
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Per configurare un certificato client:
  - Si dispone dell'indirizzo IP o del nome di dominio del nodo di amministrazione.
  - Se è stato configurato il certificato dell'interfaccia di gestione StorageGRID, si dispone della CA, del certificato client e della chiave privata utilizzati per configurare il certificato dell'interfaccia di gestione.
  - Per caricare il certificato, la chiave privata del certificato è disponibile sul computer locale.
  - La chiave privata deve essere stata salvata o registrata al momento della creazione. Se non si dispone della chiave privata originale, è necessario crearne una nuova.
- Per modificare un certificato client:
  - Si dispone dell'indirizzo IP o del nome di dominio del nodo di amministrazione.
  - Per caricare il proprio certificato o un nuovo certificato, la chiave privata, il certificato client e la CA (se utilizzata) sono disponibili sul computer locale.

## Aggiungere certificati client

Per aggiungere il certificato client, attenersi a una delle seguenti procedure:

- [Certificato dell'interfaccia di gestione già configurato](#)
- [CERTIFICATO client emesso DALLA CA](#)
- [Certificato generato da Grid Manager](#)

### Certificato dell'interfaccia di gestione già configurato

Utilizzare questa procedura per aggiungere un certificato client se un certificato dell'interfaccia di gestione è già configurato utilizzando una CA, un certificato client e una chiave privata forniti dal cliente.

#### Fasi

1. In Grid Manager, seleziona **Configurazione > Sicurezza > Certificati** e quindi seleziona la scheda **Client**.
2. Selezionare **Aggiungi**.
3. Immettere un nome per il certificato.
4. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow prometheus** (Consenti prometheus).
5. Selezionare **continua**.
6. Per il passo **Allega certificati**, caricare il certificato dell'interfaccia di gestione.
  - a. Selezionare **carica certificato**.
  - b. Selezionare **Sfoglia** e selezionare il file di certificato dell'interfaccia di gestione (.pem).
    - Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.
    - Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.
  - c. Selezionare **Crea** per salvare il certificato in Grid Manager.

Il nuovo certificato viene visualizzato nella scheda Client.
7. [Configurare uno strumento di monitoraggio esterno](#), Come Grafana.

### CERTIFICATO client emesso DALLA CA

Utilizzare questa procedura per aggiungere un certificato client amministratore se non è stato configurato un certificato dell'interfaccia di gestione e si intende aggiungere un certificato client per Prometheus che utilizza un certificato client emesso dalla CA e una chiave privata.

#### Fasi

1. Eseguire i passaggi da a ["configurare un certificato dell'interfaccia di gestione"](#).
2. In Grid Manager, seleziona **Configurazione > Sicurezza > Certificati** e quindi seleziona la scheda **Client**.
3. Selezionare **Aggiungi**.
4. Immettere un nome per il certificato.
5. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow prometheus** (Consenti prometheus).



6. Selezionare **continua**.
7. Per il passo **Allega certificati**, caricare i file di certificato client, chiave privata e bundle CA:
  - a. Selezionare **carica certificato**.
  - b. Selezionare **Sfoglia** e selezionare il certificato client, la chiave privata e i file bundle CA (.pem).
    - Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.
    - Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.
  - c. Selezionare **Crea** per salvare il certificato in Grid Manager.

I nuovi certificati vengono visualizzati nella scheda Client.

8. [Configurare uno strumento di monitoraggio esterno](#), Come Grafana.

#### Certificato generato da Grid Manager

Utilizzare questa procedura per aggiungere un certificato client amministratore se non è stato configurato un certificato dell'interfaccia di gestione e si intende aggiungere un certificato client per Prometheus che utilizza la funzione di generazione del certificato in Grid Manager.

#### Fasi

1. In Grid Manager, seleziona **Configurazione > Sicurezza > Certificati** e quindi seleziona la scheda **Client**.
2. Selezionare **Aggiungi**.
3. Immettere un nome per il certificato.
4. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow prometheus** (Consenti prometheus).
5. Selezionare **continua**.
6. Per il passo **Allega certificati**, selezionare **genera certificato**.
7. Specificare le informazioni del certificato:
  - **Oggetto** (opzionale): Nome distinto (DN) o oggetto X.509 del proprietario del certificato.
  - **Giorni validi**: Il numero di giorni in cui il certificato generato è valido, a partire dal momento in cui viene generato.
  - **Add key usage Extensions** (Aggiungi estensioni utilizzo chiave): Se selezionata (impostazione predefinita e consigliata), l'utilizzo della chiave e le estensioni estese dell'utilizzo della chiave vengono aggiunte al certificato generato.

Queste estensioni definiscono lo scopo della chiave contenuta nel certificato.



Lasciare questa casella di controllo selezionata a meno che non si verifichino problemi di connessione con client meno recenti quando i certificati includono queste estensioni.

8. Selezionare **generate**.
9. selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.



Non sarà possibile visualizzare la chiave privata del certificato dopo aver chiuso la finestra di dialogo. Copiare o scaricare la chiave in un luogo sicuro.

- Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.
- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy private key** (Copia chiave privata) per copiare la chiave privata del certificato e incollarla altrove.
- Selezionare **Download private key** (Scarica chiave privata) per salvare la chiave privata come file.

Specificare il nome del file della chiave privata e la posizione di download.

10. Selezionare **Crea** per salvare il certificato in Grid Manager.

Il nuovo certificato viene visualizzato nella scheda Client.

11. In Grid Manager, seleziona **Configurazione > Sicurezza > Certificati** e quindi seleziona la scheda **Globale**.
12. Selezionare **certificato interfaccia di gestione**.
13. Selezionare **Usa certificato personalizzato**.
14. Caricare i file `certificate.pem` e `private_key.pem` dal [dettagli del certificato del client](#) passaggio. Non è necessario caricare il bundle CA.
  - a. Selezionare **carica certificato**, quindi selezionare **continua**.
  - b. Caricare ciascun file di certificato (`.pem`).
  - c. Selezionare **Save** (Salva) per salvare il certificato in Grid Manager.

Il nuovo certificato viene visualizzato nella pagina Management Interface certificate (certificato interfaccia di gestione).

15. [Configurare uno strumento di monitoraggio esterno](#), Come Grafana.

#### Configura uno strumento di monitoraggio esterno

##### Fasi

1. Configurare le seguenti impostazioni sullo strumento di monitoraggio esterno, ad esempio Grafana.

- a. **Nome:** Immettere un nome per la connessione.

StorageGRID non richiede queste informazioni, ma è necessario fornire un nome per verificare la connessione.

- b. **URL:** Immettere il nome di dominio o l'indirizzo IP per il nodo di amministrazione. Specificare HTTPS e la porta 9091.

Ad esempio: `https://admin-node.example.com:9091`

c. Abilitare **TLS Client Auth** e con **CA Certate**.

d. In TLS/SSL Auth Details (Dettagli autorizzazione TLS/SSL), copiare e incollare:

- Il certificato CA dell'interfaccia di gestione a **CA Cert**
- Il certificato del client a **Client Cert**
- La chiave privata per **chiave client**

e. **ServerName**: Immettere il nome di dominio del nodo di amministrazione.

Il nome server deve corrispondere al nome di dominio così come appare nel certificato dell'interfaccia di gestione.

2. Salvare e verificare il certificato e la chiave privata copiati da StorageGRID o da un file locale.

Ora puoi accedere alle metriche Prometheus da StorageGRID con il tuo tool di monitoraggio esterno.

Per informazioni sulle metriche, vedere ["Istruzioni per il monitoraggio di StorageGRID"](#).

## Modificare i certificati client

È possibile modificare un certificato client amministratore per modificarne il nome, abilitare o disabilitare l'accesso Prometheus o caricare un nuovo certificato quando quello corrente è scaduto.

### Fasi

1. Selezionare **Configurazione > Sicurezza > Certificati** e quindi selezionare la scheda **Client**.

Le date di scadenza del certificato e le autorizzazioni di accesso Prometheus sono elencate nella tabella. Se un certificato scade presto o è già scaduto, viene visualizzato un messaggio nella tabella e viene attivato un avviso.

2. Selezionare il certificato che si desidera modificare.

3. Selezionare **Modifica**, quindi selezionare **Modifica nome e permesso**

4. Immettere un nome per il certificato.

5. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow prometheus** (Consenti prometheus).

6. Selezionare **continua** per salvare il certificato in Grid Manager.

Il certificato aggiornato viene visualizzato nella scheda Client.

## Allegare un nuovo certificato client

È possibile caricare un nuovo certificato una volta scaduto il certificato corrente.

### Fasi

1. Selezionare **Configurazione > Sicurezza > Certificati** e quindi selezionare la scheda **Client**.

Le date di scadenza del certificato e le autorizzazioni di accesso Prometheus sono elencate nella tabella. Se un certificato scade presto o è già scaduto, viene visualizzato un messaggio nella tabella e viene attivato un avviso.

2. Selezionare il certificato che si desidera modificare.

3. Selezionare **Edit** (Modifica), quindi un'opzione di modifica.

## Carica certificato

Copiare il testo del certificato per incollarlo altrove.

- a. Selezionare **carica certificato**, quindi selezionare **continua**.
- b. Caricare il nome del certificato client (.pem).

Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione .pem.

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.
- c. Selezionare **Crea** per salvare il certificato in Grid Manager.

Il certificato aggiornato viene visualizzato nella scheda Client.

## Generare un certificato

Generare il testo del certificato da incollare altrove.

- a. Selezionare **genera certificato**.
- b. Specificare le informazioni del certificato:
  - **Oggetto** (opzionale): Nome distinto (DN) o oggetto X.509 del proprietario del certificato.
  - **Giorni validi**: Il numero di giorni in cui il certificato generato è valido, a partire dal momento in cui viene generato.
  - **Add key usage Extensions** (Aggiungi estensioni utilizzo chiave): Se selezionata (impostazione predefinita e consigliata), l'utilizzo della chiave e le estensioni estese dell'utilizzo della chiave vengono aggiunte al certificato generato.

Queste estensioni definiscono lo scopo della chiave contenuta nel certificato.



Lasciare questa casella di controllo selezionata a meno che non si verifichino problemi di connessione con client meno recenti quando i certificati includono queste estensioni.

- c. Selezionare **generate**.
- d. Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.



Non sarà possibile visualizzare la chiave privata del certificato dopo aver chiuso la finestra di dialogo. Copiare o scaricare la chiave in un luogo sicuro.

- Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del

certificato e incollarlo altrove.

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy private key** (Copia chiave privata) per copiare la chiave privata del certificato e incollarla altrove.
- Selezionare **Download private key** (Scarica chiave privata) per salvare la chiave privata come file.

Specificare il nome del file della chiave privata e la posizione di download.

- e. Selezionare **Crea** per salvare il certificato in Grid Manager.

Il nuovo certificato viene visualizzato nella scheda Client.

## Scaricare o copiare i certificati client

È possibile scaricare o copiare un certificato client da utilizzare altrove.

### Fasi

1. Selezionare **Configurazione > Sicurezza > Certificati** e quindi selezionare la scheda **Client**.
2. Selezionare il certificato che si desidera copiare o scaricare.
3. Scaricare o copiare il certificato.

#### Scaricare il file del certificato

Scaricare il file del certificato `.pem`.

- a. Selezionare **Scarica certificato**.
- b. Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

#### Copia certificato

Copiare il testo del certificato per incollarlo altrove.

- a. Selezionare **Copy certificate PEM** (Copia certificato PEM).
- b. Incollare il certificato copiato in un editor di testo.
- c. Salvare il file di testo con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

## Rimuovere i certificati client

Se non è più necessario un certificato client amministratore, è possibile rimuoverlo.

### Fasi

1. Selezionare **Configurazione > Sicurezza > Certificati** e quindi selezionare la scheda **Client**.
2. Selezionare il certificato che si desidera rimuovere.
3. Selezionare **Delete** (Elimina), quindi confermare.



Per rimuovere fino a 10 certificati, selezionare ciascun certificato da rimuovere nella scheda Client, quindi selezionare **azioni > Elimina**.

Dopo la rimozione di un certificato, i client che hanno utilizzato il certificato devono specificare un nuovo certificato client per accedere al database StorageGRID Prometheus.

## Configurare le impostazioni di sicurezza

### Gestire i criteri TLS e SSH

I criteri TLS e SSH determinano i protocolli e le crittografia utilizzati per stabilire connessioni TLS sicure con le applicazioni client e connessioni SSH sicure ai servizi StorageGRID interni.

Il criterio di sicurezza controlla il modo in cui TLS e SSH crittografano i dati in movimento. In generale, utilizzare il criterio di compatibilità moderno (predefinito), a meno che il sistema non debba essere conforme ai criteri comuni o non sia necessario utilizzare altre crittografia.



