Configura i server di gestione delle chiavi

StorageGRID software

NetApp
July 23, 2026

This PDF was generated from https://docs.netapp.com/it-it/storagegrid-120/admin/kms-configuring.html on July 23, 2026. Always check docs.netapp.com for the latest.

Sommario

Configura i server di gestione delle chiavi

Scopri i server di gestione delle chiavi in StorageGRID

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

StorageGRID supporta solo alcuni server di gestione delle chiavi. Per un elenco dei prodotti e delle versioni supportati, usa il "NetApp Interoperability Matrix Tool (IMT)".

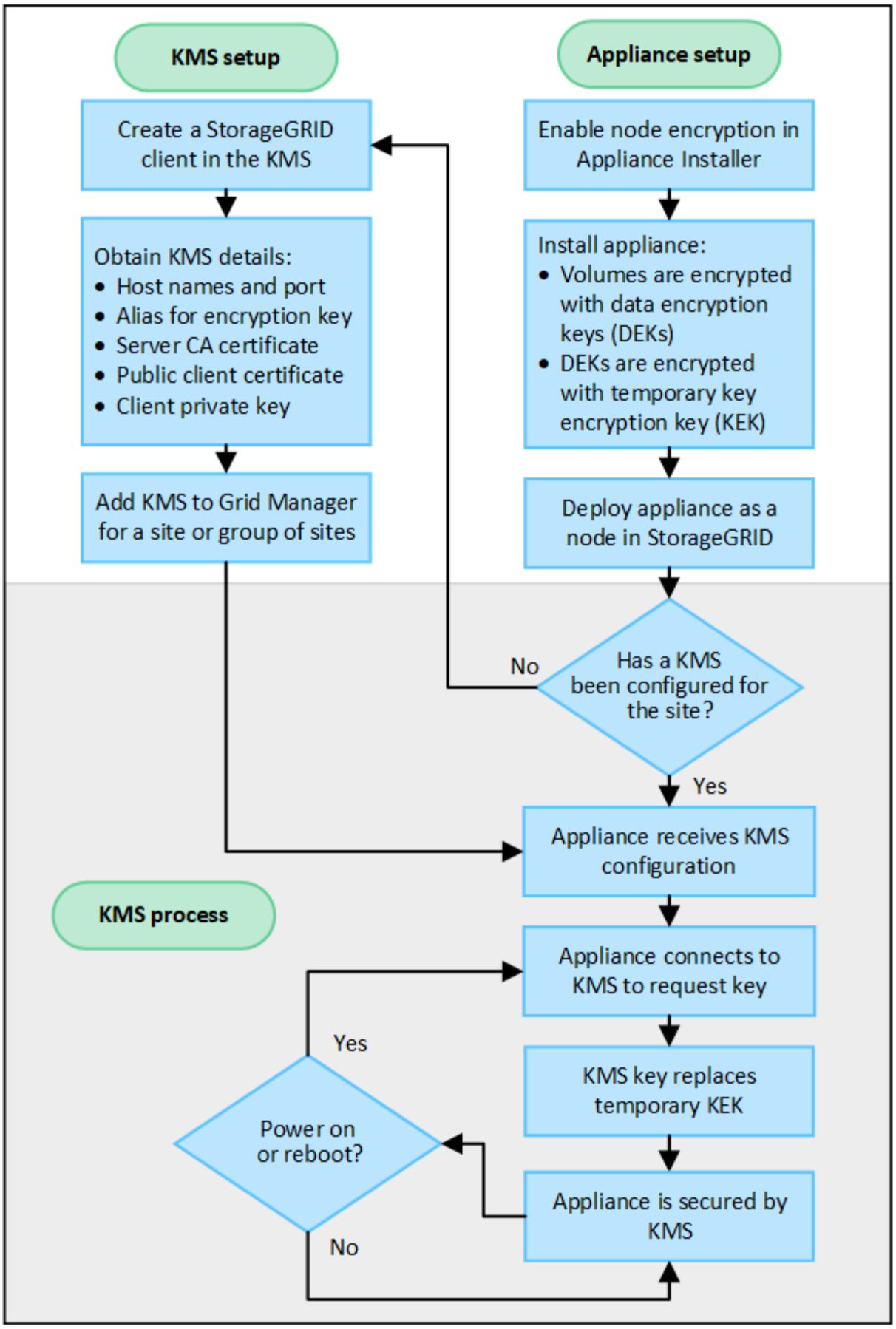
Puoi usare uno o più server di gestione delle chiavi per gestire le chiavi di crittografia dei nodi per qualsiasi nodo appliance StorageGRID che abbia l'impostazione **Crittografia nodo** abilitata durante l'installazione. Usare server di gestione delle chiavi con questi nodi appliance ti permette di proteggere i tuoi dati anche se un'appliance viene rimossa dal data center. Dopo che i volumi dell'appliance sono stati crittografati, non puoi accedere ai dati sull'appliance a meno che il nodo possa comunicare con il KMS.

> StorageGRID non crea né gestisce le chiavi esterne utilizzate per crittografare e decrittografare i nodi dell'appliance. Se vuoi usare un server di gestione delle chiavi esterno per proteggere i dati di StorageGRID, devi sapere come configurare quel server e come gestire le chiavi di crittografia. Eseguire attività di gestione delle chiavi non rientra in queste istruzioni. Se hai bisogno di aiuto, consulta la documentazione del tuo server di gestione delle chiavi o contatta il supporto tecnico.

