Gestire la sicurezza

StorageGRID software

NetApp
December 03, 2025

Sommario

Gestire la sicurezza

Gestire la sicurezza

È possibile configurare diverse impostazioni di sicurezza da Grid Manager per proteggere il sistema StorageGRID .

Gestisci la crittografia

StorageGRID offre diverse opzioni per la crittografia dei dati. Dovresti"rivedere 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" utilizzato per le connessioni HTTP o i certificati client utilizzati per autenticare l'identità di un client o di un utente sul server.

Configurare i server di gestione delle chiavi

Utilizzando un"server di gestione delle chiavi" consente di proteggere i dati StorageGRID anche se un dispositivo viene rimosso dal data center. Dopo aver crittografato i volumi dell'appliance, non sarà possibile accedere ai dati sull'appliance a meno che il nodo non sia in grado di comunicare con il KMS.

> Per utilizzare la gestione delle chiavi di crittografia, è necessario abilitare l'impostazione **Crittografia nodo** per ogni appliance durante l'installazione, prima che l'appliance venga aggiunta alla griglia.

Gestisci le impostazioni proxy

Se si utilizzano servizi della piattaforma S3 o pool di archiviazione cloud, è possibile configurare un"server proxy di archiviazione" tra i nodi di archiviazione e gli endpoint S3 esterni. Se si inviano pacchetti AutoSupport tramite HTTPS o HTTP, è possibile configurare un"server proxy di amministrazione" tra i nodi amministrativi e il supporto tecnico.

Controllare i firewall

Per migliorare la sicurezza del sistema, è possibile controllare l'accesso ai nodi di amministrazione StorageGRID aprendo o chiudendo porte specifiche a livello"firewall esterno" . È inoltre possibile controllare l'accesso alla rete per ciascun nodo configurandone"firewall interno" . È possibile impedire l'accesso a tutte le porte, ad eccezione di quelle necessarie per la distribuzione.

Esaminare i metodi di crittografia StorageGRID

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

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

Opzione di crittografia	Come funziona	Si applica a
Server di gestione delle chiavi (KMS) in Grid Manager	Voi"configurare un server di gestione delle chiavi" per il sito StorageGRID e "abilitare la crittografia dei nodi per l'appliance" . Quindi, un nodo appliance si connette al KMS per richiedere una chiave di crittografia (KEK). Questa chiave crittografa e decrittografa la chiave di crittografia dei dati (DEK) su ciascun volume.	Nodi dell'appliance in cui è abilitata la **Crittografia nodo** durante l'installazione. Tutti i dati presenti 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 le appliance di servizi.
Pagina Crittografia unità nel programma di installazione dell'appliance StorageGRID	Se l'appliance contiene unità che supportano la crittografia hardware, è possibile impostare una passphrase dell'unità durante l'installazione. Quando si imposta una passphrase per l'unità, è impossibile per chiunque recuperare dati validi dalle unità rimosse dal sistema, a meno che non si conosca la passphrase. Prima di iniziare l'installazione, vai su **Configura hardware** > **Crittografia unità** per impostare una passphrase dell'unità che si applichi a tutte le unità auto-crittografanti gestite da StorageGRID in un nodo.	Dispositivi che contengono unità auto-crittografanti. Tutti i dati presenti sulle unità protette sono protetti contro la perdita fisica o la rimozione dal data center. La crittografia dell'unità non si applica alle unità gestite SANtricity. Se si dispone di un dispositivo di archiviazione con unità auto-crittografanti e controller SANtricity , è possibile abilitare la sicurezza delle unità in SANtricity.
Sicurezza dell'unità in SANtricity System Manager	Se la funzionalità Drive Security è abilitata per l'appliance StorageGRID , è possibile utilizzare "Gestore del sistema SANtricity" per creare e gestire la chiave di sicurezza. La chiave è necessaria per accedere ai dati presenti sulle unità protette.	Dispositivi di archiviazione dotati di unità FDE (Full Disk Encryption) o unità auto-crittografanti. Tutti i dati presenti sulle unità protette sono protetti contro la perdita fisica o la rimozione dal data center. Non può essere utilizzato con alcuni elettrodomestici o con apparecchi di servizio.
Crittografia degli oggetti memorizzati	Si abilita il"Crittografia degli oggetti memorizzati" opzione nel Grid Manager. Se abilitata, tutti i nuovi oggetti che non sono crittografati a livello di bucket o a livello di oggetto vengono crittografati durante l'acquisizione.	Dati di oggetti S3 appena acquisiti. Gli oggetti archiviati esistenti 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	Si invia una richiesta PutBucketEncryption per abilitare la crittografia per il bucket. Tutti i nuovi oggetti che non sono crittografati a livello di oggetto vengono crittografati durante l'acquisizione.	Solo dati di oggetti S3 appena acquisiti. È necessario specificare la crittografia per il bucket. Gli oggetti bucket esistenti non sono crittografati. I metadati degli oggetti e altri dati sensibili non sono crittografati. "Operazioni sui bucket"
Crittografia lato server (SSE) degli oggetti S3	Si invia una richiesta S3 per memorizzare un oggetto e includere `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 degli oggetti e altri dati sensibili non sono crittografati. StorageGRID gestisce le chiavi. "Utilizzare la crittografia lato server"
Crittografia lato server degli oggetti S3 con chiavi fornite dal cliente (SSE-C)	Si invia una richiesta S3 per memorizzare un oggetto e si includono 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 degli oggetti e altri dati sensibili non sono crittografati. Le chiavi vengono gestite all'esterno di StorageGRID. "Utilizzare la crittografia lato server"
Crittografia del volume esterno o dell'archivio dati	Per crittografare un intero volume o un intero datastore, è possibile utilizzare un metodo di crittografia esterno a StorageGRID , se supportato dalla piattaforma di distribuzione.	Tutti i dati degli oggetti, i metadati e i dati di configurazione del sistema, presupponendo che ogni volume o archivio dati sia crittografato. Un metodo di crittografia esterno garantisce 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	Si utilizza un metodo di crittografia esterno a StorageGRID per crittografare i dati e i metadati degli oggetti prima che vengano acquisiti in StorageGRID.	Solo dati e metadati degli oggetti (i dati di configurazione del sistema non sono crittografati). Un metodo di crittografia esterno garantisce 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 mediante crittografia lato client"

Utilizzare più metodi di crittografia

A seconda delle esigenze, è possibile utilizzare più di un metodo di crittografia contemporaneamente. Per esempio:

- È possibile utilizzare un KMS per proteggere i nodi degli apparecchi e anche utilizzare la funzionalità di sicurezza dell'unità in SANtricity System Manager per "crittografare due volte" i dati sulle unità auto-crittografanti negli stessi apparecchi.
- È possibile utilizzare un KMS per proteggere i dati sui nodi dell'appliance e utilizzare anche l'opzione di crittografia degli oggetti archiviati 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'abilitazione di più livelli di crittografia comporta un costo aggiuntivo in termini di prestazioni.

Gestisci i certificati

Gestire i certificati di sicurezza

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

StorageGRID utilizza due tipi di certificati di sicurezza:

- **I certificati del server** sono obbligatori quando si utilizzano connessioni HTTPS. I certificati server vengono utilizzati per stabilire connessioni sicure tra client e server, autenticando l'identità di un server rispetto ai suoi client e fornendo un percorso di comunicazione sicuro per i dati. Sia il server che il client dispongono ciascuno di una copia del certificato.
- I **certificati client** autenticano l'identità di un client o di un utente sul server, garantendo 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 verifica questo certificato confrontando la firma del server con la firma presente sulla propria copia del certificato. Se le firme corrispondono, il client avvia una sessione con il server

utilizzando la stessa chiave pubblica.

StorageGRID funge da server per alcune connessioni (ad esempio l'endpoint del bilanciatore del carico) o da client per altre connessioni (ad esempio il servizio di replica CloudMirror).

Certificato CA predefinito della griglia

StorageGRID include un'autorità di certificazione (CA) integrata che genera un certificato CA Grid interno durante l'installazione del sistema. Per impostazione predefinita, il certificato Grid CA viene utilizzato per proteggere il traffico StorageGRID interno. Un'autorità di certificazione (CA) esterna può rilasciare certificati personalizzati pienamente conformi alle policy di sicurezza delle informazioni della tua organizzazione. Sebbene sia possibile utilizzare il certificato Grid CA per un ambiente non di produzione, la procedura consigliata per un ambiente di produzione è quella di utilizzare certificati personalizzati firmati da un'autorità di certificazione esterna. Sono supportate anche le connessioni non protette senza certificato, ma non sono consigliate.

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

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

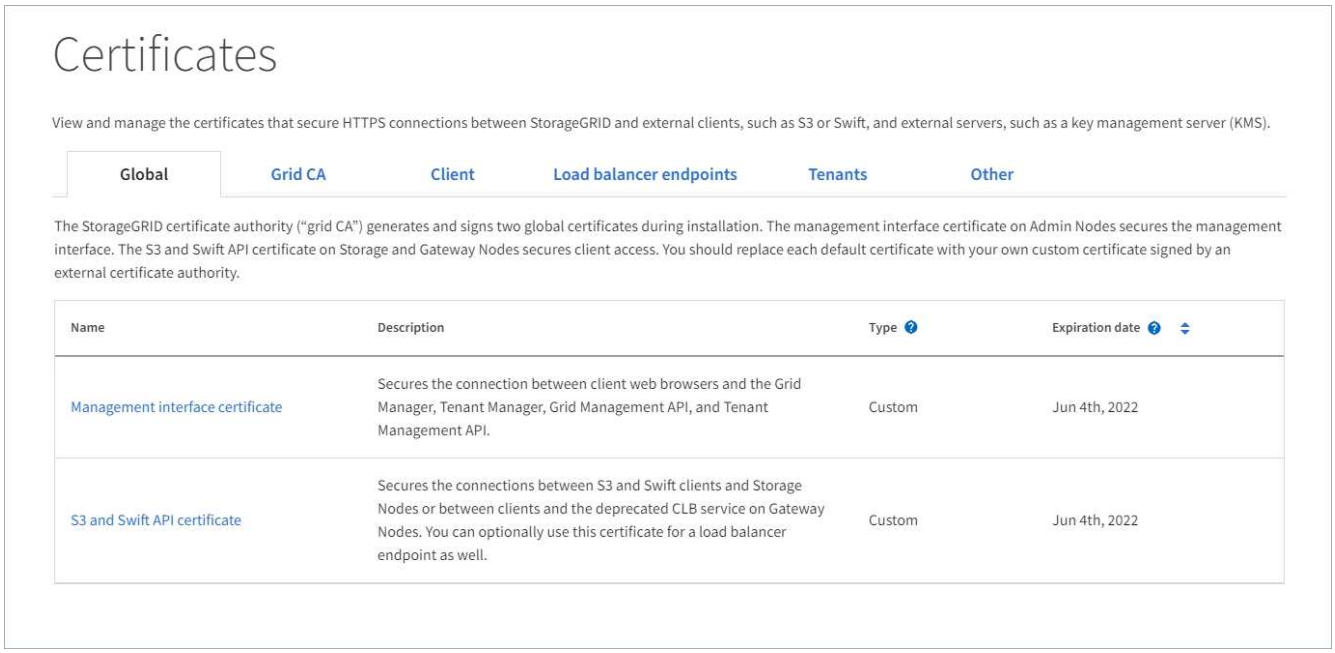
Le varianti dei tipi di certificato server e client vengono implementate in diversi modi. Prima di configurare il sistema, è necessario disporre di tutti i certificati necessari per la configurazione specifica StorageGRID .

