Gestisci la sicurezza

StorageGRID software

NetApp
July 23, 2026

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

Sommario

Gestisci la sicurezza

Gestisci la sicurezza in StorageGRID

Puoi configurare diverse impostazioni di sicurezza dal Grid Manager per aiutare a proteggere il tuo sistema StorageGRID.

Gestisci la crittografia

StorageGRID offre diverse opzioni per la crittografia dei dati. Dovresti "esamina i metodi di crittografia disponibili" per determinare quali soddisfano i tuoi requisiti di protezione dei dati.

Gestisci i certificati

Puoi "configurare e gestire i certificati del server" utilizzare per le connessioni HTTP o i certificati client usati per autenticare l'identità di un client o di un utente presso il server.

Configura i server di gestione delle chiavi

L'utilizzo di un "server di gestione delle chiavi" ti permette di proteggere i dati di StorageGRID anche se un'appliance viene rimossa dal data center. Dopo che i volumi dell'appliance sono stati crittografati, non puoi accedere a nessun dato sull'appliance a meno che il nodo possa comunicare con il KMS.

> Per utilizzare la gestione delle chiavi di crittografia, devi abilitare l'impostazione **Crittografia nodo** per ogni appliance durante l'installazione, prima che l'appliance venga aggiunta al grid.

Gestisci le impostazioni proxy

Se utilizzi i servizi della piattaforma S3 o i Cloud Storage Pools, puoi configurare un "storage proxy server" tra i nodi di storage e gli endpoint S3 esterni. Se invii pacchetti AutoSupport tramite HTTPS o HTTP, puoi configurare un "proxy server di amministrazione" tra i nodi di amministrazione e il supporto tecnico.

Controlla i firewall

Per migliorare la sicurezza del tuo sistema, puoi controllare l'accesso ai nodi di amministrazione StorageGRID aprendo o chiudendo porte specifiche al "firewall esterno". Puoi anche controllare l'accesso di rete a ciascun nodo configurando il suo "firewall interno". Puoi impedire l'accesso a tutte le porte tranne quelle necessarie per la tua distribuzione.

Esamina i metodi di crittografia di StorageGRID

StorageGRID offre diverse opzioni per la crittografia dei dati. Dovresti esaminare i metodi disponibili per capire quali soddisfano i tuoi requisiti di protezione dei dati.

La tabella fornisce una panoramica high-level dei metodi di crittografia disponibili in StorageGRID.

Opzione di crittografia	Come funziona	Si applica a
Server di gestione delle chiavi (KMS) in Grid Manager	Tu "configurare un server di gestione delle chiavi" per il sito StorageGRID e "abilita la crittografia del nodo per l'appliance". Poi, un nodo appliance si connette al KMS per richiedere una key encryption key (KEK). Questa chiave crittografa e decrittografa la data encryption key (DEK) su ogni volume.	Nodi appliance con **Node Encryption** abilitata durante l'installazione. Tutti i dati sull'appliance sono protetti contro la perdita fisica o la rimozione dal data center. **Nota**: La gestione delle chiavi di crittografia con un KMS è supportata solo per i nodi di archiviazione e i servizi appliance.
Pagina di crittografia delle unità in StorageGRID Appliance Installer	Se l'appliance contiene unità che supportano la crittografia hardware, puoi impostare una passphrase per l'unità durante l'installazione. Quando imposti una passphrase per l'unità, è impossibile per chiunque recuperare dati validi dalle unità rimosse dal sistema, a meno che non conosca la passphrase. Prima di iniziare l'installazione, vai su **Configura hardware** > **Crittografia unità** per impostare una passphrase che si applica a tutte le unità autocrittografanti gestite da StorageGRID in un nodo.	Dispositivi dotati di unità a crittografia automatica. Tutti i dati presenti sulle unità protette sono al riparo da smarrimento fisico o rimozione dal data center. La crittografia delle unità non si applica alle unità gestite da SANtricity. Se hai un appliance di storage con unità a crittografia automatica e controller SANtricity, puoi abilitare la sicurezza delle unità in SANtricity.
Sicurezza dei dischi in SANtricity System Manager	Se la funzionalità Drive Security è abilitata per il tuo appliance StorageGRID, puoi usare "SANtricity System Manager" per creare e gestire la chiave di sicurezza. La chiave è necessaria per accedere ai dati sulle unità protette.	Dispositivi di archiviazione dotati di unità con crittografia completa del disco (FDE) o unità a crittografia automatica. Tutti i dati presenti sulle unità protette sono al riparo da perdita fisica o rimozione dal data center. Non può essere utilizzato con alcuni dispositivi di archiviazione o con qualsiasi dispositivo di servizio.
${post_edited_translations.segment}	Abiliti l'opzione "${post_edited_translations.segment}" nel Grid Manager. Quando è abilitata, tutti i nuovi oggetti che non sono crittografati a livello di bucket o a livello di oggetto vengono crittografati durante l'ingestione.	Dati degli oggetti S3 appena acquisiti. Gli oggetti già memorizzati non sono crittografati. I metadati degli oggetti e altri dati sensibili non sono crittografati.

Opzione di crittografia	Come funziona	Si applica a
crittografia del bucket S3	Invii una richiesta PutBucketEncryption per abilitare la crittografia per il bucket. Tutti i nuovi oggetti che non sono crittografati a livello di oggetto vengono crittografati durante l'ingestione.	Solo dati di oggetti S3 appena acquisiti. È necessario specificare la crittografia per il bucket. Gli oggetti del bucket esistenti non vengono crittografati. I metadati degli oggetti e altri dati sensibili non vengono crittografati. "Operazioni sui bucket"
Crittografia lato server (SSE) degli oggetti S3	Invii una richiesta S3 per memorizzare un oggetto e includi l'`x-amz-server-side-encryption`intestazione della richiesta.	Solo dati di oggetti S3 appena acquisiti. È necessario specificare la crittografia per l'oggetto. I metadati dell'oggetto e altri dati sensibili non vengono crittografati. StorageGRID gestisce le chiavi. "${post_edited_translations.segment}"
Crittografia lato server degli oggetti S3 con chiavi fornite dal cliente (SSE-C)	Invii una richiesta S3 per memorizzare un oggetto e includi tre intestazioni di richiesta. • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	Solo dati di oggetti S3 appena acquisiti. È necessario specificare la crittografia per l'oggetto. I metadati dell'oggetto e altri dati sensibili non vengono crittografati. Le chiavi sono gestite al di fuori di StorageGRID. "${post_edited_translations.segment}"
Crittografia di volumi o datastore esterni	Utilizzi un metodo di crittografia esterno a StorageGRID per crittografare un intero volume o datastore, se la tua piattaforma di distribuzione lo supporta.	Tutti i dati degli oggetti, i metadati e i dati di configurazione del sistema, assumendo che ogni volume o datastore sia crittografato. 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.

Opzione di crittografia	Come funziona	Si applica a
Crittografia degli oggetti al di fuori di StorageGRID	Utilizzi un metodo di crittografia esterno a StorageGRID per crittografare i dati degli oggetti e i metadati prima che vengano importati in StorageGRID.	Solo i dati e i metadati degli oggetti (i dati di configurazione del sistema non sono crittografati). 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. "Amazon Simple Storage Service - Guida per l'utente: Protezione dei dati tramite crittografia lato client"

Usa più metodi di crittografia

A seconda delle tue esigenze, puoi usare più di un metodo di crittografia contemporaneamente. Ad esempio:

- Puoi usare un KMS per proteggere i nodi dell'appliance e anche la funzionalità di sicurezza delle unità in SANtricity System Manager per "crittografare due volte" i dati sulle unità a crittografia automatica presenti nelle stesse appliance.
- Puoi usare un KMS per proteggere i dati sui nodi dell'appliance e anche l'opzione Stored object encryption per crittografare tutti gli oggetti quando vengono acquisiti.

Se solo una piccola parte dei tuoi oggetti richiede la crittografia, valuta la possibilità di controllare la crittografia a livello di bucket o di singolo oggetto. L'attivazione di più livelli di crittografia comporta un costo aggiuntivo in termini di prestazioni.

Informazioni correlate

"Scopri le opzioni di crittografia certificate FIPS"

Gestisci i certificati

Gestisci i certificati di sicurezza in StorageGRID

${post_edited_translations.segment}

${post_edited_translations.segment}

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

Quando un client si connette al server tramite HTTPS, il server risponde con il certificato del server, che contiene una chiave pubblica. Il client confronta la firma del server con la firma sulla propria copia del certificato. Se le firme corrispondono, il client avvia una sessione con il server utilizzando la stessa chiave

pubblica.

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

${post_edited_translations.segment}

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

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

- ${post_edited_translations.segment}
- Tutti i certificati personalizzati devono soddisfare i "Linee guida per l'hardening del sistema per i certificati server".
- ${post_edited_translations.segment}

> StorageGRID include anche certificati CA del sistema operativo che sono uguali su tutti i grid. In ambienti di produzione, assicurati di specificare un certificato personalizzato firmato da un'autorità di certificazione esterna al posto del certificato CA del sistema operativo.

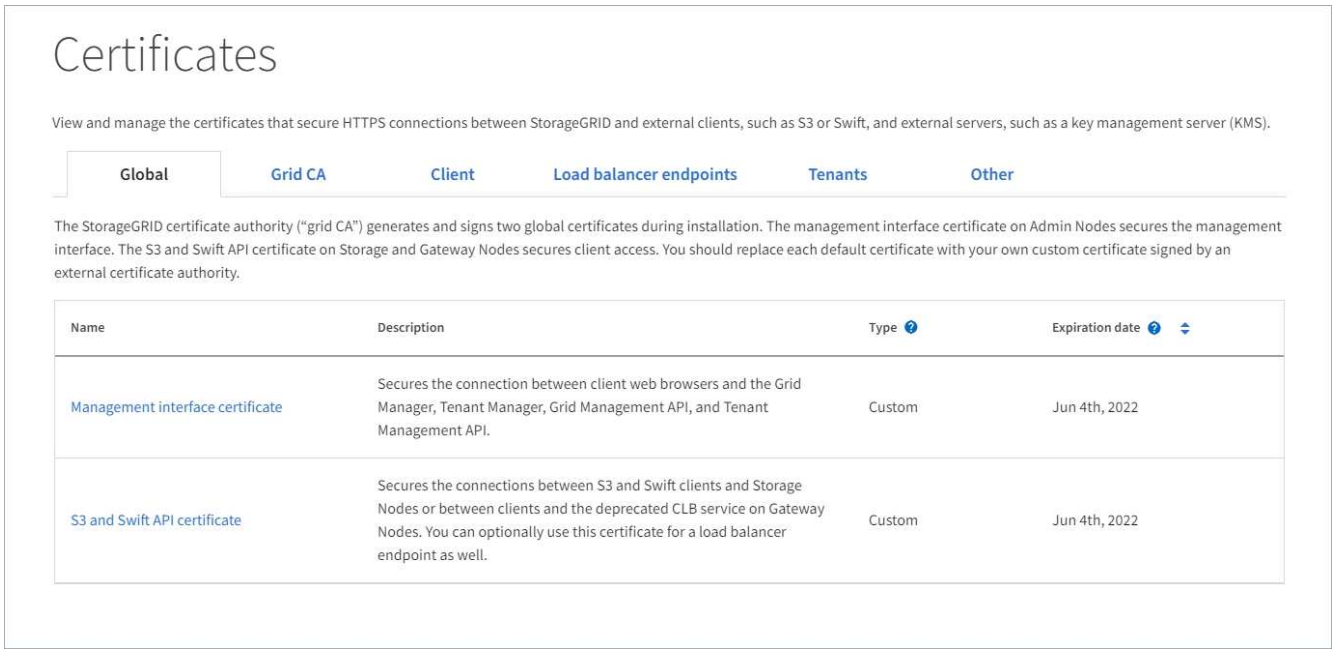
Le varianti dei tipi di certificati server e client vengono implementate in diversi modi. Dovresti avere pronti tutti i certificati necessari per la tua specifica configurazione di StorageGRID prima di configurare il sistema.

Certificati di sicurezza di accesso

Puoi accedere alle informazioni su tutti i certificati StorageGRID in un'unica posizione, insieme ai collegamenti al flusso di lavoro di configurazione per ciascun certificato.

Passaggi

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



2. Seleziona una scheda nella pagina Certificati per informazioni su ciascuna categoria di certificati e per accedere alle impostazioni del certificato. Puoi accedere a una scheda se hai la "${post_edited_translations.segment}".

