



# **Gestire le impostazioni di sicurezza**

## **StorageGRID**

NetApp  
October 03, 2025

# Sommario

Gestire le impostazioni di sicurezza . . . . .	1
Gestire i certificati . . . . .	1
Informazioni sui certificati di sicurezza . . . . .	1
Configurare i certificati del server . . . . .	12
Configurare i certificati client . . . . .	23
Configurare i server di gestione delle chiavi . . . . .	31
Configurazione dei server di gestione delle chiavi: Panoramica . . . . .	31
Esaminare i metodi di crittografia StorageGRID . . . . .	31
Panoramica di KMS e configurazione dell'appliance . . . . .	34
Considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi . . . . .	37
Considerazioni per la modifica del KMS per un sito . . . . .	40
Configurare StorageGRID come client nel KMS . . . . .	43
Aggiunta di un server di gestione delle chiavi (KMS) . . . . .	44
Visualizza i dettagli di KMS . . . . .	52
Visualizzare i nodi crittografati . . . . .	53
Modifica di un server di gestione delle chiavi (KMS) . . . . .	56
Rimozione di un server di gestione delle chiavi (KMS) . . . . .	58
Gestire le impostazioni del proxy . . . . .	60
Configurare le impostazioni del proxy di storage . . . . .	60
Configurare le impostazioni del proxy amministratore . . . . .	61
Gestire reti client non attendibili . . . . .	63
Gestisci reti client non attendibili: Panoramica . . . . .	63
Specificare che la rete client del nodo non è attendibile . . . . .	63

# Gestire le impostazioni di sicurezza

## Gestire i certificati

### Informazioni sui 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 utilizzando HTTPS, il server risponde con il certificato del server, che contiene una chiave pubblica. Il client verifica questo certificato confrontando la firma del server con la firma sulla 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 include un'autorità di certificazione (CA) incorporata che genera un certificato Grid CA interno durante l'installazione del sistema. Il certificato Grid CA viene utilizzato, per impostazione predefinita, per proteggere il traffico StorageGRID interno. Un'autorità di certificazione esterna (CA) può emettere certificati personalizzati pienamente conformi ai criteri di sicurezza delle informazioni dell'organizzazione. Sebbene sia possibile utilizzare il certificato Grid CA per un ambiente non di produzione, la procedura consigliata per un ambiente di produzione consiste nell'utilizzare certificati personalizzati firmati da un'autorità di certificazione esterna. Sono supportate anche le connessioni non protette senza certificato, ma non sono 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 il [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.

1. Da Grid Manager, selezionare **CONFIGURATION Security Certificates**.

### 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 CAClientLoad balancer endpointsTenantsOther

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 solo se si dispone dell'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.
  - **Endpoint del bilanciamento del carico:** Protegge le connessioni tra i client S3 e Swift 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 a StorageGRID dai browser Web e dai client API S3 e Swift 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 client alle interfacce di gestione StorageGRID.
- [Certificato API S3 e Swift](#): Protegge le connessioni API del client ai nodi di storage, ai nodi di amministrazione e ai nodi gateway, utilizzati dalle applicazioni client S3 e Swift per caricare e scaricare i dati degli oggetti.

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 e Swift](#) Utilizzato per le connessioni Storage Node, CLB service (obsoleto) e load balancer endpoint (opzionale).
- [Ripristinare il certificato dell'interfaccia di gestione predefinita](#).
- [Ripristinare il certificato API S3 e Swift predefinito](#).
- [Utilizzare uno script per generare un nuovo certificato autofirmato dell'interfaccia di gestione](#).
- Copiare o scaricare [certificato dell'interfaccia di gestione](#) oppure [Certificato API S3 e Swift](#).

## CA griglia

Il [Certificato Grid CA](#), Generata 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 modificarla.

## Client

[Certificati client](#), Generata da un'autorità di certificazione esterna, protegge le connessioni tra i tool di monitoraggio esterni e il database 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 eseguire 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](#), Che vengono caricati o generati, proteggono le connessioni tra i client S3 e Swift e il servizio bilanciamento del carico StorageGRID sui nodi gateway e sui nodi amministrativi.

La tabella degli endpoint del bilanciamento del carico dispone di una riga per ciascun endpoint del bilanciamento del carico configurato e indica se per l'endpoint viene utilizzato il certificato API S3 e Swift globale o un certificato dell'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:

- [Selezionare un nome di endpoint per aprire una scheda del browser con informazioni sull'endpoint del bilanciamento del carico, inclusi i dettagli del certificato.](#)
- [Specificare un certificato endpoint per il bilanciamento del carico per FabricPool.](#)
- [Utilizza il certificato globale S3 e Swift API](#) invece di generare un nuovo certificato endpoint per il bilanciamento del carico.

### Tenant

I tenant possono utilizzare [certificati del server di federazione delle identità](#) oppure [certificati endpoint del servizio di piattaforma](#) Per proteggere le 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 di federazione delle identità](#)
- [Certificati Cloud Storage Pool](#)
- [Certificati KMS \(Key Management Server\)](#)
- [Certificati Single Sign-on](#)
- [Certificati di notifica degli avvisi via email](#)
- [Certificati server syslog esterni](#)

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 dell'autorizzazione appropriata.

È possibile:

- [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 un certificato Cloud Storage Pool per S3, C2S S3 o Azure](#)
- [Specificare manualmente un certificato SSO per l'attendibilità della parte che si basa](#)
- [Specificare un certificato per le notifiche e-mail di avviso](#)
- [Specificare un certificato server syslog esterno](#)

## Dettagli del certificato di sicurezza

Di seguito sono descritti i tipi di certificato di protezione, con collegamenti ad articoli che contengono 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 sicurezza certificati</b> , selezionare la scheda <b>Globale</b> , quindi selezionare <b>certificato dell'interfaccia di gestione</b>	<a href="#">Configurare i certificati dell'interfaccia di gestione</a>

#### Certificato API S3 e Swift

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica le connessioni client protette S3 o Swift a un nodo di storage, al servizio di bilanciamento del carico di connessione (CLB) obsoleto su un nodo gateway e agli endpoint del bilanciamento del carico (opzionale).	<b>CONFIGURAZIONE sicurezza certificati</b> , selezionare la scheda <b>Globale</b> , quindi selezionare <b>S3 and Swift API certificate</b>	<a href="#">Configurare i certificati API S3 e Swift</a>

#### Certificato Grid CA

Vedere [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>	<b>CONFIGURAZIONE sicurezza certificati</b> , quindi selezionare la scheda <b>Client</b>	<a href="#">Configurare i certificati client</a>

**Certificato endpoint per il bilanciamento del carico**

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	<p>Autentica la connessione tra i client S3 o Swift e il servizio bilanciamento del carico StorageGRID sui nodi gateway e sui nodi di amministrazione. 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 anche possibile utilizzare una versione personalizzata del <a href="#">Global Certificato API S3 e Swift</a> Certificato 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 rete endpoint del bilanciamento 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 di federazione delle identità

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra StorageGRID e un provider di identità esterno, ad esempio Active Directory, OpenLDAP o Oracle Directory Server. Utilizzato per la federazione delle identità, che consente ai gruppi di amministrazione e agli utenti di essere gestiti da un sistema esterno.	<b>CONFIGURAZIONE controllo accessi federazione identità</b>	<a href="#">USA la federazione delle identità</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 STORAGE (S3) 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 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 Storage Pools</b>	<a href="#">Creare un pool di storage cloud</a>

#### 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 sicurezza Server di gestione delle chiavi</b>	<a href="#">Aggiunta del server di gestione delle chiavi (KMS)</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 controllo di accesso Single Sign-on</b>	<a href="#">Configurare il single sign-on</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 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 monitoraggio Audit e server syslog</b> , quindi selezionare <b>Configura server syslog esterno</b>	<a href="#">Configurare un server syslog esterno</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. È possibile configurare una connessione client S3 o Swift all'endpoint del bilanciamento del carico e caricare lo stesso certificato nel 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 verifica questo certificato confrontando la firma del server con la firma sulla 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.