Certificati di sicurezza di accesso

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

Passi

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



2. Selezionare una scheda nella pagina Certificati per informazioni su ciascuna categoria di certificato e per accedere alle impostazioni del certificato. Puoi accedere a una scheda se hai"autorizzazione appropriata" .

   - **Globale**: Protegge l'accesso a StorageGRID da browser Web e client API esterni.
   - **Grid CA**: protegge il traffico StorageGRID interno.
   - **Client**: protegge le connessioni tra client esterni e il database StorageGRID Prometheus.
   - **Endpoint del bilanciatore del carico**: protegge le connessioni tra i client S3 e il bilanciatore del carico StorageGRID .
   - **Tenant**: protegge le connessioni ai server di federazione delle identità o dagli endpoint dei servizi di piattaforma alle risorse di archiviazione S3.
   - **Altro**: protegge le connessioni StorageGRID che richiedono certificati specifici.

     Di seguito viene descritta ogni scheda con link ad ulteriori dettagli sul certificato.

Globale

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

- Certificato di interfaccia di gestione: Protegge le connessioni del browser Web del client alle interfacce di gestione StorageGRID .
- Certificato API S3: Protegge le connessioni API client ai nodi di archiviazione, ai nodi di amministrazione e ai nodi gateway, che le applicazioni client S3 utilizzano per caricare e scaricare i dati degli oggetti.

Le informazioni sui certificati globali installati includono:

- **Nome**: Nome del certificato con collegamento alla gestione del certificato.
- **Descrizione**
- **Tipo**: personalizzato o predefinito. + Per una maggiore sicurezza della rete, dovresti sempre utilizzare un certificato personalizzato.
- **Data di scadenza**: se si utilizza il certificato predefinito, non viene visualizzata alcuna data di scadenza.

Puoi:

- Sostituisci i certificati predefiniti con certificati personalizzati firmati da un'autorità di certificazione esterna per migliorare la sicurezza della griglia:
  - "Sostituisci il certificato dell'interfaccia di gestione predefinita generata da StorageGRID"utilizzato per le connessioni Grid Manager e Tenant Manager.
  - "Sostituisci il certificato API S3"utilizzato per le connessioni del nodo di archiviazione e dell'endpoint del bilanciatore del carico (facoltativo).
- "Ripristina il certificato dell'interfaccia di gestione predefinita" .
- "Ripristina il certificato API S3 predefinito" .
- "Utilizzare uno script per generare un nuovo certificato di interfaccia di gestione autofirmato" .
- Copia o scarica il"certificato di interfaccia di gestione" O"Certificato API S3" .

Griglia CA

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

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

Puoi"copia o scarica il certificato Grid CA" , ma non puoi cambiarlo.

Cliente

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

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

Puoi:

- "Carica o genera un nuovo certificato client."
- Seleziona un nome di certificato per visualizzarne i dettagli, dove puoi:
  - "Cambia il nome del certificato client."
  - "Imposta l'autorizzazione di accesso a Prometheus."
  - "Carica e sostituisci il certificato client."
  - "Copia o scarica il certificato client."
  - "Rimuovere il certificato client."
- Seleziona **Azioni** per eseguire rapidamente"modificare" ,"allegare" , O"rimuovere" un certificato client. È possibile selezionare fino a 10 certificati client e rimuoverli contemporaneamente utilizzando **Azioni** > **Rimuovi**.

Endpoint del bilanciatore del carico

Certificati degli endpoint del bilanciatore del caricoproteggere le connessioni tra i client S3 e il servizio StorageGRID Load Balancer sui nodi gateway e sui nodi amministrativi.

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

> 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 del carico", compresi i dettagli del suo certificato.
- "Specificare un certificato dell'endpoint del bilanciatore del carico per FabricPool."
- "Utilizzare il certificato API S3 globale"invece di generare un nuovo certificato dell'endpoint del bilanciatore del carico.

inquilini

Gli inquilini possono utilizzarecertificati del server di federazione delle identità Ocertificati endpoint del servizio di piattaforma per proteggere le loro connessioni con StorageGRID.

La tabella dei tenant contiene una riga per ogni 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 di tenant per accedere a Tenant Manager"
- "Seleziona un nome tenant per visualizzare i dettagli della federazione dell'identità del tenant"
- "Seleziona un nome tenant per visualizzare i dettagli dei servizi della piattaforma tenant"
- "Specificare un certificato dell'endpoint del servizio di piattaforma durante la creazione dell'endpoint"

Altro

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

- Certificati del pool di archiviazione cloud
- Certificati di notifica di avviso via e-mail
- Certificati del server syslog esterno
- Certificati di connessione alla federazione di rete
- Certificati di federazione delle identità
- Certificati del server di gestione delle chiavi (KMS)
- Certificati Single Sign-On

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

> ⓘ È possibile visualizzare e accedere alle informazioni per altri certificati solo se si dispone dell'"autorizzazione appropriata" .

Puoi:

- "Specificare un certificato Cloud Storage Pool per S3, C2S S3 o Azure"
- "Specificare un certificato per le notifiche e-mail di avviso"
- "Utilizzare un certificato per un server syslog esterno"
- "Ruotare i certificati di connessione della federazione di rete"
- "Visualizzare e modificare un certificato di federazione delle identità"
- "Carica i certificati del server e del client del server di gestione delle chiavi (KMS)"
- "Specificare manualmente un certificato SSO per un trust della parte affidabile"

Dettagli del certificato di sicurezza

Di seguito viene descritto ciascun tipo di certificato di sicurezza, con link alle istruzioni di implementazione.

Certificato di interfaccia di gestione

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

Certificato API S3

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica le connessioni client S3 sicure a un nodo di archiviazione e agli endpoint del bilanciatore del carico (facoltativo).	**CONFIGURAZIONE** > **Sicurezza** > **Certificati**, seleziona la scheda **Globale**, quindi seleziona **Certificato API S3**	"Configurare i certificati API S3"

Certificato CA di Grid

Vedi ilDescrizione del certificato CA Grid predefinito .

Certificato client amministratore

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Cliente	Installato su ciascun client, consente a StorageGRID di autenticare l'accesso dei client esterni. • Consente ai client esterni autorizzati di accedere al database StorageGRID Prometheus. • Consente il monitoraggio sicuro di StorageGRID tramite strumenti esterni.	**CONFIGURAZIONE** > **Sicurezza** > **Certificati** e quindi selezionare la scheda **Client**	"Configurare i certificati client"

Certificato dell'endpoint del bilanciatore del carico

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra i client S3 e il servizio StorageGRID Load Balancer sui nodi gateway e sui nodi amministrativi. È possibile caricare o generare un certificato del bilanciatore del carico quando si configura un endpoint del bilanciatore del carico. Le applicazioni client utilizzano il certificato del bilanciatore del carico quando si connettono a StorageGRID per salvare e recuperare i dati degli oggetti. Puoi anche utilizzare una versione personalizzata del globaleCertificato API S3 certificato per autenticare le connessioni al servizio Load Balancer. Se il certificato globale viene utilizzato per autenticare le connessioni del bilanciatore del carico, non è necessario caricare o generare un certificato separato per ogni endpoint del bilanciatore del carico. **Nota:** il certificato utilizzato per l'autenticazione del bilanciatore del carico è il certificato più utilizzato durante il normale funzionamento StorageGRID .	**CONFIGURAZIONE** > **Rete** > **Endpoint del bilanciatore del carico**	• "Configurare gli endpoint del bilanciatore del carico" • "Creare un endpoint del bilanciatore del carico per FabricPool"

Certificato endpoint del pool di archiviazione cloud

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione da un pool di archiviazione cloud StorageGRID a una posizione di archiviazione esterna, ad esempio S3 Glacier o Microsoft Azure Blob Storage. Per ogni tipo di provider cloud è richiesto un certificato diverso.	**ILM** > **Pool di archiviazione**	"Creare un pool di archiviazione cloud"

Certificato di notifica di avviso via e-mail

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	Autentica la connessione tra un server di posta elettronica SMTP e StorageGRID utilizzata per le notifiche di avviso. • Se le comunicazioni con il server SMTP richiedono Transport Layer Security (TLS), è necessario specificare il certificato CA del server di posta elettronica. • Specificare un certificato client solo se il server di posta elettronica SMTP richiede certificati client per l'autenticazione.	**AVVISI** > **Configurazione e-mail**	"Imposta notifiche e-mail per gli avvisi"

Certificato del server syslog esterno

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

Certificato di connessione alla federazione di rete

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	Autenticare e crittografare le informazioni inviate tra l'attuale sistema StorageGRID e un'altra griglia in una connessione di federazione di griglia.	**CONFIGURAZIONE** > **Sistema** > **Federazione di griglia**	• "Creare connessioni di federazione di griglia" • "Ruota i certificati di connessione"

Certificato di federazione dell'identità

Tipo di certificato	Descrizione	Posizione di navigazione	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 di gruppi di amministratori e utenti da parte di un sistema esterno.	**CONFIGURAZIONE** > **Controllo accessi** > **Federazione identità**	"Utilizzare la federazione delle identità"

Certificato del server di gestione delle chiavi (KMS)

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	Autentica la connessione tra StorageGRID e un server di gestione delle chiavi esterno (KMS), che fornisce chiavi di crittografia ai nodi dell'appliance StorageGRID .	**CONFIGURAZIONE** > **Sicurezza** > **Server di gestione delle chiavi**	"Aggiungi server di gestione delle chiavi (KMS)"

Certificato endpoint dei servizi di piattaforma

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione dal servizio della piattaforma StorageGRID a una risorsa di archiviazione S3.	**Gestore inquilino** > **ARCHIVIAZIONE (S3)** > **Endpoint dei servizi della piattaforma**	"Crea endpoint dei servizi della piattaforma" "Modifica endpoint dei servizi della piattaforma"

Certificato Single Sign-On (SSO)

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra i servizi di federazione delle identità, come Active Directory Federation Services (AD FS) e StorageGRID , utilizzati per le richieste Single Sign-On (SSO).	**CONFIGURAZIONE** > **Controllo accessi** > **Single sign-on**	"Configurare l'accesso singolo"

Esempi di certificati

Esempio 1: servizio Load Balancer

In questo esempio, StorageGRID funge da server.

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

basata sulla chiave privata.

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

Esempio 2: Server di gestione delle chiavi esterno (KMS)

In questo esempio, StorageGRID funge da client.