   - **Globale**: Protegge l'accesso a StorageGRID da browser web e client API esterni.
   - **Grid CA**: Protegge il traffico interno di StorageGRID.
   - **Client**: Protegge le connessioni tra i client esterni e il database StorageGRID Prometheus.
   - **Endpoint del bilanciatore di carico**: Protegge le connessioni tra i client S3 e il Load Balancer di StorageGRID.
   - ${post_edited_translations.segment}
   - **Altro**: Protegge le connessioni StorageGRID che richiedono certificati specifici.

     ${post_edited_translations.segment}

Globale

I certificati globali proteggono l'accesso a StorageGRID dai browser web e dai client API S3 esterni. Durante l'installazione, l'autorità di certificazione di StorageGRID genera inizialmente due certificati globali. La best practice per un ambiente di produzione è utilizzare certificati personalizzati firmati da un'autorità di certificazione esterna.

- <<${post_edited_translations.segment}>>: Protegge le connessioni del browser web del client alle interfacce di gestione di StorageGRID.
- Certificato API S3: protegge le connessioni API client a Storage Node, Admin Node e Gateway Node, utilizzate dalle applicazioni client S3 per caricare e scaricare i dati oggetto.

Le informazioni relative ai certificati globali installati includono:

- **Nome**: Nome del certificato con link per gestire il certificato.
- **Descrizione**
- **Tipo**: Personalizzato o predefinito. + Dovresti sempre usare un certificato personalizzato per migliorare la sicurezza della grid.
- ${post_edited_translations.segment}

Puoi:

- ${post_edited_translations.segment}
  - "Sostituisci il certificato dell'interfaccia di gestione predefinito generato da StorageGRID" utilizzato per le connessioni di Grid Manager e Tenant Manager.
  - "Sostituisci il certificato API S3" utilizzato per le connessioni dello Storage Node e dell'endpoint del bilanciatore di carico (opzionale).
- "Ripristina il certificato predefinito dell'interfaccia di gestione".
- "${post_edited_translations.segment}".
- "${post_edited_translations.segment}".
- Copia o scarica il "${post_edited_translations.segment}" o "Certificato API S3".

${post_edited_translations.segment}

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

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

Puoi "${post_edited_translations.segment}" farlo, ma non puoi cambiarlo.

${post_edited_translations.segment}

Certificati client, generati da un'autorità di certificazione esterna, proteggono le connessioni tra gli strumenti di monitoraggio esterni e il database Prometheus di StorageGRID.

La tabella dei certificati contiene una riga per ogni certificato client configurato e indica se il certificato può essere utilizzato per accedere al database di Prometheus, insieme alla data di scadenza del certificato.

Puoi:

- "${post_edited_translations.segment}"
- Seleziona il nome di un certificato per visualizzare i dettagli del certificato, dove puoi:
  - "Modifica il nome del certificato client."
  - "Imposta le autorizzazioni di accesso a Prometheus."
  - "Carica e sostituisci il certificato client."
  - "Copia o scarica il certificato client."
  - "${post_edited_translations.segment}"
- Seleziona **Azioni** per "modifica", "allegare" o "rimuovi" rapidamente un certificato client. Puoi selezionare fino a 10 certificati client e rimuoverli contemporaneamente utilizzando **Azioni** > **Rimuovi**.

${post_edited_translations.segment}

<<${post_edited_translations.segment},Certificati endpoint del load balancer>>Proteggi le connessioni tra i client S3 e il servizio StorageGRID Load Balancer sui Gateway Nodes e Admin Nodes.

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

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

Puoi:

- "Visualizza un endpoint del bilanciatore di carico", inclusi i dettagli del relativo certificato.
- "Specifica un certificato dell'endpoint del bilanciatore del carico per FabricPool."
- "Usa il certificato API S3 globale" invece di generare un nuovo certificato per l'endpoint del bilanciatore di carico.

Tenant

I tenant possono utilizzare certificati del server di federazione delle identità o ${post_edited_translations.segment} per proteggere le proprie connessioni con StorageGRID.

La tabella dei tenant contiene una riga per ciascun tenant e indica se ogni tenant ha l'autorizzazione a utilizzare la propria fonte di identità o i servizi della piattaforma.

Puoi:

- "Seleziona un nome tenant per accedere al Tenant Manager"
- "Seleziona un nome tenant per visualizzare i dettagli della federazione delle identità del tenant"
- "Seleziona un nome tenant per visualizzare i dettagli dei servizi della piattaforma del tenant"
- "${post_edited_translations.segment}"

Altro

StorageGRID utilizza altri certificati di sicurezza per scopi specifici. Questi certificati sono elencati in base alla loro funzione. Altri certificati di sicurezza includono:

- Certificati del Cloud Storage Pool
- Certificati di notifica degli avvisi email
- Certificati del server syslog esterno
- Certificati di connessione alla grid federation
- Certificati di federazione delle identità
- <<${post_edited_translations.segment},Certificati del server di gestione delle chiavi (KMS)>>
- Certificati di single sign-on

Le informazioni indicano il tipo di certificato che una funzione utilizza e le date di scadenza del certificato server e client, se applicabile. Se selezioni il nome di una funzione, si apre una scheda del browser dove puoi visualizzare e modificare i dettagli del certificato.

> Puoi visualizzare e accedere alle informazioni relative ad altri certificati solo se hai la "${post_edited_translations.segment}".

Puoi:

- "Specifica un certificato Cloud Storage Pool per S3, C2S S3 o Azure"
- "Specifica un certificato per le notifiche email di avviso"
- "Usa un certificato per un server syslog esterno"
- "${post_edited_translations.segment}"
- "Visualizza e modifica un certificato di federazione delle identità"
- "Carica i certificati del server e del client del server di gestione delle chiavi (KMS)"
- "Specifica manualmente un certificato SSO per un trust della relying party"

Dettagli del certificato di sicurezza

Ciascun tipo di certificato di sicurezza è descritto di seguito, con link alle istruzioni per l'implementazione.

${post_edited_translations.segment}

Tipo di certificato	Descrizione	${post_edited_translations.segment}	Dettagli
Server	Autentica la connessione tra i browser web dei client e l'interfaccia di gestione di StorageGRID, consentendo agli utenti di accedere a Grid Manager e Tenant Manager senza avvisi di sicurezza. ${post_edited_translations.segment} Puoi usare il certificato predefinito creato durante l'installazione oppure caricare un certificato personalizzato.	${post_edited_translations.segment}	"${post_edited_translations.segment}"

Certificato API S3

Tipo di certificato	Descrizione	${post_edited_translations.segment}	Dettagli
Server	${post_edited_translations.segment}	**Configurazione** > **Sicurezza** > **Certificati**, seleziona la scheda **Globale** e poi seleziona **Certificato API S3**	"Configura i certificati API S3"

Certificato CA Grid

Vedi la Descrizione del certificato CA Grid predefinito.

certificato client amministratore

Tipo di certificato	Descrizione	${post_edited_translations.segment}	Dettagli
${post_edited_translations.segment}	${post_edited_translations.segment} • Consente ai client esterni autorizzati di accedere al database Prometheus di StorageGRID. • Consente il monitoraggio sicuro di StorageGRID tramite strumenti esterni.	**Configurazione** > **Sicurezza** > **Certificati** e poi seleziona la scheda **Client**	"Configura i certificati client"

${post_edited_translations.segment}

Tipo di certificato	Descrizione	${post_edited_translations.segment}	Dettagli
Server	Autentica la connessione tra i client S3 e il servizio Load Balancer di StorageGRID sui nodi Gateway e sui nodi Admin. Puoi caricare o generare un certificato del load balancer quando configuri un endpoint del load balancer. Le applicazioni client utilizzano il certificato del load balancer durante la connessione a StorageGRID per salvare e recuperare i dati degli oggetti. Puoi anche usare una versione personalizzata del Certificato API S3 certificato globale per autenticare le connessioni al servizio Load Balancer. Se usi il certificato globale per autenticare le connessioni al Load Balancer, non devi caricare o generare un certificato separato per ogni endpoint del Load Balancer. ${post_edited_translations.segment}	**Configurazione** > **Rete** > **Endpoint del bilanciatore di carico**	• "${post_edited_translations.segment}" • "Crea un endpoint del bilanciatore di carico per FabricPool"

Certificato endpoint di Cloud Storage Pool

Tipo di certificato	Descrizione	${post_edited_translations.segment}	Dettagli
Server	Autentica la connessione da un StorageGRID Cloud Storage Pool a una posizione di archiviazione esterna, come S3 Glacier o Microsoft Azure Blob storage. È necessario un certificato diverso per ogni tipo di cloud provider.	**ILM** > **Pool di storage**	"${post_edited_translations.segment}"

Certificato di notifica di avviso email

Tipo di certificato	Descrizione	${post_edited_translations.segment}	Dettagli
Server e client	Autentica la connessione tra un server email SMTP e StorageGRID che viene utilizzato per le notifiche di avviso. • Se la comunicazione con il server SMTP richiede Transport Layer Security (TLS), devi specificare il certificato CA del server email. • ${post_edited_translations.segment}	**Avvisi** > **Configurazione email**	"${post_edited_translations.segment}"

Certificato del server syslog esterno

Tipo di certificato	Descrizione	${post_edited_translations.segment}	Dettagli
Server	${post_edited_translations.segment} **Nota:** Un certificato per server syslog esterno non è richiesto per le connessioni TCP, RELP/TCP e UDP a un server syslog esterno.	**Configurazione** > **Monitoraggio** > **Audit and syslog server**	"Usa un server syslog esterno"

${post_edited_translations.segment}

Tipo di certificato	Descrizione	${post_edited_translations.segment}	Dettagli
Server e client	Autentica e crittografa le informazioni inviate tra il sistema StorageGRID corrente e un'altra grid in una connessione di federazione di grid.	${post_edited_translations.segment}	• "Crea connessioni di federazione della griglia" • "Ruota i certificati di connessione"

Certificato di federazione dell'identità

Tipo di certificato	Descrizione	${post_edited_translations.segment}	Dettagli
Server	Autentica la connessione tra StorageGRID e un provider di identità esterno, come Active Directory, OpenLDAP o Oracle Directory Server. Utilizzato per la federazione delle identità, che consente la gestione dei gruppi di amministratori e degli utenti da parte di un sistema esterno.	${post_edited_translations.segment}	"${post_edited_translations.segment}"

${post_edited_translations.segment}

Tipo di certificato	Descrizione	${post_edited_translations.segment}	Dettagli
Server e client	Autentica la connessione tra StorageGRID e un server di gestione delle chiavi (KMS) esterno, che fornisce le chiavi di crittografia ai nodi dell'appliance StorageGRID.	${post_edited_translations.segment}	"${post_edited_translations.segment}"

Certificato endpoint dei servizi della piattaforma

Tipo di certificato	Descrizione	${post_edited_translations.segment}	Dettagli
Server	${post_edited_translations.segment}	**Tenant Manager** > **STORAGE (S3)** > **Endpoint dei servizi della piattaforma**	"Crea un endpoint per i servizi della piattaforma" "${post_edited_translations.segment}"

Certificato di single sign-on (SSO)

Tipo di certificato	Descrizione	${post_edited_translations.segment}	Dettagli
Server	Autentica la connessione tra i servizi di federazione delle identità, come Active Directory Federation Services (AD FS), e StorageGRID che vengono utilizzati per le richieste di single sign-on (SSO).	${post_edited_translations.segment}	"Configura single sign-on"

${post_edited_translations.segment}

Esempio 1: Servizio di bilanciamento del carico

${post_edited_translations.segment}

1. ${post_edited_translations.segment}
2. Configuri una connessione client S3 all'endpoint del bilanciatore di carico e carichi lo stesso certificato sul client.
3. Quando il client vuole salvare o recuperare dati, si connette all'endpoint del bilanciatore di carico tramite HTTPS.
4. ${post_edited_translations.segment}
5. Il client confronta la firma del server con la firma presente sulla sua 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 esterno di gestione delle chiavi (KMS)

In questo esempio, StorageGRID funge da client.

1. Utilizzando un software esterno per la gestione delle chiavi (KMS), configuri StorageGRID come client KMS e ottieni un certificato server firmato da una CA, un certificato client pubblico e la chiave privata per il certificato client.
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
4. ${post_edited_translations.segment}
5. Il server KMS risponde utilizzando la connessione validata.

Tipi di certificati server supportati in StorageGRID

${post_edited_translations.segment}

Il tipo di cifratura per il criterio di sicurezza deve corrispondere al tipo di certificato del server. Ad esempio, le cifrature RSA richiedono certificati RSA e le cifrature ECDSA richiedono certificati ECDSA. Consulta "Gestisci i certificati di sicurezza". Se configuri un criterio di sicurezza personalizzato non compatibile con il certificato del server, puoi "${post_edited_translations.segment}".