## Configurare i certificati del server

### Tipi di certificato server supportati

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

Per ulteriori informazioni su come StorageGRID protegge le connessioni client per l'API REST, vedere [Utilizzare S3](#) oppure [USA Swift](#).

### 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 del server guasto, l'avviso **scadenza del certificato del server per l'interfaccia di gestione** viene attivato quando il certificato del server sta per scadere. Se necessario, è possibile visualizzare la scadenza del certificato corrente selezionando **CONFIGURAZIONE sicurezza certificati** e osservando 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.
- Tu [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).
- **Certificate private key** (chiave privata certificato): Il file di chiave privata del certificato del server personalizzato (.key).



Le chiavi private EC devono essere 224 bit o superiori. Le chiavi private RSA devono essere 2048 bit o superiori.

- **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:

- **Domain name**: 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.
- **Oggetto**: Nome distinto (DN) o oggetto X.509 del proprietario del certificato.
- **Giorni validi**: Numero di giorni successivi alla creazione della scadenza del certificato.

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.

#### Di cosa hai bisogno

- Si dispone di autorizzazioni di accesso specifiche.
- Hai il `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 in `Passwords.txt` file.
  - c. Immettere il seguente comando per passare a root: `su -`
  - d. Immettere la password elencata in `Passwords.txt` file.

Una volta effettuato l'accesso 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 di amministrazione. 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` a `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 `--days` argomento per eseguire l'override del periodo di validità predefinito.



Il periodo di validità di un certificato inizia quando `make-certificate` è 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:
  - a. Accedere a Grid Manager.
  - b. Selezionare **CONFIGURAZIONE sicurezza certificati**
  - c. 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

1. Selezionare **CONFIGURAZIONE sicurezza certificati**.
2. Nella scheda **Global**, selezionare **Management interface certificate**.
3. Selezionare la scheda **Server** o **bundle CA**, quindi scaricare o copiare il certificato.

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

Scarica il certificato o il bundle CA .pem file. 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 e Swift

È possibile sostituire o ripristinare il certificato server utilizzato per le connessioni client S3 o Swift ai nodi di storage, al servizio di bilanciamento del carico di connessione (CLB) obsoleto sui nodi gateway o agli endpoint del bilanciamento del carico. Il certificato del server personalizzato sostitutivo è specifico dell'organizzazione.

#### 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.

Una volta completata la configurazione sul server, potrebbe essere necessario installare anche il certificato Grid CA nel client S3 o Swift API che verrà utilizzato per accedere al sistema, a seconda dell'autorità di certificazione (CA) root in uso.



Per garantire che le operazioni non vengano interrotte da un certificato server guasto, l'avviso **scadenza del certificato server globale per S3 e Swift API** viene attivato quando il certificato del server root sta per scadere. Se necessario, è possibile visualizzare la scadenza del certificato corrente selezionando **CONFIGURAZIONE sicurezza certificati** e osservando la data di scadenza del certificato API S3 e Swift nella scheda Globale.

È possibile caricare o generare un certificato S3 e Swift API personalizzato.

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

##### **Fasi**

1. Selezionare **CONFIGURAZIONE sicurezza certificati**.
2. Nella scheda **Global**, selezionare **S3 and Swift API 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).
- **Certificate private key** (chiave privata certificato): Il file di chiave privata del certificato del server personalizzato (.key).



Le chiavi private EC devono essere 224 bit o superiori. Le chiavi private RSA devono essere 2048 bit o superiori.

- **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 il PEM per ogni certificato S3 e Swift API 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 successive nuove connessioni client S3 e Swift.

## Generare un certificato

Generare i file dei certificati del server.

a. Selezionare **genera certificato**.

b. Specificare le informazioni del certificato:

- **Domain name**: 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.
- **Oggetto**: Nome distinto (DN) o oggetto X.509 del proprietario del certificato.
- **Giorni validi**: Numero di giorni successivi alla creazione della scadenza del certificato.

c. Selezionare **generate**.

d. Selezionare **Dettagli certificato** per visualizzare i metadati e il PEM per il certificato S3 e Swift API 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 successive nuove connessioni client S3 e Swift.

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 e Swift personalizzato, la pagina del certificato API S3 e Swift visualizza informazioni dettagliate sul certificato per il certificato API S3 e Swift personalizzato in uso. + è possibile scaricare o copiare il PEM del certificato secondo necessità.

#### Ripristinare il certificato API S3 e Swift predefinito

È possibile ripristinare l'utilizzo del certificato API S3 e Swift predefinito per le connessioni dei client S3 e Swift ai nodi di storage e al servizio CLB obsoleto sui nodi gateway. Tuttavia, non è possibile utilizzare il certificato S3 e Swift API predefinito per un endpoint di bilanciamento del carico.

#### Fasi

1. Selezionare **CONFIGURAZIONE sicurezza certificati**.
2. Nella scheda **Global**, selezionare **S3 and Swift API certificate**.
3. Selezionare **Usa certificato predefinito**.

Quando si ripristina la versione predefinita del certificato globale S3 e Swift API, i file di certificato del server personalizzati configurati vengono cancellati e non possono essere ripristinati dal sistema. Il certificato API S3 e Swift predefinito verrà utilizzato per le successive nuove connessioni dei client S3 e Swift ai nodi di storage e al servizio CLB obsoleto sui nodi gateway.

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

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

È possibile salvare o copiare i contenuti dei certificati API S3 e Swift per utilizzarli altrove.

### Fasi

1. Selezionare **CONFIGURAZIONE sicurezza certificati**.
2. Nella scheda **Global**, selezionare **S3 and Swift API certificate**.
3. Selezionare la scheda **Server** o **bundle CA**, quindi scaricare o copiare il certificato.

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

Scarica il certificato o il bundle CA .pem file. 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 S3](#)
- [USA Swift](#)
- [Configurare i nomi di dominio degli endpoint API 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.

### Di cosa hai bisogno

- Hai 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 **CONFIGURATION Security Certificates**, quindi selezionare la scheda **Grid CA**.
2. Nella sezione **Certificate PEM**, scaricare o copiare il certificato.

#### Scaricare il file del certificato

Scarica il certificato .pem file.

- 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.

### Di cosa hai bisogno

- Si dispone di autorizzazioni di accesso specifiche.
- Hai 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](#).



Il servizio di bilanciamento del carico di connessione (CLB) separato sui nodi gateway è obsoleto e non è consigliato per l'utilizzo con 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.

Consultare le informazioni su [utilizzo generale dei certificati di sicurezza](#) e [configurazione di certificati server personalizzati](#).



Per garantire che le operazioni non vengano interrotte da un certificato del server guasto, l'avviso **scadenza dei certificati client configurati nella pagina certificati** viene attivato quando il certificato del server sta per scadere. Se necessario, è possibile visualizzare la scadenza del certificato corrente selezionando **CONFIGURAZIONE sicurezza certificati** e osservando 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 appliance appositamente configurati, consultare le informazioni specifiche su [Caricamento di un certificato del client KMS](#).