1. Utilizzando il software Key Management Server esterno, è possibile configurare StorageGRID come client KMS e ottenere un certificato server firmato da una CA, un certificato client pubblico e la chiave privata per il certificato client.
2. Utilizzando Grid Manager, puoi configurare un server KMS e caricare i certificati del server e del client, nonché la chiave privata del client.
3. Quando un nodo StorageGRID necessita di una chiave di crittografia, invia una richiesta al server KMS che include i dati del certificato e una firma basata sulla chiave privata.
4. Il server KMS convalida la firma del certificato e decide che StorageGRID può essere considerato attendibile.
5. Il server KMS risponde utilizzando la connessione convalidata.

Tipi di certificati server supportati

Il sistema StorageGRID supporta certificati personalizzati crittografati con RSA o ECDSA (Elliptic Curve Digital Signature Algorithm).

> Il tipo di cifratura per la policy di sicurezza deve corrispondere al tipo di certificato del server. Ad esempio, i cifrari RSA richiedono certificati RSA, mentre i cifrari ECDSA richiedono certificati ECDSA. Vedere "Gestire i certificati di sicurezza" . Se si configura un criterio di sicurezza personalizzato che non è compatibile con il certificato del server, è possibile"ripristinare temporaneamente la politica di sicurezza predefinita" .

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

Configurare i certificati dell'interfaccia di gestione

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

Informazioni su questo compito

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

Poiché per tutti i nodi amministrativi viene utilizzato un singolo certificato di interfaccia di gestione personalizzata, è necessario specificare il certificato come certificato jolly o multidominio se i client devono verificare il nome host durante la connessione a Grid Manager e Tenant Manager. Definisci il certificato

personalizzato in modo che corrisponda a tutti i nodi amministrativi nella griglia.

È necessario completare la configurazione sul server e, a seconda dell'autorità di certificazione radice (CA) utilizzata, gli utenti potrebbero dover installare anche il certificato Grid CA nel browser Web che utilizzeranno per accedere a Grid Manager e Tenant Manager.

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

Se si accede a Grid Manager o Tenant Manager utilizzando un nome di dominio anziché un indirizzo IP, il browser visualizza un errore di certificato senza un'opzione per ignorarlo se si verifica una delle seguenti situazioni:

- Il certificato dell'interfaccia di gestione personalizzata scade.
- Voiripristinare un certificato di interfaccia di gestione personalizzato al certificato del server predefinito .

Aggiungi un certificato di interfaccia di gestione personalizzato

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

Passi

1. Selezionare **CONFIGURAZIONE** > **Sicurezza** > **Certificati**.
2. Nella scheda **Globale**, seleziona **Certificato dell'interfaccia di gestione**.
3. Seleziona **Usa certificato personalizzato**.
4. Carica o genera il certificato.

Carica il certificato

Caricare i file del certificato del server richiesti.

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

     Le chiavi private EC devono essere di 224 bit o più grandi. Le chiavi private RSA devono essere di 2048 bit o più grandi.

   - **Bundle CA**: un singolo file facoltativo contenente i certificati di ciascuna autorità di certificazione (CA) emittente intermedia. Il file dovrebbe contenere ciascuno dei file di certificato CA codificati in PEM, concatenati nell'ordine della catena di certificati.
c. Espandi **Dettagli certificato** per visualizzare i metadati di ciascun certificato caricato. Se hai caricato un bundle CA facoltativo, ogni certificato verrà visualizzato in una scheda separata.
   - Selezionare **Scarica certificato** per salvare il file del certificato oppure selezionare **Scarica bundle CA** per salvare il bundle del certificato.

     Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione `.pem` .

   Ad esempio: `storagegrid_certificate.pem`

   - Selezionare **Copia certificato PEM** o **Copia pacchetto CA PEM** per copiare il contenuto del certificato e incollarlo altrove.
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

Generare i file del certificato del server.

La procedura consigliata per un ambiente di produzione è quella di utilizzare un certificato di interfaccia di gestione personalizzato firmato da un'autorità di certificazione esterna.

a. Seleziona **Genera certificato**.
b. Specificare le informazioni del certificato:

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

Campo	Descrizione
Proprietà intellettuale	Uno o più indirizzi IP da includere nel certificato.
Oggetto (facoltativo)	Soggetto X.509 o nome distinto (DN) del proprietario del certificato. Se non viene immesso alcun valore in questo campo, il certificato generato utilizza il primo nome di dominio o indirizzo IP come nome comune (CN) del soggetto.
Giorni validi	Numero di giorni dopo la creazione in cui scade il certificato.
Aggiungi estensioni di utilizzo delle chiavi	Se selezionata (impostazione predefinita e consigliata), le estensioni per l'utilizzo delle chiavi e per l'utilizzo esteso delle chiavi vengono aggiunte al certificato generato. Queste estensioni definiscono lo scopo della chiave contenuta nel certificato. **Nota**: lasciare selezionata questa casella di controllo a meno che non si riscontrino problemi di connessione con client più vecchi quando i certificati includono queste estensioni.

c. Seleziona **Genera**.

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

   - Selezionare **Scarica certificato** per salvare il file del certificato.

     Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione `.pem`.

     Ad esempio: `storagegrid_certificate.pem`

   - Selezionare **Copia certificato PEM** per copiare il contenuto del certificato e incollarlo 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, attendere fino a un giorno affinché tutti gli avvisi di scadenza del certificato correlati vengano cancellati.

6. Dopo aver aggiunto un certificato di interfaccia di gestione personalizzato, la pagina Certificato di interfaccia di gestione visualizza informazioni dettagliate sui certificati in uso. + È possibile scaricare o copiare il certificato PEM a seconda delle necessità.

Ripristina il certificato dell'interfaccia di gestione predefinita

È possibile tornare a utilizzare il certificato dell'interfaccia di gestione predefinito per le connessioni Grid

Manager e Tenant Manager.

Passi

1. Selezionare **CONFIGURAZIONE** > **Sicurezza** > **Certificati**.
2. Nella scheda **Globale**, seleziona **Certificato dell'interfaccia di gestione**.
3. Selezionare **Usa certificato predefinito**.

   Quando si ripristina il certificato dell'interfaccia di gestione predefinita, i file del certificato del server personalizzato configurati vengono eliminati e non possono essere recuperati dal sistema. Per tutte le successive nuove connessioni client verrà utilizzato il certificato dell'interfaccia di gestione predefinita.

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

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

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

Prima di iniziare

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

Informazioni su questo compito

La procedura migliore per un ambiente di produzione è quella di utilizzare un certificato firmato da un'autorità di certificazione esterna.

Passi

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

   Quando si accede come root, il prompt cambia da `$` A `#` .

3. Configurare StorageGRID con un nuovo certificato autofirmato.

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

   - Per `--domains` , utilizzare i caratteri jolly per rappresentare i nomi di dominio completi di tutti i nodi di amministrazione. Per esempio, `*.ui.storagegrid.example.com` usa il carattere jolly * per rappresentare `admin1.ui.storagegrid.example.com` E `admin2.ui.storagegrid.example.com` .
   - Impostato `--type` A `management` per configurare il certificato dell'interfaccia di gestione, utilizzato da Grid Manager e Tenant Manager.
   - Per impostazione predefinita, i certificati generati sono validi per un anno (365 giorni) e devono essere ricreati prima della scadenza. Puoi usare il `--days` argomento per sovrascrivere il periodo di validità

predefinito.

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

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

L'output risultante contiene il certificato pubblico richiesto dal client API di gestione.

4. Seleziona e copia il certificato.

   Includi i tag BEGIN e END nella tua selezione.

5. Disconnettersi dalla shell dei comandi. `$ exit`
6. Conferma che il certificato è stato configurato:
   a. Accedi al Grid Manager.
   b. Selezionare **CONFIGURAZIONE** > **Sicurezza** > **Certificati**
   c. Nella scheda **Globale**, seleziona **Certificato dell'interfaccia di gestione**.
7. Configura il tuo client di gestione per utilizzare il certificato pubblico che hai copiato. Includi i tag BEGIN e END.

Scarica o copia il certificato dell'interfaccia di gestione

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

Passi

1. Selezionare **CONFIGURAZIONE** > **Sicurezza** > **Certificati**.
2. Nella scheda **Globale**, seleziona **Certificato dell'interfaccia di gestione**.
3. Selezionare la scheda **Server** o **bundle CA**, quindi scaricare o copiare il certificato.

Scarica il file del certificato o il pacchetto CA

Scarica il certificato o il pacchetto CA `.pem` file. Se si utilizza un bundle CA facoltativo, ogni certificato nel bundle viene visualizzato nella propria sotto-scheda.

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

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

b. Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione `.pem` .

   Ad esempio: `storagegrid_certificate.pem`

Copia certificato o pacchetto CA PEM

Copia il testo del certificato per incollarlo altrove. Se si utilizza un bundle CA facoltativo, ogni certificato nel bundle viene visualizzato nella propria sotto-scheda.

a. Selezionare **Copia certificato PEM** o **Copia pacchetto CA PEM**.

   Se si copia un bundle CA, tutti i certificati nelle schede secondarie del bundle 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`

Configurare i certificati API S3

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

I dettagli su Swift sono stati rimossi da questa versione del sito di documentazione. Vedere "StorageGRID 11.8: configurare i certificati API S3 e Swift" .

Informazioni su questo compito

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

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

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

radice (CA) che stai utilizzando.

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

È possibile caricare o generare un certificato API S3 personalizzato.

Aggiungi un certificato API S3 personalizzato

Passi

1. Selezionare **CONFIGURAZIONE** > **Sicurezza** > **Certificati**.
2. Nella scheda **Globale**, seleziona **Certificato API S3**.
3. Seleziona **Usa certificato personalizzato**.
4. Carica o genera il certificato.

Carica il certificato

Caricare i file del certificato del server richiesti.

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

     Le chiavi private EC devono essere di 224 bit o più grandi. Le chiavi private RSA devono essere di 2048 bit o più grandi.

   - **Bundle CA**: un singolo file facoltativo contenente i certificati di ciascuna autorità di certificazione emittente intermedia. Il file dovrebbe contenere ciascuno dei file di certificato CA codificati in PEM, concatenati nell'ordine della catena di certificati.
c. Selezionare i dettagli del certificato per visualizzare i metadati e il PEM per ciascun certificato API S3 personalizzato caricato. Se hai caricato un bundle CA facoltativo, ogni certificato verrà visualizzato in una scheda separata.
   - Selezionare **Scarica certificato** per salvare il file del certificato oppure selezionare **Scarica bundle CA** per salvare il bundle del certificato.

     Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione `.pem` .

     Ad esempio: `storagegrid_certificate.pem`

   - Selezionare **Copia certificato PEM** o **Copia pacchetto CA PEM** per copiare il contenuto del certificato e incollarlo altrove.
d. Seleziona **Salva**.