StorageGRID configurazione del server e dell'appliance di gestione delle chiavi

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

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



${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

Passaggio	${post_edited_translations.segment}
Accedi al software KMS e aggiungi un client per StorageGRID a ciascun KMS o cluster KMS.	"Configura StorageGRID come client nel KMS"
Ottieni le informazioni necessarie per il client StorageGRID sul KMS.	"Configura StorageGRID come client nel KMS"
${post_edited_translations.segment}	"Aggiungi un server di gestione delle chiavi (KMS)"

Configura l'appliance

La configurazione di un nodo appliance per l'utilizzo con KMS include i seguenti high-level passaggi.

1. Durante la fase di configurazione hardware dell'installazione dell'appliance, usa StorageGRID Appliance Installer per abilitare l'impostazione **Node Encryption** per l'appliance.

   > Non puoi abilitare l'impostazione **Crittografia nodo** dopo che un appliance è stato aggiunto al grid, e non puoi usare la gestione delle chiavi esterne per gli appliance che non hanno la crittografia del nodo abilitata.

2. Esegui l'installer dell'appliance StorageGRID. Durante l'installazione, a ciascun volume dell'appliance viene assegnata una chiave di crittografia dei dati (DEK) casuale, 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 master (KEK). La KEK iniziale è una chiave temporanea che crittografa i DEK finché l'appliance non può connettersi al KMS.
3. Aggiungi il nodo dell'appliance a StorageGRID.

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

${post_edited_translations.segment}

La crittografia con gestione delle chiavi include i seguenti high-level passaggi che vengono eseguiti automaticamente.

1. Quando installi un dispositivo con crittografia del nodo 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 del KMS.
   - Se per il sito non è ancora stato configurato un KMS, i dati sull'appliance continuano a essere crittografati tramite la KEK temporanea finché non configuri un KMS per il sito e l'appliance riceve la configurazione del KMS.
2. ${post_edited_translations.segment}

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 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 sopravvive a un'interruzione di alimentazione o a un riavvio.

Requisiti e considerazioni relativi al server di gestione delle chiavi StorageGRID

${post_edited_translations.segment}

Quale versione di KMIP è supportata?

StorageGRID supporta KMIP versione 1.4.

"Specifiche del Key Management Interoperability Protocol Version 1.4"

Quali sono le considerazioni relative alla rete?

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

${post_edited_translations.segment}

Quali versioni di TLS sono supportate?

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

StorageGRID negozia il protocollo e la cifratura (TLS 1.2) o la suite di cifratura (TLS 1.3) con il KMS al momento della connessione. Per vedere quali versioni di protocollo e cifrature/suite di cifratura sono disponibili, consulta la `tlsOutbound` sezione dei criteri TLS e SSH attivi della grid (**Configurazione** > **Sicurezza Impostazioni di sicurezza**).

Quali appliance sono supportati?

Puoi usare un server di gestione delle chiavi (KMS) per gestire le chiavi di crittografia per qualsiasi StorageGRID appliance nella tua grid che abbia l'impostazione **Node Encryption** abilitata. Questa impostazione può essere abilitata solo durante la fase di configurazione hardware dell'installazione dell'appliance tramite StorageGRID Appliance Installer.

> Non puoi abilitare la crittografia dei nodi dopo che un appliance è stato aggiunto al grid e non puoi usare la gestione delle chiavi esterna per gli appliance che non hanno la crittografia dei nodi abilitata.

Puoi usare il KMS configurato per gli appliance e i nodi appliance di StorageGRID.

${post_edited_translations.segment}

- Nodi distribuiti come macchine virtuali (VM)
- ${post_edited_translations.segment}

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

Quando devo configurare i server di gestione delle chiavi?

Per una nuova installazione, di solito dovresti configurare uno o più server di gestione chiave in Grid Manager prima di creare i tenant. Questo ordine garantisce che i nodi siano protetti prima che venga memorizzato qualsiasi dato oggetto su di essi.