Per ulteriori informazioni su come StorageGRID protegge le connessioni dei client, vedi "Sicurezza per i client S3".

Configura i certificati dell'interfaccia di gestione in StorageGRID

Puoi sostituire il certificato predefinito dell'interfaccia di gestione con un singolo certificato personalizzato che permette agli utenti di accedere a Grid Manager e Tenant Manager senza visualizzare avvisi di sicurezza. Puoi anche ripristinare il certificato predefinito dell'interfaccia di gestione o generarne uno nuovo.

Informazioni su questa attività

Per impostazione predefinita, ogni Admin Node riceve un certificato firmato dalla CA della grid. Puoi sostituire questi certificati firmati dalla CA con un singolo certificato dell'interfaccia di gestione personalizzato comune e con la relativa chiave privata.

Poiché per tutti i nodi Admin viene utilizzato un singolo certificato di interfaccia di gestione personalizzato, devi specificare il certificato come wildcard o multi-domain certificate se i client devono verificare il nome host quando si connettono a Grid Manager e Tenant Manager. Definisci il certificato personalizzato in modo che corrisponda a tutti i nodi Admin nella grid.

Devi completare la configurazione sul server e, a seconda dell'autorità di certificazione radice (CA) che stai utilizzando, gli utenti potrebbero anche dover installare il certificato CA di Grid nel browser web che useranno per accedere a Grid Manager e Tenant Manager.

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

Se accedi a Grid Manager o Tenant Manager utilizzando un domain name invece di un indirizzo IP, il browser mostra un errore relativo al certificato senza possibilità di ignorarlo se si verifica una delle seguenti situazioni:

- Il certificato della tua interfaccia di gestione personalizzata sta per scadere.
- Tu ripristinare dal certificato di interfaccia di gestione personalizzato al certificato server predefinito.

Aggiungi un certificato di interfaccia di gestione personalizzato

Per aggiungere un certificato di interfaccia di gestione personalizzato, puoi fornire il tuo certificato oppure generarne uno usando Grid Manager.

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Certificati**.

2. ${post_edited_translations.segment}
3. Seleziona **Usa certificato personalizzato**.
4. Carica o genera il certificato.

Carica il certificato

Carica i file del certificato server richiesti.

a. Seleziona **Carica certificato**.

b. Carica i file del certificato server richiesti:

- **Certificato del server**: Il file del certificato server personalizzato (codificato in formato PEM).
- **Chiave privata del certificato**: Il file della chiave privata del certificato del server personalizzato (`.key`).

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

- **CA bundle**: un singolo file opzionale contenente i certificati di ciascuna autorità di certificazione (CA) emittente intermedia. Il file deve contenere ciascuno dei file di certificato CA codificati in PEM, concatenati nell'ordine della catena di certificati.

c. Espandi **Dettagli del certificato** per vedere i metadati di ogni certificato che hai caricato. Se hai caricato un CA bundle opzionale, ogni certificato viene visualizzato nella sua scheda.

- Seleziona **Scarica certificato** per salvare il file del certificato o seleziona **Scarica pacchetto CA** per salvare il pacchetto di certificati.

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

  Ad esempio: `storagegrid_certificate.pem`

- ${post_edited_translations.segment}

d. Seleziona **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.

Genera certificato

Genera i file del certificato del server.

> La best practice per un ambiente di produzione è usare un certificato di interfaccia di gestione personalizzato firmato da un'autorità di certificazione esterna.

a. Seleziona **Genera certificato**.

b. ${post_edited_translations.segment}

Campo	Descrizione
domain name	Uno o più fully qualified domain name da includere nel certificato. Usa un * come carattere jolly per rappresentare più domain name.
IP	Uno o più indirizzi IP da includere nel certificato.

Campo	Descrizione
${post_edited_translations.segment}	Soggetto o nome distinto (DN) X.509 del titolare del certificato. ${post_edited_translations.segment}
Giorni di validità	${post_edited_translations.segment}
Aggiungi estensioni di utilizzo chiave	${post_edited_translations.segment} Queste estensioni definiscono lo scopo della chiave contenuta nel certificato. **Nota**: Lascia questa casella di controllo selezionata, a meno che tu non abbia problemi di connessione con client meno recenti quando i certificati includono queste estensioni.

c. Seleziona **Genera**.

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

- ${post_edited_translations.segment}

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

  Ad esempio: `storagegrid_certificate.pem`

- Seleziona **Copia certificato PEM** per copiare il contenuto del certificato da incollare altrove.

e. Seleziona **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. Aggiorna la pagina per assicurarti che il browser web sia aggiornato.

> Dopo aver caricato o generato un nuovo certificato, attendi fino a un giorno perché eventuali avvisi di scadenza del certificato correlato vengano eliminati.

6. Dopo che aggiungi un certificato di interfaccia di gestione personalizzato, la pagina Certificato di interfaccia di gestione mostra informazioni dettagliate sui certificati in uso. Puoi scaricare o copiare il PEM del certificato secondo necessità.

Ripristina il certificato predefinito dell'interfaccia di gestione

Puoi tornare a usare il certificato di interfaccia di gestione predefinito per le connessioni di Grid Manager e Tenant Manager.

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Certificati**.
2. ${post_edited_translations.segment}

3. Seleziona **Usa certificato predefinito**.

   Quando ripristini il certificato dell'interfaccia di gestione predefinito, i file del certificato del server personalizzato che hai configurato vengono eliminati e non possono essere recuperati dal sistema. Il certificato dell'interfaccia di gestione predefinito viene utilizzato per tutte le nuove connessioni client successive.

4. Aggiorna la pagina per assicurarti che il browser web sia aggiornato.

${post_edited_translations.segment}

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

Prima di iniziare

- Hai "autorizzazioni di accesso specifiche".
- Hai il file `Passwords.txt`.

Informazioni su questa attività

La best practice per un ambiente di produzione è utilizzare un certificato firmato da un'autorità di certificazione esterna.

Passaggi

1. Ottieni il fully qualified domain name (FQDN) di ciascun Admin Node.
2. Accedi al nodo amministratore principale:
   a. Inserisci il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Inserisci la password indicata nel file `Passwords.txt`.
   c. Inserisci il seguente comando per passare all'utente root: `su -`
   d. Inserisci la password indicata nel file `Passwords.txt`.

      Quando sei connesso come root, il prompt cambia da `$` a `#`.

3. ${post_edited_translations.segment}

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

   - Per `--domains`, usa i caratteri jolly per rappresentare i fully qualified domain name di tutti gli Admin Node. Ad esempio, `*.ui.storagegrid.example.com` usa il carattere jolly * per rappresentare `admin1.ui.storagegrid.example.com` e `admin2.ui.storagegrid.example.com`.
   - Imposta `--type` su `management` per configurare il certificato dell'interfaccia di gestione, che viene utilizzato da Grid Manager e Tenant Manager.
   - Per impostazione predefinita, i certificati generati sono validi per un anno (365 giorni) e devi ricrearli prima della scadenza. Puoi usare l' `--days`argomento per modificare il periodo di validità predefinito.

     > Il periodo di validità di un certificato inizia quando `make-certificate` viene eseguito. Devi assicurarti che il client di gestione sia sincronizzato con la stessa sorgente oraria di StorageGRID; altrimenti, 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 dell'API di gestione.

4. Seleziona e copia il certificato.

   Includi i tag BEGIN e END nella tua selezione.

5. Disconnettiti dalla shell dei comandi. `$ exit`
6. Conferma che il certificato è stato configurato:
   a. Accedi al Grid Manager.
   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}
7. Configura il client di gestione in modo che utilizzi il certificato pubblico che hai copiato. Includi i tag BEGIN e END.

Scarica o copia il certificato dell'interfaccia di gestione

${post_edited_translations.segment}

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Certificati**.
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}

${post_edited_translations.segment}

Scarica il file del certificato o del pacchetto CA `.pem`. Se utilizzi un pacchetto CA opzionale, ogni certificato del pacchetto viene visualizzato in una propria sotto-scheda.

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

   ${post_edited_translations.segment}

b. Specifica il nome del file del certificato e la posizione di download. Salva il file con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Copia certificato o bundle CA PEM

Copia il testo del certificato per incollarlo altrove. Se usi un pacchetto CA opzionale, ogni certificato del pacchetto viene visualizzato nella sua sottoscheda.

a. Seleziona **Copia certificato PEM** o **Copia bundle CA PEM**.

   Se copi un bundle di CA, tutti i certificati nelle schede secondarie del bundle di CA vengono copiati insieme.

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

c. Salva il file di testo con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Configura i certificati API S3 in StorageGRID

Puoi sostituire o ripristinare il certificato server utilizzato per le connessioni client S3 ai nodi di Storage o agli endpoint del bilanciamento del carico. Il certificato server personalizzato sostitutivo è specifico per la tua organizzazione.

I dettagli relativi a Swift sono stati rimossi da questa versione del sito della documentazione. Vedi "StorageGRID 11.8: Configura i certificati S3 e Swift API".

Informazioni su questa attività

Per impostazione predefinita, a ogni Storage Node viene rilasciato 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 corrispondente chiave privata.

Un singolo certificato server personalizzato viene utilizzato per tutti i Storage Node, quindi devi specificare il certificato come certificato wildcard o multi-dominio se i client devono verificare l'hostname quando si connettono all'endpoint di storage. Definisci il certificato personalizzato in modo che corrisponda a tutti i Storage Node nella griglia.

${post_edited_translations.segment}

Per garantire che le operazioni non vengano interrotte da un certificato server non valido, l'avviso **Scadenza del certificato server globale per l'API S3** viene attivato quando il certificato server root sta per scadere. Se necessario, puoi verificare quando scade il certificato corrente selezionando **Configurazione** > **Sicurezza** > **Certificati** e controllando la Data di scadenza del certificato dell'API S3 nella scheda Globale.

Puoi caricare o generare un certificato API S3 personalizzato.

${post_edited_translations.segment}

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Certificati**.
2. ${post_edited_translations.segment}
3. Seleziona **Usa certificato personalizzato**.
4. Carica o genera il certificato.

Carica il certificato

Carica i file del certificato server richiesti.

a. Seleziona **Carica certificato**.
b. Carica i file del certificato server richiesti:
   - **Certificato del server**: Il file del certificato server personalizzato (codificato in formato PEM).
   - **Chiave privata del certificato**: Il file della chiave privata del certificato del server personalizzato (`.key`).

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

   - **CA bundle**: un singolo file opzionale contenente i certificati di ciascuna autorità di certificazione emittente intermedia. Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati nell'ordine della catena di certificati.
c. Seleziona i dettagli del certificato per visualizzare i metadati e il PEM per ogni certificato API S3 personalizzato che hai caricato. Se hai caricato un bundle CA facoltativo, ogni certificato viene visualizzato nella sua scheda.
   - Seleziona **Scarica certificato** per salvare il file del certificato o seleziona **Scarica pacchetto CA** per salvare il pacchetto di certificati.

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

   Ad esempio: `storagegrid_certificate.pem`

   - ${post_edited_translations.segment}
d. Seleziona **Salva**.

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

Genera certificato

Genera i file del certificato del server.

a. Seleziona **Genera certificato**.
b. ${post_edited_translations.segment}

Campo	Descrizione
domain name	Uno o più fully qualified domain name da includere nel certificato. Usa un * come carattere jolly per rappresentare più domain name.
IP	Uno o più indirizzi IP da includere nel certificato.
${post_edited_translations.segment}	Soggetto o nome distinto (DN) X.509 del titolare del certificato. ${post_edited_translations.segment}

Campo	Descrizione
Giorni di validità	${post_edited_translations.segment}
Aggiungi estensioni di utilizzo chiave	${post_edited_translations.segment} Queste estensioni definiscono lo scopo della chiave contenuta nel certificato. **Nota**: Lascia questa casella di controllo selezionata, a meno che tu non abbia problemi di connessione con client meno recenti quando i certificati includono queste estensioni.

c. Seleziona **Genera**.

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

- ${post_edited_translations.segment}

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

  Ad esempio: `storagegrid_certificate.pem`

- Seleziona **Copia certificato PEM** per copiare il contenuto del certificato da incollare altrove.

e. Seleziona **Salva**.

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

5. ${post_edited_translations.segment}

> Dopo aver caricato o generato un nuovo certificato, attendi fino a un giorno perché eventuali avvisi di scadenza del certificato correlato vengano eliminati.