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

Genera certificato

Generare i file del certificato del server.

a. Seleziona **Genera certificato**.
b. Specificare le informazioni del certificato:

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

Campo	Descrizione
Oggetto (facoltativo)	Soggetto X.509 o nome distinto (DN) del proprietario del certificato. Se non viene immesso alcun valore in questo campo, il certificato generato utilizza il primo nome di dominio o indirizzo IP come nome comune (CN) del soggetto.
Giorni validi	Numero di giorni dopo la creazione in cui scade il certificato.
Aggiungi estensioni di utilizzo delle chiavi	Se selezionata (impostazione predefinita e consigliata), le estensioni per l'utilizzo delle chiavi e per l'utilizzo esteso delle chiavi vengono aggiunte al certificato generato. Queste estensioni definiscono lo scopo della chiave contenuta nel certificato. **Nota**: lasciare selezionata questa casella di controllo a meno che non si riscontrino problemi di connessione con client più vecchi quando i certificati includono queste estensioni.

c. Seleziona **Genera**.

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

   - Selezionare **Scarica certificato** per salvare il file del certificato.

     Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione `.pem`.

     Ad esempio: `storagegrid_certificate.pem`

   - Selezionare **Copia certificato PEM** per copiare il contenuto del certificato e incollarlo altrove.

e. Seleziona **Salva**.

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

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

   Dopo aver caricato o generato un nuovo certificato, attendere fino a un giorno affinché tutti gli avvisi di scadenza del certificato correlati vengano cancellati.

6. Aggiorna la pagina per assicurarti che il browser web sia aggiornato.
7. Dopo aver aggiunto un certificato API S3 personalizzato, la pagina del certificato API S3 visualizza informazioni dettagliate sul certificato API S3 personalizzato in uso. + È possibile scaricare o copiare il certificato PEM a seconda delle necessità.

Ripristina il certificato API S3 predefinito

È possibile tornare a utilizzare il certificato API S3 predefinito per le connessioni client S3 ai nodi di archiviazione. Tuttavia, non è possibile utilizzare il certificato API S3 predefinito per un endpoint del bilanciatore del carico.

Passi

1. Selezionare **CONFIGURAZIONE** > **Sicurezza** > **Certificati**.
2. Nella scheda **Globale**, seleziona **Certificato API S3**.
3. Selezionare **Usa certificato predefinito**.

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

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

   Se si dispone dell'autorizzazione di accesso Root e per le connessioni degli endpoint del bilanciatore del carico è stato utilizzato il certificato API S3 personalizzato, verrà visualizzato un elenco degli endpoint del bilanciatore del carico che non saranno più accessibili utilizzando il certificato API S3 predefinito. Vai a"Configurare gli endpoint del bilanciatore del carico" per modificare o rimuovere gli endpoint interessati.

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

Scarica o copia il certificato API S3

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

Passi

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

Scarica il file del certificato o il pacchetto CA

Scarica il certificato o il pacchetto CA `.pem` file. Se si utilizza un bundle CA facoltativo, ogni certificato nel bundle viene visualizzato nella propria sotto-scheda.

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

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

b. Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione `.pem` .

   Ad esempio: `storagegrid_certificate.pem`

Copia certificato o pacchetto CA PEM

Copia il testo del certificato per incollarlo altrove. Se si utilizza un bundle CA facoltativo, ogni certificato nel bundle viene visualizzato nella propria sotto-scheda.

a. Selezionare **Copia certificato PEM** o **Copia pacchetto CA PEM**.

   Se si copia un bundle CA, tutti i certificati nelle schede secondarie del bundle 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

- "Utilizzare l'API REST S3"
- "Configurare i nomi di dominio degli endpoint S3"

Copia il certificato Grid CA

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

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Hai"autorizzazioni di accesso specifiche" .

Informazioni su questo compito

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

Passi

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

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

Scarica il file del certificato

Scarica il certificato `.pem` file.

a. Seleziona **Scarica certificato**.

b. Specificare il nome del file del certificato e il percorso 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. Selezionare **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`

Configurare i certificati StorageGRID per FabricPool

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

Prima di iniziare

- Hai"autorizzazioni di accesso specifiche" .
- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .

Informazioni su questo compito

Quando si crea un endpoint del bilanciatore del carico, è possibile generare un certificato server autofirmato o caricare un certificato firmato da un'autorità di certificazione (CA) nota. Negli ambienti di produzione, è consigliabile utilizzare un certificato firmato da una CA nota. 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 passaggi seguenti forniscono linee guida generali per i client S3 che utilizzano FabricPool. Per informazioni e procedure più dettagliate, vedere"Configurare StorageGRID per FabricPool" .

Passi

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

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

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

3. Collegare StorageGRID come livello cloud in ONTAP.

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

   > Se il certificato StorageGRID è stato emesso da una CA intermedia, è necessario fornire il certificato della CA intermedia. Se il certificato StorageGRID è stato emesso direttamente dalla CA radice, è necessario fornire il certificato della CA radice.

Configurare i certificati client

I certificati client consentono ai client esterni autorizzati di accedere al database StorageGRID Prometheus, offrendo agli strumenti esterni un modo sicuro per monitorare StorageGRID.

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

Vedere"Gestire i certificati di sicurezza" E"Configurare certificati server personalizzati" .

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

> Se si utilizza un server di gestione delle chiavi (KMS) per proteggere i dati sui nodi appliance configurati in modo speciale, consultare le informazioni specifiche su"caricamento di un certificato client KMS" .

Prima di iniziare

- Hai i permessi di accesso Root.
- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Per configurare un certificato client:
  - Hai l'indirizzo IP o il nome di dominio del nodo di amministrazione.
  - Se hai configurato il certificato dell'interfaccia di gestione StorageGRID , disponi della CA, del certificato client e della 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 si dispone della chiave privata originale, è necessario crearne una nuova.
- Per modificare un certificato client:
  - Hai l'indirizzo IP o il nome di dominio del nodo di amministrazione.
  - 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, utilizzare una di queste procedure:

- Certificato dell'interfaccia di gestione già configurato
- Certificato client rilasciato da CA
- Certificato generato da Grid Manager

Certificato dell'interfaccia di gestione già configurato

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

Passi

1. In Grid Manager, seleziona **CONFIGURAZIONE** > **Sicurezza** > **Certificati** e quindi seleziona la scheda **Client**.
2. Selezionare **Aggiungi**.
3. Inserisci un nome per il certificato.
4. Per accedere alle metriche di Prometheus tramite il tuo strumento di monitoraggio esterno, seleziona **Consenti Prometheus**.
5. Selezionare **Continua**.
6. Per il passaggio **Allega certificati**, caricare il certificato dell'interfaccia di gestione.
   a. Seleziona **Carica certificato**.
   b. Selezionare **Sfoglia** e selezionare il file del certificato dell'interfaccia di gestione(`.pem`).
      - Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.
      - Selezionare **Copia certificato PEM** per copiare il contenuto del certificato e incollarlo altrove.
   c. Selezionare **Crea** per salvare il certificato in Grid Manager.

      Il nuovo certificato viene visualizzato nella scheda Client.
7. Configurare uno strumento di monitoraggio esterno, come Grafana.

Certificato client rilasciato da CA

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

Passi

1. Eseguire i passaggi per"configurare un certificato di interfaccia di gestione" .
2. In Grid Manager, seleziona **CONFIGURAZIONE** > **Sicurezza** > **Certificati** e quindi seleziona la scheda **Client**.
3. Selezionare **Aggiungi**.
4. Inserisci un nome per il certificato.
5. Per accedere alle metriche di Prometheus tramite il tuo strumento di monitoraggio esterno, seleziona **Consenti Prometheus**.

6. Selezionare **Continua**.
7. Per la fase **Allega certificati**, carica i file del certificato client, della chiave privata e del bundle CA:
   a. Seleziona **Carica certificato**.
   b. Selezionare **Sfoglia** e selezionare il certificato client, la chiave privata e i file bundle CA(`.pem`).
      - Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.
      - Selezionare **Copia certificato PEM** per copiare il contenuto del certificato e incollarlo altrove.
   c. Selezionare **Crea** per salvare il certificato in Grid Manager.

   I nuovi certificati vengono visualizzati nella scheda Client.
8. Configurare uno strumento di monitoraggio esterno, come Grafana.

Certificato generato da Grid Manager

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

Passi

1. In Grid Manager, seleziona **CONFIGURAZIONE** > **Sicurezza** > **Certificati** e quindi seleziona la scheda **Client**.
2. Selezionare **Aggiungi**.
3. Inserisci un nome per il certificato.
4. Per accedere alle metriche di Prometheus tramite il tuo strumento di monitoraggio esterno, seleziona **Consenti Prometheus**.
5. Selezionare **Continua**.
6. Per il passaggio **Allega certificati**, seleziona **Genera certificato**.
7. Specificare le informazioni del certificato:
   - **Oggetto** (facoltativo): soggetto X.509 o nome distinto (DN) del proprietario del certificato.
   - **Giorni di validità**: numero di giorni di validità del certificato generato, a partire dal momento in cui viene generato.
   - **Aggiungi estensioni per l'utilizzo delle chiavi**: se selezionato (impostazione predefinita e consigliata), le estensioni per l'utilizzo delle chiavi e l'utilizzo esteso delle chiavi vengono aggiunte al certificato generato.

     Queste estensioni definiscono lo scopo della chiave contenuta nel certificato.

     Lasciare selezionata questa casella di controllo a meno che non si riscontrino problemi di connessione con client più vecchi quando i certificati includono queste estensioni.
8. Seleziona **Genera**.
9. Selezionare **Dettagli del certificato client** per visualizzare i metadati del certificato e il PEM del certificato.

Dopo aver chiuso la finestra di dialogo, non sarà possibile visualizzare la chiave privata del certificato. Copia o scarica la chiave in un luogo sicuro.

- Selezionare **Copia certificato PEM** per copiare il contenuto del certificato e incollarlo altrove.
- Selezionare **Scarica certificato** per salvare il file del certificato.

  Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione `.pem`.

  Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copia chiave privata** per copiare la chiave privata del certificato e incollarla altrove.
- Selezionare **Scarica chiave privata** per salvare la chiave privata come file.

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

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

    Il nuovo certificato viene visualizzato nella scheda Client.

11. In Grid Manager, seleziona **CONFIGURAZIONE** > **Sicurezza** > **Certificati** e quindi seleziona la scheda **Globale**.
12. Selezionare **Certificato interfaccia di gestione**.
13. Seleziona **Usa certificato personalizzato**.
14. Carica i file certificate.pem e private_key.pem dadettagli del certificato client fare un passo. Non è necessario caricare il bundle CA.
    a. Selezionare **Carica certificato** e poi **Continua**.
    b. Carica ogni file di certificato(`.pem`).
    c. Selezionare **Salva** per salvare il certificato in Grid Manager.

       Il nuovo certificato viene visualizzato nella pagina dei certificati dell'interfaccia di gestione.
15. Configurare uno strumento di monitoraggio esterno, come Grafana.

Configura uno strumento di monitoraggio esterno

Passi

1. Configura le seguenti impostazioni sul tuo strumento di monitoraggio esterno, come Grafana.
   a. **Nome**: inserisci un nome per la connessione.

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

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

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

   c. Abilita **TLS Client Auth** e **Con certificato CA**.
   d. In Dettagli autorizzazione TLS/SSL, copia e incolla:

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

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

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

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

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

Per informazioni sulle metriche, vedere"istruzioni per il monitoraggio StorageGRID" .