Alcuni servizi StorageGRID non sono stati aggiornati per utilizzare le crittografia di questi criteri.

### Prima di iniziare

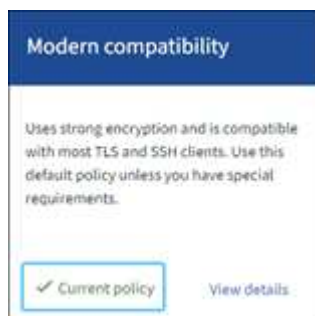
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).

### Selezionare una policy di sicurezza

#### Fasi

1. Selezionare **Configurazione > Sicurezza > Impostazioni di sicurezza**.

La scheda **TLS and SSH policies** (Criteri TLS e SSH) mostra i criteri disponibili. Il criterio attualmente attivo è contrassegnato da un segno di spunta verde sul riquadro del criterio.



2. Consulta le schede per conoscere le policy disponibili.



### Compatibilità moderna (impostazione predefinita)

Utilizza il criterio predefinito se hai bisogno di una crittografia avanzata e non hai requisiti particolari. Questa policy è compatibile con la maggior parte dei client TLS e SSH.

### Compatibilità con le versioni precedenti

Utilizzare il criterio di compatibilità Legacy se sono necessarie opzioni di compatibilità aggiuntive per i client più vecchi. Le opzioni aggiuntive presenti in questa policy potrebbero renderla meno sicura rispetto alla policy di compatibilità moderna.

### Criteri comuni

Se hai bisogno della certificazione Common Criteria, utilizza la politica Common Criteria.

### FIPS rigoroso

Utilizzare la politica FIPS strict se è richiesta la certificazione Common Criteria e si deve utilizzare il modulo NetApp Cryptographic Security Module (NCSM) 3.0.8 o NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 per le connessioni client esterne agli endpoint del bilanciatore del carico, Tenant Manager e Grid Manager. L'utilizzo di questa policy potrebbe ridurre le prestazioni.

Il modulo NCSM 3.0.8 e NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 vengono utilizzati nelle seguenti operazioni:

- NCSM
  - Connessioni TLS tra i seguenti servizi: ADC, AMS, CMN, DDS, LDR, SSM, NMS, mgmt-api, nginx, nginx-gw e cache-svc
  - Connessioni TLS tra i client e il servizio nginx-gw (endpoint del bilanciatore del carico)
  - Connessioni TLS tra i client e il servizio LDR
  - Crittografia del contenuto dell'oggetto per SSE-S3, SSE-C e impostazione di crittografia dell'oggetto archiviato
  - connessioni SSH

Per ulteriori informazioni, fare riferimento al programma di convalida degli algoritmi crittografici del NIST "[Certificato n. 4838](#)".

- Modulo API di crittografia del kernel NetApp StorageGRID

Il modulo API NetApp StorageGRID Kernel Crypto è presente solo sulle piattaforme VM e appliance StorageGRID.

- Raccolta di entropia
- Crittografia dei nodi

Per ulteriori informazioni, fare riferimento al programma di convalida degli algoritmi crittografici del NIST "[Certificati #A6242 attraverso #A6257](#)" E "[Certificato di entropia n. E223](#)".

**Nota:** Dopo aver selezionato questa policy, "[eseguire un riavvio progressivo](#)" affinché tutti i nodi attivino l'NCSM. Utilizzare **Manutenzione > Riavvio progressivo** per avviare e monitorare i riavvii.

### Personalizzato

Creare un criterio personalizzato se è necessario applicare le proprie crittografia.

Facoltativamente, se StorageGRID ha requisiti di crittografia FIPS 140, abilitare la funzionalità Modalità FIPS per utilizzare il modulo NCSM 3.0.8 e NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64:

- a. Imposta il `fipsMode` parametro a `true`.
- b. Quando richiesto, "eseguire un riavvio progressivo" affinché tutti i nodi attivino i moduli di crittografia. Utilizzare **Manutenzione > Riavvio progressivo** per avviare e monitorare i riavvii.
- c. Selezionare **Supporto > Diagnostica** per visualizzare le versioni attive del modulo FIPS.

3. Per visualizzare i dettagli relativi a crittografia, protocolli e algoritmi di ogni policy, selezionare **Visualizza dettagli**.
4. Per modificare la policy corrente, selezionare **Usa policy**.

Un segno di spunta verde viene visualizzato accanto a **policy corrente** nel riquadro del criterio.

### Creare una policy di sicurezza personalizzata

È possibile creare una policy personalizzata se è necessario applicare le proprie crittografia.

#### Fasi

1. Dal riquadro del criterio più simile al criterio personalizzato che si desidera creare, selezionare **Visualizza dettagli**.
2. Selezionare **Copia negli Appunti**, quindi selezionare **Annulla**.



3. Dal riquadro **Custom policy**, selezionare **Configure and use** (Configura e utilizza).
4. Incollare il JSON copiato e apportare le modifiche necessarie.
5. Selezionare **Usa policy**.

Un segno di spunta verde viene visualizzato accanto a **Current policy** (policy corrente) nel riquadro Custom policy (policy personalizzate).

6. Facoltativamente, selezionare **Edit Configuration** (Modifica configurazione) per apportare ulteriori modifiche al nuovo criterio personalizzato.

## Ripristinare temporaneamente il criterio di protezione predefinito

Se è stato configurato un criterio di protezione personalizzato, potrebbe non essere possibile accedere a Grid Manager se il criterio TLS configurato non è compatibile con ["certificato server configurato"](#).

È possibile ripristinare temporaneamente i criteri di protezione predefiniti.

### Fasi

1. Accedere a un nodo amministratore:
  - a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`
  - b. Immettere la password elencata nel `Passwords.txt` file.
  - c. Immettere il seguente comando per passare alla directory principale: `su -`
  - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da \$ a #.

2. Eseguire il seguente comando:

```
restore-default-cipher-configurations
```

3. Da un browser Web, accedere a Grid Manager sullo stesso nodo di amministrazione.
4. Per configurare nuovamente il criterio, procedere come [Selezionare una policy di sicurezza](#) segue.

## Configurare la sicurezza della rete e degli oggetti

È possibile configurare la protezione della rete e degli oggetti per crittografare gli oggetti archiviati, impedire determinate richieste S3 o consentire alle connessioni client ai nodi di archiviazione di utilizzare HTTP invece di HTTPS.

### Crittografia degli oggetti memorizzati

La crittografia degli oggetti memorizzati consente la crittografia di tutti i dati degli oggetti durante l'acquisizione tramite S3. Per impostazione predefinita, gli oggetti memorizzati non vengono crittografati, ma è possibile scegliere di crittografare gli oggetti utilizzando l'algoritmo di crittografia AES-128 o AES-256. Quando si attiva l'impostazione, tutti gli oggetti inseriti di recente vengono crittografati, ma non vengono apportate modifiche agli oggetti memorizzati esistenti. Se si disattiva la crittografia, gli oggetti attualmente crittografati rimangono crittografati, ma gli oggetti appena acquisiti non vengono crittografati.

L'impostazione di crittografia degli oggetti memorizzati si applica solo agli oggetti S3 che non sono stati crittografati mediante crittografia a livello di bucket o a livello di oggetto.

Per ulteriori informazioni sui metodi di crittografia StorageGRID, vedere ["Esaminare i metodi di crittografia StorageGRID"](#).

### Impedire la modifica del client

Impedisci modifica client è un'impostazione a livello di sistema. Quando si seleziona l'opzione **Impedisci modifica client**, le seguenti richieste vengono rifiutate.

## API REST S3

- Richieste DeleteBucket
- Qualsiasi richiesta di modifica dei dati di un oggetto esistente, dei metadati definiti dall'utente o del tagging degli oggetti S3

## Abilitare HTTP per le connessioni dei nodi di storage

Per impostazione predefinita, le applicazioni client utilizzano il protocollo di rete HTTPS per qualsiasi connessione diretta ai nodi di storage. È possibile attivare il protocollo HTTP per queste connessioni, ad esempio durante il test di un grid non di produzione.

Utilizzare HTTP per le connessioni al nodo di archiviazione solo se i client S3 devono stabilire connessioni HTTP direttamente ai nodi di archiviazione. Non è necessario utilizzare questa opzione per i client che utilizzano solo connessioni HTTPS o per i client che si connettono al servizio Load Balancer (poiché è possibile ["configurare ciascun endpoint del bilanciamento del carico"](#) utilizzare HTTP o HTTPS).

Vedere ["Riepilogo: Indirizzi IP e porte per le connessioni client"](#) per informazioni sulle porte utilizzate dai client S3 durante la connessione ai nodi di archiviazione tramite HTTP o HTTPS.

## Selezionare le opzioni

### Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone dell'autorizzazione di accesso root.

### Fasi

1. Selezionare **Configurazione > Sicurezza > Impostazioni di sicurezza**.
2. Selezionare la scheda **rete e oggetti**.
3. Per la crittografia degli oggetti memorizzati, utilizzare l'impostazione **None** (predefinita) se non si desidera crittografare gli oggetti memorizzati oppure selezionare **AES-128** o **AES-256** per crittografare gli oggetti memorizzati.
4. Se si desidera impedire ai client S3 di eseguire richieste specifiche, selezionare **Impedisci modifica client**.



Se si modifica questa impostazione, l'applicazione della nuova impostazione richiede circa un minuto. Il valore configurato viene memorizzato nella cache per le prestazioni e la scalabilità.

5. Se si desidera utilizzare connessioni HTTP, selezionare **Enable HTTP for Storage Node Connections** (attiva HTTP per connessioni nodo di storage) se i client si connettono direttamente ai nodi di storage.



Prestare attenzione quando si attiva HTTP per una griglia di produzione perché le richieste verranno inviate senza crittografia.

6. Selezionare **Salva**.

## Modificare le impostazioni di sicurezza dell'interfaccia

Le impostazioni di protezione dell'interfaccia consentono di controllare se gli utenti sono

disconnessi se sono inattivi per un periodo di tempo superiore a quello specificato e se una traccia dello stack è inclusa nelle risposte di errore API.

#### Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).

#### A proposito di questa attività

La pagina **Impostazioni di protezione** include le impostazioni **Timeout inattività browser** e **traccia stack API di gestione**.

#### Timeout di inattività del browser

Indica per quanto tempo il browser di un utente può rimanere inattivo prima che l'utente venga disconnesso. L'impostazione predefinita è 15 minuti.

Il timeout di inattività del browser è controllato anche da:

- Un timer StorageGRID separato, non configurabile, incluso per la sicurezza del sistema. Ogni token di autenticazione dell'utente scade 16 ore dopo l'accesso. Quando l'autenticazione dell'utente scade, l'utente viene automaticamente disconnesso, anche se il timeout di inattività del browser è disattivato o non è stato raggiunto il valore per il timeout del browser. Per rinnovare il token, l'utente deve effettuare nuovamente l'accesso.
- Impostazioni di timeout per il provider di identità, presupponendo che SSO (Single Sign-on) sia abilitato per StorageGRID.

Se l'SSO è abilitato e il browser di un utente scade, l'utente deve reinserire le proprie credenziali SSO per accedere nuovamente a StorageGRID. Vedere ["Come funziona SSO"](#).

#### Traccia stack API di gestione

Controlla se una traccia di stack viene restituita nelle risposte di errore delle API di Gestione griglia e di Gestione tenant.

Questa opzione è disattivata per impostazione predefinita, ma potrebbe essere necessario attivarla per un ambiente di test. In generale, è necessario lasciare disattivata la traccia dello stack negli ambienti di produzione per evitare di rivelare i dettagli del software interno quando si verificano errori API.

#### Fasi

1. Selezionare **Configurazione > Sicurezza > Impostazioni di sicurezza**.
2. Selezionare la scheda **interfaccia**.
3. Per modificare l'impostazione del timeout di inattività del browser:
  - a. Espandere la fisarmonica.
  - b. Per modificare il periodo di timeout, specificare un valore compreso tra 60 secondi e 7 giorni. Il timeout predefinito è di 15 minuti.
  - c. Per disattivare questa funzione, deselezionare la casella di controllo.
  - d. Selezionare **Salva**.

La nuova impostazione non influisce sugli utenti che hanno effettuato l'accesso. Per rendere effettiva la nuova impostazione di timeout, gli utenti devono eseguire nuovamente l'accesso o aggiornare il browser.

4. Per modificare l'impostazione per la traccia stack API di gestione:
  - a. Espandere la fisarmonica.
  - b. Selezionare la casella di controllo per restituire una traccia di stack nelle risposte agli errori di API di Gestione griglia e di Gestione tenant.