6. Aggiorna la pagina per assicurarti che il browser web sia aggiornato.
7. Dopo che aggiungi un certificato API S3 personalizzato, la pagina del certificato API S3 mostra informazioni dettagliate sul certificato API S3 personalizzato in uso. Puoi scaricare o copiare il PEM del certificato come necessario.

${post_edited_translations.segment}

Puoi ripristinare l'utilizzo del certificato API S3 predefinito per le connessioni dei client S3 ai Storage Node. Tuttavia, non puoi utilizzare il certificato API S3 predefinito per un endpoint del bilanciatore del carico.

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Certificati**.
2. ${post_edited_translations.segment}
3. Seleziona **Usa certificato predefinito**.

Quando ripristini la versione predefinita del certificato API S3 globale, i file del certificato server personalizzato che hai configurato vengono eliminati e non possono essere recuperati dal sistema. Il certificato API S3 predefinito verrà utilizzato per le nuove connessioni client S3 successive ai Storage Nodes.

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

   Se hai il permesso di accesso Root e per le connessioni agli endpoint del bilanciatore di carico è stato utilizzato un certificato API S3 personalizzato, viene visualizzato un elenco degli endpoint del bilanciatore di carico che non saranno più accessibili utilizzando il certificato API S3 predefinito. Vai su "${post_edited_translations.segment}" per modificare o rimuovere gli endpoint interessati.

5. Aggiorna la pagina per assicurarti che il browser web sia aggiornato.

${post_edited_translations.segment}

Puoi salvare o copiare il contenuto del certificato API S3 per usarlo altrove.

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Certificati**.
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}

${post_edited_translations.segment}

Scarica il file del certificato o del pacchetto CA `.pem`. Se utilizzi un pacchetto CA opzionale, ogni certificato del pacchetto viene visualizzato in una propria sotto-scheda.

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

   ${post_edited_translations.segment}

b. Specifica il nome del file del certificato e la posizione di download. Salva il file con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Copia certificato o bundle CA PEM

Copia il testo del certificato per incollarlo altrove. Se usi un pacchetto CA opzionale, ogni certificato del pacchetto viene visualizzato nella sua sottoscheda.

a. Seleziona **Copia certificato PEM** o **Copia bundle CA PEM**.

   Se copi un bundle di CA, tutti i certificati nelle schede secondarie del bundle di CA vengono copiati insieme.

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

c. Salva il file di testo con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Informazioni correlate

- "${post_edited_translations.segment}"
- "Configura i nomi di dominio degli endpoint S3"

Copia il certificato CA della griglia StorageGRID

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

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".

Informazioni su questa attività

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

Passaggi

1. ${post_edited_translations.segment}
2. Nella sezione **Certificato PEM**, scarica o copia il certificato.

Scarica il file del certificato

Scarica il file del certificato `.pem`.

a. Seleziona **Scarica certificato**.
b. Specifica il nome del file del certificato e la posizione di download. Salva il file con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Copia certificato PEM

Copia il testo del certificato per incollarlo altrove.

a. Seleziona **Copia certificato PEM**.
b. Incolla il certificato copiato in un editor di testo.
c. Salva il file di testo con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Configura i certificati StorageGRID per FabricPool

Per i client S3 che eseguono una convalida rigorosa del nome host e non supportano la disabilitazione di tale convalida, come i client ONTAP che utilizzano FabricPool, puoi generare o caricare un certificato server quando configuri l'endpoint del bilanciatore di

carico.

Prima di iniziare

- Hai "autorizzazioni di accesso specifiche".
- Sei connesso a Grid Manager utilizzando un "browser web supportato".

Informazioni su questa attività

Quando crei un endpoint per il bilanciamento del carico, puoi generare un certificato server autofirmato oppure caricare un certificato firmato da una certificate authority (CA) riconosciuta. Negli ambienti di produzione, dovresti usare un certificato firmato da una CA riconosciuta. I certificati firmati da una CA possono essere ruotati senza interruzioni. Sono anche più sicuri perché offrono una migliore protezione contro gli attacchi man-in-the-middle.

I seguenti passaggi forniscono linee guida generali per i client S3 che utilizzano FabricPool. Per informazioni e procedure più dettagliate, vedi "Configura StorageGRID per FabricPool".

Passaggi

1. Facoltativamente, puoi configurare un gruppo ad alta disponibilità (HA) da utilizzare per FabricPool.
2. Crea un endpoint del bilanciatore di carico S3 che FabricPool possa utilizzare.

   Quando crei un endpoint di bilanciamento del carico HTTPS, ti viene chiesto di caricare il certificato del server, la chiave privata del certificato e, facoltativamente, il bundle di CA.

3. Collega StorageGRID come livello cloud in ONTAP.

   Specifica la porta dell'endpoint del bilanciatore di carico e il fully qualified domain name utilizzato nel certificato CA che hai caricato. Poi, fornisci il certificato CA.

   Se il certificato StorageGRID è stato emesso da una CA intermedia, devi fornire il certificato della CA intermedia. Se il certificato StorageGRID è stato emesso direttamente dalla Root CA, devi fornire il certificato della Root CA.

Configura i certificati client in StorageGRID

I certificati client consentono ai client esterni autorizzati di accedere al database StorageGRID, fornendo un metodo sicuro per consentire agli strumenti esterni di monitorare StorageGRID.

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

Vedi "Gestisci i certificati di sicurezza" e "Configura certificati server personalizzati".

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

Se usi un server di gestione delle chiavi (KMS) per proteggere i dati sui nodi dell'appliance configurati in modo speciale, consulta le informazioni specifiche su "caricamento di un certificato client KMS".

Prima di iniziare

- ${post_edited_translations.segment}
- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Per configurare un certificato client:
  - Hai l'indirizzo IP o domain name del nodo Admin.
  - Se hai configurato il certificato dell'interfaccia di gestione di StorageGRID, hai la CA, il certificato client e la chiave privata utilizzati per configurare il certificato dell'interfaccia di gestione.
  - Per caricare il tuo certificato, la chiave privata del certificato è disponibile sul tuo computer locale.
  - La chiave privata deve essere stata salvata o registrata al momento della sua creazione. Se non hai la chiave privata originale, devi crearne una nuova.
- Per modificare un certificato client:
  - Hai l'indirizzo IP o domain name del nodo Admin.
  - Per caricare il tuo certificato o un nuovo certificato, la chiave privata, il certificato client e la CA (se utilizzata) sono disponibili sul tuo computer locale.

Aggiungi certificati client

Per aggiungere il certificato client, usa una di queste procedure:

- Certificato dell'interfaccia di gestione già configurato
- Certificato client emesso da CA
- <<${post_edited_translations.segment}>>

Certificato dell'interfaccia di gestione già configurato

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

Passaggi

1. Nel Grid Manager, seleziona **Configurazione** > **Sicurezza** > **Certificati** e poi seleziona la scheda **Client**.
2. Seleziona **Aggiungi**.
3. Inserisci il nome del certificato.
4. Per accedere alle metriche Prometheus utilizzando il tuo strumento di monitoraggio esterno, seleziona **Consenti prometheus**.
5. Seleziona **Continue**.
6. Nella fase **Allega certificati**, carica il certificato dell'interfaccia di gestione.
   a. Seleziona **Carica certificato**.
   b. Seleziona **Sfoglia** e seleziona il file del certificato dell'interfaccia di gestione (`.pem`).
      - Seleziona **Dettagli del certificato client** per visualizzare i metadati del certificato e il PEM del certificato.

- Seleziona **Copia certificato PEM** per copiare il contenuto del certificato da incollare altrove.

c. Seleziona **Crea** per salvare il certificato in Grid Manager.

Il nuovo certificato viene visualizzato nella scheda Client.

7. Configura uno strumento di monitoraggio esterno, come Grafana.

Certificato client emesso da CA

Usa questa procedura per aggiungere un certificato client amministratore se non hai configurato un certificato dell'interfaccia di gestione e prevedi di aggiungere un certificato client per Prometheus che utilizza un certificato client e una chiave privata emessi da una CA.

Passaggi

1. Esegui i passaggi per "configurare un certificato di interfaccia di gestione".
2. Nel Grid Manager, seleziona **Configurazione** > **Sicurezza** > **Certificati** e poi seleziona la scheda **Client**.
3. Seleziona **Aggiungi**.
4. Inserisci il nome del certificato.
5. Per accedere alle metriche Prometheus utilizzando il tuo strumento di monitoraggio esterno, seleziona **Consenti prometheus**.
6. Seleziona **Continue**.
7. ${post_edited_translations.segment}
   a. Seleziona **Carica certificato**.
   b. Seleziona **Sfoglia** e seleziona il certificato client, la chiave privata e i file del bundle CA (`.pem`).
      - Seleziona **Dettagli del certificato client** per visualizzare i metadati del certificato e il PEM del certificato.
      - Seleziona **Copia certificato PEM** per copiare il contenuto del certificato da incollare altrove.
   c. Seleziona **Crea** per salvare il certificato in Grid Manager.

   ${post_edited_translations.segment}
8. Configura uno strumento di monitoraggio esterno, come Grafana.

${post_edited_translations.segment}

${post_edited_translations.segment}

Passaggi

1. Nel Grid Manager, seleziona **Configurazione** > **Sicurezza** > **Certificati** e poi seleziona la scheda **Client**.
2. Seleziona **Aggiungi**.
3. Inserisci il nome del certificato.
4. Per accedere alle metriche Prometheus utilizzando il tuo strumento di monitoraggio esterno, seleziona **Consenti prometheus**.
5. Seleziona **Continue**.
6. Per la fase **Allega certificati**, seleziona **Genera certificato**.
7. ${post_edited_translations.segment}

- ${post_edited_translations.segment}
- **Giorni di validità**: Il numero di giorni in cui il certificato generato è valido, a partire dal momento in cui viene generato.
- **Aggiungi estensioni di utilizzo della chiave**: se selezionata (impostazione predefinita e consigliata), le estensioni di utilizzo della chiave e di utilizzo esteso della chiave vengono aggiunte al certificato generato.

  Queste estensioni definiscono lo scopo della chiave contenuta nel certificato.

  ${post_edited_translations.segment}

8. Seleziona **Genera**.
9. Seleziona **Dettagli del certificato client** per visualizzare i metadati del certificato e il PEM del certificato.

   Non potrai visualizzare la chiave privata del certificato dopo aver chiuso la finestra di dialogo. Copia o scarica la chiave in un luogo sicuro.

   - Seleziona **Copia certificato PEM** per copiare il contenuto del certificato da incollare altrove.
   - ${post_edited_translations.segment}

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

   Ad esempio: `storagegrid_certificate.pem`

   - Seleziona **Copia chiave privata** per copiare la chiave privata del certificato da incollare altrove.
   - Seleziona **Download private key** per salvare la chiave privata come file.

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

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

    Il nuovo certificato viene visualizzato nella scheda Client.

11. ${post_edited_translations.segment}
12. Seleziona **Management Interface certificate**.
13. Seleziona **Usa certificato personalizzato**.
14. Carica i file certificate.pem e private_key.pem dal dettagli del certificato clientpassaggio. Non è necessario caricare il bundle CA.
    a. Seleziona **Carica certificato** e poi seleziona **Continua**.
    b. Carica ciascun file del certificato (`.pem`).
    c. Seleziona **Salva** per salvare il certificato in Grid Manager.

       Il nuovo certificato appare nella pagina dei certificati dell'interfaccia di gestione.

15. Configura uno strumento di monitoraggio esterno, come Grafana.

${post_edited_translations.segment}

Passaggi

1. Configura le seguenti impostazioni sul tuo strumento di monitoraggio esterno, come Grafana.
   a. ${post_edited_translations.segment}

      StorageGRID non richiede queste informazioni, ma devi fornire un nome per testare la connessione.

   b. **URL**: Inserisci il domain name o l'indirizzo IP per l'Admin Node. Specifica HTTPS e la porta 9091.

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

   c. ${post_edited_translations.segment}
   d. Nella sezione Dettagli autenticazione TLS/SSL, copia e incolla:
      - L'interfaccia di gestione del certificato CA su **CA Cert**
      - Il certificato client su **Client Cert**
      - La chiave privata per **Client Key**
   e. **ServerName**: Inserisci il domain name dell'Admin Node.

      ServerName deve corrispondere al domain name come appare nel certificato dell'interfaccia di gestione.

2. Salva e testa il certificato e la chiave privata che hai copiato da StorageGRID o da un file locale.

   ${post_edited_translations.segment}

   Per informazioni sulle metriche, consulta "${post_edited_translations.segment}".

${post_edited_translations.segment}

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

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Certificati** e poi seleziona la scheda **Client**.

