Configurare i server di gestione delle chiavi

StorageGRID software

NetApp
December 03, 2025

Sommario

Configurare i server di gestione delle chiavi . . . 1
- Che cos'è un server di gestione delle chiavi (KMS)? . . . 1
- Configurazione KMS e appliance . . . 1
  - Configurare il server di gestione delle chiavi (KMS) . . . 1
  - Impostare l'apparecchio . . . 2
  - Processo di crittografia della gestione delle chiavi (avviene automaticamente) . . . 2
- Considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi . . . 3
  - Quale versione di KMIP è supportata? . . . 3
  - Quali sono le considerazioni da fare in merito alla rete? . . . 3
  - Quali versioni di TLS sono supportate? . . . 3
  - Quali elettrodomestici sono supportati? . . . 3
  - Quando dovrei configurare i server di gestione delle chiavi? . . . 4
  - Di quanti server di gestione delle chiavi ho bisogno? . . . 4
  - Cosa succede quando si ruota una chiave? . . . 5
  - Posso riutilizzare un nodo appliance dopo averlo crittografato? . . . 5
- Considerazioni sulla modifica del KMS per un sito . . . 6
  - Casi d'uso per modificare il KMS utilizzato per un sito . . . 7
- Configurare StorageGRID come client nel KMS . . . 8
- Aggiungere un server di gestione delle chiavi (KMS) . . . 9
  - Passaggio 1: dettagli KMS . . . 10
  - Passaggio 2: carica il certificato del server . . . 11
    - Passaggio 3: Carica i certificati client . . . 11
- Gestire un KMS . . . 12
  - Visualizza i dettagli KMS . . . 12
  - Gestisci i certificati . . . 14
  - Visualizza i nodi crittografati . . . 14
  - Modifica un KMS . . . 16
  - Rimuovere un server di gestione delle chiavi (KMS) . . . 18

Configurare i server di gestione delle chiavi

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

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

StorageGRID supporta solo determinati server di gestione delle chiavi. Per un elenco dei prodotti e delle versioni supportati, utilizzare "Strumento matrice di interoperabilità NetApp (IMT)" .

È possibile utilizzare uno o più server di gestione delle chiavi per gestire le chiavi di crittografia dei nodi per tutti i nodi dell'appliance StorageGRID in cui è abilitata l'impostazione **Crittografia nodi** durante l'installazione. Utilizzando server di gestione delle chiavi con questi nodi appliance è possibile proteggere i dati anche se un'appliance viene rimossa dal data center. Dopo aver crittografato i volumi dell'appliance, non sarà possibile accedere ai dati sull'appliance a meno che il nodo non sia in grado di comunicare con il KMS.

> StorageGRID non crea né gestisce le chiavi esterne utilizzate per crittografare e decrittografare i nodi dell'appliance. Se si prevede di 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 di attività di gestione chiave esula dallo scopo di queste istruzioni. Se hai bisogno di aiuto, consulta la documentazione del tuo server di gestione delle chiavi o contatta l'assistenza tecnica.

Configurazione KMS e appliance

Prima di poter utilizzare un server di gestione delle chiavi (KMS) per proteggere i dati StorageGRID sui nodi dell'appliance, è necessario completare due attività di configurazione: impostare uno o più server KMS e abilitare la crittografia dei nodi per i nodi dell'appliance. Una volta completate queste due attività di configurazione, il processo di gestione delle chiavi avviene automaticamente.

Il diagramma di flusso mostra i passaggi principali per utilizzare un KMS per proteggere i dati StorageGRID sui nodi dell'appliance.

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

Configurare il server di gestione delle chiavi (KMS)

La configurazione di un server di gestione delle chiavi comprende i seguenti passaggi generali.

Fare un passo	Fare riferimento a
Accedi al software KMS e aggiungi un client per StorageGRID a ciascun KMS o cluster KMS.	"Configurare StorageGRID come client nel KMS"

Fare un passo	Fare riferimento a
Ottenere le informazioni richieste per il client StorageGRID sul KMS.	"Configurare StorageGRID come client nel KMS"
Aggiungere il KMS a Grid Manager, assegnarlo a un singolo sito o a un gruppo predefinito di siti, caricare i certificati richiesti e salvare la configurazione del KMS.	"Aggiungere un server di gestione delle chiavi (KMS)"

Impostare l'apparecchio

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

1. Durante la fase di configurazione hardware dell'installazione dell'appliance, utilizzare StorageGRID Appliance Installer per abilitare l'impostazione **Crittografia nodo** per l'appliance.

> Non è possibile abilitare l'impostazione **Crittografia nodo** dopo aver aggiunto un'appliance alla griglia e non è possibile utilizzare la gestione delle chiavi esterne per le appliance che non hanno la crittografia 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 dati casuale (DEK), come segue:
   - Le DEK vengono utilizzate 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 è crittografato da una chiave di crittografia a chiave master (KEK). La KEK iniziale è una chiave temporanea che crittografa le DEK finché l'appliance non riesce a connettersi al KMS.
3. Aggiungere il nodo dell'appliance a StorageGRID.

Vedere "Abilita la crittografia del nodo" per i dettagli.