Lasciare la traccia dello stack disattivata negli ambienti di produzione per evitare di rivelare dettagli software interni quando si verificano errori API.

- c. Selezionare **Salva**.

## Gestisci l'accesso SSH esterno

Gestisci l'accesso SSH per il traffico in entrata nella griglia bloccando o consentendo l'accesso esterno. La gestione dell'accesso esterno SSH non ha alcun impatto sul traffico tra i nodi della griglia.

### Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).

### A proposito di questa attività

Per migliorare la sicurezza del sistema, l'accesso SSH esterno è bloccato per impostazione predefinita. Se devi eseguire attività che richiedono l'accesso SSH in ingresso, come la risoluzione dei problemi, consenti temporaneamente l'accesso esterno. Una volta completata l'attività, blocca l'accesso esterno.

### Fasi

1. Selezionare **Configurazione > Sicurezza > Impostazioni di sicurezza**.
2. Selezionare la scheda **Blocca SSH**.
3. Utilizzare l'opzione **Blocca accesso SSH in ingresso** per gestire l'accesso SSH esterno:
  - a. Selezionare la casella di controllo per bloccare l'accesso (impostazione predefinita).
  - b. Deseleziona la casella di controllo per consentire l'accesso.



Richiede l'accesso sulla porta 22 tra il laptop di servizio e tutti gli altri nodi della griglia. Una volta completata l'attività di manutenzione, rimuovere l'accesso alla porta 22.

4. Selezionare **Salva**.

## Configurare i server di gestione delle chiavi

### Che cos'è un server di gestione delle chiavi (KMS)?

Un server di gestione delle chiavi (KMS) è un sistema esterno di terze parti che fornisce chiavi di crittografia ai nodi dell'appliance StorageGRID nel sito StorageGRID associato utilizzando il protocollo KMIP (Key Management Interoperability Protocol).

StorageGRID supporta solo alcuni server di gestione delle chiavi. Per un elenco dei prodotti e delle versioni supportate, utilizzare ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

È possibile utilizzare uno o più server di gestione delle chiavi per gestire le chiavi di crittografia dei nodi di qualsiasi appliance StorageGRID con l'impostazione **crittografia dei nodi** attivata durante l'installazione. L'utilizzo di server di gestione delle chiavi con questi nodi appliance consente di proteggere i dati anche in caso di rimozione di un'appliance dal data center. Una volta crittografati i volumi dell'appliance, non è possibile accedere ai dati dell'appliance a meno che il nodo non sia in grado di comunicare con il KMS.



StorageGRID non crea o gestisce le chiavi esterne utilizzate per crittografare e decrittare i nodi dell'appliance. Se si intende utilizzare un server di gestione delle chiavi esterno per proteggere i dati StorageGRID, è necessario comprendere come configurare tale server e come gestire le chiavi di crittografia. L'esecuzione delle attività di gestione chiave non rientra nell'ambito di queste istruzioni. Per assistenza, consultare la documentazione relativa al server di gestione delle chiavi o contattare il supporto tecnico.

## Configurazione dei KMS e dell'appliance

Prima di utilizzare un server di gestione delle chiavi (KMS) per proteggere i dati StorageGRID sui nodi appliance, è necessario completare due attività di configurazione: La configurazione di uno o più server KMS e l'abilitazione della crittografia dei nodi per i nodi appliance. Una volta completate queste due attività di configurazione, il processo di gestione delle chiavi viene eseguito automaticamente.

Il diagramma di flusso mostra i passaggi di alto livello per l'utilizzo di un KMS per proteggere i dati StorageGRID sui nodi dell'appliance.

Il diagramma di flusso mostra la configurazione di KMS e dell'appliance in parallelo; tuttavia, è possibile configurare i server di gestione delle chiavi prima o dopo aver attivato la crittografia dei nodi per i nuovi nodi appliance, in base ai requisiti.

### Configurare il server di gestione delle chiavi (KMS)

La configurazione di un server di gestione delle chiavi include i seguenti passaggi di alto livello.

Fase	Fare riferimento a.
Accedere al software KMS e aggiungere un client per StorageGRID a ciascun cluster KMS o KMS.	<a href="#">"Configurare StorageGRID come client nel KMS"</a>
Ottenere le informazioni richieste per il client StorageGRID sul KMS.	<a href="#">"Configurare StorageGRID come client nel KMS"</a>
Aggiungere il KMS al Grid Manager, assegnarlo a un singolo sito o a un gruppo predefinito di siti, caricare i certificati richiesti e salvare la configurazione del KMS.	<a href="#">"Aggiunta di un server di gestione delle chiavi (KMS)"</a>

### Configurare l'apparecchio

La configurazione di un nodo appliance per l'utilizzo di KMS include i seguenti passaggi di alto livello.

1. Durante la fase di configurazione hardware dell'installazione dell'appliance, utilizzare il programma di

installazione dell'appliance StorageGRID per attivare l'impostazione **crittografia del nodo** dell'appliance.



Non è possibile attivare l'impostazione **Node Encryption** dopo l'aggiunta di un'appliance alla griglia e non è possibile utilizzare la gestione delle chiavi esterne per le appliance che non dispongono della crittografia dei nodi abilitata.

2. Eseguire il programma di installazione dell'appliance StorageGRID. Durante l'installazione, a ciascun volume dell'appliance viene assegnata una chiave di crittografia dei dati casuale (DEK), come segue:
  - I DEK vengono utilizzati per crittografare i dati su ciascun volume. Queste chiavi vengono generate utilizzando la crittografia del disco Linux Unified Key Setup (LUKS) nel sistema operativo dell'appliance e non possono essere modificate.
  - Ogni singolo DEK viene crittografato mediante una chiave di crittografia della chiave master (KEK). La chiave iniziale KEK è una chiave temporanea che crittografa i DEK fino a quando l'appliance non riesce a connettersi al KMS.
3. Aggiungere il nodo appliance a StorageGRID.

Per ulteriori informazioni, vedere ["Abilitare la crittografia del nodo"](#).

### Processo di crittografia per la gestione delle chiavi (si verifica automaticamente)

La crittografia per la gestione delle chiavi include i seguenti passaggi di alto livello che vengono eseguiti automaticamente.

1. Quando si installa un'appliance che ha attivato la crittografia dei nodi nella griglia, StorageGRID determina se esiste una configurazione KMS per il sito che contiene il nuovo nodo.
  - Se un KMS è già stato configurato per il sito, l'appliance riceve la configurazione KMS.
  - Se non è ancora stato configurato un KMS per il sito, i dati dell'appliance continuano a essere crittografati dalla KEK temporanea fino a quando non si configura un KMS per il sito e l'appliance non riceve la configurazione KMS.
2. L'appliance utilizza la configurazione KMS per connettersi al KMS e richiedere una chiave di crittografia.
3. Il KMS invia una chiave di crittografia all'appliance. La nuova chiave del KMS sostituisce la KEK temporanea e viene ora utilizzata per crittografare e decrittare i DEK per i volumi dell'appliance.



Tutti i dati che esistono prima che il nodo dell'appliance crittografato si connetta al KMS configurato vengono crittografati con una chiave temporanea. Tuttavia, i volumi dell'appliance non devono essere considerati protetti dalla rimozione dal data center fino a quando la chiave temporanea non viene sostituita dalla chiave di crittografia KMS.

4. Se l'appliance viene accesa o riavviata, si ricollega al KMS per richiedere la chiave. La chiave, che viene salvata nella memoria volatile, non può sopravvivere a una perdita di alimentazione o a un riavvio.

### Considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi

Prima di configurare un KMS (Key Management Server) esterno, è necessario comprendere le considerazioni e i requisiti.

#### Quale versione di KMIP è supportata?

StorageGRID supporta KMIP versione 1.4.



### Quali sono le considerazioni sulla rete?

Le impostazioni del firewall di rete devono consentire a ciascun nodo dell'appliance di comunicare attraverso la porta utilizzata per le comunicazioni KMIP (Key Management Interoperability Protocol). La porta KMIP predefinita è 5696.

È necessario assicurarsi che ogni nodo dell'appliance che utilizza la crittografia del nodo disponga dell'accesso di rete al cluster KMS o KMS configurato per il sito.

### Quali versioni di TLS sono supportate?

Le comunicazioni tra i nodi dell'appliance e il KMS configurato utilizzano connessioni TLS sicure. StorageGRID può supportare il protocollo TLS 1,2 o TLS 1,3 quando stabilisce connessioni KMIP a un cluster KMS o KMS, in base a ciò che il KMS supporta e a quale ["Policy TLS e SSH"](#) stai utilizzando.

StorageGRID negozia il protocollo e la crittografia (TLS 1.2) o la suite di crittografia (TLS 1.3) con il KMS quando effettua la connessione. Per vedere quali versioni del protocollo e cifrari/suite di cifrari sono disponibili, rivedere `tlsOutbound` sezione della policy TLS e SSH attiva della griglia (**Configurazione > Sicurezza Impostazioni di sicurezza**).

### Quali appliance sono supportate?

È possibile utilizzare un server di gestione delle chiavi (KMS) per gestire le chiavi di crittografia per qualsiasi appliance StorageGRID nel grid con l'impostazione **crittografia nodo** attivata. Questa impostazione può essere attivata solo durante la fase di configurazione hardware dell'installazione dell'appliance mediante il programma di installazione dell'appliance StorageGRID.



Non è possibile attivare la crittografia dei nodi dopo l'aggiunta di un'appliance alla griglia e non è possibile utilizzare la gestione delle chiavi esterne per le appliance che non hanno la crittografia dei nodi abilitata.

È possibile utilizzare il KMS configurato per appliance StorageGRID e nodi appliance.

Non è possibile utilizzare il KMS configurato per i nodi software-based (non-appliance), inclusi i seguenti:

- Nodi implementati come macchine virtuali (VM)
- Nodi implementati all'interno di motori container su host Linux

I nodi implementati su queste altre piattaforme possono utilizzare la crittografia all'esterno di StorageGRID a livello di datastore o disco.

### Quando è necessario configurare i server di gestione delle chiavi?

Per una nuova installazione, in genere è necessario configurare uno o più server di gestione delle chiavi in Grid Manager prima di creare tenant. Questo ordine garantisce che i nodi siano protetti prima che i dati degli oggetti siano memorizzati su di essi.

È possibile configurare i server di gestione delle chiavi in Grid Manager prima o dopo l'installazione dei nodi appliance.

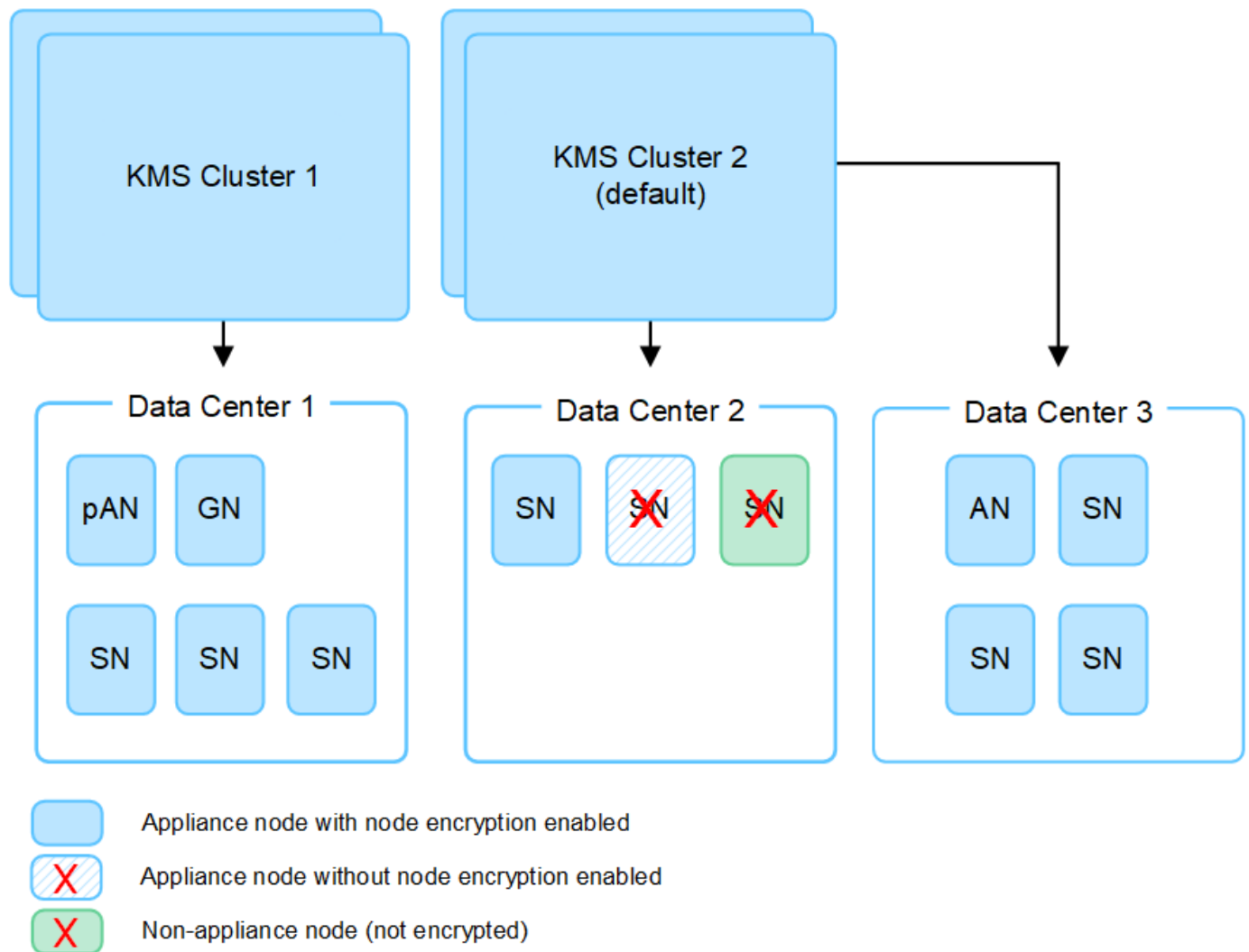
## Quanti server di gestione delle chiavi sono necessari?

