



Gestire i certificati

StorageGRID 11.9

NetApp
November 08, 2024

Sommario

- Gestire i certificati 1
 - Gestire i certificati di sicurezza 1
 - Tipi di certificato server supportati 12
 - Configurare i certificati dell'interfaccia di gestione 12
 - Configurare i certificati API S3 18
 - Copiare il certificato Grid CA 23
 - Configurare i certificati StorageGRID per FabricPool 24
 - Configurare i certificati client 25

Gestire 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 di StorageGRID e tra i componenti di StorageGRID e i sistemi esterni.

StorageGRID utilizza due tipi di certificati di sicurezza:

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

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

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

Certificato Grid CA predefinito

StorageGRID include un'autorità di certificazione (CA) incorporata che genera un certificato Grid CA interno durante l'installazione del sistema. Il certificato Grid CA viene utilizzato, per impostazione predefinita, per proteggere il traffico StorageGRID interno. Un'autorità di certificazione esterna (CA) può emettere certificati personalizzati pienamente conformi ai criteri di sicurezza delle informazioni dell'organizzazione. Sebbene sia possibile utilizzare il certificato Grid CA per un ambiente non di produzione, la procedura consigliata per un ambiente di produzione consiste nell'utilizzare certificati personalizzati firmati da un'autorità di certificazione esterna. Sono supportate anche connessioni non protette senza certificato, ma non sono consigliate.

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



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

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

Accesso ai certificati di sicurezza

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

Fasi

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

Certificates

View and manage the certificates that secure HTTPS connections between StorageGRID and external clients, such as S3 or Swift, and external servers, such as a key management server (KMS).

Global Grid CA Client Load balancer endpoints Tenants Other

The StorageGRID certificate authority ("grid CA") generates and signs two global certificates during installation. The management interface certificate on Admin Nodes secures the management interface. The S3 and Swift API certificate on Storage and Gateway Nodes secures client access. You should replace each default certificate with your own custom certificate signed by an external certificate authority.

Name	Description	Type ?	Expiration date ? ↕
Management interface certificate	Secures the connection between client web browsers and the Grid Manager, Tenant Manager, Grid Management API, and Tenant Management API.	Custom	Jun 4th, 2022
S3 and Swift API certificate	Secures the connections between S3 and Swift clients and Storage Nodes or between clients and the deprecated CLB service on Gateway Nodes. You can optionally use this certificate for a load balancer endpoint as well.	Custom	Jun 4th, 2022

2. Selezionare una scheda nella pagina certificati per informazioni su ciascuna categoria di certificati e per accedere alle impostazioni del certificato. È possibile accedere a una scheda se si dispone di **"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.
 - **Endpoints del bilanciamento del carico**: Protegge le connessioni tra i client S3 e il bilanciamento del carico StorageGRID.
 - **Tenant**: Protegge le connessioni ai server di federazione delle identità o dagli endpoint dei servizi della piattaforma alle risorse di storage S3.
 - **Altro**: Protegge le connessioni StorageGRID che richiedono certificati specifici.

Ciascuna scheda viene descritta di seguito con collegamenti a dettagli aggiuntivi del certificato.

Globale

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

- [Certificato dell'interfaccia di gestione](#): Protegge le connessioni del browser Web del client alle interfacce di gestione StorageGRID.
- [Certificato API S3](#): Protegge le connessioni API client ai nodi di archiviazione, ai nodi amministrativi e ai nodi gateway, che le applicazioni client S3 utilizzano per caricare e scaricare i dati oggetto.

Le informazioni sui certificati globali installati includono:

- **Nome**: Nome del certificato con collegamento alla gestione del certificato.
- **Descrizione**
- **Type**: Personalizzato o predefinito. + per una maggiore sicurezza della griglia, è necessario utilizzare sempre un certificato personalizzato.
- **Data di scadenza**: Se si utilizza il certificato predefinito, non viene visualizzata alcuna data di scadenza.