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

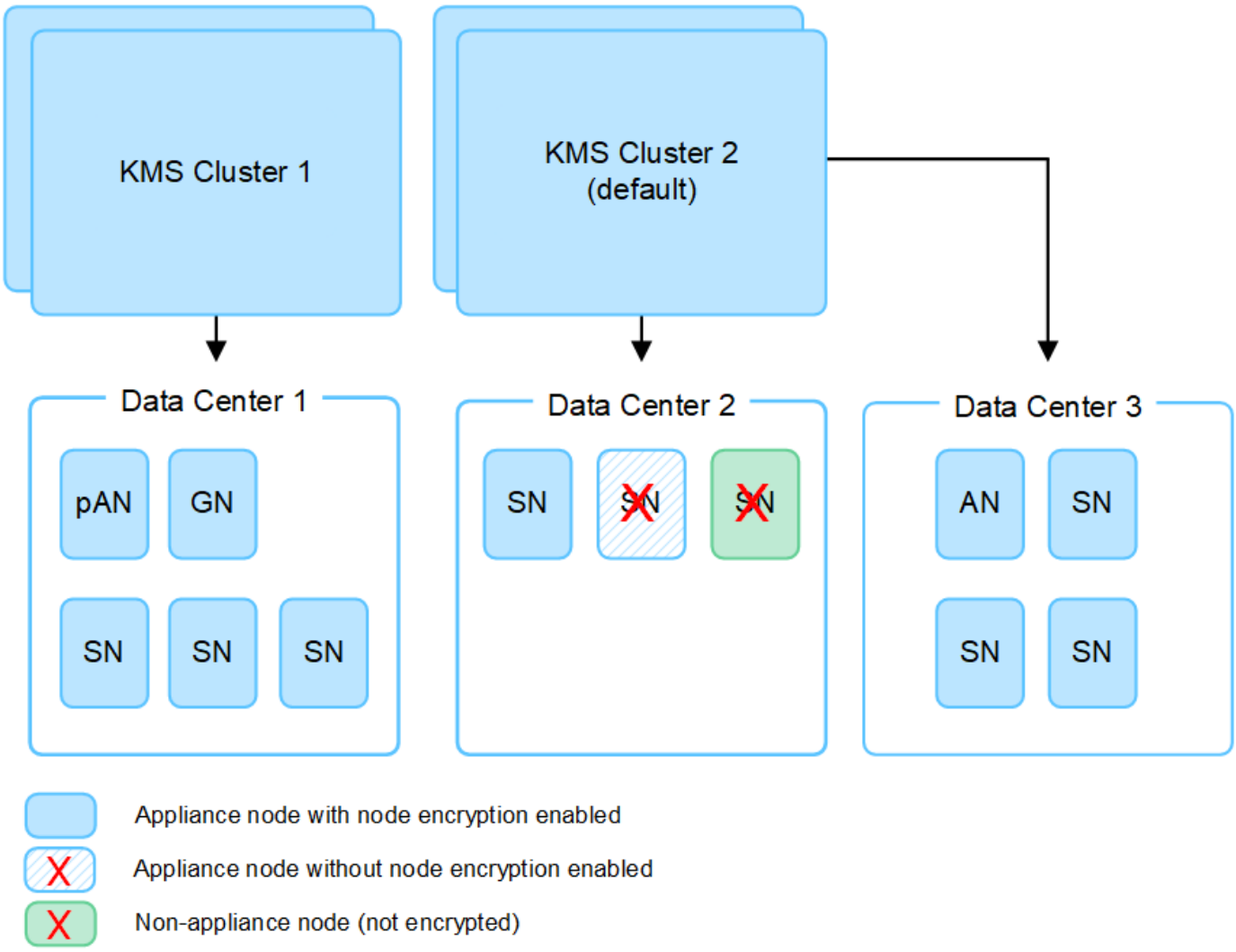
Di quanti server di gestione delle chiavi hai bisogno?

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

StorageGRID supporta l'uso di cluster KMS. Ciascun cluster KMS contiene più server di gestione delle chiavi replicati che condividono le impostazioni di configurazione e le chiavi di crittografia. L'uso di cluster KMS per la gestione delle chiavi è consigliato perché migliora le funzionalità di failover di una configurazione ad alta disponibilità.

Ad esempio, supponi che il tuo sistema StorageGRID abbia tre data center. Potresti configurare un cluster KMS per fornire una chiave a tutti i nodi appliance del Data Center 1 e un secondo cluster KMS per fornire una chiave a tutti i nodi appliance di tutti gli altri siti. Quando aggiungi il secondo cluster KMS, puoi configurare un KMS predefinito per il Data Center 2 e il Data Center 3.

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



Cosa succede quando ruoti una chiave?

Come best practice di sicurezza, dovresti "ruotare la chiave di crittografia" usata da ogni KMS configurato.

Quando è disponibile la nuova versione della chiave:

- Viene distribuita automaticamente ai nodi dell'appliance crittografata presso il sito o i 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, riceverà la nuova chiave non appena si riavvia.
- Se per qualsiasi motivo non puoi utilizzare la nuova versione della chiave per crittografare i volumi dell'appliance, viene attivato l'avviso **Rotazione della chiave di crittografia KMS non riuscita** per il nodo dell'appliance. Potresti dover contattare il supporto tecnico per risolvere questo avviso.

Posso riutilizzare un nodo dell'appliance dopo che è stato crittografato?

Se hai bisogno di installare un'appliance crittografata in un altro sistema StorageGRID, devi prima decommissionare il nodo grid per spostare i dati oggetto su un altro nodo. Quindi, puoi utilizzare StorageGRID Appliance Installer per "${post_edited_translations.segment}". La cancellazione della configurazione KMS disabilita l'impostazione **Node Encryption** 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 presenti sul dispositivo non sono più accessibili e sono bloccati in modo permanente.