È possibile configurare uno o più server di gestione delle chiavi esterni per fornire chiavi di crittografia ai nodi dell'appliance nel sistema StorageGRID. Ogni KMS fornisce una singola chiave di crittografia ai nodi dell'appliance StorageGRID in un singolo sito o in un gruppo di siti.

StorageGRID supporta l'utilizzo di cluster KMS. Ogni cluster KMS contiene più server di gestione delle chiavi replicati che condividono le impostazioni di configurazione e le chiavi di crittografia. Si consiglia di utilizzare i cluster KMS per la gestione delle chiavi perché migliora le funzionalità di failover di una configurazione ad alta disponibilità.

Si supponga, ad esempio, che il sistema StorageGRID disponga di tre siti per data center. È possibile configurare un cluster KMS per fornire una chiave a tutti i nodi appliance nel data center 1 e un secondo cluster KMS per fornire una chiave a tutti i nodi appliance in tutti gli altri siti. Quando si aggiunge il secondo cluster KMS, è possibile configurare un KMS predefinito per Data Center 2 e Data Center 3.

Tenere presente che non è possibile utilizzare un KMS per i nodi non appliance o per i nodi appliance che non hanno attivato l'impostazione **Node Encryption** durante l'installazione.



## Cosa succede quando si ruota una chiave?

Come Best practice per la sicurezza, è consigliabile utilizzare periodicamente ["ruotare la chiave di"](#)

[crittografia](#)"ogni KMS configurato.

Quando è disponibile la nuova versione della chiave:

- Viene distribuito automaticamente ai nodi appliance crittografati nel sito o nei siti associati al KMS. La distribuzione deve avvenire entro un'ora dalla rotazione della chiave.
- Se il nodo dell'appliance crittografato non è in linea quando viene distribuita la nuova versione della chiave, il nodo riceverà la nuova chiave non appena verrà riavviato.
- Se la nuova versione della chiave non può essere utilizzata per crittografare i volumi dell'appliance per qualsiasi motivo, viene attivato l'avviso **rotazione chiave di crittografia KMS non riuscita** per il nodo dell'appliance. Potrebbe essere necessario contattare il supporto tecnico per ottenere assistenza nella risoluzione di questo avviso.

### È possibile riutilizzare un nodo appliance dopo averlo crittografato?

Se è necessario installare un'appliance crittografata in un altro sistema StorageGRID, è necessario prima decommissionare il nodo Grid per spostare i dati degli oggetti in un altro nodo. Quindi, è possibile utilizzare il programma di installazione dell'appliance StorageGRID per ["Cancellare la configurazione KMS"](#). La cancellazione della configurazione KMS disattiva l'impostazione **crittografia nodo** e rimuove l'associazione tra il nodo appliance e la configurazione KMS per il sito StorageGRID.



Senza l'accesso alla chiave di crittografia KMS, i dati che rimangono sull'appliance non possono più essere utilizzati e bloccati in modo permanente.

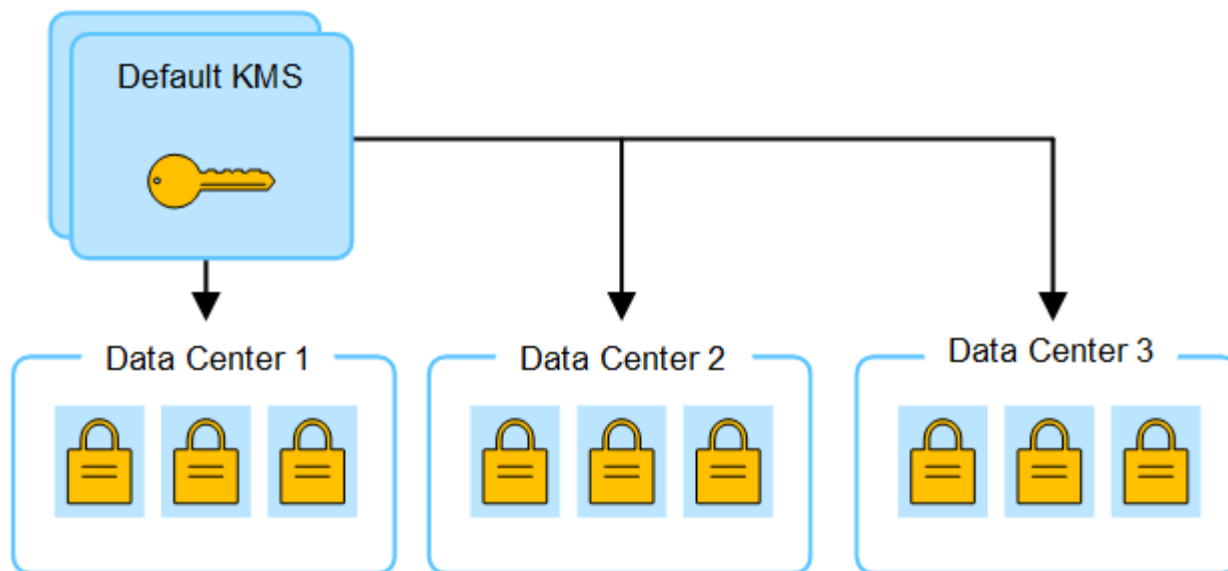
### Considerazioni per la modifica del KMS per un sito

Ciascun server di gestione delle chiavi (KMS) o cluster KMS fornisce una chiave di crittografia a tutti i nodi appliance di un singolo sito o di un gruppo di siti. Se è necessario modificare il KMS utilizzato per un sito, potrebbe essere necessario copiare la chiave di crittografia da un KMS all'altro.

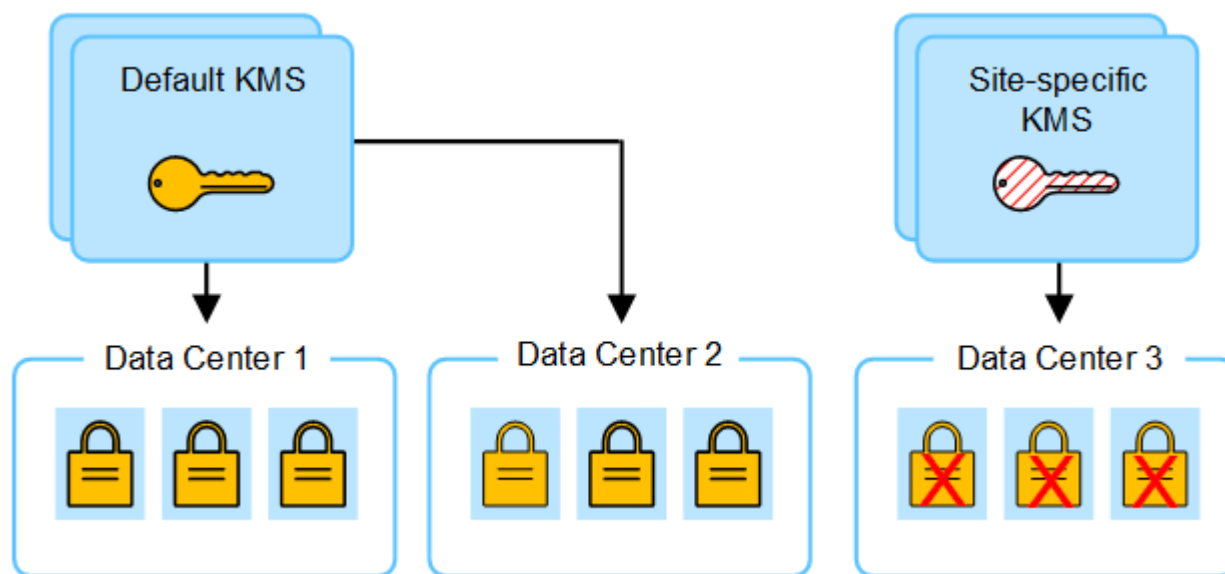
Se si modifica il KMS utilizzato per un sito, è necessario assicurarsi che i nodi appliance precedentemente crittografati in quel sito possano essere decifrati utilizzando la chiave memorizzata nel nuovo KMS. In alcuni casi, potrebbe essere necessario copiare la versione corrente della chiave di crittografia dal KMS originale al nuovo KMS. È necessario assicurarsi che il KMS disponga della chiave corretta per decrittare i nodi crittografati dell'appliance nel sito.

Ad esempio:

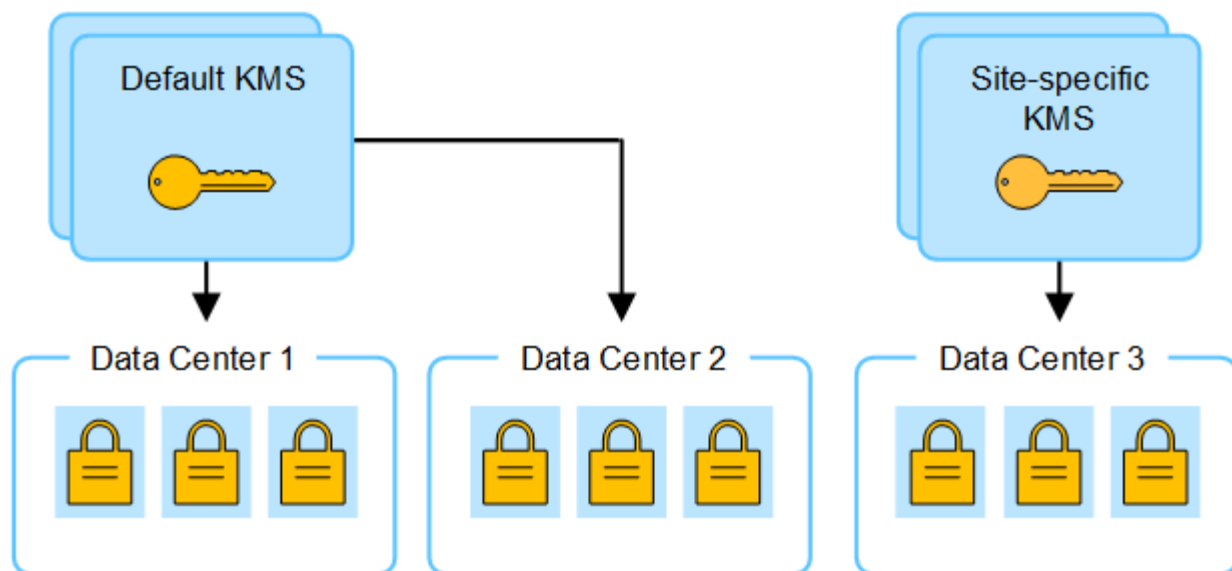
1. Inizialmente, viene configurato un KMS predefinito che si applica a tutti i siti che non dispongono di un KMS dedicato.
2. Una volta salvato il KMS, tutti i nodi appliance con l'impostazione **Node Encryption** attivata si connettono al KMS e richiedono la chiave di crittografia. Questa chiave viene utilizzata per crittografare i nodi dell'appliance in tutti i siti. La stessa chiave deve essere utilizzata anche per decrittare tali appliance.