Modifica i certificati client

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

Passi

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

Nella tabella sono elencate le date di scadenza dei certificati e le autorizzazioni di accesso a Prometheus. Se un certificato sta per scadere o è già scaduto, nella tabella viene visualizzato un messaggio e viene attivato un avviso.

2. Seleziona il certificato che vuoi modificare.
3. Seleziona **Modifica** e poi seleziona **Modifica nome e autorizzazione**
4. Inserisci un nome per il certificato.
5. Per accedere alle metriche di Prometheus tramite il tuo strumento di monitoraggio esterno, seleziona **Consenti Prometheus**.
6. Selezionare **Continua** per salvare il certificato in Grid Manager.

Il certificato aggiornato viene visualizzato nella scheda Client.

Allega nuovo certificato client

È possibile caricare un nuovo certificato quando quello attuale è scaduto.

Passi

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

Nella tabella sono elencate le date di scadenza dei certificati e le autorizzazioni di accesso a Prometheus. Se un certificato sta per scadere o è già scaduto, nella tabella viene visualizzato un messaggio e viene attivato un avviso.

2. Seleziona il certificato che vuoi modificare.
3. Selezionare **Modifica** e quindi selezionare un'opzione di modifica.

Carica il certificato

Copia il testo del certificato per incollarlo altrove.

a. Selezionare **Carica certificato** e poi **Continua**.

b. Carica il nome del certificato client(`.pem`).

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

   - Selezionare **Scarica certificato** per salvare il file del certificato.

     Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione `.pem` .

   Ad esempio: `storagegrid_certificate.pem`

   - Selezionare **Copia certificato PEM** per copiare il contenuto del certificato e incollarlo altrove.

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

   Il certificato aggiornato viene visualizzato nella scheda Client.

Genera certificato

Genera il testo del certificato da incollare altrove.

a. Seleziona **Genera certificato**.

b. Specificare le informazioni del certificato:

   - **Oggetto** (facoltativo): soggetto X.509 o nome distinto (DN) del proprietario del certificato.
   - **Giorni di validità**: numero di giorni di validità del certificato generato, a partire dal momento in cui viene generato.
   - **Aggiungi estensioni per l'utilizzo delle chiavi**: se selezionato (impostazione predefinita e consigliata), le estensioni per l'utilizzo delle chiavi e l'utilizzo esteso delle chiavi vengono aggiunte al certificato generato.

     Queste estensioni definiscono lo scopo della chiave contenuta nel certificato.

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

c. Seleziona **Genera**.

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

   Dopo aver chiuso la finestra di dialogo, non sarà possibile visualizzare la chiave privata del certificato. Copia o scarica la chiave in un luogo sicuro.

   - Selezionare **Copia certificato PEM** per copiare il contenuto del certificato e incollarlo altrove.

- Selezionare **Scarica certificato** per salvare il file del certificato.

  Specificare il nome del file del certificato e il percorso di download. Salva il file con l'estensione `.pem` .

  Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copia chiave privata** per copiare la chiave privata del certificato e incollarla altrove.
- Selezionare **Scarica chiave privata** per salvare la chiave privata come file.

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

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

Il nuovo certificato viene visualizzato nella scheda Client.

Scarica o copia i certificati client

È possibile scaricare o copiare un certificato client per utilizzarlo altrove.

Passi

1. Selezionare **CONFIGURAZIONE** > **Sicurezza** > **Certificati** e quindi selezionare la scheda **Client**.
2. Seleziona il certificato che vuoi copiare o scaricare.
3. Scarica o copia il certificato.

Scarica il file del certificato

Scarica il certificato `.pem` file.

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

   Ad esempio: `storagegrid_certificate.pem`

Copia il certificato

Copia il testo del certificato per incollarlo altrove.

a. Selezionare **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`

Rimuovere i certificati client

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

Passi

1. Selezionare **CONFIGURAZIONE** > **Sicurezza** > **Certificati** e quindi selezionare la scheda **Client**.
2. Seleziona il certificato che desideri rimuovere.
3. Selezionare **Elimina** e quindi confermare.

> Per rimuovere fino a 10 certificati, seleziona ciascun certificato da rimuovere nella scheda Client, 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.

Configurare le impostazioni di sicurezza

Gestire la politica TLS e SSH

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

La policy di sicurezza controlla il modo in cui TLS e SSH crittografano i dati in movimento. In generale, utilizzare il criterio di compatibilità moderna (predefinito), a meno che il sistema non debba essere conforme ai Common Criteria o non sia necessario utilizzare altri cifrari.

> Alcuni servizi StorageGRID non sono stati aggiornati per utilizzare le cifrature in queste policy.

Prima di iniziare

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

Seleziona una politica di sicurezza

Passi

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

   La scheda **Criteri TLS e SSH** mostra i criteri disponibili. La policy attualmente attiva è contrassegnata da un segno di spunta verde nel riquadro della policy.

2. Esamina i riquadri per scoprire le policy disponibili.

Politica	Descrizione
Compatibilità moderna (predefinita)	Utilizzare il criterio predefinito se è necessaria una crittografia avanzata e a meno che non si abbiano requisiti particolari. Questa policy è compatibile con la maggior parte dei client TLS e SSH.
Compatibilità legacy	Utilizza questa policy se hai bisogno di opzioni di compatibilità aggiuntive per i client più vecchi. Le opzioni aggiuntive presenti in questa policy potrebbero renderla meno sicura rispetto alla policy di compatibilità moderna.
Criteri comuni	Utilizzare questa politica se è necessaria la certificazione Common Criteria.
FIPS rigoroso	Utilizzare questa policy se è richiesta la certificazione Common Criteria e si deve utilizzare NetApp Cryptographic Security Module 3.0.8 per le connessioni client esterne agli endpoint del bilanciatore del carico, Tenant Manager e Grid Manager. L'utilizzo di questa policy potrebbe ridurre le prestazioni. **Nota**: Dopo aver selezionato questa policy, tutti i nodi devono essere"riavviato in modo progressivo" per attivare il modulo di sicurezza crittografica NetApp . Utilizzare **Manutenzione** > **Riavvio progressivo** per avviare e monitorare i riavvii.
Costume	Crea una policy personalizzata se devi applicare i tuoi cifrari.

3. Per visualizzare i dettagli sui cifrari, i protocolli e gli algoritmi di ogni policy, seleziona **Visualizza dettagli**.
4. Per modificare la policy corrente, seleziona **Usa policy**.

   Accanto a **Criterio attuale** nel riquadro del criterio appare un segno di spunta verde.

Crea una policy di sicurezza personalizzata

È possibile creare una policy personalizzata se è necessario applicare cifrari personalizzati.

Passi

1. Dal riquadro della policy più simile alla policy personalizzata che desideri creare, seleziona **Visualizza dettagli**.
2. Selezionare **Copia negli appunti**, quindi selezionare **Annulla**.

3. Dal riquadro **Criterio personalizzato**, seleziona **Configura e usa**.
4. Incolla il JSON che hai copiato e apporta le modifiche necessarie.
5. Seleziona **Utilizza policy**.

   Accanto a **Criterio attuale** nel riquadro Criterio personalizzato appare un segno di spunta verde.

6. Facoltativamente, seleziona **Modifica configurazione** per apportare ulteriori modifiche alla nuova policy personalizzata.

Ripristina temporaneamente la politica di sicurezza predefinita

Se hai configurato un criterio di sicurezza personalizzato, potresti non essere in grado di accedere a Grid Manager se il criterio TLS configurato non è compatibile con"certificato del server configurato" .

È possibile ripristinare temporaneamente i criteri di sicurezza predefiniti.

Passi

1. Accedi a un nodo di amministrazione:
   a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`
   b. Inserisci la password elencata nel `Passwords.txt` file.
   c. Immettere il seguente comando per passare alla root: `su -`
   d. Inserisci la password elencata nel `Passwords.txt` file.

      Quando si accede come root, il prompt cambia da `$` A `#` .

2. Esegui il seguente comando:

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

3. Da un browser Web, accedi a Grid Manager sullo stesso nodo di amministrazione.
4. Segui i passaggi inSeleziona una politica di sicurezza per configurare nuovamente la policy.

Configurare la sicurezza della rete e degli oggetti

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

Crittografia degli oggetti memorizzati

La crittografia degli oggetti archiviati consente la crittografia di tutti i dati degli oggetti quando vengono acquisiti tramite S3. Per impostazione predefinita, gli oggetti archiviati non sono crittografati, ma è possibile scegliere di crittografarli utilizzando l'algoritmo di crittografia AES-128 o AES-256. Quando si abilita l'impostazione, tutti gli oggetti appena acquisiti vengono crittografati, ma non viene apportata alcuna modifica agli oggetti archiviati esistenti. Se si disabilita la crittografia, gli oggetti attualmente crittografati rimangono crittografati, ma gli oggetti appena 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 di oggetto.

Per maggiori dettagli sui metodi di crittografia StorageGRID , vedere"Esaminare i metodi di crittografia StorageGRID" .

Impedisci la modifica del client

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

API REST S3

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

Abilita HTTP per le connessioni del nodo di archiviazione

Per impostazione predefinita, le applicazioni client utilizzano il protocollo di rete HTTPS per tutte le connessioni dirette ai nodi di archiviazione. Facoltativamente, è possibile abilitare HTTP per queste connessioni, ad esempio quando si testa una griglia non di produzione.

Utilizzare HTTP per le connessioni ai nodi di archiviazione solo se i client S3 devono effettuare connessioni HTTP direttamente ai nodi di archiviazione. Non è necessario utilizzare questa opzione per i client che utilizzano solo connessioni HTTPS o per i client che si connettono al servizio Load Balancer (perché è possibile"configurare ogni endpoint del bilanciatore del carico" per utilizzare HTTP o HTTPS).

Vedere"Riepilogo: indirizzi IP e porte per le connessioni client" per scoprire quali porte utilizzano i client S3 quando si connettono ai nodi di archiviazione tramite HTTP o HTTPS.

Seleziona le opzioni

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Hai i permessi di accesso Root.

Passi

1. Selezionare **CONFIGURAZIONE** > **Sicurezza** > **Impostazioni di sicurezza**.
2. Selezionare la scheda **Rete e oggetti**.
3. Per la crittografia degli oggetti archiviati, utilizzare l'impostazione **Nessuno** (predefinita) se non si desidera che gli oggetti archiviati vengano crittografati oppure selezionare **AES-128** o **AES-256** per crittografare gli oggetti archiviati.
4. Facoltativamente, seleziona **Impedisci modifica client** se vuoi impedire ai client S3 di effettuare richieste specifiche.

> Se si modifica questa impostazione, ci vorrà circa un minuto prima che la nuova impostazione venga applicata. Il valore configurato viene memorizzato nella cache per migliorare le prestazioni e il ridimensionamento.

5. Facoltativamente, selezionare **Abilita HTTP per le connessioni ai nodi di archiviazione** se i client si connettono direttamente ai nodi di archiviazione e si desidera utilizzare le connessioni HTTP.

> Prestare attenzione quando si abilita HTTP per una griglia di produzione perché le richieste verranno inviate non crittografate.