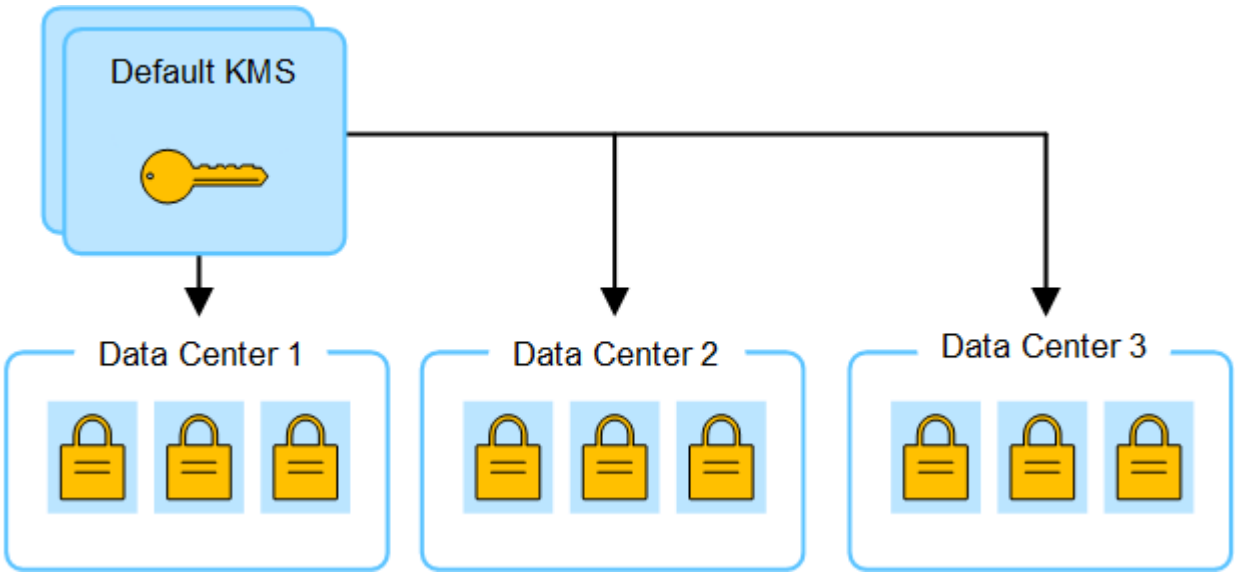
Considerazioni sulla modifica del KMS per un sito StorageGRID

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

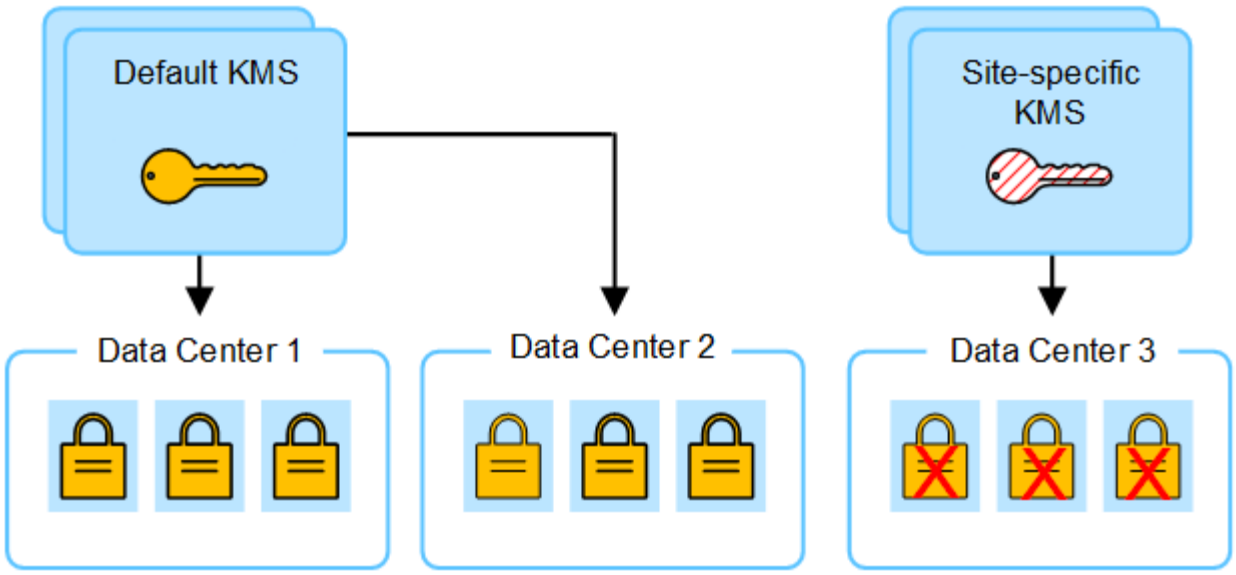
Se modifichi il KMS utilizzato per un sito, devi assicurarti che i nodi appliance precedentemente crittografati in quel sito possano essere decrittografati utilizzando la chiave memorizzata sul nuovo KMS. In alcuni casi, potrebbe essere necessario copiare la versione corrente della chiave di crittografia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

Ad esempio:

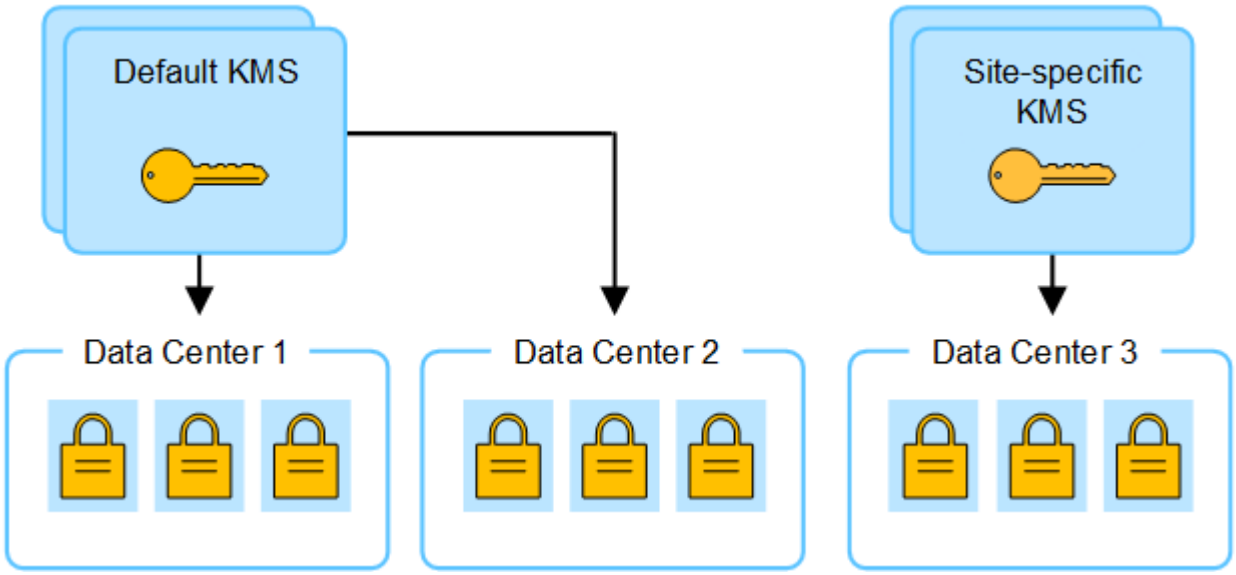
1. ${post_edited_translations.segment}
2. Quando il KMS viene salvato, tutti i nodi appliance che hanno l'impostazione **Node Encryption** abilitata si connettono al KMS e richiedono la chiave di crittografia. Questa chiave viene utilizzata per crittografare i nodi appliance in tutti i siti. Questa stessa chiave deve essere utilizzata anche per decrittografare tali appliance.



3. Decidi 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 tenti 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, copi la versione corrente della chiave di crittografia dal KMS predefinito al nuovo KMS. (Tecnicamente, copi 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 ha la chiave corretta per decrittografare i nodi dell'appliance nel Data Center 3, quindi può essere salvata in StorageGRID.



Casi d'uso per cambiare quale KMS viene utilizzato per un sito

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

Caso d'uso per la modifica del KMS di un sito	Passaggi necessari
Hai una o più voci KMS specifiche per il sito e vuoi usarne una come KMS predefinito.	Modifica il KMS specifico del sito. Nel campo **Gestisce le 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 hanno un KMS dedicato. "Modifica un server di gestione delle chiavi (KMS)"

Caso d'uso per la modifica del KMS di un sito	Passaggi necessari
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 nella nuova sede sono già stati crittografati dal KMS predefinito, usa il software KMS per copiare la versione corrente della chiave di crittografia dal KMS predefinito a un nuovo KMS. 2. Tramite Grid Manager, aggiungi il nuovo KMS e seleziona il sito. "Aggiungi un server di gestione delle chiavi (KMS)"
Vuoi che il KMS per un sito usi un server diverso.	1. Se i nodi dell'appliance presenti nel sito sono già stati crittografati dal KMS esistente, usa il software KMS per copiare la versione corrente della chiave di crittografia dal KMS esistente al nuovo KMS. 2. Tramite Grid Manager, modifica la configurazione KMS esistente e inserisci il nuovo host name o indirizzo IP. "Aggiungi un server di gestione delle chiavi (KMS)"

Configura StorageGRID come client nel KMS

Devi configurare StorageGRID come client per ogni 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, usa il "NetApp Interoperability Matrix Tool (IMT)".

Passaggi

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:
   - Utilizza la pagina di gestione delle chiavi del tuo prodotto KMS. Crea una chiave di crittografia AES per ogni KMS o cluster KMS.

     ${post_edited_translations.segment}

   - Fai creare la chiave a StorageGRID. Ti verrà richiesto quando esegui il test e salvi dopo "${post_edited_translations.segment}".
3. Annota le seguenti informazioni per ogni KMS o cluster KMS.

   ${post_edited_translations.segment}

   - ${post_edited_translations.segment}
   - Porta KMIP utilizzata dal KMS.
   - Alias della chiave per la chiave di crittografia nel KMS.

4. Per ogni KMS o cluster KMS, ottieni un certificato server firmato da un'autorità di certificazione (CA) o un pacchetto di certificati che contiene 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 con StorageGRID.

   - ${post_edited_translations.segment}
   - Il campo Subject Alternative Name (SAN) in ogni certificato server deve includere il fully qualified domain name (FQDN) o l'indirizzo IP a cui StorageGRID si connetterà.

     > Quando configuri il KMS in StorageGRID, devi inserire gli stessi FQDN o indirizzi IP nel campo **Hostname**.

   - ${post_edited_translations.segment}
5. ${post_edited_translations.segment}

   Il certificato client consente a StorageGRID di autenticarsi presso il KMS.