3. Si decide di aggiungere un KMS specifico del sito per un sito (data center 3 nella figura). Tuttavia, poiché i nodi dell'appliance sono già crittografati, si verifica un errore di convalida quando si tenta di salvare la configurazione per il KMS specifico del sito. L'errore si verifica perché il KMS specifico del sito non dispone della chiave corretta per decrittare i nodi in quel sito.



4. Per risolvere il problema, copiare la versione corrente della chiave di crittografia dal KMS predefinito al nuovo KMS. Tecnicamente, si copia la chiave originale in una nuova chiave con lo stesso alias. La chiave originale diventa una versione precedente della nuova chiave). Il KMS specifico del sito dispone ora della chiave corretta per decrittografare i nodi appliance nel data center 3, in modo che possa essere salvato in StorageGRID.



### Casi di utilizzo per la modifica del KMS utilizzato per un sito

La tabella riassume i passaggi necessari per i casi più comuni di modifica del KMS per un sito.

Caso d'utilizzo per la modifica del KMS di un sito	Passaggi richiesti
Si dispone di una o più voci KMS specifiche del sito e si desidera utilizzarne una come KMS predefinito.	<p>Modificare il KMS specifico del sito. Nel campo <b>Gestisci chiavi per</b>, selezionare <b>Siti non gestiti da un altro KMS (KMS predefinito)</b>. Il KMS specifico del sito verrà ora utilizzato come KMS predefinito. Si applica a tutti i siti che non dispongono di un KMS dedicato.</p> <p><a href="#">"Modifica di un server di gestione delle chiavi (KMS)"</a></p>
Si dispone di un KMS predefinito e si aggiunge un nuovo sito in un'espansione. Non si desidera utilizzare il KMS predefinito per il nuovo sito.	<ol style="list-style-type: none"> <li>Se i nodi dell'appliance nel nuovo sito sono già stati crittografati con il KMS predefinito, utilizzare il software KMS per copiare la versione corrente della chiave di crittografia dal KMS predefinito a un nuovo KMS.</li> <li>Utilizzando Grid Manager, aggiungere il nuovo KMS e selezionare il sito.</li> </ol> <p><a href="#">"Aggiunta di un server di gestione delle chiavi (KMS)"</a></p>
Si desidera che il KMS di un sito utilizzi un server diverso.	<ol style="list-style-type: none"> <li>Se i nodi dell'appliance nel sito sono già stati crittografati dal KMS esistente, utilizzare il software KMS per copiare la versione corrente della chiave di crittografia dal KMS esistente al nuovo KMS.</li> <li>Utilizzando Grid Manager, modificare la configurazione KMS esistente e inserire il nuovo nome host o indirizzo IP.</li> </ol> <p><a href="#">"Aggiunta di un server di gestione delle chiavi (KMS)"</a></p>

## Configurare StorageGRID come client nel KMS

È necessario configurare StorageGRID come client per ogni server di gestione delle chiavi esterno o cluster KMS prima di poter aggiungere KMS a StorageGRID.



Queste istruzioni si applicano a Thales CipherTrust Manager e Hashicorp Vault. Per un elenco dei prodotti e delle versioni supportate, utilizzare ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

### Fasi

1. Dal software KMS, creare un client StorageGRID per ogni cluster KMS o KMS che si intende utilizzare.

Ogni KMS gestisce una singola chiave di crittografia per i nodi delle appliance StorageGRID in un singolo sito o in un gruppo di siti.

2. creare una chiave utilizzando uno dei due metodi seguenti:
  - Utilizzare la pagina di gestione delle chiavi del prodotto KMS. Creare una chiave di crittografia AES per ogni cluster KMS o KMS.

La chiave di crittografia deve essere 2,048 bit o superiore e deve essere esportabile.

- Chiedere a StorageGRID di creare la chiave. Verrà richiesto quando si esegue il test e si salva dopo ["caricamento dei certificati client"](#).

3. Registrare le seguenti informazioni per ciascun cluster KMS o KMS.

Queste informazioni sono necessarie quando si aggiunge il KMS a StorageGRID:

- Nome host o indirizzo IP per ciascun server.
- Porta KMIP utilizzata dal KMS.
- Alias chiave per la chiave di crittografia nel KMS.

4. Per ogni cluster KMS o KMS, ottenere un certificato server firmato da un'autorità di certificazione (CA) o un bundle di certificati che contenga ciascuno dei file di certificato CA con codifica PEM, concatenati nell'ordine della catena di certificati.

Il certificato del server consente al KMS esterno di autenticarsi su StorageGRID.

- Il certificato deve utilizzare il formato X.509 codificato con Privacy Enhanced Mail (PEM) base-64.
- Il campo Subject alternative Name (SAN) in ciascun certificato del server deve includere il nome di dominio completo (FQDN) o l'indirizzo IP a cui StorageGRID si conatterà.



Quando si configura il KMS in StorageGRID, è necessario immettere gli stessi FQDN o indirizzi IP nel campo **Nome host**.

- Il certificato del server deve corrispondere al certificato utilizzato dall'interfaccia KMIP del KMS, che in genere utilizza la porta 5696.

5. Ottenere il certificato del client pubblico rilasciato a StorageGRID dal KMS esterno e la chiave privata per il certificato del client.

Il certificato client consente a StorageGRID di autenticarsi nel KMS.

## Aggiunta di un server di gestione delle chiavi (KMS)

Utilizzare la procedura guidata del server di gestione delle chiavi StorageGRID per aggiungere ogni cluster KMS o KMS.

### Prima di iniziare

- È stata esaminata la ["considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi"](#).
- Si dispone di ["StorageGRID configurato come client nel KMS"](#), e si dispone delle informazioni necessarie per ogni cluster KMS o KMS.
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).

### A proposito di questa attività

Se possibile, configurare qualsiasi server di gestione delle chiavi specifico del sito prima di configurare un KMS predefinito che si applica a tutti i siti non gestiti da un altro KMS. Se si crea prima il KMS predefinito, tutte le appliance crittografate con nodo nella griglia verranno crittografate con il KMS predefinito. Se si desidera creare un KMS specifico del sito in un secondo momento, è necessario prima copiare la versione corrente della chiave di crittografia dal KMS predefinito al nuovo KMS. Per ulteriori informazioni, vedere ["Considerazioni per la modifica del KMS per un sito"](#).

### Fase 1: Dettagli DI KMS

Nella fase 1 (dettagli KMS) della procedura guidata Add a Key Management Server (Aggiungi un server di gestione delle chiavi), vengono forniti dettagli sul cluster KMS o KMS.

#### Fasi

1. Selezionare **Configurazione > Sicurezza > Server di gestione delle chiavi**.

Viene visualizzata la pagina Key management server (Server di gestione delle chiavi) con la scheda Configuration details (Dettagli di configurazione) selezionata.

2. Selezionare **Crea**.

Viene visualizzata la fase 1 (dettagli KMS) della procedura guidata Add a Key Management Server (Aggiungi un server di gestione delle chiavi).

3. Immettere le seguenti informazioni per il KMS e il client StorageGRID configurati in tale KMS.

Campo	Descrizione
Nome KMS	Un nome descrittivo per aiutarti a identificare questo KMS. Deve essere compreso tra 1 e 64 caratteri.
Nome della chiave	L'alias esatto della chiave per il client StorageGRID nel KMS. Deve essere compreso tra 1 e 255 caratteri.  <b>Nota:</b> Se non è stata creata una chiave utilizzando il prodotto KMS, verrà richiesto di fare in modo che StorageGRID crei la chiave.

Campo	Descrizione
Gestisce le chiavi per	<p>Il sito StorageGRID che sarà associato a questo KMS. Se possibile, è necessario configurare qualsiasi server di gestione delle chiavi specifico del sito prima di configurare un KMS predefinito che si applica a tutti i siti non gestiti da un altro KMS.</p> <ul style="list-style-type: none"> <li>• Selezionare un sito se il KMS gestirà le chiavi di crittografia per i nodi dell'appliance in un sito specifico.</li> <li>• Selezionare <b>Siti non gestiti da un altro KMS (KMS predefinito)</b> per configurare un KMS predefinito che si applicherà a tutti i siti che non dispongono di un KMS dedicato e a tutti i siti aggiunti nelle espansioni successive.</li> </ul> <p><b>Nota:</b> Quando si salva la configurazione KMS, si verifica Un errore di convalida se si seleziona un sito precedentemente crittografato dal KMS predefinito ma non si fornisce la versione corrente della chiave di crittografia originale al nuovo KMS.</p>
Porta	La porta utilizzata dal server KMS per le comunicazioni KMIP (Key Management Interoperability Protocol). Il valore predefinito è 5696, ovvero la porta standard KMIP.
Nome host	<p>Il nome di dominio completo o l'indirizzo IP del KMS.</p> <p><b>Nota:</b> il campo Subject alternative Name (SAN) del certificato del server deve includere l'FQDN o l'indirizzo IP immesso qui. In caso contrario, StorageGRID non sarà in grado di connettersi al KMS o a tutti i server di un cluster KMS.</p>

4. Se si sta configurando un cluster KMS, selezionare **Add another hostname** (Aggiungi un altro nome host) per aggiungere un nome host per ciascun server del cluster.
5. Selezionare **continua**.

## Fase 2: Caricare il certificato del server

Nella fase 2 (carica certificato server) della procedura guidata Add a Key Management Server (Aggiungi un server di gestione delle chiavi), viene caricato il certificato del server (o bundle di certificati) per il KMS. Il certificato del server consente al KMS esterno di autenticarsi su StorageGRID.

### Fasi

1. Dal **passaggio 2 (carica certificato server)**, individuare la posizione del certificato server o del bundle di certificati salvato.
2. Caricare il file del certificato.

Vengono visualizzati i metadati del certificato del server.



Se hai caricato un bundle di certificati, i metadati di ciascun certificato vengono visualizzati nella relativa scheda.



3. Selezionare **continua**.

### passaggio 3: Caricamento dei certificati client

Nella fase 3 (carica certificati client) della procedura guidata Add a Key Management Server (Aggiungi un server di gestione delle chiavi), vengono caricati il certificato client e la chiave privata del certificato client. Il certificato client consente a StorageGRID di autenticarsi nel KMS.

#### Fasi

1. Dal **passaggio 3 (carica certificati client)**, individuare la posizione del certificato client.
2. Caricare il file di certificato del client.

Vengono visualizzati i metadati del certificato client.

3. Individuare la posizione della chiave privata per il certificato client.
4. Caricare il file della chiave privata.
5. Selezionare **Test e salvare**.

Se una chiave non esiste, viene richiesto di crearne una da StorageGRID.

Vengono verificate le connessioni tra il server di gestione delle chiavi e i nodi dell'appliance. Se tutte le connessioni sono valide e la chiave corretta viene trovata nel KMS, il nuovo server di gestione delle chiavi viene aggiunto alla tabella nella pagina Server di gestione delle chiavi.



Subito dopo aver aggiunto un KMS, lo stato del certificato nella pagina Server gestione chiavi viene visualizzato come Sconosciuto. Per ottenere lo stato effettivo di ciascun certificato, StorageGRID potrebbe impiegare fino a 30 minuti. È necessario aggiornare il browser Web per visualizzare lo stato corrente.

6. Se viene visualizzato un messaggio di errore quando si seleziona **Test and Save** (verifica e salva), rivedere i dettagli del messaggio e selezionare **OK**.

Ad esempio, se un test di connessione non riesce, potrebbe essere visualizzato un errore 422: Unprocessable Entity.

7. Se si desidera salvare la configurazione corrente senza verificare la connessione esterna, selezionare **Force Save** (forza salvataggio).



Selezionando **forza salvataggio** viene salvata la configurazione KMS, ma non viene eseguita una verifica della connessione esterna da ciascuna appliance a quel KMS. In caso di problemi con la configurazione, potrebbe non essere possibile riavviare i nodi dell'appliance che hanno attivato la crittografia dei nodi nel sito interessato. È possibile che l'accesso ai dati venga perso fino a quando i problemi non vengono risolti.

8. Controllare l'avviso di conferma e selezionare **OK** se si desidera forzare il salvataggio della configurazione.

La configurazione KMS viene salvata ma la connessione al KMS non viene verificata.

## Gestire un KMS

La gestione di un server di gestione delle chiavi (KMS) comporta la visualizzazione o la

modifica dei dettagli, la gestione dei certificati, la visualizzazione dei nodi crittografati e la rimozione di un KMS quando non è più necessario.

#### Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazione di accesso richiesta"](#).