## Di cosa hai bisogno

- Si dispone dell'autorizzazione di accesso root.
- Hai 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 un certificato client, seguire la procedura relativa allo scenario in uso:

- [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, selezionare **CONFIGURATION Security Certificates**, quindi selezionare la scheda **Client**.
2. Selezionare **Aggiungi**.
3. Immettere un nome di certificato contenente almeno 1 e non più di 32 caratteri.
4. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow Prometheus** (Consenti Prometheus).
5. Nella sezione **tipo di certificato**, caricare il certificato dell'interfaccia di gestione .pem file.
  - a. Selezionare **carica certificato**, quindi selezionare **continua**.
  - b. Caricare 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.
6. 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.

- f. 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](#).

#### 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 passi da a. [configurare un certificato dell'interfaccia di gestione](#).
2. In Grid Manager, selezionare **CONFIGURATION Security Certificates**, quindi selezionare la scheda **Client**.
3. Selezionare **Aggiungi**.
4. Immettere un nome di certificato contenente almeno 1 e non più di 32 caratteri.
5. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow Prometheus** (Consenti Prometheus).
6. Nella sezione **tipo di certificato**, caricare il certificato client, la chiave privata e il bundle CA .pem file:
  - a. Selezionare **carica certificato**, quindi selezionare **continua**.
  - b. Caricare i file di certificato client, chiave privata e 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.

7. 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.

f. 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](#).

### 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, selezionare **CONFIGURATION Security Certificates**, quindi selezionare la scheda **Client**.
2. Selezionare **Aggiungi**.
3. Immettere un nome di certificato contenente almeno 1 e non più di 32 caratteri.
4. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow Prometheus** (Consenti Prometheus).
5. Nella sezione **tipo di certificato**, selezionare **genera certificato**.
6. Specificare le informazioni del certificato:
  - **Domain name:** Uno o più nomi di dominio pienamente qualificati del nodo admin da includere nel certificato. Utilizzare un \* come carattere jolly per rappresentare più nomi di dominio.
  - **IP:** Uno o più indirizzi IP del nodo amministrativo da includere nel certificato.

- **Oggetto:** Nome distinto (DN) o oggetto X.509 del proprietario del certificato.

7. Selezionare **generate**.

8. 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.

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

Il nuovo certificato viene visualizzato nella scheda Client.

10. In Grid Manager, selezionare **CONFIGURATION Security Certificates**, quindi selezionare la scheda **Global**.

11. Selezionare **certificato interfaccia di gestione**.

12. Selezionare **Usa certificato personalizzato**.

13. Caricare i file `certificate.pem` e `private_key.pem` da [dettagli del certificato del client](#) fase. Non è necessario caricare il bundle CA.

- Selezionare **carica certificato**, quindi selezionare **continua**.
- Caricare ciascun file di certificato (`.pem`).
- Selezionare **Crea** per salvare il certificato in Grid Manager.

Il nuovo certificato viene visualizzato nella scheda Client.

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

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

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

- 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 del client dell'interfaccia di gestione per **CA Cert** e **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.

f. 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**, 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 di certificato contenente almeno 1 e non più di 32 caratteri.
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**, 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:

- **Domain name:** 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.
- **Oggetto:** Nome distinto (DN) o oggetto X.509 del proprietario del certificato.
- **Giorni validi:** Numero di giorni successivi alla creazione della scadenza del certificato.

- 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**, 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

Scarica il certificato .pem file.

- 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**, 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 i server di gestione delle chiavi

### Configurazione dei server di gestione delle chiavi: Panoramica

È possibile configurare uno o più server di gestione delle chiavi (KMS) esterni per proteggere i dati su nodi appliance appositamente configurati.

#### 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).

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.

### Esaminare i metodi di crittografia StorageGRID

StorageGRID offre una serie di 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	Configurare un server di gestione delle chiavi per il sito StorageGRID ( <b>CONFIGURAZIONE sicurezza server di gestione delle chiavi</b> ) e abilitare la crittografia dei nodi per l'appliance. 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.	<p>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.</p> <div>  <p>La gestione delle chiavi di crittografia con un KMS è supportata solo per i nodi di storage e le appliance di servizio.</p> </div>
Protezione dei dischi in Gestione di sistema SANtricity	Se la funzione protezione disco è attivata per un'appliance di storage, è possibile utilizzare Gestione sistema di SANtricity per creare e gestire la chiave di sicurezza. La chiave è necessaria per accedere ai dati sui dischi protetti.	<p>Appliance di storage con dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard). Tutti i dati presenti sulle unità protette sono protetti da perdita fisica o rimozione dal data center. Non può essere utilizzato con alcune appliance di storage o con altre appliance di servizio.</p> <ul style="list-style-type: none"> <li>• <a href="#">Appliance di storage SG6000</a></li> <li>• <a href="#">Appliance di storage SG5700</a></li> <li>• <a href="#">Appliance di storage SG5600</a></li> </ul>
Opzione della griglia di crittografia degli oggetti memorizzati	L'opzione <b>Stored Object Encryption</b> può essere attivata in Grid Manager ( <b>CONFIGURATION System Grid options</b> ). 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.	<p>Dati S3 e Swift di recente acquisizione.</p> <p>Gli oggetti memorizzati esistenti non vengono crittografati. I metadati degli oggetti e altri dati sensibili non vengono crittografati.</p> <ul style="list-style-type: none"> <li>• <a href="#">Configurare la crittografia degli oggetti memorizzati</a></li> </ul>

Opzione di crittografia	Come funziona	Valido per
Crittografia bucket S3	Viene inviata una richiesta di crittografia PUT Bucket per abilitare la crittografia per il bucket. Tutti i nuovi oggetti non 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> <ul style="list-style-type: none"> <li>• <a href="#">Utilizzare S3</a></li> </ul>
Crittografia a oggetti lato server (SSE) S3	Viene inviata una richiesta S3 per memorizzare un oggetto e includere <code>x-amz-server-side-encryption</code> 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> <ul style="list-style-type: none"> <li>• <a href="#">Utilizzare S3</a></li> </ul>
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>• <code>x-amz-server-side-encryption-customer-algorithm</code></li> <li>• <code>x-amz-server-side-encryption-customer-key</code></li> <li>• <code>x-amz-server-side-encryption-customer-key-MD5</code></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> <ul style="list-style-type: none"> <li>• <a href="#">Utilizzare S3</a></li> </ul>
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> <ul style="list-style-type: none"> <li>• <a href="#">"Amazon Simple Storage Service - Guida per gli sviluppatori: Protezione dei dati mediante crittografia lato client"</a></li> </ul>