Processo di crittografia della gestione delle chiavi (avviene automaticamente)

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

1. Quando si installa un'appliance con crittografia dei nodi abilitata nella griglia, StorageGRID determina se esiste una configurazione KMS per il sito che contiene il nuovo nodo.
   - Se per il sito è già stato configurato un KMS, l'appliance riceve la configurazione KMS.
   - Se non è ancora stato configurato un KMS per il sito, i dati sull'appliance continuano a essere crittografati dalla KEK temporanea finché 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 ora viene utilizzata per crittografare e decrittografare le DEK per i volumi dell'appliance.

Tutti i dati esistenti prima che il nodo dell'appliance crittografata 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 finché la chiave temporanea non viene sostituita dalla chiave di crittografia KMS.

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

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

Prima di configurare un server di gestione delle chiavi esterno (KMS), è necessario comprendere le considerazioni e i requisiti.

Quale versione di KMIP è supportata?

StorageGRID supporta KMIP versione 1.4.

"Specifiche del protocollo di interoperabilità per la gestione delle chiavi versione 1.4"

Quali sono le considerazioni da fare in merito alla rete?

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

È necessario assicurarsi che ogni nodo dell'appliance che utilizza la crittografia dei nodi abbia accesso alla rete del KMS o del cluster KMS configurato per il sito.

Quali versioni di TLS sono supportate?

Le comunicazioni tra i nodi dell'appliance e il KMS configurato utilizzano connessioni TLS sicure. StorageGRID può supportare il protocollo TLS 1.2 o TLS 1.3 quando effettua connessioni KMIP a un KMS o a un cluster KMS, in base a ciò che il KMS supporta e a quale"Politica TLS e SSH" che stai utilizzando.

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

Quali elettrodomestici sono supportati?

È possibile utilizzare un server di gestione delle chiavi (KMS) per gestire le chiavi di crittografia per qualsiasi appliance StorageGRID nella griglia in cui sia abilitata l'impostazione **Crittografia nodo**. Questa impostazione può essere abilitata solo durante la fase di configurazione hardware dell'installazione dell'appliance tramite StorageGRID Appliance Installer.

Non è possibile abilitare la crittografia dei nodi dopo aver aggiunto un'appliance alla griglia e non è possibile utilizzare la gestione delle chiavi esterne per le appliance che non hanno la crittografia dei nodi abilitata.

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

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

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

I nodi distribuiti su queste altre piattaforme possono utilizzare la crittografia al di fuori di StorageGRID a livello di datastore o disco.

Quando dovrei 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 i tenant. Questo ordine garantisce che i nodi siano protetti prima che i dati degli oggetti vengano memorizzati su di essi.

È possibile configurare i server di gestione delle chiavi in Grid Manager prima o dopo aver installato i nodi dell'appliance.

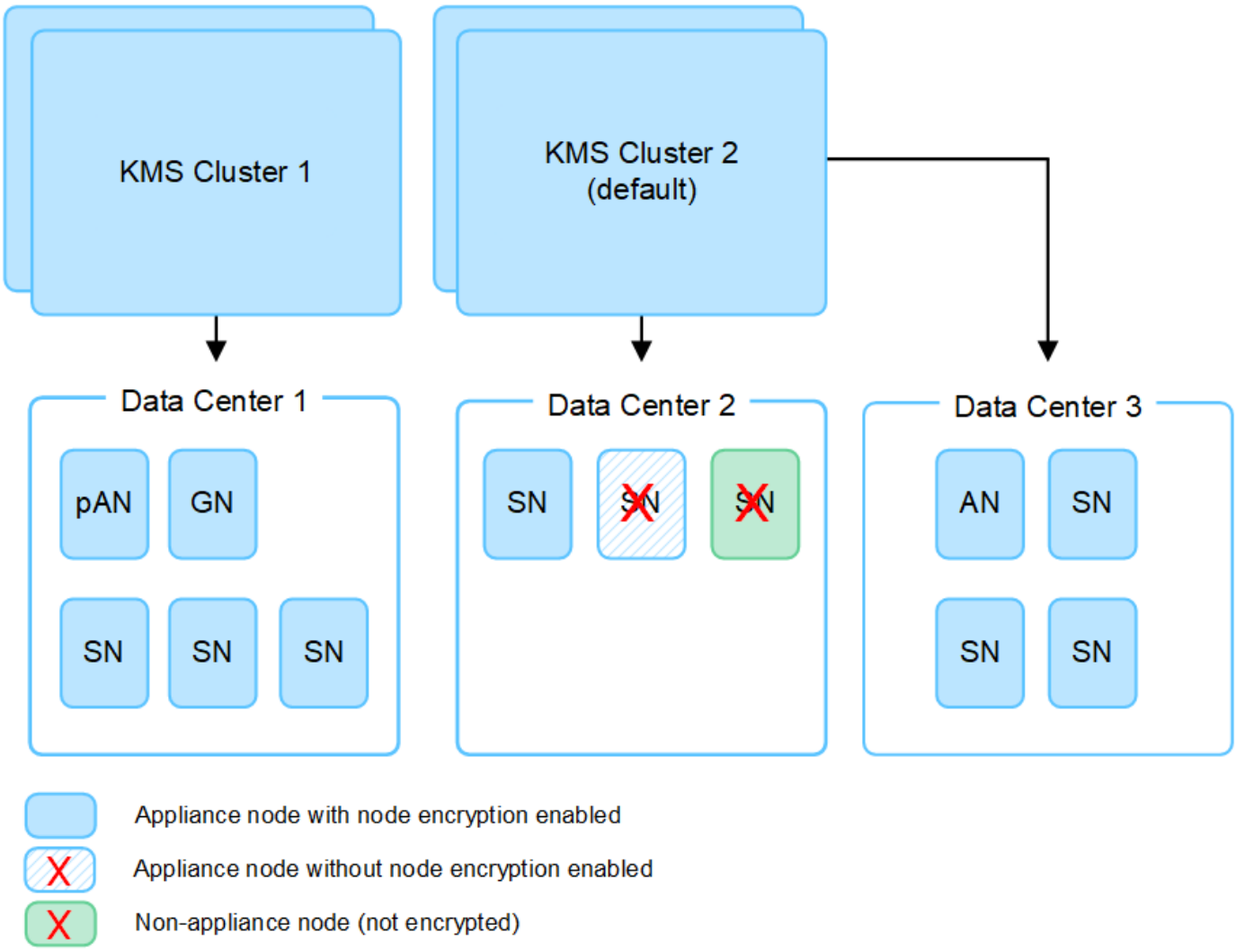
Di quanti server di gestione delle chiavi ho bisogno?