#### Visualizza i dettagli di KMS

È possibile visualizzare informazioni su ciascun server di gestione delle chiavi (KMS) nel sistema StorageGRID, inclusi i dettagli delle chiavi e lo stato corrente dei certificati server e client.

#### Fasi

1. Selezionare **Configurazione > Sicurezza > Server di gestione delle chiavi**.

Viene visualizzata la pagina del server di gestione delle chiavi con le seguenti informazioni:

- La scheda Dettagli configurazione elenca tutti i server di gestione delle chiavi configurati.
  - La scheda nodi crittografati elenca tutti i nodi con la crittografia dei nodi abilitata.
2. Per visualizzare i dettagli di un KMS specifico ed eseguire operazioni su tale KMS, selezionare il nome del KMS. Nella pagina dei dettagli del KMS sono elencate le seguenti informazioni:

Campo	Descrizione
Gestisce le chiavi per	Il sito StorageGRID associato al KMS.  Questo campo visualizza il nome di un sito StorageGRID specifico o <b>Siti non gestiti da un altro KMS (KMS predefinito)</b> .
Nome host	Il nome di dominio completo o l'indirizzo IP del KMS.  Se è presente un cluster di due server di gestione delle chiavi, vengono elencati il nome di dominio completo o l'indirizzo IP di entrambi i server. Se in un cluster sono presenti più di due server di gestione delle chiavi, viene elencato il nome di dominio completo o l'indirizzo IP del primo KMS insieme al numero di server di gestione delle chiavi aggiuntivi nel cluster.  Ad esempio: 10.10.10.10 and 10.10.10.11 O 10.10.10.10 and 2 others.  Per visualizzare tutti i nomi host in un cluster, selezionare un KMS e selezionare <b>Modifica</b> o <b>azioni &gt; Modifica</b> .

3. Selezionare una scheda nella pagina dei dettagli KMS per visualizzare le seguenti informazioni:

Scheda	Campo	Descrizione
Dettagli chiave	Nome della chiave	L'alias della chiave per il client StorageGRID nel KMS.

Scheda	Campo	Descrizione
UID chiave	L'identificatore univoco dell'ultima versione della chiave.	Ultima modifica
La data e l'ora dell'ultima versione della chiave.	Certificato del server	Metadati
I metadati del certificato, come il numero di serie, la data e l'ora di scadenza e il PEM del certificato.	Certificato PEM	Il contenuto del file PEM (privacy Enhanced mail) per il certificato.
Certificato del client	Metadati	I metadati del certificato, come il numero di serie, la data e l'ora di scadenza e il PEM del certificato.

4. tutte le volte che richiesto dalle procedure di sicurezza dell'organizzazione, selezionare **Rotate key**, oppure utilizzare il software KMS, per creare una nuova versione della chiave.

Quando la rotazione della chiave ha esito positivo, i campi UID chiave e ultima modifica vengono aggiornati.



Se si ruota la chiave di crittografia utilizzando il software KMS, ruotarla dall'ultima versione utilizzata della chiave a una nuova versione della stessa chiave. Non ruotare su una chiave completamente diversa.

Non tentare mai di ruotare una chiave cambiando il nome della chiave (alias) per il KMS. StorageGRID richiede che tutte le versioni delle chiavi utilizzate in precedenza (così come quelle future) siano accessibili dal KMS con lo stesso alias della chiave. Se si modifica l'alias della chiave per un KMS configurato, StorageGRID potrebbe non essere in grado di decrittare i dati.

## Gestire i certificati

Risolvere tempestivamente eventuali problemi relativi ai certificati server o client. Se possibile, sostituire i certificati prima che scadano.



Per mantenere l'accesso ai dati, è necessario risolvere al più presto eventuali problemi di certificato.

## Fasi

1. Selezionare **Configurazione > Sicurezza > Server di gestione delle chiavi**.
2. Nella tabella, esaminare il valore della scadenza del certificato per ogni KMS.
3. Se la scadenza del certificato per qualsiasi KMS è sconosciuta, attendere fino a 30 minuti, quindi aggiornare il browser Web.

4. Se la colonna scadenza certificato indica che un certificato è scaduto o è prossimo alla scadenza, selezionare il KMS per accedere alla pagina dei dettagli del KMS.
  - a. Selezionare **certificato server** e verificare il valore del campo "scade il".
  - b. Per sostituire il certificato, selezionare **Modifica certificato** per caricare un nuovo certificato.
  - c. Ripetere questi passaggi secondari e selezionare **Client certificate** invece di Server certificate (certificato server).
5. Quando vengono attivati gli avvisi **scadenza certificato CA KMS**, **scadenza certificato client KMS** e **scadenza certificato server KMS**, annotare la descrizione di ciascun avviso ed eseguire le azioni consigliate.

Per ottenere gli aggiornamenti alla scadenza del certificato, StorageGRID potrebbe richiedere fino a 30 minuti. Aggiornare il browser Web per visualizzare i valori correnti.



Se lo stato del certificato **Server è sconosciuto**, assicurarsi che il KMS consenta di ottenere un certificato server senza richiedere un certificato client.

## Visualizzare i nodi crittografati

È possibile visualizzare informazioni sui nodi appliance nel sistema StorageGRID per i quali è stata attivata l'impostazione **crittografia nodo**.

### Fasi

1. Selezionare **Configurazione > Sicurezza > Server di gestione delle chiavi**.

Viene visualizzata la pagina Key Management Server (Server di gestione delle chiavi). La scheda Dettagli configurazione mostra tutti i server di gestione delle chiavi configurati.

2. Nella parte superiore della pagina, selezionare la scheda **nodi crittografati**.

La scheda nodi crittografati elenca i nodi appliance nel sistema StorageGRID con l'impostazione **crittografia nodo** attivata.

3. Esaminare le informazioni contenute nella tabella per ciascun nodo appliance.

Colonna	Descrizione
Nome del nodo	Il nome del nodo appliance.
Tipo di nodo	Il tipo di nodo: Storage, Admin o Gateway.
Sito	Il nome del sito StorageGRID in cui è installato il nodo.
Nome KMS	<p>Il nome descrittivo del KMS utilizzato per il nodo.</p> <p>Se non è elencato alcun KMS, selezionare la scheda Dettagli di configurazione per aggiungere un KMS.</p> <p><a href="#">"Aggiunta di un server di gestione delle chiavi (KMS)"</a></p>

Colonna	Descrizione
UID chiave	<p>ID univoco della chiave di crittografia utilizzata per crittografare e decrittare i dati sul nodo dell'appliance. Per visualizzare un UID chiave completo, selezionare il testo.</p> <p>Un trattino (--) indica che l'UID della chiave non è noto, probabilmente a causa di un problema di connessione tra il nodo dell'appliance e il KMS.</p>
Stato	<p>Lo stato della connessione tra il KMS e il nodo dell'appliance. Se il nodo è connesso, l'indicatore data e ora viene aggiornato ogni 30 minuti. L'aggiornamento dello stato di connessione può richiedere alcuni minuti dopo le modifiche della configurazione KMS.</p> <p><b>Nota:</b> aggiornare il browser Web per visualizzare i nuovi valori.</p>

4. Se la colonna Status (Stato) indica un problema KMS, risolverlo immediatamente.

Durante le normali operazioni KMS, lo stato sarà **connesso a KMS**. Se un nodo viene disconnesso dalla rete, viene visualizzato lo stato di connessione del nodo (amministrativamente inattivo o Sconosciuto).

Gli altri messaggi di stato corrispondono agli avvisi StorageGRID con gli stessi nomi:

- Impossibile caricare la configurazione KMS
- Errore di connettività KMS
- Nome chiave di crittografia KMS non trovato
- Rotazione della chiave di crittografia KMS non riuscita
- La chiave KMS non è riuscita a decrittare un volume dell'appliance
- KMS non configurato

Eseguire le azioni consigliate per questi avvisi.



È necessario affrontare immediatamente qualsiasi problema per garantire la completa protezione dei dati.

## Modificare un KMS

Potrebbe essere necessario modificare la configurazione di un server di gestione delle chiavi, ad esempio, se un certificato sta per scadere.

### Prima di iniziare

- Se si prevede di aggiornare il sito selezionato per un KMS, è stata esaminata la ["Considerazioni per la modifica del KMS per un sito"](#).
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).

### Fasi

1. Selezionare **Configurazione > Sicurezza > Server di gestione delle chiavi**.

Viene visualizzata la pagina Key management server (Server di gestione delle chiavi) che mostra tutti i server di gestione delle chiavi configurati.

2. Selezionare il KMS che si desidera modificare e selezionare **azioni > Modifica**.

Puoi anche modificare un KMS selezionando il nome del KMS nella tabella e selezionando **Edit** nella pagina dei dettagli del KMS.

3. Facoltativamente, aggiornare i dettagli nel **Passo 1 (dettagli KMS)** della procedura guidata Modifica un server di gestione delle chiavi.

Campo	Descrizione
Nome KMS	Un nome descrittivo per aiutarti a identificare questo KMS. Deve essere compreso tra 1 e 64 caratteri.
Nome della chiave	L'alias esatto della chiave per il client StorageGRID nel KMS. Deve essere compreso tra 1 e 255 caratteri.  È sufficiente modificare il nome della chiave solo in rari casi. Ad esempio, è necessario modificare il nome della chiave se l'alias viene rinominato in KMS o se tutte le versioni della chiave precedente sono state copiate nella cronologia delle versioni del nuovo alias.
Gestisce le chiavi per	Se si sta modificando un KMS specifico del sito e non si dispone già di un KMS predefinito, selezionare <b>Sites Not Managed by another KMS (default KMS)</b> (Siti non gestiti da un altro KMS (default KMS)*). Questa selezione converte un KMS specifico del sito nel KMS predefinito, che verrà applicato a tutti i siti che non dispongono di un KMS dedicato e a tutti i siti aggiunti in un'espansione.  <b>Nota:</b> se stai modificando un KMS specifico del sito, non puoi selezionare un altro sito. Se stai modificando il KMS predefinito, non puoi selezionare un sito specifico.
Porta	La porta utilizzata dal server KMS per le comunicazioni KMIP (Key Management Interoperability Protocol). Il valore predefinito è 5696, ovvero la porta standard KMIP.
Nome host	Il nome di dominio completo o l'indirizzo IP del KMS.  <b>Nota:</b> il campo Subject alternative Name (SAN) del certificato del server deve includere l'FQDN o l'indirizzo IP immesso qui. In caso contrario, StorageGRID non sarà in grado di connettersi al KMS o a tutti i server di un cluster KMS.

4. Se si sta configurando un cluster KMS, selezionare **Add another hostname** (Aggiungi un altro nome host) per aggiungere un nome host per ciascun server del cluster.
5. Selezionare **continua**.

Viene visualizzata la fase 2 (carica certificato server) della procedura guidata Modifica un server di gestione delle chiavi.

6. Se è necessario sostituire il certificato del server, selezionare **Sfoglia** e caricare il nuovo file.

7. Selezionare **continua**.

Viene visualizzata la fase 3 (carica certificati client) della procedura guidata Modifica un server di gestione delle chiavi.

8. Se è necessario sostituire il certificato client e la chiave privata del certificato client, selezionare **Browse** (Sfoglia) e caricare i nuovi file.

9. Selezionare **Test e salvare**.

Vengono testate le connessioni tra il server di gestione delle chiavi e tutti i nodi di appliance con crittografia a nodo nei siti interessati. Se tutte le connessioni dei nodi sono valide e la chiave corretta viene trovata nel KMS, il server di gestione delle chiavi viene aggiunto alla tabella nella pagina Server di gestione delle chiavi.

10. Se viene visualizzato un messaggio di errore, esaminare i dettagli del messaggio e selezionare **OK**.

Ad esempio, se il sito selezionato per questo KMS è già gestito da un altro KMS o se un test di connessione non ha avuto esito positivo, potrebbe essere visualizzato un errore 422: Unprocessable Entity.

11. Se è necessario salvare la configurazione corrente prima di risolvere gli errori di connessione, selezionare **Imponi salvataggio**.



Selezionando **forza salvataggio** viene salvata la configurazione KMS, ma non viene eseguita una verifica della connessione esterna da ciascuna appliance a quel KMS. In caso di problemi con la configurazione, potrebbe non essere possibile riavviare i nodi dell'appliance che hanno attivato la crittografia dei nodi nel sito interessato. È possibile che l'accesso ai dati venga perso fino a quando i problemi non vengono risolti.

La configurazione KMS viene salvata.

12. Controllare l'avviso di conferma e selezionare **OK** se si desidera forzare il salvataggio della configurazione.

La configurazione del KMS viene salvata, ma la connessione al KMS non viene verificata.