## Utilizzare più metodi di crittografia

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

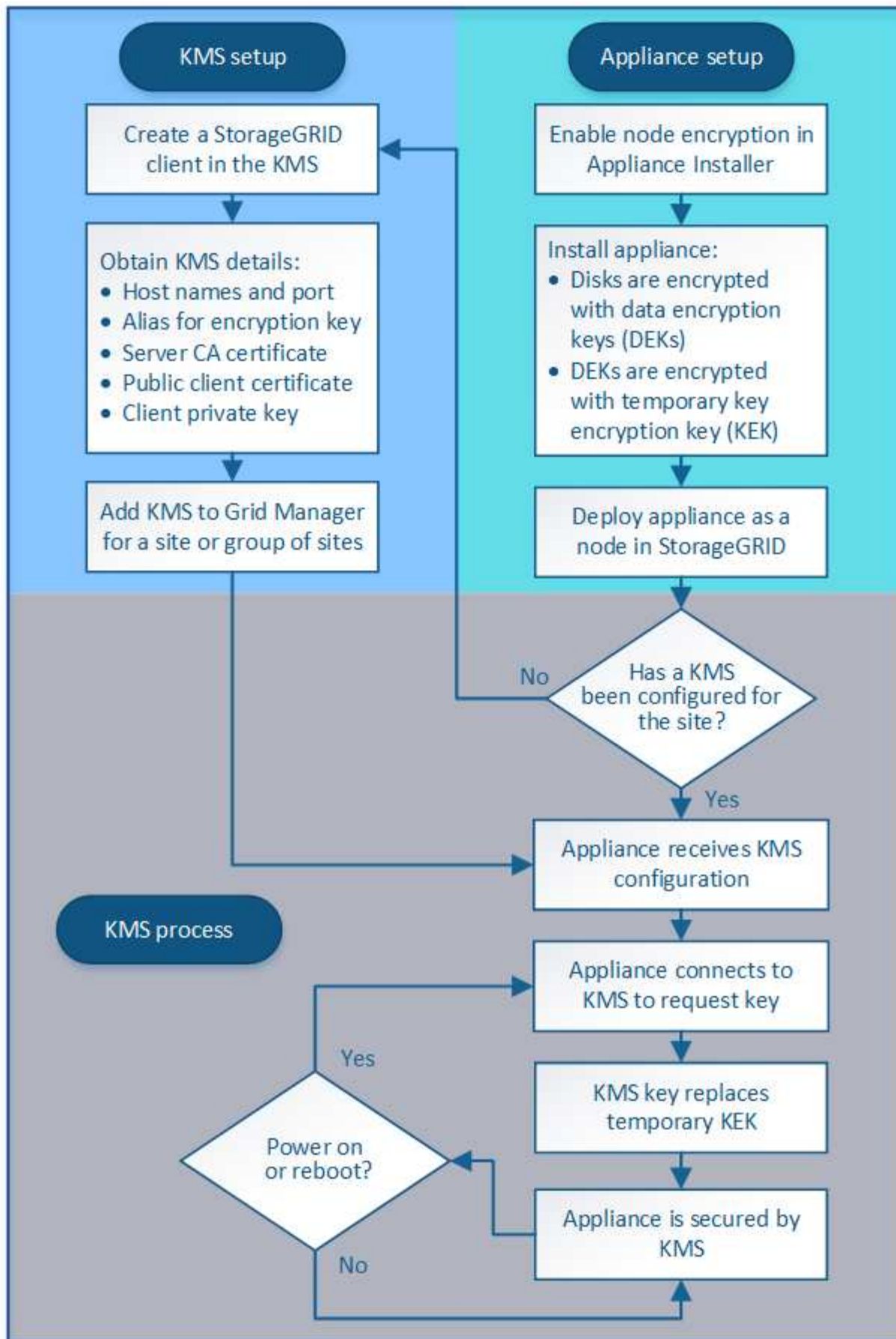
- È possibile utilizzare un KMS per proteggere i nodi dell'appliance e la funzione di sicurezza del disco di Gestione di sistema di SANtricity per "crittografare `din doppio`" i dati sulle unità con crittografia automatica delle stesse appliance.
- È possibile utilizzare un KMS per proteggere i dati sui nodi dell'appliance e l'opzione griglia crittografia 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.

## Panoramica di KMS e configurazione 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 del nodo 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, fare riferimento a quanto segue:

- [Appliance di servizi SG100 e SG1000](#)
- [Appliance di storage SG6000](#)
- [Appliance di storage SG5700](#)
- [Appliance di storage SG5600](#)

## 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.

### Quali sono i requisiti KMIP?

StorageGRID supporta KMIP versione 1.4.

["Key Management Interoperability Protocol Specification versione 1.4"](#)

Le comunicazioni tra i nodi dell'appliance e il KMS configurato utilizzano connessioni TLS sicure. StorageGRID supporta i seguenti cifrari TLS v1.2 per KMIP:

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384

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.

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.

### 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 attivato la crittografia dei nodi.

È possibile utilizzare il KMS configurato per i seguenti appliance StorageGRID e nodi appliance:

Appliance	Tipo di nodo
Appliance di servizi SG1000	Nodo Admin o nodo gateway
Appliance di servizi SG100	Nodo Admin o nodo gateway
Appliance di storage SG6000	Nodo di storage
Appliance di storage SG5700	Nodo di storage
Appliance di storage SG5600	Nodo di storage

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?

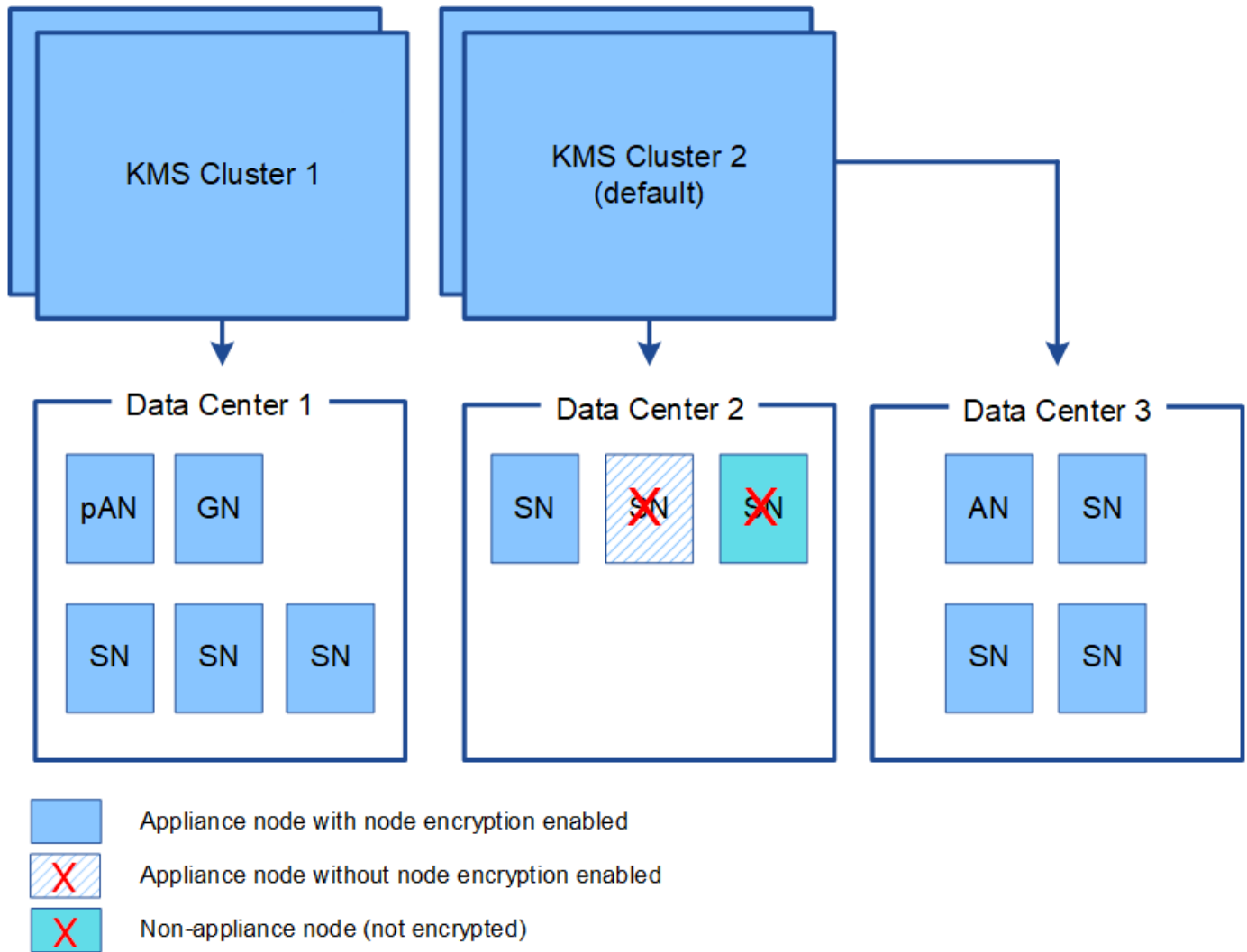
È possibile configurare uno o più server di gestione delle chiavi esterni per fornire chiavi di crittografia ai nodi dell'appliance nel sistema StorageGRID. Ogni KMS fornisce una singola chiave di crittografia ai nodi dell'appliance StorageGRID in un singolo sito o in un gruppo di siti.