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'uso di cluster KMS. Ogni cluster KMS contiene più server di gestione delle chiavi replicati che condividono impostazioni di configurazione e chiavi di crittografia. Si consiglia di utilizzare cluster KMS per la gestione delle chiavi perché migliorano le capacità di failover di una configurazione ad alta disponibilità.

Ad esempio, supponiamo che il tuo sistema StorageGRID abbia tre siti di data center. È possibile configurare un cluster KMS per fornire una chiave a tutti i nodi dell'appliance nel Data Center 1 e un secondo cluster KMS per fornire una chiave a tutti i nodi dell'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.

Tieni presente che non puoi utilizzare un KMS per nodi non appliance o per nodi appliance per i quali non è stata abilitata l'impostazione **Crittografia nodo** durante l'installazione.



Cosa succede quando si ruota una chiave?

Come buona pratica di sicurezza, dovresti periodicamente"ruotare la chiave di crittografia" utilizzato da ciascun KMS configurato.

Quando sarà disponibile la nuova versione della chiave:

- Viene distribuito automaticamente ai nodi dell'appliance crittografata nel sito o nei siti associati al KMS. La distribuzione dovrebbe avvenire entro un'ora dalla rotazione della chiave.
- Se il nodo dell'appliance crittografata è offline quando viene distribuita la nuova versione della chiave, il nodo riceverà la nuova chiave non appena si riavvia.
- Se per qualsiasi motivo non è possibile utilizzare la nuova versione della chiave per crittografare i volumi dell'appliance, viene attivato l'avviso **Rotazione chiave di crittografia KMS non riuscita** per il nodo dell'appliance. Potrebbe essere necessario contattare l'assistenza tecnica per ricevere aiuto nella risoluzione di questo avviso.

Posso riutilizzare un nodo appliance dopo averlo crittografato?

Se è necessario installare un'appliance crittografata in un altro sistema StorageGRID , è necessario prima disattivare il nodo della griglia per spostare i dati dell'oggetto su un altro nodo. Quindi, è possibile utilizzare StorageGRID Appliance Installer per "cancellare la configurazione KMS" . La cancellazione della

configurazione KMS disabilita l'impostazione **Crittografia nodo** e rimuove l'associazione tra il nodo dell'appliance e la configurazione KMS per il sito StorageGRID .

> Senza accesso alla chiave di crittografia KMS, tutti i dati rimasti sul dispositivo non saranno più accessibili e saranno bloccati in modo permanente.