6. Seleziona **Salva**.

Modificare le impostazioni di sicurezza dell'interfaccia

Le impostazioni di sicurezza dell'interfaccia consentono di controllare se gli utenti vengono disconnessi se rimangono inattivi per un periodo di tempo superiore a quello specificato e se una traccia dello stack viene inclusa nelle risposte di errore dell'API.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Hai"Permesso di accesso root" .

Informazioni su questo compito

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 da quanto segue:

- 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 dell'utente. Quando scade l'autenticazione di un utente, l'utente viene automaticamente disconnesso, anche se il timeout di inattività del browser è disabilitato o il valore per il timeout del browser non è stato raggiunto. Per rinnovare il token, l'utente deve effettuare nuovamente l'accesso.
- Impostazioni di timeout per il provider di identità, presupponendo che l'accesso Single Sign-On (SSO) sia abilitato per StorageGRID.

  Se l'SSO è abilitato e il browser di un utente scade, l'utente deve reinserire le proprie credenziali SSO per accedere nuovamente a StorageGRID . Vedere "Configurare l'accesso singolo" .

Stack trace dell'API di gestione

Controlla se viene restituita una traccia dello stack nelle risposte di errore dell'API Grid Manager e Tenant Manager.

Questa opzione è disabilitata per impostazione predefinita, ma potrebbe essere opportuno abilitare questa funzionalità per un ambiente di prova. In generale, negli ambienti di produzione è consigliabile lasciare la traccia dello stack disabilitata per evitare di rivelare dettagli software interni quando si verificano errori API.

Passi

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

      La nuova impostazione non ha effetto sugli utenti che hanno effettuato l'accesso. Gli utenti devono effettuare nuovamente l'accesso o aggiornare il browser affinché la nuova impostazione di timeout abbia effetto.
4. Per modificare l'impostazione per la traccia dello stack dell'API di gestione:
   a. Espandi la fisarmonica.
   b. Selezionare la casella di controllo per restituire una traccia dello stack nelle risposte di errore dell'API Grid Manager e Tenant Manager.

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

   c. Seleziona **Salva**.

Configurare i server di gestione delle chiavi

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

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

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

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

StorageGRID non crea né gestisce le chiavi esterne utilizzate per crittografare e decrittografare i nodi dell'appliance. Se si prevede di utilizzare un server di gestione delle chiavi esterno per proteggere i dati StorageGRID , è necessario comprendere come configurare tale server e come gestire le chiavi di crittografia. L'esecuzione di attività di gestione chiave esula dallo scopo di queste istruzioni. Se hai bisogno di aiuto, consulta la documentazione del tuo server di gestione delle chiavi o contatta l'assistenza tecnica.

Configurazione KMS e appliance

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

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

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

Configurare il server di gestione delle chiavi (KMS)

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

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

Impostare l'apparecchio

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

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

Non è possibile abilitare l'impostazione **Crittografia nodo** dopo aver aggiunto un'appliance alla griglia e non è possibile utilizzare la gestione delle chiavi esterne per le appliance che non hanno la crittografia nodo abilitata.

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

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

Processo di crittografia della gestione delle chiavi (avviene automaticamente)

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

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

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

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

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

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

Quale versione di KMIP è supportata?

StorageGRID supporta KMIP versione 1.4.

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

Quali sono le considerazioni da fare in merito alla rete?

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

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

Quali versioni di TLS sono supportate?

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

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

Quali elettrodomestici sono supportati?

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

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

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

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

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

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

Quando dovrei configurare i server di gestione delle chiavi?

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

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

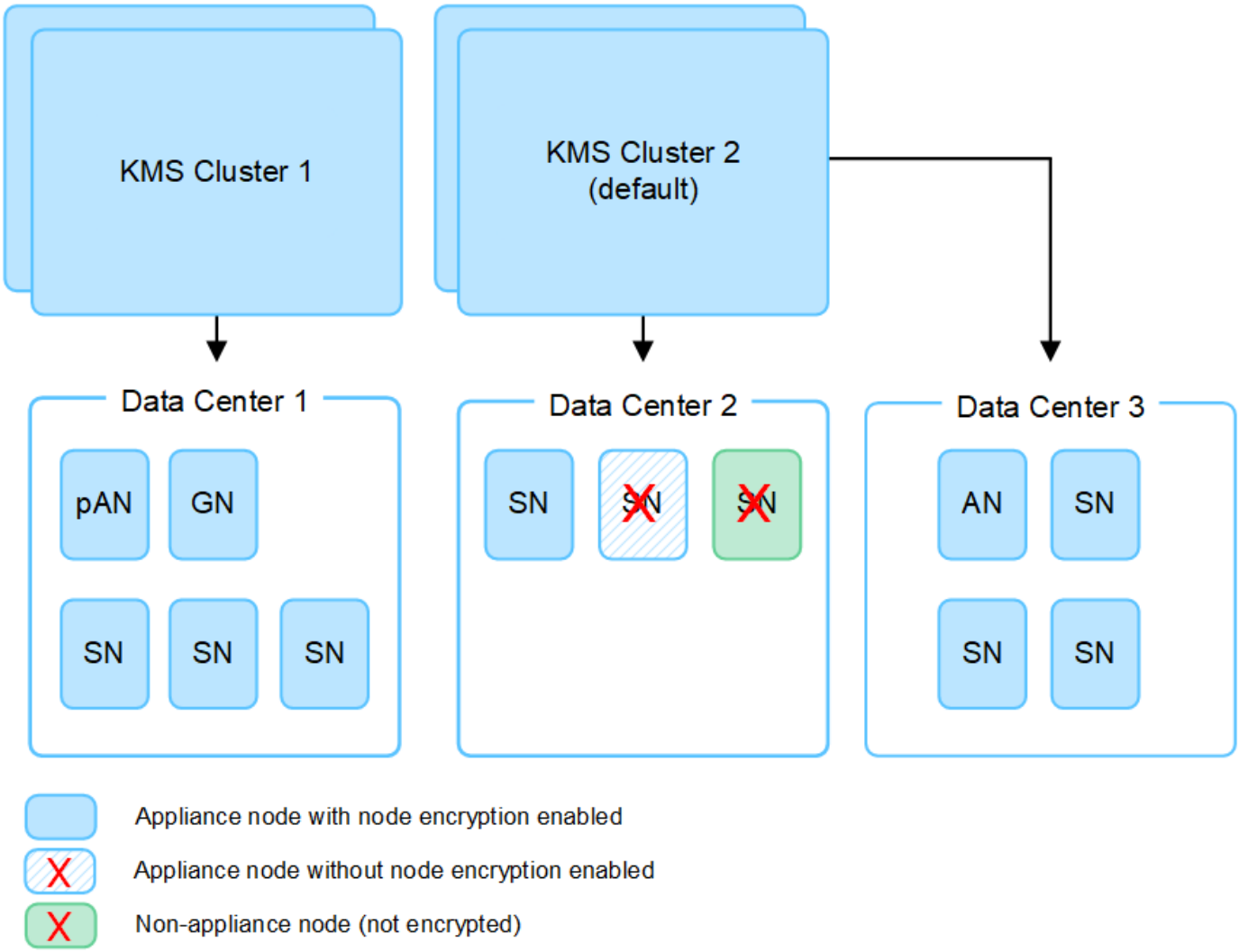
Di quanti server di gestione delle chiavi ho bisogno?

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

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

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

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



Cosa succede quando si ruota una chiave?

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

Quando sarà disponibile la nuova versione della chiave:

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

dell'appliance. Potrebbe essere necessario contattare l'assistenza tecnica per ricevere aiuto nella risoluzione di questo avviso.

Posso riutilizzare un nodo appliance dopo averlo crittografato?

Se è necessario installare un'appliance crittografata in un altro sistema StorageGRID , è necessario prima disattivare il nodo della griglia per spostare i dati dell'oggetto su un altro nodo. Quindi, è possibile utilizzare StorageGRID Appliance Installer per "cancellare la configurazione KMS" . La cancellazione della configurazione KMS disabilita l'impostazione **Crittografia nodo** e rimuove l'associazione tra il nodo dell'appliance e la configurazione KMS per il sito StorageGRID .

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

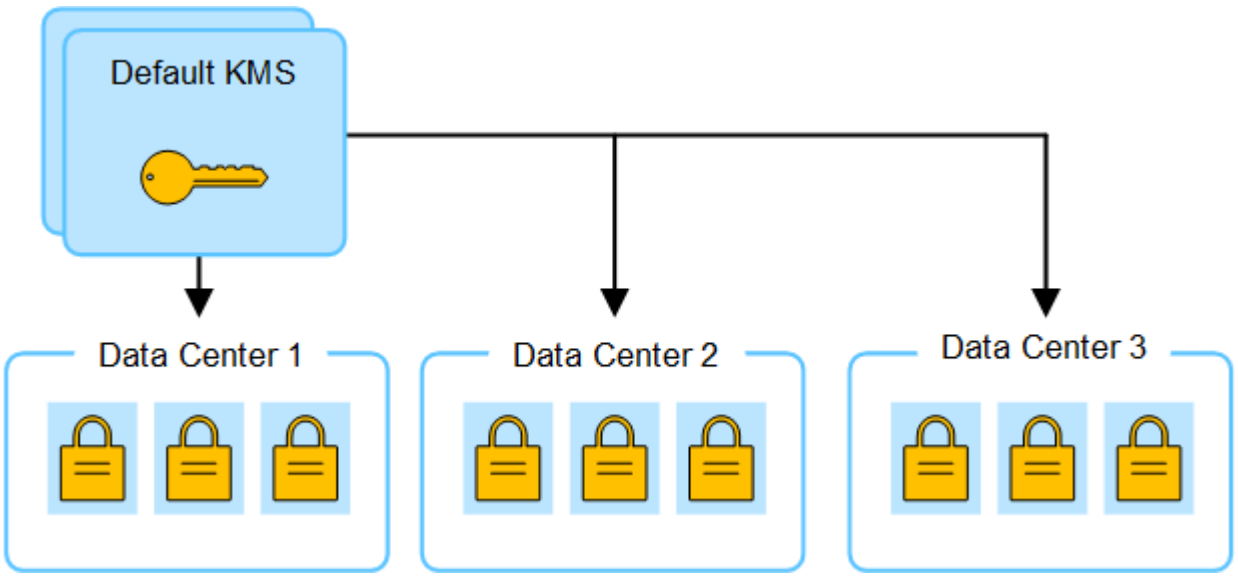
Considerazioni sulla modifica del KMS per un sito