   Le date di scadenza dei certificati e i permessi di accesso a Prometheus sono elencati nella tabella. Se un certificato scade a breve o è già scaduto, viene visualizzato un messaggio nella tabella e viene attivato un avviso.

2. Seleziona il certificato che desideri modificare.
3. ${post_edited_translations.segment}
4. Inserisci il nome del certificato.
5. Per accedere alle metriche Prometheus utilizzando il tuo strumento di monitoraggio esterno, seleziona **Consenti prometheus**.
6. Seleziona **Continua** per salvare il certificato in Grid Manager.

   Il certificato aggiornato viene visualizzato nella scheda Client.

${post_edited_translations.segment}

Puoi caricare un nuovo certificato quando quello attuale è scaduto.

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Certificati** e poi seleziona la scheda **Client**.

   Le date di scadenza dei certificati e i permessi di accesso a Prometheus sono elencati nella tabella. Se un certificato scade a breve o è già scaduto, viene visualizzato un messaggio nella tabella e viene attivato un avviso.

2. Seleziona il certificato che desideri modificare.
3. ${post_edited_translations.segment}

Carica il certificato

Copia il testo del certificato per incollarlo altrove.

a. Seleziona **Carica certificato** e poi seleziona **Continua**.
b. Carica il nome del certificato client (`.pem`).

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

   - ${post_edited_translations.segment}

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

   Ad esempio: `storagegrid_certificate.pem`

   - Seleziona **Copia certificato PEM** per copiare il contenuto del certificato da incollare altrove.
c. Seleziona **Crea** per salvare il certificato in Grid Manager.

   Il certificato aggiornato viene visualizzato nella scheda Client.

Genera certificato

${post_edited_translations.segment}

a. Seleziona **Genera certificato**.
b. ${post_edited_translations.segment}

   - ${post_edited_translations.segment}
   - **Giorni di validità**: Il numero di giorni in cui il certificato generato è valido, a partire dal momento in cui viene generato.
   - **Aggiungi estensioni di utilizzo della chiave**: se selezionata (impostazione predefinita e consigliata), le estensioni di utilizzo della chiave e di utilizzo esteso della chiave vengono aggiunte al certificato generato.

     Queste estensioni definiscono lo scopo della chiave contenuta nel certificato.

     ${post_edited_translations.segment}
c. Seleziona **Genera**.
d. Seleziona **Dettagli del certificato client** per visualizzare i metadati del certificato e il PEM del certificato.

   Non potrai visualizzare la chiave privata del certificato dopo aver chiuso la finestra di dialogo. Copia o scarica la chiave in un luogo sicuro.

   - Seleziona **Copia certificato PEM** per copiare il contenuto del certificato da incollare altrove.
   - ${post_edited_translations.segment}

     Specifica il nome del file del certificato e la posizione di download. Salva il file con l'estensione

`.pem`.

Ad esempio: `storagegrid_certificate.pem`

- Seleziona **Copia chiave privata** per copiare la chiave privata del certificato da incollare altrove.
- Seleziona **Download private key** per salvare la chiave privata come file.

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

e. Seleziona **Crea** per salvare il certificato in Grid Manager.

Il nuovo certificato viene visualizzato nella scheda Client.

Scarica o copia i certificati client

${post_edited_translations.segment}

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Certificati** e poi seleziona la scheda **Client**.
2. Seleziona il certificato che desideri copiare o scaricare.
3. Scarica o copia il certificato.

Scarica il file del certificato

Scarica il file del certificato `.pem`.

a. Seleziona **Scarica certificato**.
b. Specifica il nome del file del certificato e la posizione di download. Salva il file con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Copia certificato

Copia il testo del certificato per incollarlo altrove.

a. Seleziona **Copia certificato PEM**.
b. Incolla il certificato copiato in un editor di testo.
c. Salva il file di testo con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

${post_edited_translations.segment}

Se non hai più bisogno di un certificato client amministratore, puoi rimuoverlo.

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Certificati** e poi seleziona la scheda **Client**.
2. Seleziona il certificato che desideri rimuovere.
3. Seleziona **Elimina** e poi conferma.

> Per rimuovere fino a 10 certificati, seleziona ciascun certificato da rimuovere nella scheda Client e quindi seleziona **Azioni** > **Elimina**.

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

Configura le impostazioni di sicurezza

Gestisci la policy TLS e SSH in StorageGRID

La policy TLS e SSH determina quali protocolli e algoritmi di crittografia vengono utilizzati per stabilire connessioni TLS sicure con le applicazioni client e connessioni SSH sicure con i servizi interni di StorageGRID.

La policy di sicurezza controlla come TLS e SSH crittografano i dati in transito. In generale, usa la policy di compatibilità Modern (predefinita), a meno che il tuo sistema non debba essere conforme ai Common Criteria o tu abbia bisogno di usare altri cifrari.

> Alcuni servizi StorageGRID non sono stati aggiornati per utilizzare i cifrari in queste policy.

Prima di iniziare

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

Seleziona una politica di sicurezza

Passaggi

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

   La scheda **Policy TLS e SSH** mostra le policy disponibili. La policy attualmente attiva è indicata da un segno di spunta verde sul riquadro della policy.

2. Consulta le schede per conoscere le policy disponibili.

Compatibilità moderna (impostazione predefinita)

Utilizza il criterio predefinito se hai bisogno di una crittografia forte e non hai esigenze particolari. Questo criterio è compatibile con la maggior parte dei client TLS e SSH.

Compatibilità legacy

Utilizza la policy di compatibilità Legacy se hai bisogno di opzioni di compatibilità aggiuntive per i client meno recenti. Le opzioni aggiuntive in questa policy potrebbero renderla meno sicura rispetto alla policy di compatibilità Modern.

Common Criteria

Usa la policy Common Criteria se hai bisogno della certificazione Common Criteria.

FIPS rigoroso

Usa la policy FIPS strict se hai bisogno della certificazione Common Criteria e devi usare il NetApp Cryptographic Security Module (NCSM) 3.0.8 o il NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 module per le connessioni client esterne agli endpoint del load balancer, a Tenant Manager e a Grid Manager. L'uso di questa policy potrebbe ridurre le prestazioni.

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

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

  Per ulteriori informazioni, consulta il NIST Cryptographic Algorithm Validation Program "${post_edited_translations.segment}".

- NetApp StorageGRID modulo API crittografica del kernel

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

  - Raccolta entropia
  - Crittografia dei nodi

  Per ulteriori informazioni, consulta il Programma di convalida degli algoritmi crittografici NIST "Certificati n. A6242 - n. A6257" e "${post_edited_translations.segment}".

Nota: dopo aver selezionato questa policy, "esegui un riavvio progressivo" per tutti i nodi per attivare l'NCSM. Usa **Manutenzione** > **Riavvio progressivo** per avviare e monitorare i riavvii.

Personalizzato

Crea una policy personalizzata se devi applicare i tuoi algoritmi di crittografia.

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

a. Imposta il `fipsMode` parametro su `true`.

b. Quando richiesto, "esegui un riavvio progressivo" per attivare i moduli di crittografia su tutti i nodi. Usa **Manutenzione** > **Riavvio progressivo** per avviare e monitorare i riavvii.

c. Seleziona **Support** > **Diagnostics** per visualizzare le versioni attive del modulo FIPS.

3. Per vedere i dettagli sui cifrari, i protocolli e gli algoritmi di ciascuna policy, seleziona **Visualizza dettagli**.
4. Per modificare i criteri correnti, seleziona **Usa criteri**.

${post_edited_translations.segment}

Crea una policy di sicurezza personalizzata

Puoi creare una policy personalizzata se hai bisogno di applicare i tuoi algoritmi di crittografia.

Passaggi

1. Dalla sezione della policy più simile alla policy personalizzata che vuoi creare, seleziona **Visualizza dettagli**.
2. ${post_edited_translations.segment}

3. ${post_edited_translations.segment}
4. Incolla il JSON che hai copiato e apporta le modifiche necessarie.
5. ${post_edited_translations.segment}

   Accanto a **Politica attuale** nella sezione delle politiche personalizzate compare un segno di spunta verde.

6. ${post_edited_translations.segment}

Ripristina temporaneamente i criteri di sicurezza predefiniti

Se hai configurato una policy di sicurezza personalizzata, potresti non essere in grado di accedere al Grid Manager se la policy TLS configurata è incompatibile con il "certificato server configurato".

Puoi ripristinare temporaneamente la policy di sicurezza predefinita.

Passaggi

1. Accedi a un nodo amministratore:
   a. Inserisci il seguente comando: `ssh admin@Admin_Node_IP`
   b. Inserisci la password indicata nel file `Passwords.txt`.
   c. Inserisci il seguente comando per passare all'utente root: `su -`
   d. Inserisci la password indicata nel file `Passwords.txt`.

   Quando sei connesso come root, il prompt cambia da `$` a `#`.
2. Eseguire il seguente comando:

   ```
   restore-default-cipher-configurations
   ```
3. ${post_edited_translations.segment}
4. Segui i passaggi in Seleziona una politica di sicurezza per configurare nuovamente i criteri.

Configurare la sicurezza di rete e degli oggetti di StorageGRID

Puoi configurare la sicurezza di rete e degli oggetti per crittografare gli oggetti archiviati, impedire determinate richieste S3 o consentire alle connessioni client ai Storage Node di usare HTTP invece di HTTPS.

${post_edited_translations.segment}

La crittografia degli oggetti memorizzati consente la crittografia di tutti i dati degli oggetti al momento dell'acquisizione tramite S3. Per impostazione predefinita, gli oggetti memorizzati non sono crittografati, ma puoi scegliere di crittografarli utilizzando l'algoritmo di crittografia AES-128 o AES-256. Quando abiliti l'impostazione, tutti i nuovi oggetti acquisiti vengono crittografati, ma non viene apportata alcuna modifica agli oggetti memorizzati esistenti. Se disabiliti la crittografia, gli oggetti attualmente crittografati rimangono tali, ma i nuovi oggetti acquisiti non vengono crittografati.

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

Per maggiori dettagli sui metodi di crittografia di StorageGRID, vedi "Esamina i metodi di crittografia di StorageGRID".

${post_edited_translations.segment}

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

${post_edited_translations.segment}

- DeleteBucket richieste
- ${post_edited_translations.segment}

Abilita HTTP per le connessioni ai nodi di archiviazione

Per impostazione predefinita, le applicazioni client utilizzano il protocollo di rete HTTPS per qualsiasi connessione diretta ai nodi di storage. Facoltativamente, puoi abilitare l'HTTP per queste connessioni, ad esempio durante il test di una grid non di produzione.

Utilizza HTTP per le connessioni ai nodi di archiviazione solo se i client S3 devono stabilire connessioni HTTP direttamente ai nodi di archiviazione. Non devi usare questa opzione per i client che utilizzano solo connessioni HTTPS o per i client che si connettono al servizio Load Balancer (perché puoi "${post_edited_translations.segment}" usare sia HTTP che HTTPS).

Consulta "Riepilogo: indirizzi IP e porte per le connessioni client" per sapere quali porte utilizzano i client S3 quando si connettono ai Storage Node tramite HTTP o HTTPS.

Seleziona opzioni

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- ${post_edited_translations.segment}

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Impostazioni di sicurezza**.
2. ${post_edited_translations.segment}
3. Per la crittografia degli oggetti memorizzati, usa l'impostazione **Nessuno** (predefinita) se non vuoi che gli oggetti memorizzati siano crittografati, oppure seleziona **AES-128** o **AES-256** per crittografare gli oggetti memorizzati.
4. Seleziona facoltativamente **Impedisci la modifica del client** se vuoi impedire ai client S3 di effettuare richieste specifiche.

   Se modifichi questa impostazione, ci vorrà circa un minuto per applicare la nuova impostazione. Il valore configurato viene memorizzato nella cache per performance e scalabilità.

5. ${post_edited_translations.segment}

   Fai attenzione quando abiliti HTTP per una griglia di produzione perché le richieste verranno inviate senza crittografia.

6. Seleziona **Salva**.

Modificare le impostazioni di sicurezza dell'interfaccia StorageGRID

${post_edited_translations.segment}

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "Permesso di accesso root".

Informazioni su questa attività

La pagina **Impostazioni di sicurezza** include le impostazioni **Timeout di inattività del browser** e **Stack trace dell'API di gestione**.

Timeout di inattività del browser

Indica per quanto tempo il browser di un utente può rimanere inattivo prima che l'utente venga disconnesso. Il valore predefinito è 15 minuti.