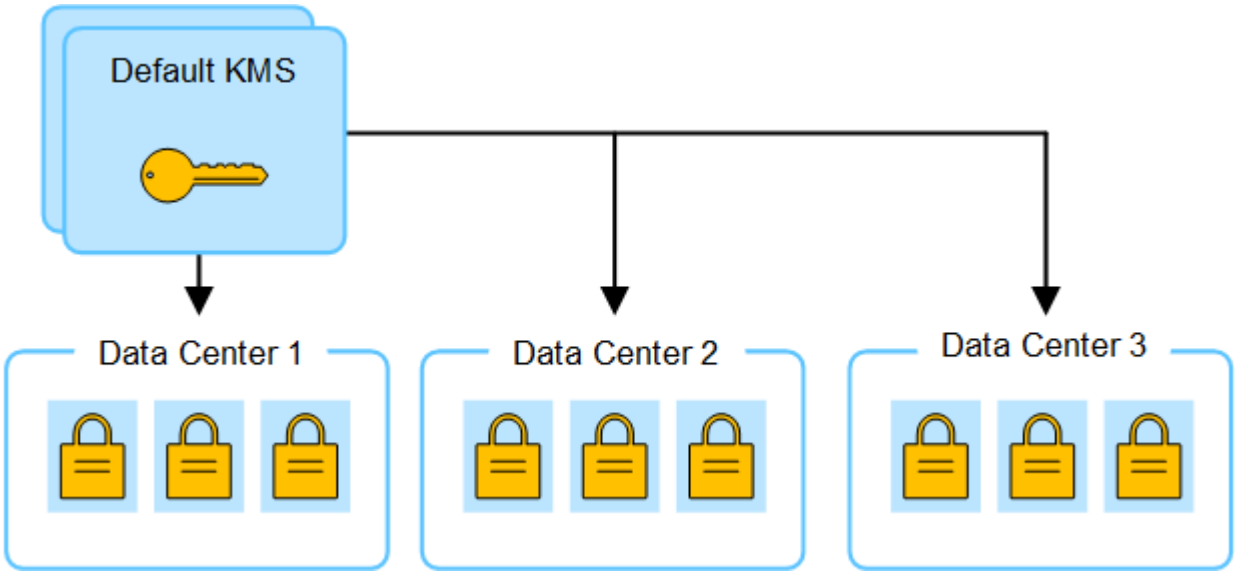
Considerazioni sulla modifica del KMS per un sito

Ogni server di gestione delle chiavi (KMS) o cluster KMS fornisce una chiave di crittografia a tutti i nodi dell'appliance in un singolo sito o in 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 a un altro.

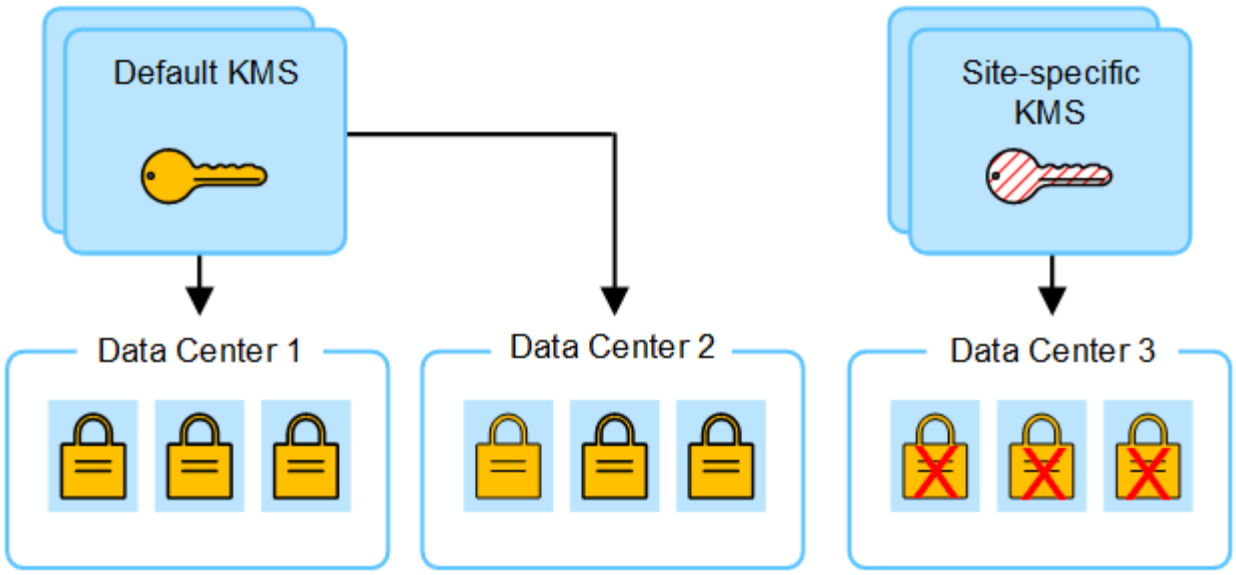
Se si modifica il KMS utilizzato per un sito, è necessario assicurarsi che i nodi dell'appliance precedentemente crittografati in quel sito possano essere decrittografati utilizzando la chiave memorizzata sul nuovo KMS. In alcuni casi, potrebbe essere necessario copiare la versione corrente della chiave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

Per esempio:

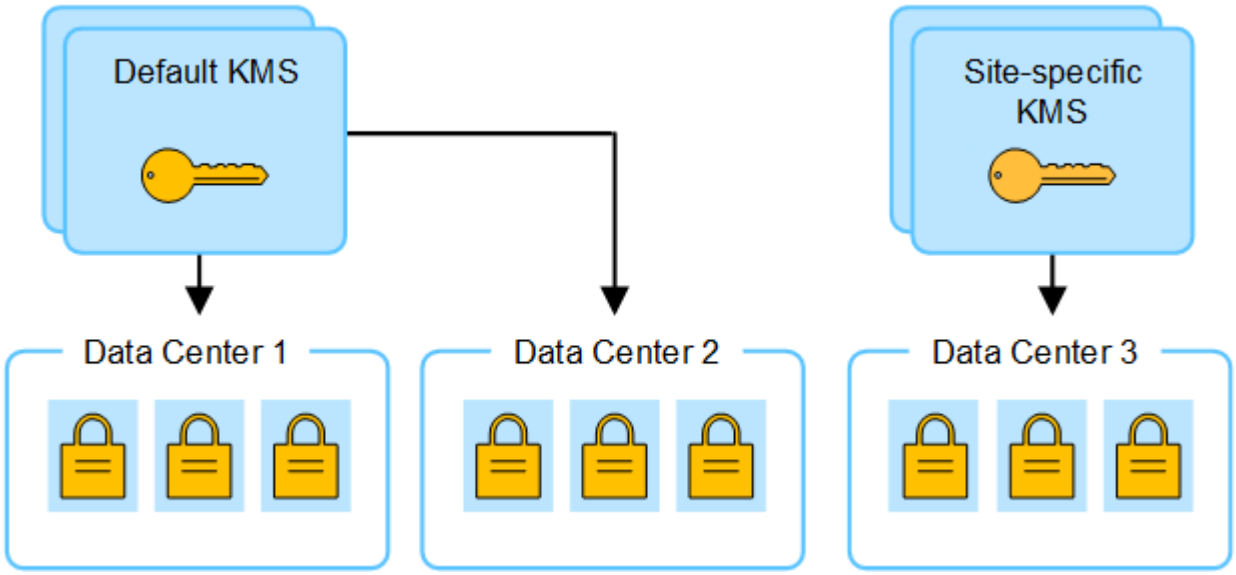
1. Inizialmente si configura un KMS predefinito che si applica a tutti i siti che non dispongono di un KMS dedicato.
2. Una volta salvato il KMS, tutti i nodi dell'appliance in cui è abilitata l'impostazione **Crittografia nodo** si connettono al KMS e richiedono la chiave di crittografia. Questa chiave viene utilizzata per crittografare i nodi dell'appliance in tutti i siti. La stessa chiave deve essere utilizzata anche per decifrare tali apparecchi.



3. Si decide di aggiungere un KMS specifico 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 decrittografare 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 ora dispone della chiave corretta per decrittografare i nodi dell'appliance nel Data Center 3, in modo che possa essere salvata in StorageGRID.



Casi d'uso per modificare il KMS utilizzato per un sito

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

Caso d'uso per la modifica del KMS di un sito	Passaggi richiesti
Hai una o più voci KMS specifiche del sito e vuoi usarne una come KMS predefinito.	Modifica il KMS specifico del sito. Nel campo **Gestisci chiavi per**, seleziona **Siti non gestiti da un altro KMS (KMS predefinito)**. Il KMS specifico del sito verrà ora utilizzato come KMS predefinito. Si applicherà a tutti i siti che non dispongono di un KMS dedicato. "Modifica un server di gestione delle chiavi (KMS)"
Hai un KMS predefinito e aggiungi un nuovo sito in un'espansione. Non vuoi utilizzare il KMS predefinito per il nuovo sito.	1. Se i nodi dell'appliance nel nuovo sito sono già stati crittografati dal KMS predefinito, utilizzare il software KMS per copiare la versione corrente della chiave di crittografia dal KMS predefinito a un nuovo KMS. 2. Utilizzando Grid Manager, aggiungi il nuovo KMS e seleziona il sito. "Aggiungere un server di gestione delle chiavi (KMS)"
Si desidera che il KMS di un sito utilizzi un server diverso.	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. 2. Utilizzando Grid Manager, modifica la configurazione KMS esistente e inserisci il nuovo nome host o indirizzo IP. "Aggiungere un server di gestione delle chiavi (KMS)"

Configurare StorageGRID come client nel KMS

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

Queste istruzioni si applicano a Thales CipherTrust Manager e Hashicorp Vault. Per un elenco dei prodotti e delle versioni supportati, utilizzare "Strumento matrice di interoperabilità NetApp (IMT)" .

Passi

1. Dal software KMS, crea un client StorageGRID per ogni KMS o cluster KMS che intendi utilizzare.

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

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

     La chiave di crittografia deve essere pari o superiore a 2.048 bit e deve essere esportabile.

   - Chiedi a StorageGRID di creare la chiave. Ti verrà chiesto quando esegui il test e salvi dopo"caricamento dei certificati client" .

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

   Quando aggiungi il KMS a StorageGRID, hai bisogno di queste informazioni:

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

4. Per ogni KMS o cluster 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 codificati in 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 Base-64 Privacy Enhanced Mail (PEM).
   - 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 client pubblico rilasciato a StorageGRID dal KMS esterno e la chiave privata per il certificato client.

   Il certificato client consente a StorageGRID di autenticarsi al KMS.

Aggiungere un server di gestione delle chiavi (KMS)

Per aggiungere ciascun KMS o cluster KMS, utilizzare la procedura guidata StorageGRID Key Management Server.

Prima di iniziare

- Hai esaminato il"considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi" .
- Hai"StorageGRID configurato come client nel KMS" e disponi delle informazioni richieste per ciascun KMS o cluster KMS.
- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Tu hai il"Permesso di accesso root" .