Aggiungi un server di gestione delle chiavi in StorageGRID

${post_edited_translations.segment}

Prima di iniziare

- Hai esaminato il "Considerazioni e requisiti per l'utilizzo di un key management server".
- Hai "configurato StorageGRID come client nel KMS" e hai le informazioni necessarie per ogni KMS o cluster KMS.
- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Permesso di accesso root".

Informazioni su questa attività

Se possibile, configura prima i server di gestione delle chiavi specifici del sito, prima di configurare un KMS predefinito che si applica a tutti i siti non gestiti da un altro KMS. Se crei prima il KMS predefinito, tutti gli appliance con crittografia dei nodi nella grid saranno crittografati dal KMS predefinito. Se vuoi creare un KMS specifico del sito in seguito, devi prima copiare la versione attuale della chiave di crittografia dal KMS predefinito al nuovo KMS. Vedi "Considerazioni sulla modifica del KMS per un sito" per i dettagli.

${post_edited_translations.segment}

Nel passaggio 1 (Dettagli KMS) della procedura guidata Aggiungi un Key Management Server, fornisci i dettagli relativi al KMS o al cluster KMS.

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Key management server**.

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

2. Seleziona **Create**.

   Viene visualizzato il passaggio 1 (dettagli KMS) della procedura guidata Add a Key Management Server.

3. Inserisci le seguenti informazioni per il KMS e il client StorageGRID che hai configurato in quel KMS.

Campo	Descrizione
Nome KMS	Un nome descrittivo che ti aiuti a identificare questo KMS. Deve essere compreso tra 1 e 64 caratteri.
Nome chiave	L'alias esatto della chiave per il client StorageGRID nel KMS. Deve essere compreso tra 1 e 255 caratteri. **Nota**: Se non hai creato una chiave utilizzando il tuo prodotto KMS, ti verrà richiesto di farla creare da StorageGRID.
Gestisce le chiavi per	Il sito StorageGRID che sarà associato a questo KMS. Se possibile, dovresti configurare i server di gestione delle chiavi specifici del sito prima di configurare un KMS predefinito da applicare a tutti i siti non gestiti da un altro KMS. • Seleziona 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 hanno un KMS dedicato e a tutti i siti che aggiungi nelle espansioni successive. **Nota:** Si verifica un errore di convalida quando salvi la configurazione KMS se selezioni un sito che era stato precedentemente crittografato dal KMS predefinito ma non hai fornito la versione corrente della chiave di crittografia originale al nuovo KMS.
Porta	La porta che il server KMS utilizza per le comunicazioni Key Management Interoperability Protocol (KMIP). Il valore predefinito è 5696, che è la porta standard KMIP.
Nome host	Il fully qualified domain name o l'indirizzo IP del KMS. **Nota:** il campo Subject Alternative Name (SAN) del certificato del server deve includere l'FQDN o l'indirizzo IP che inserisci qui. In caso contrario, StorageGRID non sarà in grado di connettersi al KMS o a tutti i server in un cluster KMS.

4. ${post_edited_translations.segment}
5. Seleziona **Continue**.

Passaggio 2: Carica il certificato del server

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

Passaggi

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

   Vengono visualizzati i metadati del certificato del server.

   ${post_edited_translations.segment}

3. Seleziona **Continue**.

Passaggio 3: Carica i certificati client

Nel passaggio 3 (Caricamento dei certificati client) della procedura guidata Aggiungi un Key Management Server, carichi il certificato client e la chiave privata del certificato client. Il certificato client consente a StorageGRID di autenticarsi presso il KMS.

Passaggi

1. Dal **Passaggio 3 (Carica i certificati client)**, vai alla posizione del certificato client.
2. ${post_edited_translations.segment}

   Vengono visualizzati i metadati del certificato client.

3. Vai alla posizione della chiave privata per il certificato client.
4. Carica il file della chiave privata.
5. Seleziona **Test and save**.

   Se la chiave non esiste, ti verrà chiesto di farne creare una a StorageGRID.

   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 Key Management Server.

   Subito dopo che aggiungi un KMS, lo stato del certificato nella pagina Key Management Server appare come "Sconosciuto". Potrebbero volerci fino a 30 minuti perché StorageGRID ottenga lo stato effettivo di ciascun certificato. Devi aggiornare il browser web per vedere lo stato attuale.

6. Se viene visualizzato un messaggio di errore quando selezioni **Verifica e salva**, controlla i dettagli del messaggio e poi seleziona **OK**.

   ${post_edited_translations.segment}

7. ${post_edited_translations.segment}

   Se selezioni **Force save** salvi la configurazione KMS, ma la connessione esterna da ciascuna appliance a quel KMS non viene testata. In caso di problemi con la configurazione, potresti non essere in grado di riavviare i nodi appliance che hanno la crittografia dei nodi abilitata nel sito interessato. Potresti perdere l'accesso ai dati fino alla risoluzione dei problemi.

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

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

Gestire un key management server in StorageGRID

${post_edited_translations.segment}

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "autorizzazione di accesso richiesta".

Visualizza i dettagli KMS

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

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Key management server**.