## Rimozione di un server di gestione delle chiavi (KMS)

In alcuni casi, potrebbe essere necessario rimuovere un server di gestione delle chiavi. Ad esempio, è possibile rimuovere un KMS specifico del sito se il sito è stato decommissionato.

### Prima di iniziare

- È stata esaminata la ["considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi"](#).
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).

### A proposito di questa attività

È possibile rimuovere un KMS nei seguenti casi:

- È possibile rimuovere un KMS specifico del sito se il sito è stato decommissionato o se il sito non include nodi appliance con crittografia del nodo attivata.

- È possibile rimuovere il KMS predefinito se esiste già un KMS specifico del sito per ogni sito che ha nodi appliance con crittografia del nodo attivata.

## Fasi

1. Selezionare **Configurazione > Sicurezza > Server di gestione delle chiavi**.

Viene visualizzata la pagina Key management server (Server di gestione delle chiavi) che mostra tutti i server di gestione delle chiavi configurati.

2. Selezionare il KMS che si desidera rimuovere e selezionare **azioni > Rimuovi**.

Puoi anche rimuovere un KMS selezionando il nome del KMS nella tabella e selezionando **Remove** dalla pagina dei dettagli del KMS.

3. Verificare che quanto segue sia vero:

- Si sta rimuovendo un KMS specifico del sito per un sito che non dispone di un nodo appliance con crittografia del nodo attivata.
- Si sta rimuovendo il KMS predefinito, ma esiste già un KMS specifico del sito per ogni sito con crittografia del nodo.

4. Selezionare **Sì**.

La configurazione KMS viene rimossa.

# Gestire le impostazioni del proxy

## Configurare il proxy di archiviazione

Se si utilizzano servizi di piattaforma o Cloud Storage Pool, è possibile configurare un proxy non trasparente tra i nodi di storage e gli endpoint S3 esterni. Ad esempio, potrebbe essere necessario un proxy non trasparente per consentire l'invio dei messaggi dei servizi della piattaforma a endpoint esterni, ad esempio un endpoint su Internet.



Le impostazioni proxy di storage configurate non si applicano agli endpoint dei servizi della piattaforma Kafka.

## Prima di iniziare

- Si dispone di ["autorizzazioni di accesso specifiche"](#).
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).

## A proposito di questa attività

È possibile configurare le impostazioni per un singolo proxy di archiviazione.

## Fasi

1. Selezionare **Configurazione > Sicurezza > Impostazioni proxy**.
2. Nella scheda **archiviazione**, selezionare la casella di controllo **Abilita proxy di archiviazione**.
3. Selezionare il protocollo per il proxy di archiviazione.
4. Immettere il nome host o l'indirizzo IP del server proxy.



5. Facoltativamente, inserire la porta utilizzata per connettersi al server proxy.

Lasciare vuoto questo campo per utilizzare la porta predefinita per il protocollo: 80 per HTTP o 1080 per SOCKS5.

6. Selezionare **Salva**.

Dopo il salvataggio del proxy di storage, è possibile configurare e testare nuovi endpoint per i servizi della piattaforma o i pool di cloud storage.



Le modifiche del proxy possono richiedere fino a 10 minuti.

7. Controllare le impostazioni del server proxy per assicurarsi che i messaggi relativi al servizio della piattaforma da StorageGRID non vengano bloccati.
8. Se è necessario disattivare un proxy di archiviazione, deselezionare la casella di controllo e selezionare **Salva**.

## Configurare le impostazioni del proxy amministratore

Se si inviano pacchetti AutoSupport utilizzando HTTP o HTTPS, è possibile configurare un server proxy non trasparente tra i nodi Admin e il supporto tecnico (AutoSupport).

Per ulteriori informazioni su AutoSupport, vedere ["Configurare AutoSupport"](#).

### Prima di iniziare

- Si dispone di ["autorizzazioni di accesso specifiche"](#).
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).

### A proposito di questa attività

È possibile configurare le impostazioni per un singolo proxy amministratore.

### Fasi

1. Selezionare **Configurazione > Sicurezza > Impostazioni proxy**.

Viene visualizzata la pagina Impostazioni proxy. Per impostazione predefinita, l'opzione Storage (archiviazione) è selezionata nel menu Tab (scheda).

2. Selezionare la scheda **Ammin**.
3. Selezionare la casella di controllo **Enable Admin Proxy** (attiva proxy amministratore).
4. Immettere il nome host o l'indirizzo IP del server proxy.
5. Inserire la porta utilizzata per la connessione al server proxy.
6. Facoltativamente, immettere un nome utente e una password per il server proxy.

Se il server proxy non richiede un nome utente o una password, lasciare vuoti questi campi.

7. Selezionare una delle seguenti opzioni:

- Se si desidera proteggere la connessione al proxy amministratore, selezionare **verifica certificato proxy**. Caricare un pacchetto CA per verificare l'autenticità dei certificati SSL presentati dal server proxy amministratore.



AutoSupport on Demand, e-Series AutoSupport tramite StorageGRID e la determinazione del percorso di aggiornamento nella pagina dell'upgrade della StorageGRID non funzionano se viene verificato un certificato proxy.

Dopo aver caricato il pacchetto CA, vengono visualizzati i relativi metadati.

- Se non si desidera convalidare i certificati quando si comunica con il server proxy dell'amministratore, selezionare **non verificare il certificato proxy**.

#### 8. Selezionare **Salva**.

Dopo aver salvato il proxy dell'amministratore, viene configurato il server proxy tra i nodi Admin e il supporto tecnico.



Le modifiche del proxy possono richiedere fino a 10 minuti.

#### 9. Se è necessario disattivare il proxy amministratore, deselezionare la casella di controllo **Abilita proxy amministratore**, quindi selezionare **Salva**.

## Firewall di controllo

### Controllare l'accesso al firewall esterno

È possibile aprire o chiudere porte specifiche sul firewall esterno.

È possibile controllare l'accesso alle interfacce utente e alle API sui nodi di amministrazione StorageGRID aprendo o chiudendo porte specifiche sul firewall esterno. Ad esempio, è possibile impedire ai tenant di connettersi a Grid Manager dal firewall, oltre a utilizzare altri metodi per controllare l'accesso al sistema.

Se si desidera configurare il firewall interno StorageGRID, vedere ["Configurare il firewall interno"](#).

Porta	Descrizione	Se la porta è aperta...
443	Porta HTTPS predefinita per i nodi di amministrazione	<p>I browser Web e i client API di gestione possono accedere a Grid Manager, Grid Management API, Tenant Manager e Tenant Management API.</p> <p><b>Nota:</b> la porta 443 viene utilizzata anche per il traffico interno.</p>
8443	Porta Grid Manager limitata sui nodi di amministrazione	<ul style="list-style-type: none"><li>• I browser Web e i client API di gestione possono accedere a Grid Manager e all'API di Grid Management utilizzando HTTPS.</li><li>• I browser Web e i client API di gestione non possono accedere a tenant Manager o all'API di gestione tenant.</li><li>• Le richieste di contenuto interno verranno rifiutate.</li></ul>

Porta	Descrizione	Se la porta è aperta...
9443	Porta limitata di Tenant Manager sui nodi di amministrazione	<ul style="list-style-type: none"> <li>• I browser Web e i client API di gestione possono accedere a Tenant Manager e all'API di gestione tenant utilizzando HTTPS.</li> <li>• I browser Web e i client API di gestione non possono accedere a Grid Manager o all'API di Grid Management.</li> <li>• Le richieste di contenuto interno verranno rifiutate.</li> </ul>



Single Sign-on (SSO) non è disponibile sulle porte limitate di Grid Manager o Tenant Manager. Se si desidera che gli utenti eseguano l'autenticazione con Single Sign-on, è necessario utilizzare la porta HTTPS predefinita (443).

#### Informazioni correlate

- ["Accedi a Grid Manager"](#)
- ["Creare un account tenant"](#)
- ["Comunicazioni esterne"](#)

## Gestire i controlli firewall interni

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

Utilizzare le tre schede della pagina di controllo Firewall per personalizzare l'accesso necessario per la griglia.

- **Privileged address list:** Utilizzare questa scheda per consentire l'accesso selezionato alle porte chiuse. È possibile aggiungere indirizzi IP o sottoreti nella notazione CIDR che possono accedere alle porte chiuse utilizzando la scheda Manage external access (Gestisci accesso esterno).
- **Gestisci accesso esterno:** Utilizzare questa scheda per chiudere le porte aperte per impostazione predefinita o riaprire le porte chiuse in precedenza.
- **Untrusted Client Network:** Utilizzare questa scheda per specificare se un nodo considera attendibile il traffico in entrata dalla rete client.

Le impostazioni di questa scheda sovrascrivono quelle della scheda Gestisci accesso esterno.

- Un nodo con una rete client non attendibile accetta solo le connessioni sulle porte endpoint del bilanciamento del carico configurate su quel nodo (endpoint globali, di interfaccia di nodo e di tipo di nodo).
- Le porte endpoint del bilanciamento del carico *sono le uniche porte aperte* sulle reti client non attendibili, indipendentemente dalle impostazioni nella scheda Gestisci reti esterne.
- Se attendibili, tutte le porte aperte nella scheda Manage external access (Gestisci accesso esterno) sono accessibili, così come tutti gli endpoint del bilanciamento del carico aperti nella rete client.



Le impostazioni effettuate in una scheda possono influire sulle modifiche di accesso apportate in un'altra scheda. Verificare le impostazioni di tutte le schede per assicurarsi che la rete funzioni nel modo previsto.

Per configurare i controlli interni del firewall, vedere ["Configurare i controlli firewall"](#).

Per ulteriori informazioni sui firewall esterni e sulla protezione della rete, vedere ["Controllare l'accesso al firewall esterno"](#).

## Elenco degli indirizzi privilegiati e schede di gestione degli accessi esterni

La scheda Privileged address list (elenco indirizzi privilegiati) consente di registrare uno o più indirizzi IP ai quali viene concesso l'accesso alle porte della griglia chiuse. La scheda Manage external access (Gestisci accesso esterno) consente di chiudere l'accesso esterno alle porte esterne selezionate o a tutte le porte esterne aperte (le porte esterne sono porte accessibili per impostazione predefinita dai nodi non grid). Queste due schede spesso possono essere utilizzate insieme per personalizzare l'esatto accesso di rete necessario per la griglia.



Per impostazione predefinita, gli indirizzi IP privilegiati non dispongono dell'accesso alla porta della griglia interna.

### Esempio 1: Utilizzare un host di collegamento per le attività di manutenzione

Si supponga di voler utilizzare un host jump (un host con protezione avanzata) per l'amministrazione di rete. È possibile utilizzare questi passaggi generali:

1. Utilizzare la scheda Privileged address list (elenco indirizzi privilegiati) per aggiungere l'indirizzo IP dell'host di collegamento.
2. Utilizzare la scheda Manage external access (Gestisci accesso esterno) per bloccare tutte le porte.



Aggiungere l'indirizzo IP privilegiato prima di bloccare le porte 443 e 8443. Tutti gli utenti attualmente connessi a una porta bloccata, incluso l'utente, perderanno l'accesso a Grid Manager, a meno che il loro indirizzo IP non sia stato aggiunto all'elenco degli indirizzi privilegiati.

Dopo aver salvato la configurazione, tutte le porte esterne sul nodo di amministrazione nella griglia verranno bloccate per tutti gli host, ad eccezione dell'host di collegamento. È quindi possibile utilizzare l'host jump per eseguire attività di manutenzione sulla griglia in modo più sicuro.

### Esempio 2: Blocco delle porte sensibili

Supponiamo di voler bloccare porte sensibili e il servizio su quella porta. È possibile seguire i seguenti passaggi generali:

1. Utilizzare la scheda Privileged address list (elenco indirizzi con privilegi) per concedere l'accesso solo agli host che devono accedere al servizio.
2. Utilizzare la scheda Manage external access (Gestisci accesso esterno) per bloccare tutte le porte.



Aggiungere l'indirizzo IP con privilegi prima di bloccare l'accesso a tutte le porte assegnate per accedere a Grid Manager e Tenant Manager (le porte preimpostate sono 443 e 8443). Tutti gli utenti attualmente connessi a una porta bloccata, incluso l'utente, perderanno l'accesso a Grid Manager, a meno che il loro indirizzo IP non sia stato aggiunto all'elenco degli indirizzi privilegiati.

Dopo aver salvato la configurazione, la porta sensibile e il servizio su quella porta saranno disponibili agli host nell'elenco degli indirizzi privilegiati. A tutti gli altri host viene negato l'accesso al servizio, indipendentemente dall'interfaccia da cui proviene la richiesta.