Informazioni su questo compito

Se possibile, configurare eventuali server di gestione delle chiavi specifici del sito prima di configurare un KMS predefinito che si applichi a tutti i siti non gestiti da un altro KMS. Se si crea prima il KMS predefinito, tutti gli apparecchi crittografati tramite nodo nella griglia verranno crittografati dal KMS predefinito. Se in un secondo momento si desidera creare un KMS specifico per il sito, è necessario prima copiare la versione corrente della chiave di crittografia dal KMS predefinito al nuovo KMS. Vedere"Considerazioni sulla modifica del KMS per un sito" per i dettagli.

Passaggio 1: dettagli KMS

Nel passaggio 1 (dettagli KMS) della procedura guidata Aggiungi un server di gestione delle chiavi, è necessario fornire dettagli sul KMS o sul cluster KMS.

Passi

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

   Viene visualizzata la pagina del server di gestione delle chiavi con la scheda Dettagli configurazione selezionata.

2. Seleziona **Crea**.

   Viene visualizzato il passaggio 1 (dettagli KMS) della procedura guidata Aggiungi un server di gestione delle chiavi.

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

Campo	Descrizione
Nome KMS	Un nome descrittivo che ti aiuti a identificare questo KMS. Deve contenere tra 1 e 64 caratteri.
Nome chiave	L'alias chiave esatto per il client StorageGRID nel KMS. Deve contenere tra 1 e 255 caratteri. **Nota**: se non hai creato una chiave utilizzando il tuo prodotto KMS, ti verrà chiesto di farla creare a StorageGRID .
Gestisce le chiavi per	Il sito StorageGRID che sarà associato a questo KMS. Se possibile, è opportuno configurare eventuali server di gestione delle chiavi specifici del sito prima di configurare un KMS predefinito che si applichi a tutti i siti non gestiti da un altro KMS. • Selezionare un sito se questo KMS gestirà le chiavi di crittografia per i nodi dell'appliance in un sito specifico. • Seleziona **Siti non gestiti da un altro KMS (KMS predefinito)** per configurare un KMS predefinito che verrà applicato a tutti i siti che non dispongono di un KMS dedicato e a tutti i siti aggiunti nelle espansioni successive. **Nota:** si verificherà un errore di convalida quando si salva la configurazione KMS se si seleziona un sito precedentemente crittografato dal KMS predefinito ma non è stata fornita la versione corrente della chiave di crittografia originale al nuovo KMS.
Porta	La porta utilizzata dal server KMS per le comunicazioni KMIP (Key Management Interoperability Protocol). Il valore predefinito è 5696, che è la porta standard KMIP.

Campo	Descrizione
Nome host	Il nome di dominio completo o l'indirizzo IP per il KMS. **Nota:** il campo Subject Alternative Name (SAN) del certificato del server deve includere l'FQDN o l'indirizzo IP immesso qui. In caso contrario, StorageGRID non sarà in grado di connettersi al KMS o a tutti i server in un cluster KMS.

4. Se si sta configurando un cluster KMS, selezionare **Aggiungi un altro nome host** per aggiungere un nome host per ciascun server nel cluster.
5. Selezionare **Continua**.

Passaggio 2: carica il certificato del server

Nel passaggio 2 (Carica certificato server) della procedura guidata Aggiungi un server di gestione delle chiavi, caricare il certificato server (o il pacchetto di certificati) per il KMS. Il certificato del server consente al KMS esterno di autenticarsi su StorageGRID.

Passi

1. Dal **Passaggio 2 (Carica certificato server)**, vai alla posizione del certificato server salvato o del pacchetto di certificati.
2. Carica il file del certificato.

   Vengono visualizzati i metadati del certificato del server.

   > Se hai caricato un pacchetto di certificati, i metadati di ciascun certificato vengono visualizzati in una scheda separata.

3. Selezionare **Continua**.

Passaggio 3: Carica i certificati client

Nel passaggio 3 (Caricamento dei certificati client) della procedura guidata Aggiungi un server di gestione delle chiavi, caricare il certificato client e la chiave privata del certificato client. Il certificato client consente a StorageGRID di autenticarsi presso il KMS.

Passi

1. Dal **Passaggio 3 (Caricamento certificati client)**, accedere alla posizione del certificato client.
2. Carica il file del certificato client.

   Vengono visualizzati i metadati del certificato client.

3. Passare alla posizione della chiave privata per il certificato client.
4. Carica il file della chiave privata.
5. Seleziona **Test e salva**.

   Se non esiste una chiave, verrà richiesto a StorageGRID di crearne una.

   Vengono testate 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 sul 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 Key Management Server appare come Sconosciuto. StorageGRID potrebbe impiegare fino a 30 minuti per ottenere lo stato effettivo di ciascun certificato. Per visualizzare lo stato attuale, è necessario aggiornare il browser web.

6. Se viene visualizzato un messaggio di errore quando si seleziona **Test e salva**, rivedere i dettagli del messaggio e quindi selezionare **OK**.

   Ad esempio, potresti ricevere un errore 422: Entità non elaborabile se un test di connessione non riesce.

7. Se è necessario salvare la configurazione corrente senza testare la connessione esterna, selezionare **Forza salvataggio**.