   ${post_edited_translations.segment}

   - La scheda Dettagli di configurazione elenca tutti i server di gestione delle chiavi configurati.
   - ${post_edited_translations.segment}

2. Per visualizzare i dettagli di un KMS specifico ed eseguire operazioni su tale KMS, seleziona il nome del KMS. La pagina dei dettagli del KMS elenca le seguenti informazioni:

Campo	Descrizione
Gestisce le chiavi per	Il sito StorageGRID associato al KMS. Questo campo visualizza il nome di uno specifico sito StorageGRID o **Siti non gestiti da un altro KMS (KMS predefinito).**
Nome host	Il fully qualified domain name o l'indirizzo IP del KMS. Se in un cluster ci sono due server di gestione delle chiavi, vengono elencati il fully qualified domain name o l'indirizzo IP di entrambi i server. Se in un cluster ci sono più di due server di gestione delle chiavi, vengono elencati il fully qualified domain name o l'indirizzo IP del primo KMS insieme al numero di server di gestione delle chiavi aggiuntivi presenti nel cluster. Ad esempio: `10.10.10.10 and 10.10.10.11` o `10.10.10.10 and 2 others`. ${post_edited_translations.segment}

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

Scheda	Campo	Descrizione
${post_edited_translations.segment}	Nome chiave	${post_edited_translations.segment}
UID chiave	L'identificativo univoco dell'ultima versione della chiave.	Ultima modifica
Data e ora dell'ultima versione della chiave.	Certificato del server	${post_edited_translations.segment}
${post_edited_translations.segment}	Certificato PEM	Il contenuto del file PEM (privacy enhanced mail) del certificato.
Certificato client	${post_edited_translations.segment}	${post_edited_translations.segment}

4. Con la frequenza richiesta dalle procedure di sicurezza della tua organizzazione, seleziona **Ruota chiave** o utilizza il software KMS per creare una nuova versione della chiave.

   Quando la rotazione delle chiavi ha esito positivo, i campi Key UID e Last modified vengono aggiornati.

> Se ruoti la chiave di crittografia utilizzando il software KMS, ruotala dall'ultima versione utilizzata a una nuova versione della stessa chiave. Non ruotare verso una chiave completamente diversa.
>
> Non tentare mai di ruotare una chiave modificandone il nome (alias) per il KMS. StorageGRID richiede che tutte le versioni di chiave utilizzate in precedenza (così come quelle future) siano accessibili dal KMS con lo stesso alias di chiave. Se cambi l'alias della chiave per un KMS configurato, StorageGRID potrebbe non riuscire a decrittografare i tuoi dati.

Gestisci i certificati

Risolvete tempestivamente qualsiasi problema relativo ai certificati del server o del client. Se possibile, sostituisci i certificati prima della loro scadenza.

> Devi risolvere al più presto eventuali problemi relativi ai certificati per mantenere l'accesso ai dati.

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Key management server**.
2. Nella tabella, osserva il valore di scadenza del certificato per ciascun KMS.
3. Se la data di scadenza del certificato per qualsiasi KMS è sconosciuta, attendi fino a 30 minuti e poi aggiorna il browser web.

4. Se la colonna Scadenza certificato indica che un certificato è scaduto o sta per scadere, seleziona il KMS per andare alla pagina dei dettagli del KMS.
   a. Seleziona **Certificato server** e verifica il valore per il campo "Scade il".
   b. ${post_edited_translations.segment}
   c. Ripeti questi passaggi secondari e seleziona **Certificato client** invece di Certificato server.
5. Quando vengono attivati gli avvisi **Scadenza del certificato CA KMS**, **Scadenza del certificato client KMS** e **Scadenza del certificato server KMS**, prendi nota della descrizione di ciascun avviso ed esegui le azioni consigliate.

   Potrebbero essere necessari fino a 30 minuti perché StorageGRID aggiorni la scadenza del certificato. Aggiorna il browser web per vedere i valori attuali.

> Se viene visualizzato lo stato **Stato del certificato del server sconosciuto**, assicurati che il KMS consenta di ottenere un certificato server senza richiedere un certificato client.

Visualizza i nodi crittografati

Puoi visualizzare le informazioni sui nodi dell'appliance nel tuo sistema StorageGRID che hanno l'impostazione **Crittografia nodo** abilitata.

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Key management server**.

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

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

   La scheda Nodi crittografati elenca i nodi dell'appliance nel tuo sistema StorageGRID che hanno l'impostazione **Crittografia nodo** abilitata.

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

Colonna	Descrizione
Nome nodo	Il nome del nodo dell'appliance.
Tipo di nodo	${post_edited_translations.segment}
Sito	Il nome del sito StorageGRID in cui è installato il nodo.
Nome KMS	Il nome descrittivo del KMS utilizzato per il nodo. Se non è presente alcun KMS nell'elenco, seleziona la scheda Dettagli di configurazione per aggiungere un KMS. "Aggiungi un server di gestione delle chiavi (KMS)"

Colonna	Descrizione
UID chiave	L'ID univoco della chiave di crittografia utilizzata per crittografare e decrittografare i dati sul nodo dell'appliance. Per visualizzare l'intero UID della chiave, seleziona il testo. ${post_edited_translations.segment}
Stato	Lo stato della connessione tra il KMS e il nodo appliance. Se il nodo è connesso, il timestamp si aggiorna ogni 30 minuti. Possono volerci diversi minuti prima che lo stato della connessione si aggiorni dopo una modifica della configurazione del KMS. **Nota:** Aggiorna il browser web per visualizzare i nuovi valori.