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 necessario ruotare periodicamente la chiave di crittografia utilizzata da ciascun KMS configurato.

Quando si ruota la chiave di crittografia, utilizzare il software KMS per eseguire la rotazione dall'ultima versione della chiave utilizzata a una nuova versione della stessa chiave. Non ruotare su una chiave completamente diversa.



Non tentare mai di ruotare una chiave modificando il nome della chiave (alias) per il KMS in Grid Manager. Al contrario, ruotare la chiave aggiornando la versione della chiave nel software KMS. Utilizzare lo stesso alias per le nuove chiavi utilizzato per le chiavi precedenti. Se si modifica l'alias della chiave per un KMS configurato, StorageGRID potrebbe non essere in grado di decrittare i dati.

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.

#### Informazioni correlate

- [Appliance di servizi SG100 e SG1000](#)
- [Appliance di storage SG6000](#)
- [Appliance di storage SG5700](#)
- [Appliance di storage SG5600](#)

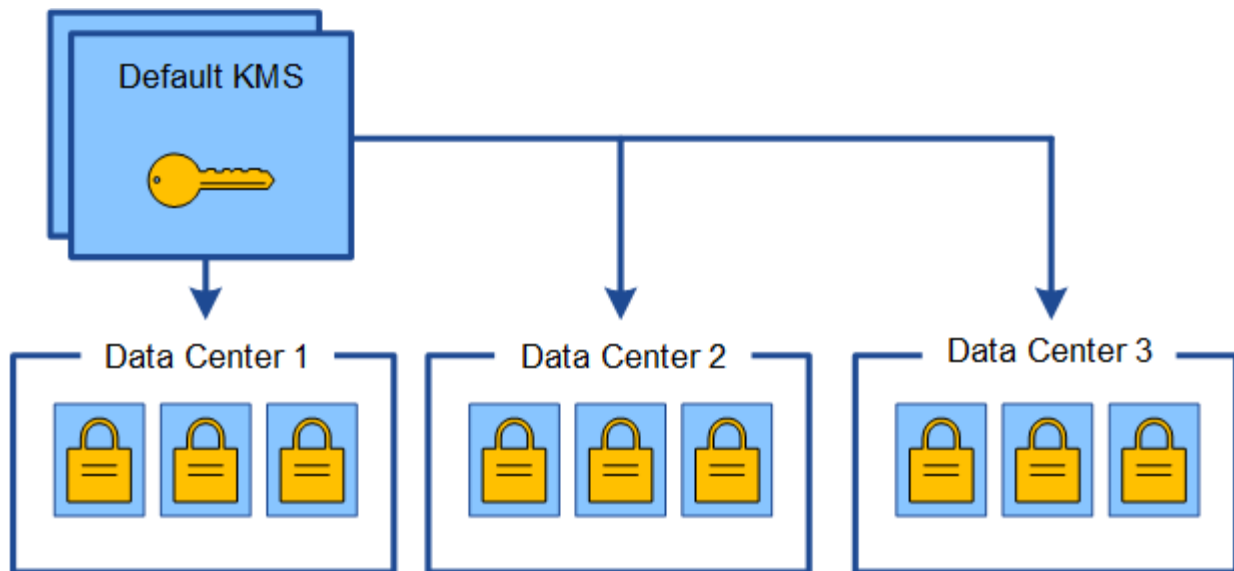
### Considerazioni per la modifica del KMS per un sito

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.

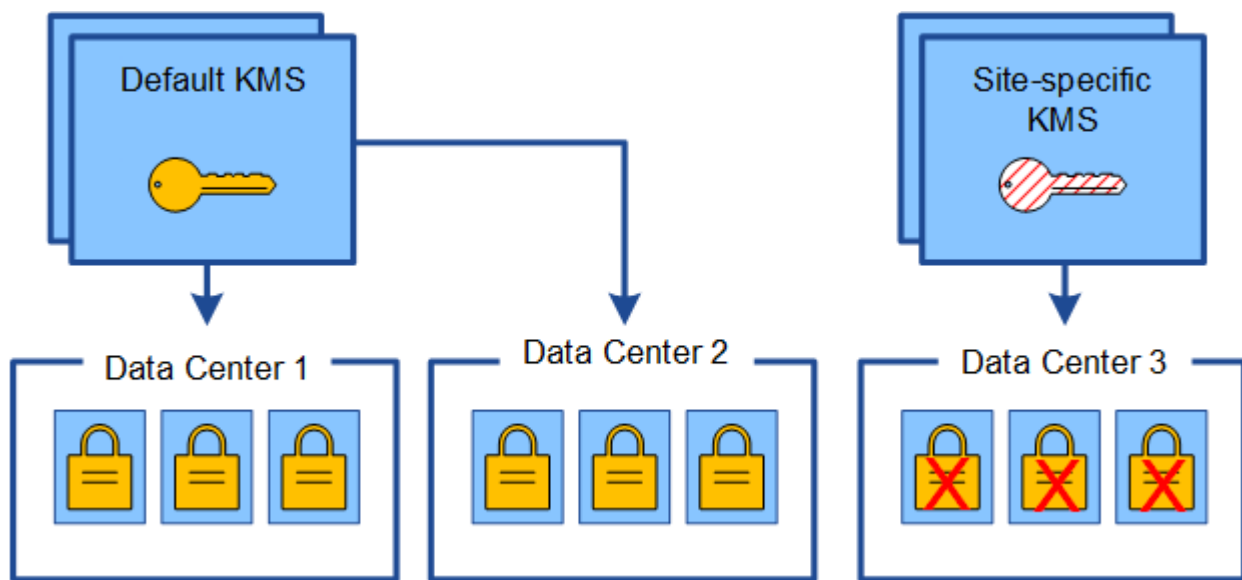
Se si modifica il KMS utilizzato per un sito, è necessario assicurarsi che i nodi appliance precedentemente crittografati in quel sito possano essere decifrati utilizzando la chiave memorizzata nel nuovo KMS. In alcuni casi, potrebbe essere necessario copiare la versione corrente della chiave di crittografia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