   > Selezionando **Forza salvataggio** la configurazione KMS viene salvata, ma non viene testata la connessione esterna da ciascun dispositivo a quel KMS. Se si verifica un problema con la configurazione, potrebbe non essere possibile riavviare i nodi dell'appliance in cui è abilitata la crittografia dei nodi nel sito interessato. Potresti perdere l'accesso ai tuoi dati finché i problemi non saranno risolti.

8. Rivedi l'avviso di conferma e seleziona **OK** se sei sicuro di voler forzare il salvataggio della configurazione.

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

Gestire un KMS

La gestione di un server di gestione delle chiavi (KMS) implica la visualizzazione o la modifica dei dettagli, la gestione dei certificati, la visualizzazione dei nodi crittografati e la rimozione di un KMS quando non è più necessario.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Tu hai il"autorizzazione di accesso richiesta" .

Visualizza i dettagli KMS

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

Passi

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

   Viene visualizzata la pagina del server di gestione delle chiavi, che mostra le seguenti informazioni:

   - Nella scheda Dettagli configurazione sono elencati tutti i server di gestione delle chiavi configurati.
   - Nella scheda Nodi crittografati sono elencati tutti i nodi in cui è abilitata la crittografia dei nodi.

2. Per visualizzare i dettagli di un KMS specifico ed eseguire operazioni su tale KMS, selezionare il nome del KMS. Nella pagina dei dettagli del KMS sono elencate le seguenti informazioni:

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

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

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

4. Seleziona **Ruota chiave** o utilizza il software KMS ogni volta che le pratiche di sicurezza della tua organizzazione lo richiedono, per creare una nuova versione della chiave.

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

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

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

Gestisci i certificati

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

Per mantenere l'accesso ai dati, è necessario risolvere il prima possibile eventuali problemi relativi ai certificati.

Passi

1. Selezionare **CONFIGURAZIONE** > **Sicurezza** > **Server di gestione delle chiavi**.
2. Nella tabella, osserva il valore della Scadenza del certificato per ciascun KMS.
3. Se la scadenza del certificato per un KMS è sconosciuta, attendere fino a 30 minuti e quindi aggiornare il browser Web.
4. Se la colonna Scadenza certificato indica che un certificato è scaduto o sta per scadere, selezionare il KMS per andare alla pagina dei dettagli del KMS.
   a. Selezionare **Certificato server** e verificare il valore per il campo "Scade il".
   b. Per sostituire il certificato, seleziona **Modifica certificato** per caricare un nuovo certificato.
   c. Ripetere questi sotto-passaggi e selezionare **Certificato client** anziché Certificato server.
5. Quando vengono attivati gli avvisi **Scadenza certificato CA KMS**, **Scadenza certificato client KMS** e **Scadenza certificato server KMS**, annotare la descrizione di ciascun avviso ed eseguire le azioni consigliate.

   Potrebbero volerci fino a 30 minuti prima che StorageGRID riceva gli aggiornamenti sulla scadenza del certificato. Aggiorna il browser web per visualizzare i valori correnti.

Se viene visualizzato lo stato **Lo stato del certificato del server è sconosciuto**, accertarsi che il KMS consenta di ottenere un certificato del server senza richiedere un certificato del client.

Visualizza i nodi crittografati

È possibile visualizzare informazioni sui nodi dell'appliance nel sistema StorageGRID in cui è abilitata l'impostazione **Crittografia nodi**.

Passi

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

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

2. Nella parte superiore della pagina, seleziona la scheda **Nodi crittografati**.

   Nella scheda Nodi crittografati sono elencati i nodi dell'appliance nel sistema StorageGRID in cui è abilitata l'impostazione **Crittografia nodi**.

3. Esaminare le informazioni nella tabella per ciascun nodo dell'appliance.

Colonna	Descrizione
Nome del nodo	Il nome del nodo dell'appliance.
Tipo di nodo	Tipo di nodo: Storage, Admin o Gateway.
Sito	Nome del sito StorageGRID in cui è installato il nodo.
Nome KMS	Nome descrittivo del KMS utilizzato per il nodo. Se non è elencato alcun KMS, selezionare la scheda Dettagli configurazione per aggiungerne uno. "Aggiungere un server di gestione delle chiavi (KMS)"
UID chiave	ID univoco della chiave di crittografia utilizzata per crittografare e decrittografare i dati sul nodo dell'appliance. Per visualizzare l'intero UID della chiave, selezionare il testo. Un trattino (--) indica che l'UID della chiave è sconosciuto, probabilmente a causa di un problema di connessione tra il nodo dell'appliance e il KMS.
Stato	Lo stato della connessione tra il KMS e il nodo dell'appliance. Se il nodo è connesso, il timestamp viene aggiornato ogni 30 minuti. Dopo le modifiche alla configurazione KMS, potrebbero essere necessari diversi minuti prima che lo stato della connessione venga aggiornato. **Nota:** aggiorna il browser web per visualizzare i nuovi valori.

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

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

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

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

Eseguire le azioni consigliate per questi avvisi.