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

   Durante il normale funzionamento di KMS, lo stato sarà **Connesso a KMS**. Se un nodo viene disconnesso dalla grid, viene visualizzato lo stato di connessione del nodo (Administratively Down o Unknown).

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

   - Impossibile caricare la configurazione KMS
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - La chiave KMS non è riuscita a decrittografare un volume dell'appliance
   - ${post_edited_translations.segment}

   Esegui le azioni consigliate per questi avvisi.

${post_edited_translations.segment}

Modifica un KMS

Potresti dover modificare la configurazione di un server di gestione delle chiavi, ad esempio se un certificato sta per scadere.

Prima di iniziare

- Se pianifichi di aggiornare il sito selezionato per un KMS, hai esaminato "considerazioni per la modifica del KMS per un sito".
- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Permesso di accesso root".

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Key management server**.

   Viene visualizzata la pagina del key management server, che mostra tutti i key management server configurati.

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

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

3. Facoltativamente, aggiorna i dettagli in **Passaggio 1 (Dettagli KMS)** della procedura guidata Modifica un Key Management Server.

Campo	Descrizione
Nome KMS	Un nome descrittivo che ti aiuti a identificare questo KMS. Deve essere compreso tra 1 e 64 caratteri.
Nome chiave	L'alias esatto della chiave per il client StorageGRID nel KMS. Deve essere compreso tra 1 e 255 caratteri. Devi modificare il nome della chiave solo in rari casi. Ad esempio, devi modificare il nome della chiave se l'alias viene rinominato nel KMS o se tutte le versioni della chiave precedente sono state copiate nella cronologia delle versioni del nuovo alias.
Gestisce le chiavi per	Se stai modificando un KMS specifico per il sito e non disponi già di un KMS predefinito, seleziona facoltativamente **Siti non gestiti da un altro KMS (KMS predefinito)**. Questa selezione converte un KMS specifico per il sito nel KMS predefinito, che si applicherà a tutti i siti che non hanno un KMS dedicato e a tutti i siti aggiunti in un'espansione. **Nota:** se stai modificando un KMS specifico del sito, non puoi selezionare un altro sito. Se stai modificando il KMS predefinito, non puoi selezionare un sito specifico.
Porta	La porta che il server KMS utilizza per le comunicazioni Key Management Interoperability Protocol (KMIP). Il valore predefinito è 5696, che è la porta standard KMIP.
Nome host	Il fully qualified domain name o l'indirizzo IP del KMS. **Nota:** il campo Subject Alternative Name (SAN) del certificato del server deve includere l'FQDN o l'indirizzo IP che inserisci qui. In caso contrario, StorageGRID non sarà in grado di connettersi al KMS o a tutti i server in un cluster KMS.

4. ${post_edited_translations.segment}
5. Seleziona **Continue**.

   ${post_edited_translations.segment}

6. Se devi sostituire il certificato del server, seleziona **Sfoglia** e carica il nuovo file.
7. Seleziona **Continue**.

   Viene visualizzato il passaggio 3 (Caricamento dei certificati client) della procedura guidata Modifica un Key Management Server.

8. Se devi sostituire il certificato client e la chiave privata del certificato client, seleziona **Sfoglia** e carica i nuovi file.
9. Seleziona **Test and save**.

   Le connessioni tra il key management server e tutti i nodi appliance con crittografia dei nodi nei siti interessati vengono testate. Se tutte le connessioni dei nodi sono valide e sul KMS viene trovata la chiave corretta, il key management server viene aggiunto alla tabella nella pagina Key Management Server.

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

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

11. Se devi salvare la configurazione corrente prima di risolvere gli errori di connessione, seleziona **Forza salvataggio**.

    > Se selezioni **Force save** salvi la configurazione KMS, ma la connessione esterna da ciascuna appliance a quel KMS non viene testata. In caso di problemi con la configurazione, potresti non essere in grado di riavviare i nodi appliance che hanno la crittografia dei nodi abilitata nel sito interessato. Potresti perdere l'accesso ai dati fino alla risoluzione dei problemi.

    La configurazione KMS è salvata.

12. Esamina 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.

${post_edited_translations.segment}

In alcuni casi, potresti voler rimuovere un server di gestione delle chiavi. Ad esempio, potresti voler rimuovere un KMS specifico del sito se hai disattivato il sito.

Prima di iniziare

- Hai esaminato il "Considerazioni e requisiti per l'utilizzo di un key management server".
- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Permesso di accesso root".

Informazioni su questa attività

Puoi rimuovere un KMS in questi casi:

- Puoi rimuovere un KMS specifico del sito se il sito è stato dismesso o se non include nodi appliance con la crittografia del nodo abilitata.
- ${post_edited_translations.segment}

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Key management server**.

   Viene visualizzata la pagina del key management server, che mostra tutti i key management server configurati.

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

   Puoi anche 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:
   - Stai rimuovendo un KMS specifico per un sito che non ha alcun nodo appliance con la crittografia del nodo abilitata.
   - Stai rimuovendo il KMS predefinito, ma esiste già un KMS specifico per ogni sito con crittografia del nodo.
4. Seleziona **Sì**.

   La configurazione KMS è stata rimossa.

Informazioni sul copyright

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

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

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ 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 CONSEQUENZIALE (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.