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

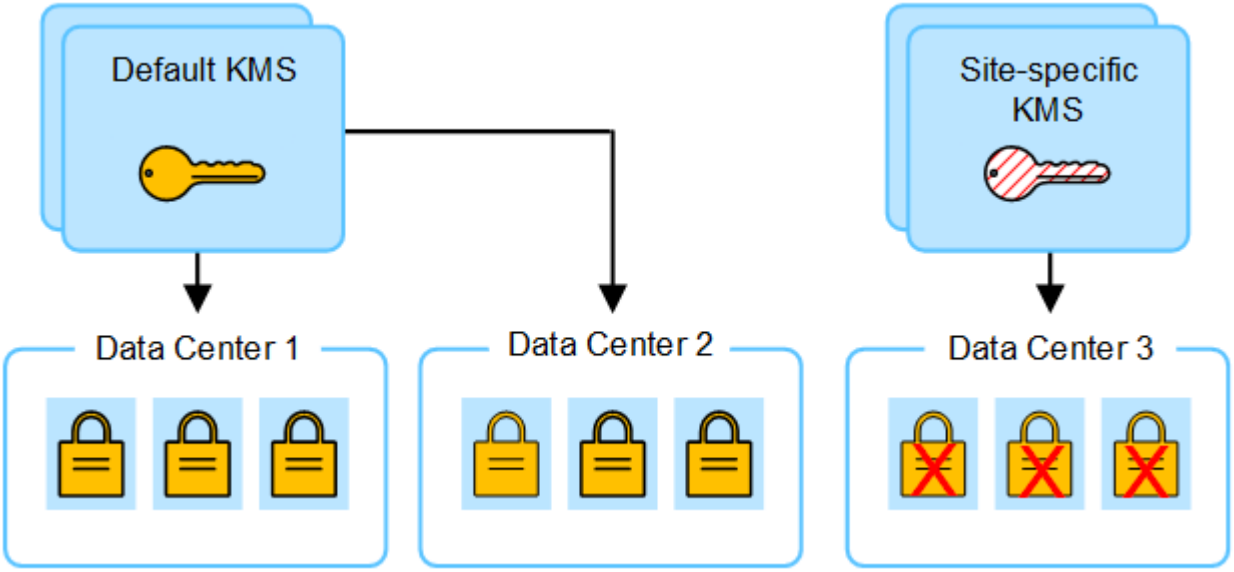
Se si modifica il KMS utilizzato per un sito, è necessario assicurarsi che i nodi dell'appliance precedentemente crittografati in quel sito possano essere decrittografati utilizzando la chiave memorizzata sul nuovo KMS. In alcuni casi, potrebbe essere necessario copiare la versione corrente della chiave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

Per esempio:

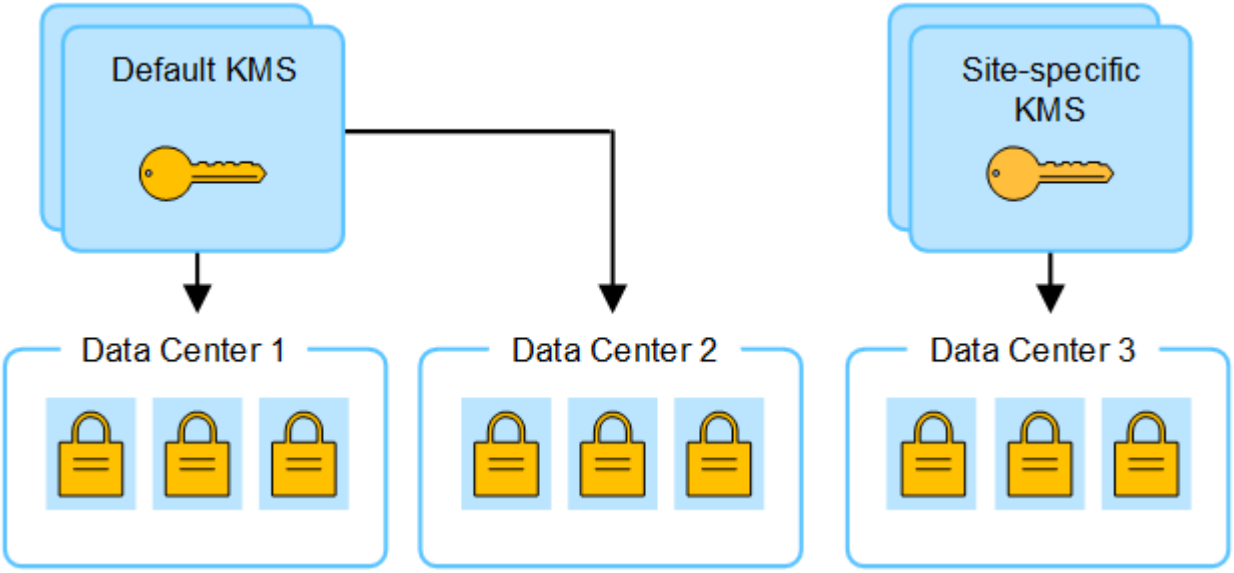
1. Inizialmente si configura un KMS predefinito che si applica a tutti i siti che non dispongono di un KMS dedicato.
2. Una volta salvato il KMS, tutti i nodi dell'appliance in cui è abilitata l'impostazione **Crittografia nodo** si connettono al KMS e richiedono la chiave di crittografia. Questa chiave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



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



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



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

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

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

Configurare StorageGRID come client nel KMS

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

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

Passi

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

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

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

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

   - Chiedi a StorageGRID di creare la chiave. Ti verrà chiesto quando esegui il test e salvi dopo"caricamento dei certificati client" .
3. Registrare le seguenti informazioni per ciascun KMS o cluster KMS.

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

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

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

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

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

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

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

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

   Il certificato client consente a StorageGRID di autenticarsi al KMS.

Aggiungere un server di gestione delle chiavi (KMS)

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

Prima di iniziare

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

Informazioni su questo compito

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

Passaggio 1: dettagli KMS

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

Passi

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

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

2. Seleziona **Crea**.

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

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

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

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

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

Passaggio 2: carica il certificato del server

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

Passi

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

   Vengono visualizzati i metadati del certificato del server.

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

3. Selezionare **Continua**.

Passaggio 3: Carica i certificati client

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

Passi

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

   Vengono visualizzati i metadati del certificato client.

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

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

   Vengono testate le connessioni tra il server di gestione delle chiavi e i nodi dell'appliance. Se tutte le connessioni sono valide e la chiave corretta viene trovata sul KMS, il nuovo server di gestione delle chiavi

viene aggiunto alla tabella nella pagina Server di gestione delle chiavi.

> Subito dopo aver aggiunto un KMS, lo stato del certificato nella pagina Key Management Server appare come Sconosciuto. StorageGRID potrebbe impiegare fino a 30 minuti per ottenere lo stato effettivo di ciascun certificato. Per visualizzare lo stato attuale, è necessario aggiornare il browser web.

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

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

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

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

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

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

Gestire un KMS

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

Prima di iniziare

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

Visualizza i dettagli KMS

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

Passi

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

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

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

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

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

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

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

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

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

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

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

Gestisci i certificati

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

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

Passi

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

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

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

Visualizza i nodi crittografati

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

Passi

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

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

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

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

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

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

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

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

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

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

Eseguire le azioni consigliate per questi avvisi.

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

Modifica un KMS

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

Prima di iniziare

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

Passi

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

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

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

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

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

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

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

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

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

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

   Viene visualizzato il passaggio 3 (Caricamento dei certificati client) della procedura guidata Modifica un server di gestione delle chiavi.

8. Se è necessario sostituire il certificato client e la chiave privata del certificato client, selezionare **Sfoglia** e caricare i nuovi file.
9. Seleziona **Test e salva**.

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

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

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

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

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

La configurazione KMS è stata salvata.

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

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

Rimuovere un server di gestione delle chiavi (KMS)

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

Prima di iniziare

- Hai esaminato il"considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi" .
- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Tu hai il"Permesso di accesso root" .

Informazioni su questo compito

È possibile rimuovere un KMS nei seguenti casi:

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

Passi

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

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

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

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

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

   La configurazione KMS è stata rimossa.

Gestisci le impostazioni proxy

Configurare il proxy di archiviazione

Se si utilizzano servizi di piattaforma o pool di archiviazione cloud, è possibile configurare un proxy non trasparente tra i nodi di archiviazione e gli endpoint S3 esterni. Ad esempio, potrebbe essere necessario un proxy non trasparente per consentire l'invio di messaggi dei servizi della piattaforma a 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" .
- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .

Informazioni su questo compito

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

Passi

1. Selezionare **CONFIGURAZIONE** > **Sicurezza** > **Impostazioni proxy**.
2. Nella scheda **Archiviazione**, seleziona la casella di controllo **Abilita proxy di archiviazione**.
3. Selezionare il protocollo per il proxy di archiviazione.
4. Inserisci il nome host o l'indirizzo IP del server proxy.
5. Facoltativamente, immettere la porta utilizzata per connettersi al server proxy.

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

6. Seleziona **Salva**.

   Dopo aver salvato il proxy di archiviazione, è possibile configurare e testare nuovi endpoint per i servizi della piattaforma o i pool di archiviazione cloud.

   > Le modifiche apportate al proxy potrebbero richiedere fino a 10 minuti per diventare effettive.

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

Configurare le impostazioni del proxy amministratore

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

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

Prima di iniziare

- Hai"autorizzazioni di accesso specifiche" .
- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .

Informazioni su questo compito

È possibile configurare le impostazioni per un singolo proxy amministratore.

Passi

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

   Viene visualizzata la pagina Impostazioni proxy. Per impostazione predefinita, nel menu delle schede è selezionata l'opzione Archiviazione.

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

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

7. Seleziona una delle seguenti opzioni:

   - Se si desidera proteggere la connessione al proxy di amministrazione, selezionare **Verifica certificato proxy**. Carica un bundle CA per verificare l'autenticità dei certificati SSL presentati dal server proxy di amministrazione.

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

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

   - Se non si desidera convalidare i certificati durante la comunicazione con il server proxy di amministrazione, selezionare **Non verificare il certificato proxy**.

8. Seleziona **Salva**.

   Dopo aver salvato il proxy di amministrazione, viene configurato il server proxy tra i nodi di amministrazione e il supporto tecnico.

   > Le modifiche apportate al proxy potrebbero richiedere fino a 10 minuti per diventare effettive.

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

Controllare i firewall

Controllare l'accesso al firewall esterno

È possibile aprire o chiudere porte specifiche sul firewall esterno.

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

Se si desidera configurare il firewall interno StorageGRID , vedere"Configurare il firewall interno" .

Porta	Descrizione	Se la porta è aperta…
443	Porta HTTPS predefinita per i nodi di amministrazione	I browser Web e i client API di gestione possono accedere a Grid Manager, Grid Management API, Tenant Manager e Tenant Management API. **Nota:** la porta 443 viene utilizzata anche per parte del traffico interno.
8443	Porta Grid Manager limitata sui nodi amministrativi	• I browser Web e i client API di gestione possono accedere a Grid Manager e alla Grid Management API tramite HTTPS. • I browser Web e i client API di gestione non possono accedere a Tenant Manager o all'API Tenant Management. • Le richieste di contenuti interni verranno respinte.
9443	Porta Tenant Manager limitata sui nodi amministrativi	• I browser Web e i client API di gestione possono accedere a Tenant Manager e all'API Tenant Management tramite HTTPS. • I browser Web e i client API di gestione non possono accedere a Grid Manager o all'API Grid Management. • Le richieste di contenuti interni verranno respinte.