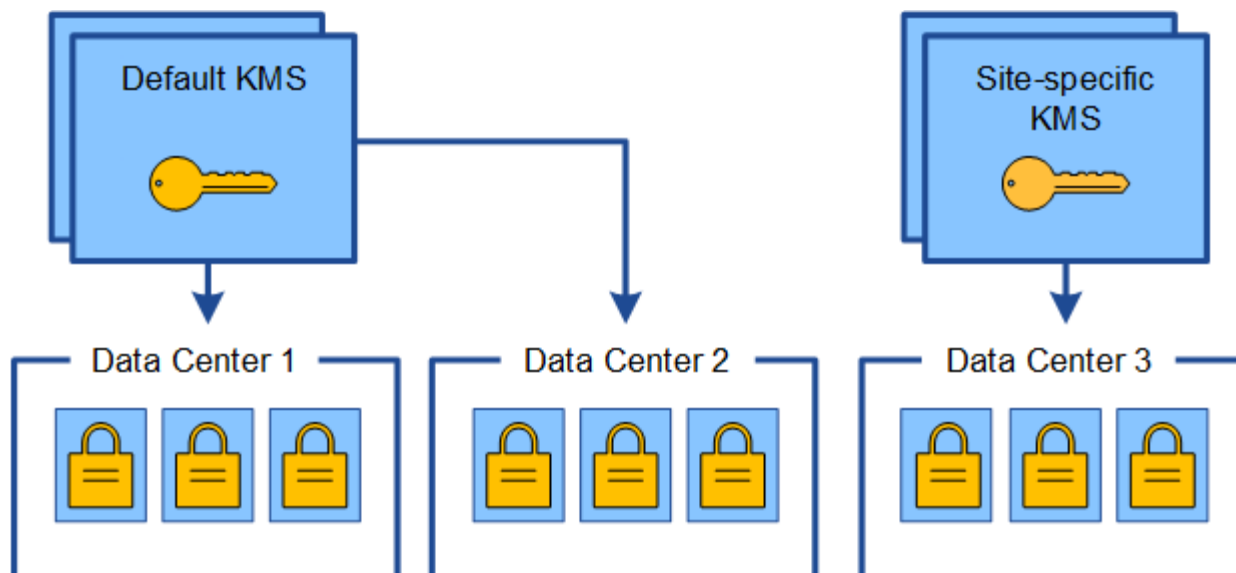
1. Inizialmente si configura un KMS predefinito che si applica a tutti i siti che non dispongono di un KMS dedicato.
2. Una volta salvato il KMS, tutti i nodi appliance con l'impostazione **Node Encryption** attivata si connettono al KMS e richiedono la chiave di crittografia. Questa chiave viene utilizzata 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 decrittare i nodi dell'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>1. 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>2. 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>

Caso d'utilizzo per la modifica del KMS di un sito	Passaggi richiesti
Si desidera che il KMS di un sito utilizzi un server diverso.	<ol style="list-style-type: none"> <li>1. 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>2. 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.

### A proposito di questa attività

Queste istruzioni si applicano a Thales CipherTrust Manager k170v, versioni 2.0, 2.1 e 2.2. In caso di domande sull'utilizzo di un altro server di gestione delle chiavi con StorageGRID, contattare il supporto tecnico.

### "Thales CipherTrust Manager"

#### 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. Dal software KMS, creare una chiave di crittografia AES per ogni cluster KMS o KMS.

La chiave di crittografia deve essere esportabile.

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.



La chiave di crittografia deve già esistere nel KMS. StorageGRID non crea o gestisce chiavi 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 connetterà.



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.

### Di cosa hai bisogno

- Hai esaminato il [considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi](#).
- Lo hai fatto [StorageGRID configurato come client nel KMSE](#) si dispone delle informazioni necessarie per ogni cluster KMS o KMS.
- Hai effettuato l'accesso a Grid Manager utilizzando un [browser web supportato](#).
- Si dispone dell'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. Vedere [Considerazioni per la modifica del KMS per un sito](#) per ulteriori informazioni.

### Fase 1: Inserire i dettagli KMS

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

#### Fasi

1. Selezionare **CONFIGURATION Security Key management server**.

Viene visualizzata la pagina Key Management Server (Server di gestione chiavi) con la scheda Configuration Details (Dettagli configurazione) selezionata.

## Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create Edit Remove

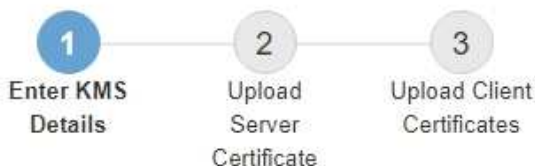
KMS Display Name ?	Key Name ?	Manages keys for ?	Hostname ?	Certificate Status ?
--------------------	------------	--------------------	------------	----------------------

No key management servers have been configured. Select **Create**.

## 2. Selezionare **Crea**.

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

### Add a Key Management Server



Enter information about the external key management server (KMS) and the StorageGRID client you configured in that KMS. If you are configuring a KMS cluster, select + to add a hostname for each server in the cluster.

KMS Display Name ?	<input type="text"/>
Key Name ?	<input type="text"/>
Manages keys for ?	-- Choose One --
Port ?	<input type="text" value="5696"/>
Hostname ?	<input type="text"/>

+

Cancel

Next

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

Campo	Descrizione
Nome visualizzato DI KMS	Un nome descrittivo per aiutarti a identificare questo KMS. Deve essere compreso tra 1 e 64 caratteri.

Campo	Descrizione
Key Name (Nome chiave)	L'alias esatto della chiave per il client StorageGRID nel KMS. Deve essere compreso tra 1 e 255 caratteri.
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 da applicare 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 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 utilizza un cluster KMS, selezionare il segno più **+** per aggiungere un nome host per ciascun server nel cluster.
5. Selezionare **Avanti**.

## 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.

### Add a Key Management Server

1

2

3

Enter KMS  
Details

Upload  
Server  
Certificate

Upload Client  
Certificates

Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server Certificate ?


2. Caricare il file del certificato.

Vengono visualizzati i metadati del certificato del server.

## Add a Key Management Server



Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server Certificate   k170vCA.pem

### Server Certificate Metadata

**Server DN:** /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA  
**Serial Number:** 71:CD:6D:72:53:B5:6D:0A:8C:69:13:0D:4D:D7:81:0E  
**Issue DN:** /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA  
**Issued On:** 2020-10-15T21:12:45.000Z  
**Expires On:** 2030-10-13T21:12:45.000Z  
**SHA-1 Fingerprint:** EE:E4:6E:17:86:DF:56:B4:F5:AF:A2:3C:BD:56:6B:10:DB:B2:5A:79

Cancel

Back

Next



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

3. Selezionare **Avanti**.

### Fase 3: Caricare i 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.

## Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate ?

Browse

Client Certificate Private Key ?

Browse

Cancel

Back

Save

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.

Vengono visualizzati i metadati per il certificato client e la chiave privata del certificato client.

## Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate ?

Browse

k170vClientCert.pem

**Server DN:** /CN=admin/UID=  
**Serial Number:** 7D:5A:8A:27:02:40:C8:F5:19:A1:28:22:E7:D6:E2:EB  
**Issue DN:** /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA  
**Issued On:** 2020-10-15T23:31:49.000Z  
**Expires On:** 2022-10-15T23:31:49.000Z  
**SHA-1 Fingerprint:** A7:10:AC:39:85:42:80:8F:FF:62:AD:A1:BD:CF:4C:90:F3:E9:36:69

Client Certificate Private Key ?

Browse

k170vClientKey.pem

Cancel

Back

Save

### 5. Selezionare **Salva**.

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 **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).

## Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate ?

Browse

k170vClientCert.pem

Server DN: /CN=admin/UID=

Serial Number: 7D:5A:8A:27:02:40:C8:F5:19:A1:28:22:E7:D6:E2:EB

Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA

Issued On: 2020-10-15T23:31:49.000Z

Expires On: 2022-10-15T23:31:49.000Z

SHA-1 Fingerprint: A7:10:AC:39:85:42:80:8F:FF:62:AD:A1:BD:CF:4C:90:F3:E9:36:69

Client Certificate Private Key ?

Browse

k170vClientKey.pem

Select **Force Save** to save this KMS without testing the external connections. If there is an issue with the configuration, you might not be able to reboot any FDE-enabled appliance nodes at the affected site, and you might lose access to your data.

Cancel

Back

Force Save

Save



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.

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

### Warning

Confirm force-saving the KMS configuration

Are you sure you want to save this KMS without testing the external connections?

If there is an issue with the configuration, you might not be able to reboot any appliance nodes with node encryption enabled at the affected site, and you might lose access to your data.

Cancel

OK

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

## Visualizza i dettagli di KMS

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

### Fasi

#### 1. Selezionare **CONFIGURATION Security Key management server**.

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.

##### Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create Edit Remove

KMS Display Name ?	Key Name ?	Manages keys for ?	Hostname ?	Certificate Status ?
Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid

#### 2. Rivedere le informazioni nella tabella per ciascun KMS.

Campo	Descrizione
Nome visualizzato DI KMS	Il nome descrittivo del KMS.
Key Name (Nome chiave)	L'alias della chiave per il client StorageGRID nel KMS.
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> .

Campo	Descrizione
Nome host	<p>Il nome di dominio completo o l'indirizzo IP del KMS.</p> <p>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.</p> <p>Ad esempio: 10.10.10.10 and 10.10.10.11 oppure 10.10.10.10 and 2 others.</p> <p>Per visualizzare tutti i nomi host in un cluster, selezionare un KMS e quindi selezionare <b>Edit</b>.</p>
Stato del certificato	<p>Stato corrente del certificato del server, del certificato CA opzionale e del certificato del client: Valido, scaduto, in fase di scadenza o sconosciuto.</p> <p><b>Nota:</b> potrebbero essere necessari 30 minuti per ottenere gli aggiornamenti dello stato del certificato da parte di StorageGRID. È necessario aggiornare il browser Web per visualizzare i valori correnti.</p>

- Se lo stato del certificato è sconosciuto, attendere fino a 30 minuti, quindi aggiornare il browser Web.



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 effettivo.

- Se la colonna Stato certificato indica che un certificato è scaduto o sta per scadere, risolvere il problema il prima possibile.

Consultare le azioni consigliate per gli avvisi **scadenza certificato CA KMS**, **scadenza certificato client KMS** e **scadenza certificato server KMS** nelle istruzioni per [Monitoraggio e risoluzione dei problemi di StorageGRID](#).



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

## 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 **CONFIGURATION Security Key management server**.

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.

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create

Edit

Remove

KMS Display Name ?	Key Name ?	Manages keys for ?	Hostname ?	Certificate Status ?
Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid

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

Key Management Server

If your StorageGRID system includes appliance nodes with Full Disk Encryption (FDE) enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID data at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

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

Configuration Details

Encrypted Nodes

Review the KMS status for all appliance nodes that have node encryption enabled. Address any issues immediately to ensure your data is fully protected. If no KMS exists for a site, select Configuration Details and add a KMS.

Nodes with Encryption Enabled

Node Name	Node Type	Site	KMS Display Name ?	Key UID ?	Status ?
SGA-010-096-104-67	Storage Node	Data Center 1	Default KMS	41b0...5c57	✓ Connected to KMS (2021-03-12 10:59:32 MST)

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

Colonna	Descrizione
Nome del nodo	Il nome del nodo appliance.



Colonna	Descrizione
Tipo di nodo	Il tipo di nodo: Storage, Admin o Gateway.
Sito	Il nome del sito StorageGRID in cui è installato il nodo.
Nome visualizzato DI 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>
UID chiave	<p>ID univoco della chiave di crittografia utilizzata per crittografare e decrittare i dati sul nodo dell'appliance. Per visualizzare un intero UID chiave, spostare il cursore sulla cella.</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> per visualizzare i nuovi valori, è necessario aggiornare il browser Web.</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

Consultare le azioni consigliate per questi avvisi nelle istruzioni di [Monitoraggio e risoluzione dei problemi di StorageGRID](#).



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

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

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

### Di cosa hai bisogno

- Hai esaminato il [considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi](#).
- Se si prevede di aggiornare il sito selezionato per un KMS, è stata esaminata la [Considerazioni per la modifica del KMS per un sito](#).
- Hai effettuato l'accesso a Grid Manager utilizzando un [browser web supportato](#).
- Si dispone dell'autorizzazione di accesso root.

### Fasi

1. Selezionare **CONFIGURATION Security Key management server**.

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

#### Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:


- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

<a href="#">+ Create</a>	<a href="#">✎ Edit</a>	<a href="#">🗑 Remove</a>			
KMS Display Name <a href="#">?</a>	Key Name <a href="#">?</a>	Manages keys for <a href="#">?</a>	Hostname <a href="#">?</a>	Certificate Status <a href="#">?</a>	
<input checked="" type="radio"/> Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid	

2. Selezionare il KMS che si desidera modificare e selezionare **Edit** (Modifica).
3. Se si desidera, aggiornare i dettagli nel **Passo 1 (Immetti dettagli KMS)** della procedura guidata Modifica un server di gestione delle chiavi.

Campo	Descrizione
Nome visualizzato DI KMS	Un nome descrittivo per aiutarti a identificare questo KMS. Deve essere compreso tra 1 e 64 caratteri.

Campo	Descrizione
Key Name (Nome chiave)	<p>L'alias esatto della chiave per il client StorageGRID nel KMS. Deve essere compreso tra 1 e 255 caratteri.</p> <p>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.</p> <div>  <p>Non tentare mai di ruotare una chiave cambiando il nome della chiave (alias) per il KMS. Al contrario, ruotare la chiave aggiornando la versione della chiave nel software 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.</p> <p><a href="#">Considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi</a></p> </div>
Gestisce le chiavi per	<p>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.</p> <p><b>Nota:</b> se si modifica un KMS specifico del sito, non è possibile selezionare un altro sito. Se si sta modificando il KMS predefinito, non è possibile selezionare un sito specifico.</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 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 il segno più **+** per aggiungere un nome host per ciascun server nel cluster.

5. Selezionare **Avanti**.

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 **Avanti**.

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 **Salva**.

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.

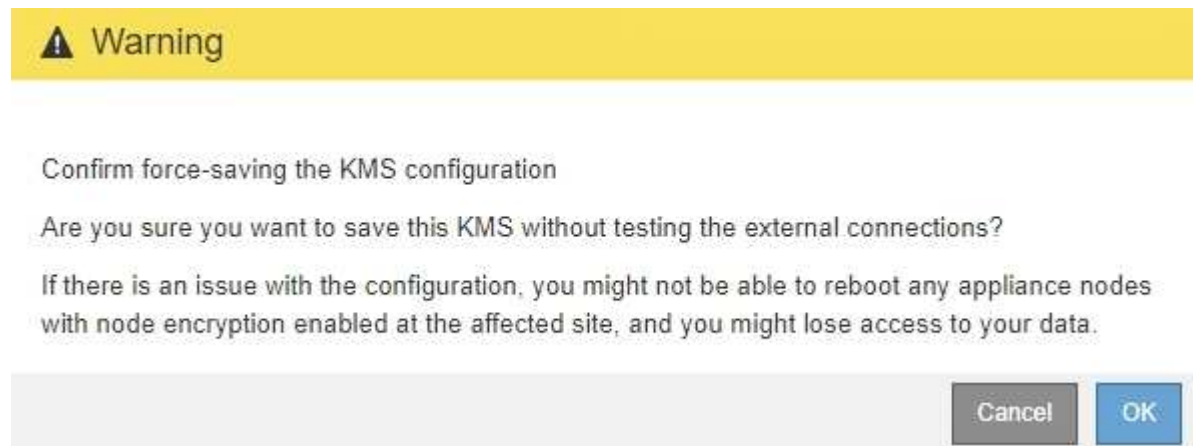
11. Se è necessario salvare la configurazione corrente prima di risolvere gli errori di connessione, selezionare **forza salvataggio**.



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.

La configurazione KMS viene salvata.

12. 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.

## 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.

### Di cosa hai bisogno

- Hai esaminato il [considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi](#).
- Hai effettuato l'accesso a Grid Manager utilizzando un [browser web supportato](#).
- Si dispone dell'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 **CONFIGURATION Security Key management server**.