Il timeout di inattività del browser è controllato anche dai seguenti:

- Un timer StorageGRID separato e non configurabile, incluso per la sicurezza del sistema. Il token di autenticazione di ciascun utente scade 16 ore dopo l'accesso. Quando l'autenticazione di un utente scade, quell'utente viene disconnesso automaticamente, anche se il timeout di inattività del browser è disabilitato o il valore del timeout del browser non è stato raggiunto. Per rinnovare il token, l'utente deve accedere di nuovo.
- ${post_edited_translations.segment}

  Se l'SSO è abilitato e il browser dell'utente va in timeout, l'utente deve reinserire le proprie credenziali SSO per accedere nuovamente a StorageGRID. Vedi "${post_edited_translations.segment}".

${post_edited_translations.segment}

${post_edited_translations.segment}

Questa opzione è disabilitata per impostazione predefinita, ma potresti voler abilitare questa funzionalità per un ambiente di test. In generale, dovresti lasciare la traccia dello stack disabilitata negli ambienti di produzione per evitare di rivelare dettagli interni del software quando si verificano errori API.

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Impostazioni di sicurezza**.
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
   a. Espandi la fisarmonica.
   b. Per modificare il periodo di timeout, specifica un valore compreso tra 60 secondi e 7 giorni. Il timeout predefinito è di 15 minuti.
   c. ${post_edited_translations.segment}
   d. Seleziona **Salva**.

      ${post_edited_translations.segment}
4. ${post_edited_translations.segment}
   a. Espandi la fisarmonica.
   b. Seleziona la casella di controllo per restituire una traccia dello stack nelle risposte di errore delle API di Grid Manager e Tenant Manager.

      ${post_edited_translations.segment}

c. Seleziona **Salva**.

Gestisci l'accesso SSH esterno in StorageGRID

Gestisci l'accesso SSH per il traffico in entrata nella grid bloccando o consentendo l'accesso esterno. Gestire l'accesso SSH esterno non ha alcun impatto sul traffico tra i nodi nella grid.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "Permesso di accesso root".

Informazioni su questa attività

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

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Impostazioni di sicurezza**.
2. Seleziona la scheda **Blocca SSH**.
3. Usa l'opzione **Blocca l'accesso SSH in entrata** per gestire l'accesso SSH esterno:
   a. ${post_edited_translations.segment}
   b. Deseleziona la casella di controllo per consentire l'accesso.

   > Richiede l'accesso sulla porta 22 tra il laptop di servizio e tutti gli altri nodi della griglia. Rimuovi l'accesso sulla porta 22 quando completi l'attività di manutenzione.

4. Seleziona **Salva**.

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)".

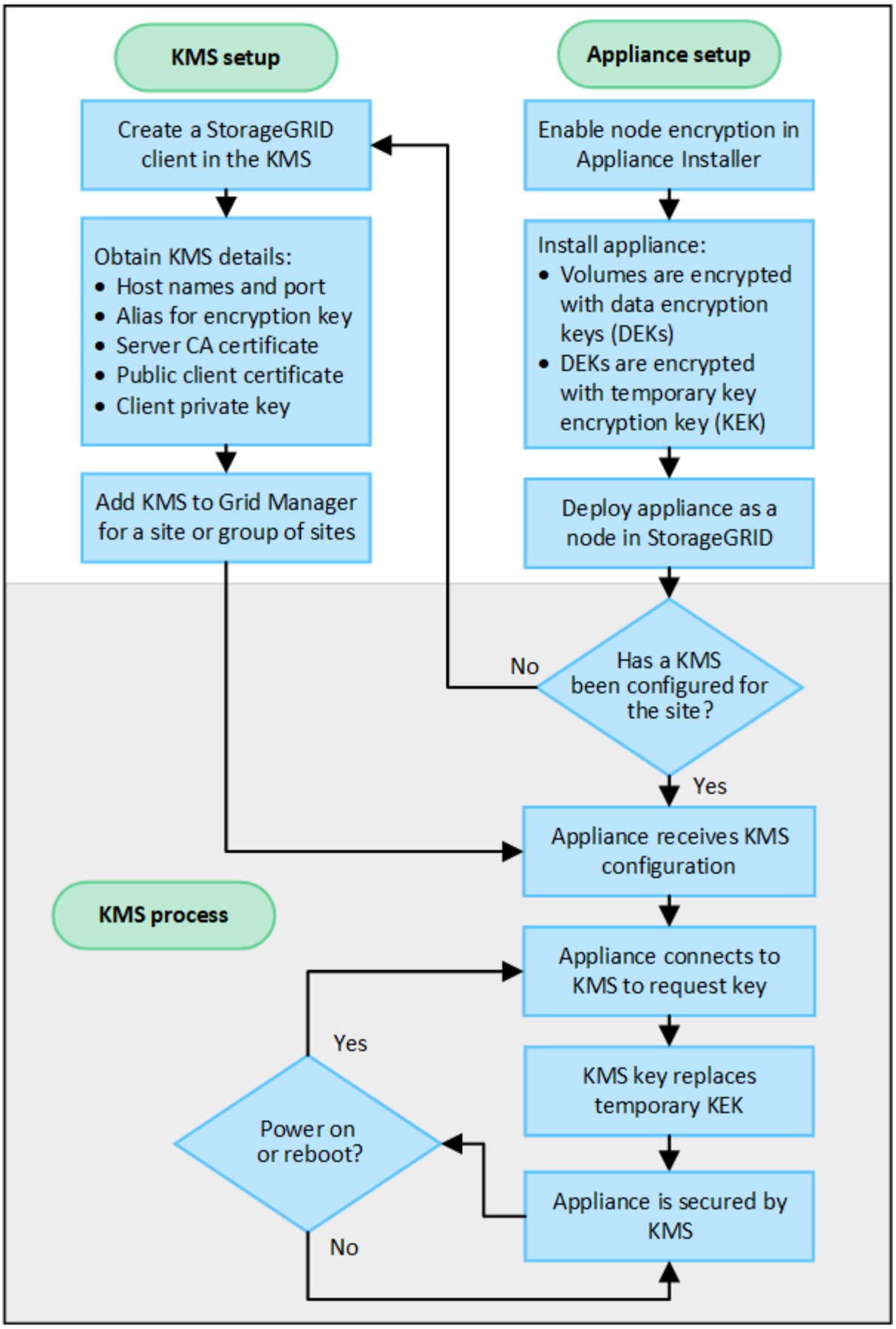
Puoi usare uno o più server di gestione delle chiavi per gestire le chiavi di crittografia dei nodi per qualsiasi nodo appliance StorageGRID che abbia l'impostazione **Crittografia nodo** abilitata durante l'installazione. Usare server di gestione delle chiavi con questi nodi appliance ti permette di 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.

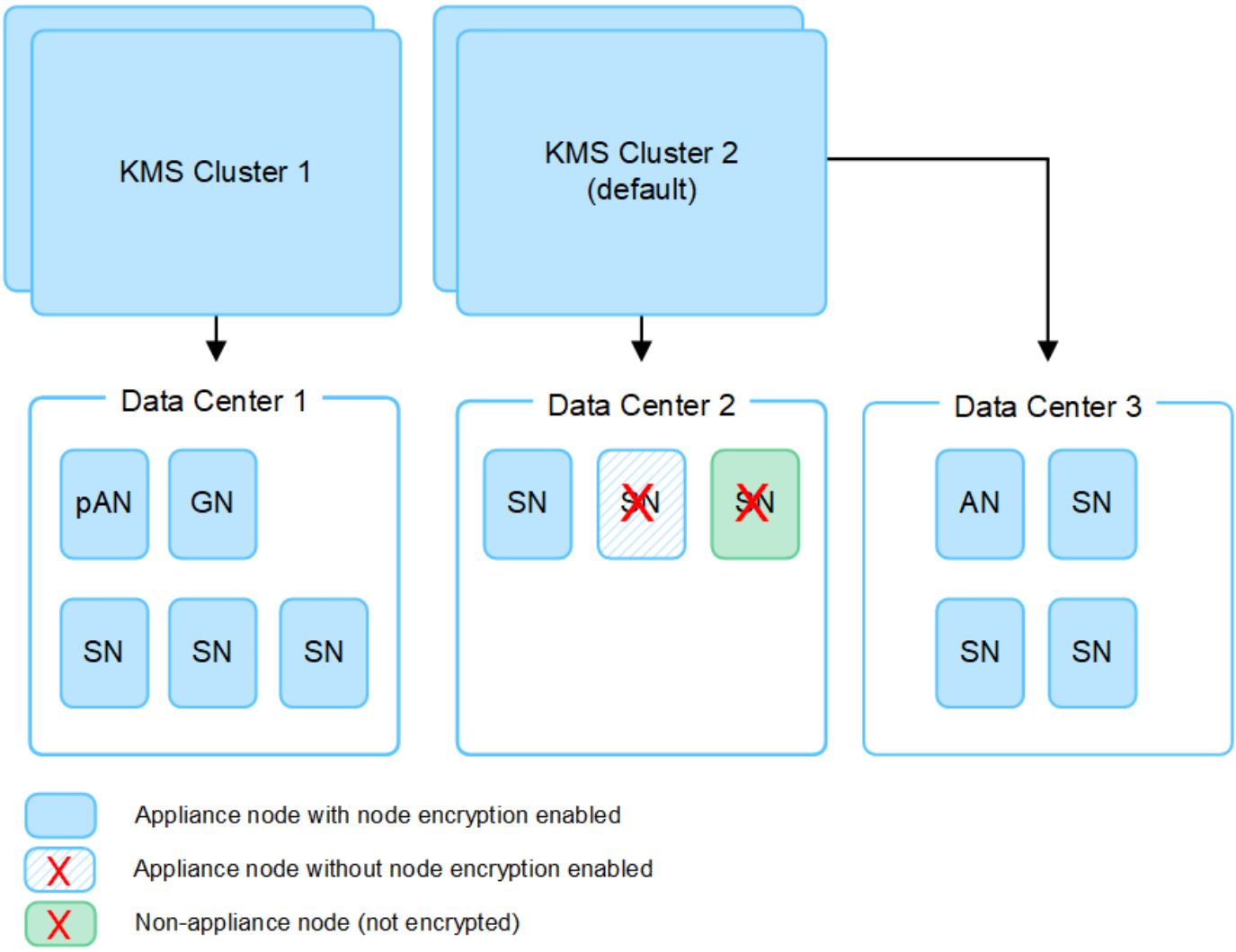
Di quanti server di gestione delle chiavi hai bisogno?

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.

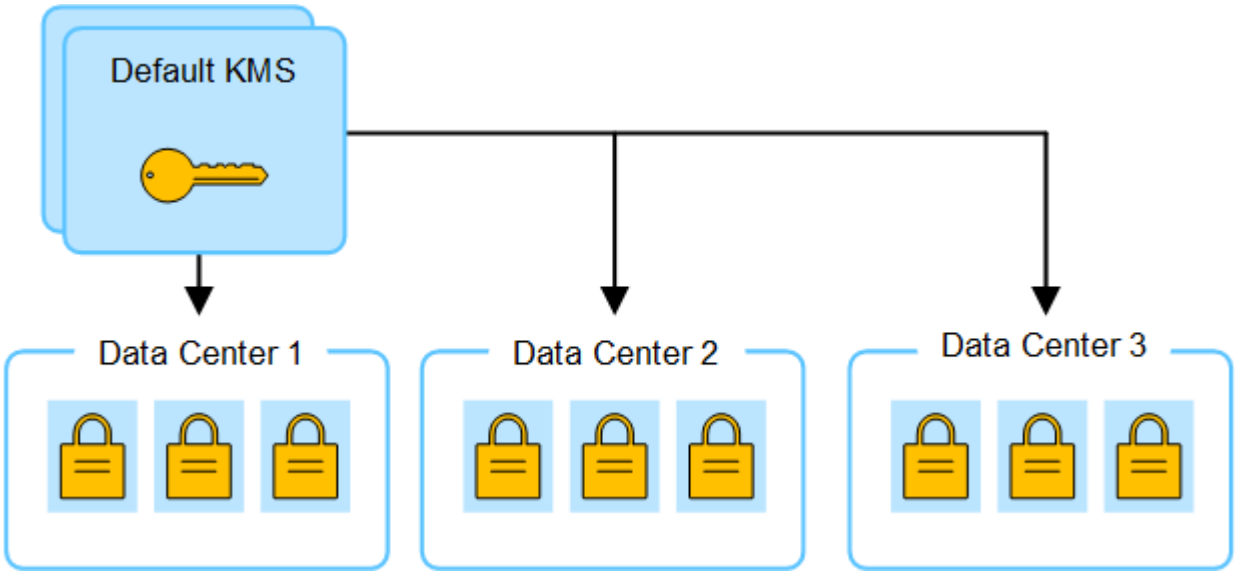
Considerazioni sulla modifica del KMS per un sito StorageGRID

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.