### Esempio 3: Disattivazione dell'accesso ai servizi inutilizzati

A livello di rete, è possibile disattivare alcuni servizi che non si intende utilizzare. Ad esempio, per bloccare il traffico client HTTP S3, utilizzare l'interruttore nella scheda Gestisci accesso esterno per bloccare la porta 18084.

### Scheda Untrusted Client Networks

Se si utilizza una rete client, è possibile proteggere StorageGRID da attacchi ostili accettando il traffico client in entrata solo su endpoint configurati esplicitamente.

Per impostazione predefinita, la rete client su ciascun nodo della griglia è *trusted*. Ovvero, per impostazione predefinita, StorageGRID considera attendibili le connessioni in entrata a ciascun nodo di rete su tutti ["porte esterne disponibili"](#).

È possibile ridurre la minaccia di attacchi ostili al sistema StorageGRID specificando che la rete client di ciascun nodo è *non attendibile*. Se la rete client di un nodo non è attendibile, il nodo accetta solo connessioni in entrata su porte esplicitamente configurate come endpoint del bilanciamento del carico. Vedere ["Configurare gli endpoint del bilanciamento del carico"](#) e ["Configurare i controlli firewall"](#).

### Esempio 1: Il nodo gateway accetta solo richieste HTTPS S3

Si supponga che un nodo gateway rifiuti tutto il traffico in entrata sulla rete client, ad eccezione delle richieste HTTPS S3. Eseguire le seguenti operazioni generali:

1. Dalla ["Endpoint del bilanciamento del carico"](#) pagina, configurare un endpoint di bilanciamento del carico per S3 su HTTPS sulla porta 443.
2. Dalla pagina di controllo Firewall, selezionare Untrusted (non attendibile) per specificare che la rete client sul nodo gateway non è attendibile.

Dopo aver salvato la configurazione, tutto il traffico in entrata sulla rete client del nodo gateway viene interrotto, ad eccezione delle richieste HTTPS S3 sulla porta 443 e delle richieste ICMP echo (ping).

### Esempio 2: Storage Node invia richieste di servizi della piattaforma S3

Si supponga di voler attivare il traffico dei servizi della piattaforma S3 in uscita da un nodo di storage, ma di voler impedire qualsiasi connessione in entrata a tale nodo di storage sulla rete client. Eseguire questa fase generale:

- Dalla scheda Untrusted Client Networks (reti client non attendibili) della pagina di controllo Firewall, indicare che la rete client nel nodo di storage non è attendibile.

Dopo aver salvato la configurazione, il nodo di storage non accetta più alcun traffico in entrata sulla rete client, ma continua a consentire le richieste in uscita verso destinazioni di servizi della piattaforma configurate.

### Esempio 3: Limitazione dell'accesso a Grid Manager a una subnet

Si supponga di voler consentire l'accesso a Grid Manager solo su una subnet specifica. Attenersi alla seguente procedura:

1. Collegare la rete client dei nodi di amministrazione alla subnet.
2. Utilizzare la scheda Untrusted Client Network (rete client non attendibile) per configurare la rete client come non attendibile.
3. Quando si crea un endpoint per il bilanciamento del carico dell'interfaccia di gestione, immettere la porta e selezionare l'interfaccia di gestione a cui la porta accede.
4. Selezionare **Sì** per la rete client non attendibile.
5. Utilizzare la scheda Manage external access (Gestisci accesso esterno) per bloccare tutte le porte esterne (con o senza indirizzi IP privilegiati impostati per gli host esterni alla subnet).

Dopo aver salvato la configurazione, solo gli host della subnet specificata possono accedere a Grid Manager. Tutti gli altri host sono bloccati.

## Configurare il firewall interno

È possibile configurare il firewall StorageGRID per controllare l'accesso di rete a porte specifiche sui nodi StorageGRID.

### Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).
- Sono state esaminate le informazioni in ["Gestire i controlli firewall"](#) e ["Linee guida per il networking"](#).
- Se si desidera che un nodo Admin o un nodo gateway accetti il traffico in entrata solo su endpoint configurati esplicitamente, sono stati definiti gli endpoint del bilanciamento del carico.



Quando si modifica la configurazione della rete client, le connessioni client esistenti potrebbero non riuscire se gli endpoint del bilanciamento del carico non sono stati configurati.

### A proposito di questa attività

StorageGRID include un firewall interno su ciascun nodo che consente di aprire o chiudere alcune porte sui nodi della griglia. È possibile utilizzare le schede di controllo Firewall per aprire o chiudere le porte aperte per impostazione predefinita in Grid Network, Admin Network e Client Network. È inoltre possibile creare un elenco di indirizzi IP privilegiati che possono accedere alle porte della griglia chiuse. Se si utilizza una rete client, è possibile specificare se un nodo considera attendibile il traffico in entrata dalla rete client ed è possibile configurare l'accesso a porte specifiche sulla rete client.

Limitare il numero di porte aperte agli indirizzi IP esterni alla griglia solo a quelle assolutamente necessarie migliora la sicurezza della griglia. Utilizzare le impostazioni di ciascuna delle tre schede di controllo del firewall per assicurarsi che siano aperte solo le porte necessarie.

Per ulteriori informazioni sull'utilizzo dei controlli firewall, inclusi esempi, vedere ["Gestire i controlli firewall"](#).

Per ulteriori informazioni sui firewall esterni e sulla protezione della rete, vedere ["Controllare l'accesso al firewall esterno"](#).

## Accedere ai controlli firewall

### Fasi

1. Selezionare **Configurazione > Sicurezza > Controllo firewall**.

Le tre schede di questa pagina sono descritte in "[Gestire i controlli firewall](#)".

2. Selezionare una scheda qualsiasi per configurare i controlli del firewall.

È possibile utilizzare queste schede in qualsiasi ordine. Le configurazioni impostate su una scheda non limitano le operazioni che è possibile eseguire sulle altre schede; tuttavia, le modifiche alla configurazione apportate su una scheda potrebbero modificare il comportamento delle porte configurate su altre schede.

### Elenco di indirizzi con privilegi

La scheda elenco indirizzi privilegiati consente agli host di accedere alle porte chiuse per impostazione predefinita o chiuse dalle impostazioni della scheda Gestisci accesso esterno.

Per impostazione predefinita, gli indirizzi IP e le subnet privilegiati non dispongono di accesso alla rete interna. Inoltre, gli endpoint del bilanciamento del carico e le porte aggiuntive aperte nella scheda Privileged address list (elenco indirizzi con privilegi) sono accessibili anche se bloccati nella scheda Manage external access (Gestisci accesso esterno).



Le impostazioni della scheda elenco indirizzi privilegiati non possono sostituire quelle della scheda rete client non attendibile.

### Fasi

1. Nella scheda Privileged address list (elenco indirizzi privilegiati), inserire l'indirizzo o la subnet IP che si desidera concedere l'accesso alle porte chiuse.
2. Facoltativamente, selezionare **Aggiungi un altro indirizzo IP o subnet nella notazione CIDR** per aggiungere altri client con privilegi.



Aggiungere il minor numero possibile di indirizzi all'elenco dei privilegi.

3. Facoltativamente, selezionare **Allow Privileged IP address to access StorageGRID internal ports** (Consenti indirizzi IP privilegiati per l'accesso alle porte interne di Vedere "[Porte interne StorageGRID](#)").



Questa opzione rimuove alcune protezioni per i servizi interni. Se possibile, lasciarlo disattivato.

4. Selezionare **Salva**.

### Gestire l'accesso esterno

Quando una porta viene chiusa nella scheda Manage external access (Gestisci accesso esterno), non è possibile accedervi da alcun indirizzo IP non Grid, a meno che non si aggiunga l'indirizzo IP all'elenco degli indirizzi privilegiati. Per impostazione predefinita, è possibile chiudere solo le porte aperte e solo quelle chiuse.



Le impostazioni della scheda **Manage external access** (Gestisci accesso esterno) non possono sostituire quelle della scheda **Untrusted Client Network** (rete client non attendibile). Ad esempio, se un nodo non è attendibile, la porta SSH/22 viene bloccata sulla rete client anche se è aperta nella scheda **Manage external access** (Gestisci accesso esterno). Le impostazioni della scheda **Untrusted Client Network** (rete client non attendibile) sovrascrivono le porte chiuse (ad esempio 443, 8443, 9443) della rete client.

## Fasi

1. Selezionare **Gestisci accesso esterno**. La scheda visualizza una tabella con tutte le porte esterne (porte accessibili per impostazione predefinita dai nodi non griglia) per i nodi della griglia.
2. Configurare le porte che si desidera aprire e chiudere utilizzando le seguenti opzioni:
  - Utilizzare il pulsante di commutazione accanto a ciascuna porta per aprire o chiudere la porta selezionata.
  - Selezionare **Open all displayed ports** (Apri tutte le porte visualizzate) per aprire tutte le porte elencate nella tabella.
  - Selezionare **Chiudi tutte le porte visualizzate** per chiudere tutte le porte elencate nella tabella.



Se si chiudono le porte 443 o 8443 di Grid Manager, tutti gli utenti attualmente connessi a una porta bloccata, incluso l'utente, perderanno l'accesso a Grid Manager, a meno che il loro indirizzo IP non sia stato aggiunto all'elenco degli indirizzi privilegiati.



Utilizzare la barra di scorrimento sul lato destro della tabella per verificare di aver visualizzato tutte le porte disponibili. Utilizzare il campo di ricerca per trovare le impostazioni di qualsiasi porta esterna immettendo un numero di porta. È possibile inserire un numero di porta parziale. Ad esempio, se si immette **2**, vengono visualizzate tutte le porte che hanno la stringa "2" come parte del loro nome.

3. Selezionare **Salva**

## Rete client non attendibile

Se la rete client di un nodo non è attendibile, il nodo accetta solo il traffico in entrata sulle porte configurate come endpoint del bilanciamento del carico e, facoltativamente, le porte aggiuntive selezionate in questa scheda. È inoltre possibile utilizzare questa scheda per specificare l'impostazione predefinita per i nuovi nodi aggiunti in un'espansione.



Le connessioni client esistenti potrebbero non riuscire se gli endpoint del bilanciamento del carico non sono stati configurati.

Le modifiche apportate alla configurazione nella scheda **Untrusted Client Network** (rete client non attendibile) sovrascrivono le impostazioni nella scheda **Manage external access** (Gestisci accesso esterno).

## Fasi

1. Selezionare **Untrusted Client Network**.
2. Nella sezione **Set New Node Default** (Imposta nuovo nodo predefinito), specificare l'impostazione predefinita quando si aggiungono nuovi nodi alla griglia in una procedura di espansione.
  - **Trusted** (impostazione predefinita): Quando un nodo viene aggiunto in un'espansione, la sua rete client viene considerata attendibile.



- **Untrusted:** Quando un nodo viene aggiunto in un'espansione, la sua rete client non è attendibile.

Se necessario, è possibile tornare a questa scheda per modificare l'impostazione di un nuovo nodo specifico.



Questa impostazione non influisce sui nodi esistenti nel sistema StorageGRID.

3. Utilizzare le seguenti opzioni per selezionare i nodi che devono consentire le connessioni client solo su endpoint del bilanciamento del carico configurati esplicitamente o su porte selezionate aggiuntive:

- Selezionare **Untrust on displayed nodes** per aggiungere tutti i nodi visualizzati nella tabella all'elenco Untrusted Client Network (rete client non attendibile).
- Selezionare **Trust on displayed nodes** per rimuovere tutti i nodi visualizzati nella tabella dall'elenco Untrusted Client Network (rete client non attendibile).
- Utilizzare l'interruttore accanto a ciascun nodo per impostare la rete client come attendibile o non attendibile per il nodo selezionato.

Ad esempio, è possibile selezionare **Untrust on displayed nodes** per aggiungere tutti i nodi all'elenco Untrusted Client Network (rete client non attendibile), quindi utilizzare il pulsante di attivazione accanto a un singolo nodo per aggiungere tale singolo nodo all'elenco Trusted Client Network (rete client attendibile).



Utilizzare la barra di scorrimento sul lato destro della tabella per verificare di aver visualizzato tutti i nodi disponibili. Utilizzare il campo di ricerca per trovare le impostazioni per qualsiasi nodo immettendo il nome del nodo. È possibile immettere un nome parziale. Ad esempio, se si immette un valore **GW**, vengono visualizzati tutti i nodi che hanno la stringa "GW" come parte del loro nome.

4. Selezionare **Salva**.

Le nuove impostazioni del firewall vengono applicate e applicate immediatamente. Le connessioni client esistenti potrebbero non riuscire se gli endpoint del bilanciamento del carico non sono stati configurati.

## Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.