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

Informazioni correlate

- "Sign in a Grid Manager"
- "Crea un account inquilino"
- "Comunicazioni esterne"

Gestire i controlli del firewall interno

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

Utilizza le tre schede nella pagina di controllo del firewall per personalizzare l'accesso necessario per la tua griglia.

- **Elenco indirizzi privilegiati**: utilizzare questa scheda per consentire l'accesso selezionato alle porte chiuse. È possibile aggiungere indirizzi IP o subnet in notazione CIDR che possono accedere alle porte chiuse utilizzando la scheda Gestisci accesso esterno.
- **Gestisci accesso esterno**: usa questa scheda per chiudere le porte aperte per impostazione predefinita o per riaprire quelle chiuse in precedenza.
- **Rete client non attendibile**: utilizzare questa scheda per specificare se un nodo considera attendibile il traffico in entrata dalla rete client.

  Le impostazioni in questa scheda sostituiscono quelle nella scheda Gestisci accesso esterno.

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

> ⓘ Le impostazioni effettuate in una scheda possono influire sulle modifiche di accesso effettuate in un'altra scheda. Assicurati di controllare le impostazioni in tutte le schede per verificare che la tua rete si comporti come previsto.

Per configurare i controlli del firewall interno, vedere"Configurare i controlli del firewall" .

Per ulteriori informazioni sui firewall esterni e sulla sicurezza di rete, vedere"Controllare l'accesso al firewall esterno" .

Elenco indirizzi privilegiati e schede Gestisci accesso esterno

La scheda Elenco indirizzi privilegiati consente di registrare uno o più indirizzi IP a cui è concesso l'accesso alle porte della griglia chiuse. La scheda Gestisci accesso esterno consente di chiudere l'accesso esterno alle porte esterne selezionate o a tutte le porte esterne aperte (le porte esterne sono porte accessibili per impostazione predefinita dai nodi non di griglia). Spesso è possibile utilizzare insieme queste due schede per personalizzare l'esatto accesso alla rete che si desidera consentire alla propria griglia.

> ⓘ Per impostazione predefinita, gli indirizzi IP privilegiati non hanno accesso alla porta della griglia interna.

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

Supponiamo di voler utilizzare un jump host (un host con sicurezza rafforzata) per l'amministrazione della rete. Potresti seguire questi passaggi generali:

1. Utilizzare la scheda Elenco indirizzi privilegiati per aggiungere l'indirizzo IP dell'host jump.
2. Utilizzare la scheda Gestisci accesso esterno per bloccare tutte le porte.

> Aggiungere l'indirizzo IP privilegiato prima di bloccare le porte 443 e 8443. Tutti gli utenti attualmente connessi a una porta bloccata, incluso 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 sul nodo di amministrazione nella griglia verranno bloccate per tutti gli host, ad eccezione dell'host jump. È quindi possibile utilizzare l'host jump per eseguire attività di manutenzione sulla griglia in modo più sicuro.

Esempio 2: Bloccare le porte sensibili

Supponiamo di voler bloccare porte sensibili e il servizio su quella porta (ad esempio, SSH sulla porta 22). È possibile seguire i seguenti passaggi generali:

1. Utilizzare la scheda Elenco indirizzi privilegiati per concedere l'accesso solo agli host che necessitano di accedere al servizio.
2. Utilizzare la scheda Gestisci accesso esterno per bloccare tutte le porte.

> Aggiungere 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). Tutti gli utenti attualmente connessi a 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, la porta 22 e il servizio SSH saranno disponibili per gli host nell'elenco degli indirizzi privilegiati. A tutti gli altri host verrà negato l'accesso al servizio, indipendentemente dall'interfaccia da cui proviene la richiesta.

Esempio 3: Disabilitare l'accesso ai servizi non utilizzati

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

Scheda Reti client non attendibili

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

Per impostazione predefinita, la rete client su ciascun nodo della griglia è *attendibile*. Ciò significa che, per impostazione predefinita, StorageGRID considera attendibili le connessioni in ingresso a ciascun nodo della griglia su tutti"porte esterne disponibili" .

È possibile ridurre la minaccia di attacchi ostili al sistema StorageGRID specificando che la rete client su ciascun nodo sia *non attendibile*. Se la rete client di un nodo non è attendibile, il nodo accetta solo connessioni in entrata su porte configurate esplicitamente come endpoint del bilanciatore del carico. Vedere"Configurare gli

endpoint del bilanciatore del carico" E"Configurare i controlli del firewall" .

Esempio 1: il nodo gateway accetta solo richieste HTTPS S3

Supponiamo di voler far sì che un nodo gateway rifiuti tutto il traffico in entrata sulla rete client, ad eccezione delle richieste HTTPS S3. Dovresti eseguire questi passaggi generali:

1. Dal"Endpoint del bilanciatore del carico" pagina, configura un endpoint del bilanciatore del carico per S3 su HTTPS sulla porta 443.
2. Nella pagina Controllo firewall, selezionare Non attendibile per specificare che la rete client sul nodo gateway non è attendibile.

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

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

Supponiamo di voler abilitare il traffico dei servizi della piattaforma S3 in uscita da un nodo di archiviazione, ma di voler impedire qualsiasi connessione in ingresso a tale nodo di archiviazione sulla rete client. Dovresti eseguire questo passaggio generale:

- Dalla scheda Reti client non attendibili della pagina di controllo del firewall, indicare che la rete client sul nodo di archiviazione non è attendibile.

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

Esempio 3: limitazione dell'accesso a Grid Manager a una subnet

Supponiamo di voler consentire l'accesso a Grid Manager solo su una subnet specifica. Dovresti eseguire i seguenti passaggi:

1. Collega la rete client dei tuoi nodi amministrativi alla subnet.
2. Utilizzare la scheda Rete client non attendibile per configurare la rete client come non attendibile.
3. Quando si crea un endpoint del bilanciatore del carico dell'interfaccia di gestione, immettere la porta e selezionare l'interfaccia di gestione a cui la porta accederà.
4. Selezionare **Sì** per Rete client non attendibile.
5. Utilizzare la scheda Gestisci accesso esterno per bloccare tutte le porte esterne (con o senza indirizzi IP privilegiati impostati per gli host esterni a quella subnet).

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

Configurare il firewall interno

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Hai"autorizzazioni di accesso specifiche" .

- Hai esaminato le informazioni in"Gestire i controlli del firewall" E"Linee guida per il networking" .
- Se si desidera che un nodo di amministrazione o un nodo gateway accetti il traffico in entrata solo su endpoint configurati in modo esplicito, è necessario definire gli endpoint del bilanciatore del carico.

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

Informazioni su questo compito

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

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

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

Per ulteriori informazioni sui firewall esterni e sulla sicurezza di rete, vedere"Controllare l'accesso al firewall esterno" .

Controlli del firewall di accesso

Passi

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

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

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

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

Elenco indirizzi privilegiati

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

Per impostazione predefinita, gli indirizzi IP e le subnet privilegiati non dispongono di accesso alla griglia interna. Inoltre, gli endpoint del bilanciatore del carico e le porte aggiuntive aperte nella scheda Elenco indirizzi privilegiati sono accessibili anche se bloccati nella scheda Gestisci accesso esterno.

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

Passi

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

   Aggiungere il minor numero possibile di indirizzi all'elenco privilegiato.

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

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

4. Seleziona **Salva**.

Gestisci l'accesso esterno

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

Le impostazioni nella scheda Gestisci accesso esterno non possono sostituire 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 sovrascrivono le porte chiuse (ad esempio 443, 8443, 9443) sulla rete client.

Passi

1. Seleziona **Gestisci accesso esterno**. La scheda visualizza una tabella con tutte le porte esterne (porte accessibili per impostazione predefinita dai nodi non in griglia) per i nodi nella griglia.
2. Configura le porte che vuoi aprire e chiudere utilizzando le seguenti opzioni:
   - Utilizzare il pulsante accanto a ciascuna porta per aprire o chiudere la porta selezionata.
   - Selezionare **Apri tutte le porte visualizzate** per aprire tutte le porte elencate nella tabella.
   - Selezionare **Chiudi tutte le porte visualizzate** per chiudere tutte le porte elencate nella tabella.

   Se 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 non sia stato aggiunto all'elenco degli indirizzi privilegiati.

   Utilizzare la barra di scorrimento sul lato destro della tabella per assicurarsi di aver visualizzato tutte le porte disponibili. Utilizzare il campo di ricerca per trovare le impostazioni per qualsiasi porta esterna inserendo un numero di porta. È possibile immettere un numero di porta parziale. Ad esempio, se si immette **2**, vengono visualizzate tutte le porte che contengono la stringa "2" nel loro nome.

3. Seleziona **Salva**

Rete client non attendibile

Se la rete client di un nodo non è attendibile, il nodo accetta solo il traffico in entrata sulle porte configurate come endpoint del bilanciatore del carico e, facoltativamente, sulle porte aggiuntive selezionate in questa scheda. È possibile utilizzare questa scheda anche 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 del carico non sono stati configurati.

Le modifiche alla configurazione apportate nella scheda **Rete client non attendibile** sovrascrivono le impostazioni nella scheda **Gestisci accesso esterno**.

Passi

1. Selezionare **Rete client non attendibile**.
2. Nella sezione Imposta nuovo nodo predefinito, specificare quale deve essere l'impostazione predefinita quando vengono aggiunti nuovi nodi alla griglia in una procedura di espansione.
   - **Affidabile** (predefinito): quando un nodo viene aggiunto in un'espansione, la sua rete client è attendibile.
   - **Non attendibile**: quando un nodo viene aggiunto a un'espansione, la sua rete client non è attendibile.

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

     > Questa impostazione non influisce sui nodi esistenti nel sistema StorageGRID .
3. Utilizzare le seguenti opzioni per selezionare i nodi che devono consentire connessioni client solo su endpoint del bilanciatore del carico configurati in modo esplicito o porte aggiuntive selezionate:
   - Selezionare **Non considerare attendibili i nodi visualizzati** per aggiungere tutti i nodi visualizzati nella tabella all'elenco Reti client non attendibili.
   - Selezionare **Considera attendibili i nodi visualizzati** per rimuovere tutti i nodi visualizzati nella tabella dall'elenco Reti client non attendibili.
   - Utilizzare il pulsante di attivazione/disattivazione accanto a ciascun nodo per impostare la rete client come attendibile o non attendibile per il nodo selezionato.

     Ad esempio, è possibile selezionare **Non considerare attendibili i nodi visualizzati** per aggiungere tutti i nodi all'elenco Reti client non attendibili e quindi utilizzare il pulsante di attivazione/disattivazione accanto a un singolo nodo per aggiungere quel singolo nodo all'elenco Reti client attendibili.

     > Utilizzare la barra di scorrimento sul lato destro della tabella per assicurarsi di aver visualizzato tutti i nodi disponibili. Utilizzare il campo di ricerca per trovare le impostazioni di qualsiasi nodo immettendone il nome. È possibile immettere un nome parziale. Ad esempio, se si immette **GW**, verranno 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 non riuscire se gli endpoint del bilanciatore del carico non sono stati configurati.

Informazioni sul copyright

Informazioni sul marchio commerciale