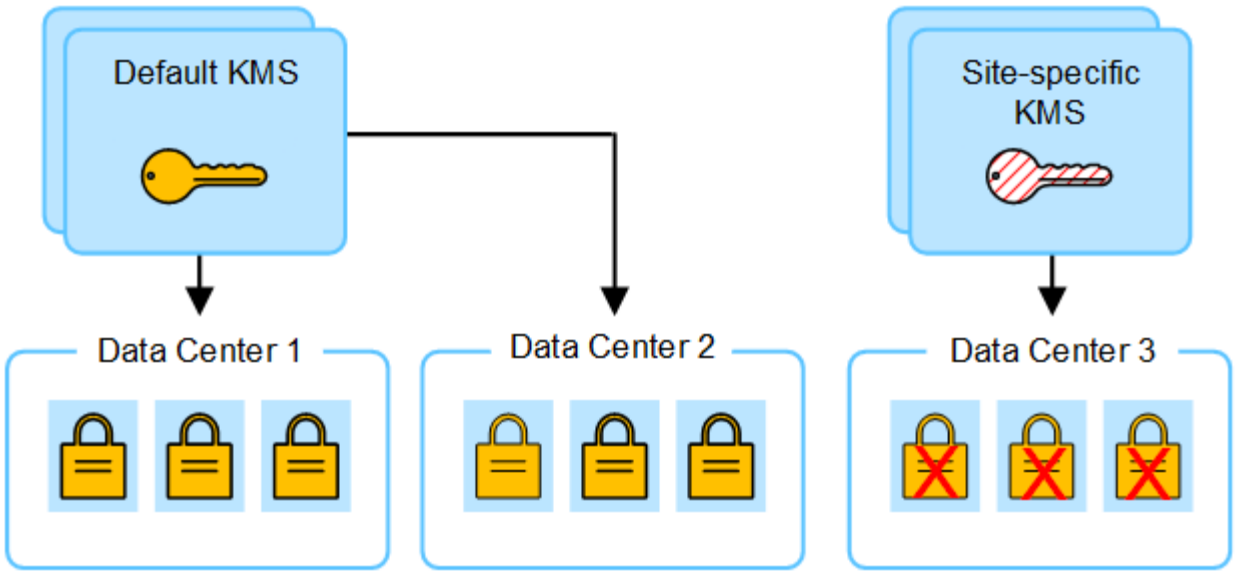
Se modifichi il KMS utilizzato per un sito, devi assicurarti che i nodi appliance precedentemente crittografati in quel sito possano essere decrittografati utilizzando la chiave memorizzata sul nuovo KMS. In alcuni casi, potrebbe essere necessario copiare la versione corrente della chiave di crittografia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

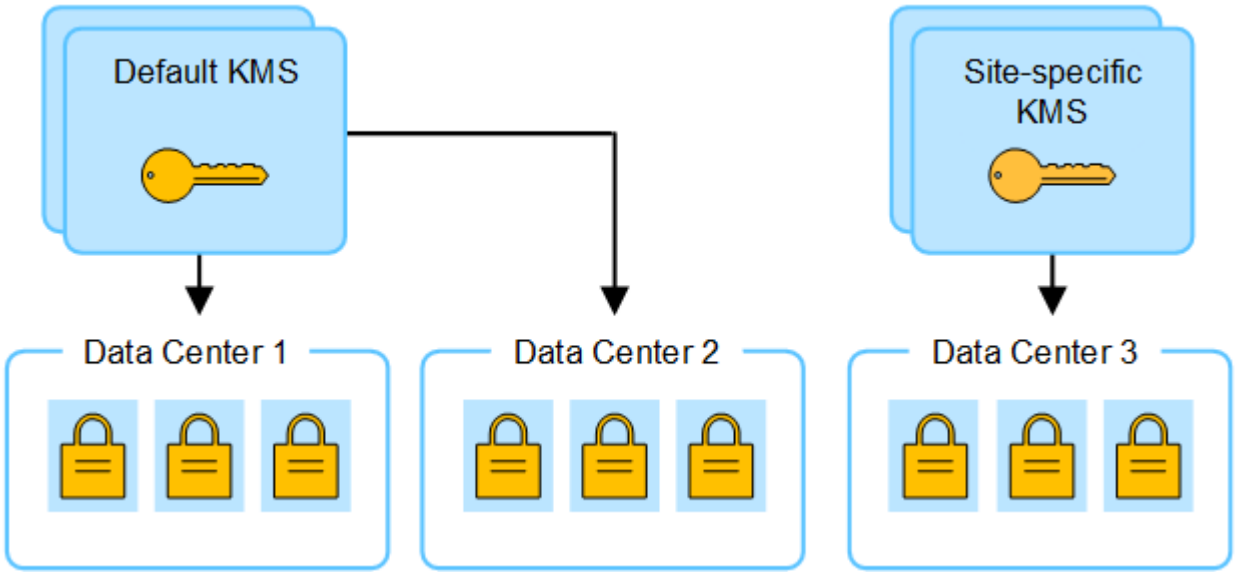
1. ${post_edited_translations.segment}
2. Quando il KMS viene salvato, tutti i nodi appliance che hanno l'impostazione **Node Encryption** abilitata si connettono al KMS e richiedono la chiave di crittografia. Questa chiave viene utilizzata per crittografare i nodi appliance in tutti i siti. Questa stessa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

Gestisci le impostazioni proxy

Configurare un proxy StorageGRID

Se usi i servizi della piattaforma o i Cloud Storage Pools, puoi configurare un proxy non trasparente tra gli Storage Nodes e gli endpoint S3 esterni. Ad esempio, potresti aver bisogno di un proxy non trasparente per permettere l'invio di messaggi dei servizi della piattaforma verso endpoint esterni, come un endpoint su internet.

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

Prima di iniziare

- Hai "autorizzazioni di accesso specifiche".
- Sei connesso a Grid Manager utilizzando un "browser web supportato".

Informazioni su questa attività

Puoi configurare le impostazioni per un singolo proxy di storage.

Passaggi

1. Seleziona **Configurazione** > **Sicurezza** > **Impostazioni proxy**.
2. Nella scheda **Archiviazione**, seleziona la casella di controllo **Abilita proxy di archiviazione**.
3. ${post_edited_translations.segment}
4. Inserisci il nome host o l'indirizzo IP del proxy server.
5. Facoltativamente, inserisci la porta utilizzata per connetterti al proxy server.

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

6. Seleziona **Salva**.

   Dopo aver salvato il proxy di archiviazione, puoi configurare e testare nuovi endpoint per i servizi della piattaforma o i Cloud Storage Pools.

Le modifiche al proxy possono richiedere fino a 10 minuti per avere effetto.

7. ${post_edited_translations.segment}
8. Se devi disabilitare un proxy storage, deseleziona la casella di controllo e seleziona **Salva**.

Configura le impostazioni proxy amministrative in StorageGRID

Se invii pacchetti AutoSupport tramite HTTP o HTTPS, puoi configurare un proxy server non trasparente tra i nodi di amministrazione e il supporto tecnico (AutoSupport).

Per ulteriori informazioni su AutoSupport, vedi "Configura AutoSupport".

Prima di iniziare

- Hai "autorizzazioni di accesso specifiche".
- Sei connesso a Grid Manager utilizzando un "browser web supportato".

Informazioni su questa attività

Puoi configurare le impostazioni per un singolo proxy admin.

Passaggi

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

   Viene visualizzata la pagina delle impostazioni proxy. Per impostazione predefinita, nel menu a schede è selezionata l'opzione Storage.

2. Seleziona la scheda **Admin**.
3. Seleziona la casella di controllo **Abilita proxy amministratore**.
4. Inserisci il nome host o l'indirizzo IP del proxy server.
5. Inserisci la porta utilizzata per connetterti al proxy server.
6. Facoltativamente, inserisci un nome utente e una password per il proxy server.

   Lascia vuoti questi campi se il tuo proxy server non richiede un nome utente o una password.

7. Seleziona una delle seguenti:

   - Se vuoi proteggere la connessione al proxy admin, seleziona **Verifica certificato proxy**. Carica un bundle CA per verificare l'autenticità dei certificati SSL presentati dal proxy server admin.

     AutoSupport on Demand, E-Series AutoSupport tramite StorageGRID e la determinazione del percorso di aggiornamento nella pagina di aggiornamento di StorageGRID non funzioneranno se viene verificato un certificato proxy.

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

   - Se non vuoi convalidare i certificati quando comunichi con il proxy server, seleziona **Non verificare il certificato proxy**.

8. Seleziona **Salva**.

   Dopo aver salvato il proxy di amministrazione, il proxy server tra i nodi di amministrazione e il supporto

tecnico viene configurato.

Le modifiche al proxy possono richiedere fino a 10 minuti per avere effetto.

9. Se devi disabilitare il proxy amministratore, deseleziona la casella di controllo **Abilita proxy amministratore** e poi seleziona **Salva**.

Controlla i firewall

Controlla l'accesso a StorageGRID tramite un firewall esterno

Puoi aprire o chiudere porte specifiche sul firewall esterno.

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

Se vuoi configurare il firewall interno di StorageGRID, vedi "Configura il firewall interno".

Porta	Descrizione	Se la porta è aperta…
443	Porta HTTPS predefinita per i nodi Admin	${post_edited_translations.segment} **Nota:** Anche la porta 443 viene utilizzata per parte del traffico interno.
8443	Porta Grid Manager con restrizioni sui nodi di amministrazione	• I browser web e i client API di gestione possono accedere a Grid Manager e all'API di gestione di Grid tramite HTTPS. • I browser web e i client API di gestione non possono accedere a Tenant Manager o alla Tenant Management API. • Le richieste di contenuti interni verranno respinte.
9443	Porta Tenant Manager con restrizioni sugli Admin Node	• I browser web e i client API di gestione possono accedere a Tenant Manager e all'API di gestione Tenant tramite HTTPS. • I browser web e i client API di gestione non possono accedere a Grid Manager o alla Grid Management API. • Le richieste di contenuti interni verranno respinte.

Il single sign-on (SSO) non è disponibile sulle porte con restrizioni di Grid Manager o Tenant Manager. Devi usare la porta HTTPS predefinita (443) se vuoi che gli utenti si autentichino con il single sign-on.

Informazioni correlate

- "Accedi al Grid Manager"

- "Crea account tenant"
- "Comunicazioni esterne"

Gestisci i controlli firewall interni in StorageGRID

StorageGRID include un firewall interno su ciascun nodo che migliora la sicurezza della tua grid consentendoti di controllare l'accesso di rete al nodo. Usa il firewall per impedire l'accesso di rete su tutte le porte ad eccezione di quelle necessarie per la tua specifica implementazione della grid. Le modifiche alla configurazione che apporti nella pagina di controllo del Firewall vengono distribuite su ciascun nodo.

${post_edited_translations.segment}

- **Elenco indirizzi privilegiati**: usa questa scheda per consentire l'accesso selezionato alle porte chiuse. Puoi aggiungere indirizzi IP o subnet in notazione CIDR che possono accedere alle porte chiuse usando la scheda Gestisci accesso esterno.
- **Gestisci l'accesso esterno**: Usa questa scheda per chiudere le porte aperte per impostazione predefinita o riaprire le porte precedentemente chiuse.
- ${post_edited_translations.segment}

  Le impostazioni in questa scheda hanno la precedenza sulle impostazioni nella scheda Gestisci accesso esterno.

  - Un nodo con una Client Network non attendibile accetterà solo connessioni sulle porte endpoint del load balancer configurate su quel nodo (endpoint globali, di interfaccia del nodo e associati al tipo di nodo).
  - Le porte endpoint del load balancer sono le uniche porte aperte sulle reti client non attendibili, indipendentemente dalle impostazioni nella scheda Manage external networks.
  - Quando sono attendibili, tutte le porte aperte nella scheda Gestisci accesso esterno sono accessibili, così come tutti gli endpoint del bilanciatore di carico aperti sulla Client Network.

> Le impostazioni che modifichi in una scheda possono influenzare le modifiche di accesso che fai in un'altra scheda. Assicurati di controllare le impostazioni in tutte le schede per essere sicuro che la tua rete si comporti come ti aspetti.

Per configurare i controlli del firewall interno, consulta "${post_edited_translations.segment}".

Per ulteriori informazioni sui firewall esterni e sulla sicurezza di rete, vedi "Controlla l'accesso tramite firewall esterno".