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

##### Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

<div><div>+ Create</div><div>Edit</div><div>Remove</div></div>				
KMS Display Name ?	Key Name ?	Manages keys for ?	Hostname ?	Certificate Status ?
<input checked="" type="radio"/> Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid

2. Selezionare il pulsante di opzione relativo al KMS che si desidera rimuovere e selezionare **Remove** (Rimuovi).
3. Esaminare le considerazioni nella finestra di dialogo di avviso.

## ⚠ Warning

### Delete KMS Configuration

You can only remove a KMS in these cases:

- You are removing a site-specific KMS for a site that has no appliance nodes with node encryption enabled.
- You are removing the default KMS, but a site-specific KMS already exists for each site with node encryption.

Are you sure you want to delete the Default KMS KMS configuration?

Cancel

OK

4. Selezionare **OK**.

La configurazione KMS viene rimossa.

## Gestire le impostazioni del proxy

### Configurare le impostazioni del proxy di storage

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.

#### Di cosa hai bisogno

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

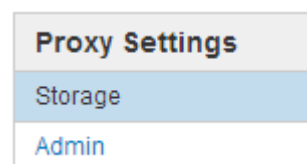
#### A proposito di questa attività

È possibile configurare le impostazioni per un singolo Storage Proxy.

#### Fasi

1. Selezionare **CONFIGURAZIONE** **sicurezza** **Impostazioni proxy**.

Viene visualizzata la pagina Storage Proxy Settings (Impostazioni proxy storage). Per impostazione predefinita, nel menu della barra laterale è selezionata l'opzione **Storage**.



2. Selezionare la casella di controllo **Enable Storage Proxy** (attiva proxy di storage).

Vengono visualizzati i campi per la configurazione di un proxy di storage.

### Storage Proxy Settings

If you are using platform services or Cloud Storage Pools, you can configure a non-transparent proxy server between Storage Nodes and the external S3 endpoints.

Enable Storage Proxy ☒

Protocol ☐ HTTP ☐ SOCKS5

Hostname

Port (optional)

3. Selezionare il protocollo per il proxy dello storage non trasparente.
4. Immettere il nome host o l'indirizzo IP del server proxy.
5. Facoltativamente, inserire la porta utilizzata per connettersi al server proxy.

È possibile lasciare vuoto questo campo se si utilizza la porta predefinita per il protocollo: 80 per HTTP o 1080 per SOCKS5.

6. Selezionare **Salva**.

Una volta salvato il proxy dello storage, è possibile configurare e testare i 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.

### Al termine

Se è necessario disattivare un proxy di storage, deselegionare la casella di controllo **Enable Storage Proxy** (attiva proxy di storage) e selezionare **Save** (Salva).

### Informazioni correlate

- [Rete e porte per i servizi della piattaforma](#)
- [Gestire gli oggetti con ILM](#)

## Configurare le impostazioni del proxy amministratore

Se si inviano messaggi AutoSupport utilizzando HTTP o HTTPS (vedere [Configurare AutoSupport](#)), è possibile configurare un server proxy non trasparente tra i nodi di amministrazione e il supporto tecnico (AutoSupport).

### Di cosa hai bisogno

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

## A proposito di questa attività

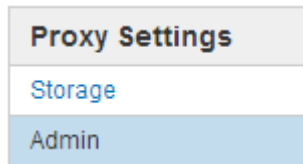
È possibile configurare le impostazioni per un singolo proxy Admin.

### Fasi

1. Selezionare **CONFIGURAZIONE** **sicurezza** **Impostazioni proxy**.

Viene visualizzata la pagina Admin Proxy Settings (Impostazioni proxy amministratore). Per impostazione predefinita, nel menu della barra laterale è selezionata l'opzione **Storage**.

2. Dal menu della barra laterale, selezionare **Admin**.



3. Selezionare la casella di controllo **Enable Admin Proxy** (attiva proxy amministratore).

#### Admin Proxy Settings

If you send AutoSupport messages using HTTPS or HTTP, you can configure a non-transparent proxy server between Admin Nodes and technical support.

Enable Admin Proxy ☒

Hostname

Port

Username (optional)

Password (optional)

4. Immettere il nome host o l'indirizzo IP del server proxy.
5. Inserire la porta utilizzata per la connessione al server proxy.
6. Se si desidera, inserire il nome utente del proxy.

Lasciare vuoto questo campo se il server proxy non richiede un nome utente.

7. Se si desidera, inserire la password del proxy.

Lasciare vuoto questo campo se il server proxy non richiede una password.

8. Selezionare **Salva**.

Una volta salvato il proxy Admin, 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, deselezionare la casella di controllo **Enable Admin Proxy** (attiva



proxy amministratore) e selezionare **Save** (Salva).

## Gestire reti client non attendibili

### Gestisci reti client non attendibili: Panoramica

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 della griglia su tutte le porte esterne disponibili (vedere le informazioni sulle comunicazioni esterne nella sezione [Linee guida per il networking](#)).

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](#).

#### 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 pagina degli endpoint del bilanciamento del carico, configurare un endpoint del bilanciamento del carico per S3 su HTTPS sulla porta 443.
2. Nella pagina Untrusted Client Networks (reti client non attendibili), 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 abilitare il traffico di servizio 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:

- Nella pagina Untrusted Client Networks (reti client non attendibili), indicare che la rete client sul nodo di storage non è attendibile.

Dopo aver salvato la configurazione, il nodo di storage non accetta più il traffico in entrata sulla rete client, ma continua a consentire le richieste in uscita ad Amazon Web Services.

### Specificare che la rete client del nodo non è attendibile

Se si utilizza una rete client, è possibile specificare se la rete client di ciascun nodo è attendibile o meno. È inoltre possibile specificare l'impostazione predefinita per i nuovi nodi aggiunti in un'espansione.

#### Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un [browser web supportato](#).

- Si dispone dell'autorizzazione di accesso root.
- 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.



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

## Fasi

1. Selezionare **CONFIGURAZIONE sicurezza reti client non attendibili**.

La pagina reti client non attendibili elenca tutti i nodi nel sistema StorageGRID. La colonna motivo non disponibile include una voce se la rete client del nodo deve essere attendibile.

### Untrusted Client Networks

If you are using a Client Network, you can specify whether a node trusts inbound traffic from the Client Network. If the Client Network is untrusted, the node only accepts inbound traffic on ports configured as [load balancer endpoints](#).

#### Set New Node Default

This setting applies to new nodes expanded into the grid.

New Node Client Network ☒ Trusted  
Default ☐ Untrusted

#### Select Untrusted Client Network Nodes

Select nodes that should have untrusted Client Network enforcement.

<input type="checkbox"/>	Node Name	Unavailable Reason
<input type="checkbox"/>	DC1-ADM1	
<input type="checkbox"/>	DC1-G1	
<input type="checkbox"/>	DC1-S1	
<input type="checkbox"/>	DC1-S2	
<input type="checkbox"/>	DC1-S3	
<input type="checkbox"/>	DC1-S4	
Client Network untrusted on 0 nodes.		

Save

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:** Quando un nodo viene aggiunto in un'espansione, la sua rete client è attendibile.
  - **Untrusted:** Quando un nodo viene aggiunto in un'espansione, la sua rete client non è attendibile. Se necessario, tornare a questa pagina per modificare l'impostazione di un nuovo nodo specifico.



Questa impostazione non influisce sui nodi esistenti nel sistema StorageGRID.

3. Nella sezione **Select untrusted Client Network Nodes** (Seleziona nodi di rete client non attendibili), selezionare i nodi che devono consentire le connessioni client solo su endpoint del bilanciamento del

carico configurati esplicitamente.

È possibile selezionare o deselectare la casella di controllo nel titolo per selezionare o deselectare tutti i nodi.

#### 4. Selezionare **Salva**.

Le nuove regole del firewall vengono aggiunte 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 © 2025 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.