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

Modifica un KMS

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

Prima di iniziare

- Se si prevede di aggiornare il sito selezionato per un KMS, è necessario aver esaminato il"considerazioni sulla modifica del KMS per un sito" .
- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Tu hai il"Permesso di accesso root" .

Passi

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

   Viene visualizzata la pagina Server di gestione delle chiavi, che mostra tutti i server di gestione delle chiavi configurati.

2. Seleziona il KMS che vuoi modificare e seleziona **Azioni** > **Modifica**.

   È anche possibile modificare un KMS selezionando il nome del KMS nella tabella e selezionando **Modifica** nella pagina dei dettagli del KMS.

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

Campo	Descrizione
Nome KMS	Un nome descrittivo che ti aiuti a identificare questo KMS. Deve contenere tra 1 e 64 caratteri.
Nome chiave	L'alias chiave esatto per il client StorageGRID nel KMS. Deve contenere tra 1 e 255 caratteri. Solo in rari casi è necessario modificare il nome della chiave. Ad esempio, è necessario modificare il nome della chiave se l'alias è stato rinominato nel KMS o se tutte le versioni della chiave precedente sono state copiate nella cronologia delle versioni del nuovo alias.

Campo	Descrizione
Gestisce le chiavi per	Se stai modificando un KMS specifico del sito e non hai ancora un KMS predefinito, seleziona facoltativamente **Siti non gestiti da un altro KMS (KMS predefinito)**. 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. **Nota:** se stai modificando un KMS specifico di un sito, non puoi selezionare un altro sito. Se stai modificando il KMS predefinito, non puoi selezionare un sito specifico.
Porta	La porta utilizzata dal server KMS per le comunicazioni KMIP (Key Management Interoperability Protocol). Il valore predefinito è 5696, che è la porta standard KMIP.
Nome host	Il nome di dominio completo o l'indirizzo IP per il KMS. **Nota:** il campo Subject Alternative Name (SAN) del certificato del server deve includere l'FQDN o l'indirizzo IP immesso qui. In caso contrario, StorageGRID non sarà in grado di connettersi al KMS o a tutti i server in un cluster KMS.

4. Se si sta configurando un cluster KMS, selezionare **Aggiungi un altro nome host** per aggiungere un nome host per ciascun server nel cluster.
5. Selezionare **Continua**.

   Viene visualizzato il passaggio 2 (Carica certificato server) della procedura guidata Modifica un server di gestione delle chiavi.

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

   Viene visualizzato il passaggio 3 (Caricamento dei 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 **Sfoglia** e caricare i nuovi file.
9. Seleziona **Test e salva**.

   Vengono testate le connessioni tra il server di gestione delle chiavi e tutti i nodi dell'appliance crittografati tramite nodo nei siti interessati. Se tutte le connessioni dei nodi sono valide e la chiave corretta viene trovata sul 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, rivedere i dettagli del messaggio e selezionare **OK**.

    Ad esempio, potresti ricevere un errore 422: Entità non elaborabile se il sito selezionato per questo KMS è già gestito da un altro KMS o se un test di connessione non è riuscito.

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

Selezionando **Forza salvataggio** la configurazione KMS viene salvata, ma non viene testata la connessione esterna da ciascun dispositivo a quel KMS. Se si verifica un problema con la configurazione, potrebbe non essere possibile riavviare i nodi dell'appliance in cui è abilitata la crittografia dei nodi nel sito interessato. Potresti perdere l'accesso ai tuoi dati finché i problemi non saranno risolti.

La configurazione KMS è stata salvata.

12. Rivedi l'avviso di conferma e seleziona **OK** se sei sicuro di voler forzare il salvataggio della configurazione.

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

Rimuovere un server di gestione delle chiavi (KMS)

In alcuni casi potrebbe essere necessario rimuovere un server di gestione delle chiavi. Ad esempio, potresti voler rimuovere un KMS specifico di un sito se hai dismesso il sito.

Prima di iniziare

- 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" .
- Tu hai il"Permesso di accesso root" .

Informazioni su questo compito

È possibile rimuovere un KMS nei seguenti casi:

- È possibile rimuovere un KMS specifico del sito se il sito è stato dismesso o se non include nodi appliance con crittografia dei nodi abilitata.
- È possibile rimuovere il KMS predefinito se per ogni sito che dispone di nodi appliance con crittografia dei nodi abilitata esiste già un KMS specifico.

Passi

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

   Viene visualizzata la pagina Server di gestione delle chiavi, che mostra tutti i server di gestione delle chiavi configurati.

2. Seleziona il KMS che vuoi rimuovere e seleziona **Azioni** > **Rimuovi**.

   È anche possibile rimuovere un KMS selezionando il nome del KMS nella tabella e selezionando **Rimuovi** dalla pagina dei dettagli del KMS.

3. Conferma che quanto segue è vero:
   - Si sta rimuovendo un KMS specifico del sito per un sito che non dispone di alcun nodo appliance con crittografia del nodo abilitata.
   - Stai rimuovendo il KMS predefinito, ma per ogni sito esiste già un KMS specifico con crittografia dei nodi.
4. Selezionare **Sì**.

   La configurazione KMS è stata rimossa.