Schede Elenco indirizzi privilegiati e Gestione accesso esterno

La scheda Elenco indirizzi privilegiati ti permette di registrare uno o più indirizzi IP a cui viene concesso l'accesso alle porte della grid che sono chiuse. La scheda Gestisci accesso esterno ti permette di chiudere l'accesso esterno a porte esterne selezionate o a tutte le porte esterne aperte (le porte esterne sono porte accessibili per impostazione predefinita dai nodi non-grid). Queste due schede spesso possono essere usate insieme per personalizzare esattamente l'accesso di rete che vuoi consentire per la tua grid.

> Gli indirizzi IP privilegiati non hanno accesso alle porte interne della griglia per impostazione predefinita.

Esempio 1: Usa un jump host per le attività di manutenzione

Supponiamo che tu voglia utilizzare un jump host (un host con sicurezza rafforzata) per l'amministrazione della rete. Puoi seguire questi passaggi generali:

1. Usa la scheda Elenco indirizzi privilegiati per aggiungere l'indirizzo IP del jump host.
2. ${post_edited_translations.segment}

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

Dopo aver salvato la configurazione, tutte le porte esterne sull'Admin Node nel tuo grid verranno bloccate per tutti gli host ad eccezione del jump host. Potrai quindi utilizzare il jump host per eseguire le attività di manutenzione sul tuo grid in modo più sicuro.

Esempio 2: Blocca le porte sensibili

Supponiamo che tu voglia bloccare le porte sensibili e il servizio su quella porta. Puoi seguire questi passaggi generali:

1. Utilizza la scheda Elenco indirizzi privilegiati per concedere l'accesso solo agli host che necessitano di accedere al servizio.
2. ${post_edited_translations.segment}

> Aggiungi l'indirizzo IP privilegiato prima di bloccare l'accesso a qualsiasi porta assegnata per accedere a Grid Manager e Tenant manager (le porte preimpostate sono 443 e 8443). Qualsiasi utente attualmente connesso su una porta bloccata, incluso te, perderà l'accesso a Grid Manager a meno che il suo indirizzo IP non sia stato aggiunto all'elenco degli indirizzi privilegiati.

Dopo aver salvato la configurazione, la porta sensibile e il servizio su quella porta sono disponibili per gli host presenti nell'elenco degli indirizzi privilegiati. Tutti gli altri host non possono accedere al servizio, indipendentemente dall'interfaccia da cui proviene la richiesta.

Esempio 3: Disabilita l'accesso ai servizi non utilizzati

A livello di rete, puoi disabilitare alcuni servizi che non intendi utilizzare. Ad esempio, per bloccare il traffico client HTTP S3, puoi usare l'interruttore nella scheda Manage external access per bloccare la porta 18084.

${post_edited_translations.segment}

Se usi una rete client, puoi contribuire a proteggere StorageGRID da attacchi malevoli accettando il traffico client in entrata solo sugli endpoint configurati esplicitamente.

Per impostazione predefinita, la Client Network su ciascun nodo della griglia è *attendibile*. Ovvero, per impostazione predefinita, StorageGRID considera attendibili le connessioni inbound verso ciascun nodo della griglia su tutte le "porte esterne disponibili".

Puoi ridurre la minaccia di attacchi ostili al tuo sistema StorageGRID specificando che la Client Network su ciascun nodo sia *non attendibile*. Se la Client Network di un nodo non è attendibile, il nodo accetta solo connessioni inbound su porte configurate esplicitamente come endpoint del bilanciatore del carico. Vedi "${post_edited_translations.segment}" e "${post_edited_translations.segment}".

Esempio 1: Il nodo gateway accetta solo richieste S3 HTTPS

Supponiamo che tu voglia che un Gateway Node rifiuti tutto il traffico inbound sulla Client Network, tranne le richieste HTTPS S3. Dovresti seguire questi passaggi generali:

1. Dalla pagina "${post_edited_translations.segment}", configura un endpoint del bilanciatore del carico per S3 su HTTPS sulla porta 443.
2. Dalla pagina di controllo del firewall, seleziona Non attendibile per specificare che la Client Network sul Gateway Node non è attendibile.

Dopo che salvi la configurazione, tutto il traffico in entrata sulla rete client del Gateway Node viene bloccato, tranne le richieste HTTPS S3 sulla porta 443 e le richieste ICMP echo (ping).

Esempio 2: Il nodo di archiviazione invia richieste dei servizi della piattaforma S3

Supponi di voler abilitare il traffico outbound dei servizi della piattaforma S3 da un Storage Node, ma di voler impedire qualsiasi connessione inbound a tale Storage Node sulla Client Network. Eseguiresti questo passaggio generale:

- ${post_edited_translations.segment}

Dopo aver salvato la configurazione, il nodo di archiviazione non accetta più traffico in entrata sulla rete client, ma continua a consentire le richieste outbound verso le destinazioni dei servizi della piattaforma configurati.

${post_edited_translations.segment}

Supponiamo che tu voglia consentire l'accesso a Grid Manager solo su una sottorete specifica. Dovresti eseguire i seguenti passaggi:

1. ${post_edited_translations.segment}
2. Usa la scheda Rete client non attendibile per configurare la rete client come non attendibile.
3. Quando crei un endpoint del bilanciatore di carico dell'interfaccia di gestione, inserisci la porta e seleziona l'interfaccia di gestione a cui la porta accederà.
4. Seleziona **Sì** per Rete client non attendibile.
5. ${post_edited_translations.segment}

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

Configurare il firewall interno di StorageGRID

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

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".
- Hai esaminato le informazioni in "Gestisci i controlli del firewall" e "Linee guida di rete".
- Se vuoi che un nodo Admin o un nodo Gateway accetti traffico in entrata solo sugli endpoint configurati esplicitamente, hai definito gli endpoint del bilanciatore di carico.

${post_edited_translations.segment}

Informazioni su questa attività

StorageGRID include un firewall interno su ciascun nodo che ti permette di aprire o chiudere alcune delle porte sui nodi della tua griglia. Puoi usare le schede di controllo del firewall per aprire o chiudere le porte che sono aperte per impostazione predefinita sulla Grid Network, Admin Network e Client Network. Puoi anche creare un elenco di indirizzi IP privilegiati che possono accedere alle porte della griglia che sono chiuse. Se usi una Client Network, puoi specificare se un nodo si fida del traffico in entrata dalla Client Network e puoi configurare l'accesso a porte specifiche sulla Client Network.

Limitare il numero di porte aperte agli indirizzi IP esterni al tuo grid solo a quelle strettamente necessarie aumenta la sicurezza del tuo grid. Usi le impostazioni su ciascuna delle tre schede di controllo del firewall per assicurarti che siano aperte solo le porte necessarie.

Per ulteriori informazioni sull'utilizzo dei controlli firewall, inclusi esempi, vedi "Gestisci i controlli del firewall".

Per ulteriori informazioni sui firewall esterni e sulla sicurezza di rete, vedi "Controlla l'accesso tramite firewall esterno".

Accedi ai controlli del firewall

Passaggi

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

   Le tre schede di questa pagina sono descritte in "Gestisci i controlli del firewall".

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

   Puoi usare queste schede in qualsiasi ordine. Le configurazioni che imposti in una scheda non limitano ciò che puoi fare nelle altre schede; tuttavia, le modifiche di configurazione che apporti in una scheda potrebbero cambiare il comportamento delle porte configurate nelle altre schede.

Elenco degli indirizzi privilegiati

Usi la scheda Elenco indirizzi privilegiati per concedere agli host l'accesso alle porte che sono chiuse per impostazione predefinita o chiuse dalle impostazioni nella scheda Gestisci accesso esterno.

Gli indirizzi IP e le subnet privilegiate non hanno accesso alla griglia interna per impostazione predefinita. Inoltre, gli endpoint del load balancer e le porte aggiuntive aperte nella scheda Privileged address list sono accessibili anche se bloccate nella scheda Manage external access.

Le impostazioni nella scheda Elenco indirizzi privilegiati non possono sovrascrivere le impostazioni nella scheda Rete client non attendibile.

Passaggi

1. Nella scheda Elenco indirizzi privilegiati, inserisci l'indirizzo o la sottorete IP a cui vuoi concedere l'accesso alle porte chiuse.
2. Facoltativamente, seleziona **Aggiungi un altro indirizzo IP o sottorete in notazione CIDR** per aggiungere altri client privilegiati.

${post_edited_translations.segment}

3. Facoltativamente, seleziona **Consenti agli indirizzi IP privilegiati di accedere alle porte interne di StorageGRID**. Vedi "Porte interne di StorageGRID".

> Questa opzione rimuove alcune protezioni per i servizi interni. Se possibile, lasciala disabilitata.

4. Seleziona **Salva**.

Gestisci l'accesso esterno

Quando una porta viene chiusa nella scheda Gestisci accesso esterno, non puoi accedervi da nessun indirizzo IP non appartenente alla griglia, a meno che tu non aggiunga l'indirizzo IP all'elenco degli indirizzi privilegiati. Puoi chiudere solo le porte aperte per impostazione predefinita e puoi aprire solo le porte che hai chiuso.

> Le impostazioni nella scheda Gestisci accesso esterno non possono sovrascrivere le impostazioni nella scheda Rete client non attendibile. Ad esempio, se un nodo non è attendibile, la porta SSH/22 viene bloccata sulla rete client anche se è aperta nella scheda Gestisci accesso esterno. Le impostazioni nella scheda Rete client non attendibile hanno la precedenza sulle porte chiuse (come 443, 8443, 9443) sulla rete client.

Passaggi

1. Seleziona **Gestisci accesso esterno**. La scheda visualizza una tabella con tutte le porte esterne (porte accessibili per impostazione predefinita dai nodi non appartenenti alla griglia) per i nodi della tua griglia.
2. Configura le porte che vuoi aprire e chiudere usando le seguenti opzioni:
   - Usa l'interruttore accanto a ogni porta per aprire o chiudere la porta selezionata.
   - Seleziona **Apri tutte le porte visualizzate** per aprire tutte le porte elencate nella tabella.
   - Seleziona **Chiudi tutte le porte visualizzate** per chiudere tutte le porte elencate nella tabella.

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

> Utilizza la barra di scorrimento sul lato destro della tabella per assicurarti di aver visualizzato tutte le porte disponibili. Utilizza il campo di ricerca per trovare le impostazioni di qualsiasi porta esterna inserendo un numero di porta. Puoi inserire anche solo una parte del numero di porta. Ad esempio, se inserisci **2**, vengono visualizzate tutte le porte che hanno la stringa "2" come parte del loro nome.

3. Seleziona **Save**

Rete client non affidabile

Se la rete client di un nodo non è considerata attendibile, il nodo accetta traffico in entrata solo sulle porte configurate come endpoint del bilanciatore di carico e, facoltativamente, sulle porte aggiuntive che selezioni in questa scheda. Puoi anche usare questa scheda per specificare l'impostazione predefinita per i nuovi nodi aggiunti in un'espansione.

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

Le modifiche di configurazione che apporti nella scheda **Rete client non attendibile** sovrascrivono le impostazioni della scheda **Gestisci accesso esterno**.

Passaggi

1. Seleziona **Rete client non attendibile**.
2. Nella sezione Imposta impostazione predefinita per i nuovi nodi, specifica quale deve essere l'impostazione predefinita quando vengono aggiunti nuovi nodi alla grid in una procedura di espansione.

   - ${post_edited_translations.segment}
   - **Non attendibile**: Quando un nodo viene aggiunto in un'espansione, la sua Client Network non è attendibile.

     Se necessario, puoi tornare a questa scheda per modificare l'impostazione di uno specifico nuovo nodo.

     ${post_edited_translations.segment}

3. ${post_edited_translations.segment}

   - ${post_edited_translations.segment}
   - Seleziona **Considera attendibili i nodi visualizzati** per rimuovere tutti i nodi visualizzati nella tabella dall'elenco Untrusted Client Network.
   - ${post_edited_translations.segment}

     ${post_edited_translations.segment}

     Utilizza la barra di scorrimento sul lato destro della tabella per assicurarti di aver visualizzato tutti i nodi disponibili. Usa il campo di ricerca per trovare le impostazioni di qualsiasi nodo inserendo il nome del nodo. Puoi inserire anche una parte del nome. Ad esempio, se inserisci **GW**, vengono visualizzati tutti i nodi che hanno la stringa "GW" come parte del loro nome.

4. Seleziona **Salva**.

   Le nuove impostazioni del firewall vengono applicate e rese effettive immediatamente. Le connessioni client esistenti potrebbero interrompersi se gli endpoint del bilanciatore del carico non sono stati configurati.

Informazioni sul copyright

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

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

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