È possibile:

- Sostituire i certificati predefiniti con certificati personalizzati firmati da un'autorità di certificazione esterna per una maggiore sicurezza della griglia:
 - ["Sostituire il certificato predefinito dell'interfaccia di gestione generata da StorageGRID"](#) Utilizzato per le connessioni di Grid Manager e Tenant Manager.
 - ["Sostituire il certificato API S3"](#) Utilizzato per connessioni endpoint nodo storage e bilanciamento del carico (opzionali).
- ["Ripristinare il certificato dell'interfaccia di gestione predefinita"](#).
- ["Ripristinare il certificato API S3 predefinito"](#).
- ["Utilizzare uno script per generare un nuovo certificato autofirmato dell'interfaccia di gestione"](#).
- Copiare o scaricare ["certificato dell'interfaccia di gestione"](#) o ["Certificato API S3"](#).

CA griglia

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

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

È possibile ["Copia o scarica il certificato Grid CA"](#), ma non è possibile modificarlo.

Client

[Certificati client](#), Generato da un'autorità di certificazione esterna, proteggere le connessioni tra gli strumenti di monitoraggio esterni e il database di StorageGRID Prometheus.

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

del certificato.

È possibile:

- ["Caricare o generare un nuovo certificato client."](#)
- Selezionare il nome di un certificato per visualizzare i dettagli del certificato in cui è possibile:
 - ["Modificare il nome del certificato client."](#)
 - ["Impostare l'autorizzazione di accesso Prometheus."](#)
 - ["Caricare e sostituire il certificato del client."](#)
 - ["Copiare o scaricare il certificato client."](#)
 - ["Rimuovere il certificato client."](#)
- Selezionare **azioni** per rapidamente ["modifica"](#), ["allega"](#) o ["rimuovere"](#) un certificato client. È possibile selezionare fino a 10 certificati client e rimuoverli contemporaneamente utilizzando **azioni > Rimuovi**.

Endpoint del bilanciamento del carico

[Certificati endpoint per il bilanciamento del carico](#) Proteggere le connessioni tra i client S3 e il servizio di bilanciamento del carico StorageGRID su nodi gateway e nodi amministrativi.

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



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

È possibile:

- ["Visualizzare un endpoint di bilanciamento del carico"](#), inclusi i dettagli del certificato.
- ["Specificare un certificato endpoint per il bilanciamento del carico per FabricPool."](#)
- ["Utilizzare il certificato API S3 globale"](#) invece di generare un nuovo certificato endpoint per il bilanciamento del carico.

Tenant

I locatari possono utilizzare [certificati del server di federazione delle identità](#) o [certificati endpoint del servizio di piattaforma](#) assicurare le loro connessioni con StorageGRID.

La tabella tenant ha una riga per ciascun tenant e indica se ciascun tenant dispone dell'autorizzazione per utilizzare la propria origine di identità o i propri servizi di piattaforma.

È possibile:

- ["Selezionare il nome di un tenant per accedere al tenant manager"](#)
- ["Selezionare un nome tenant per visualizzare i dettagli della federazione delle identità del tenant"](#)
- ["Selezionare un nome tenant per visualizzare i dettagli dei servizi della piattaforma tenant"](#)
- ["Specificare un certificato endpoint del servizio di piattaforma durante la creazione dell'endpoint"](#)

Altro

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

- [Certificati Cloud Storage Pool](#)
- [Certificati di notifica degli avvisi via email](#)
- [Certificati server syslog esterni](#)
- [Certificati di connessione Grid Federation](#)
- [Certificati di federazione delle identità](#)
- [Certificati KMS \(Key Management Server\)](#)
- [Certificati Single Sign-on](#)

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



È possibile visualizzare e accedere alle informazioni relative ad altri certificati solo se si dispone di ["autorizzazione appropriata"](#).

È possibile:

- ["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 Grid Federation"](#)
- ["Visualizzare e modificare un certificato di federazione delle identità"](#)
- ["Caricare i certificati del server e del client del server di gestione delle chiavi \(KMS\)"](#)
- ["Specificare manualmente un certificato SSO per un trust della parte che si basa"](#)

Dettagli del certificato di sicurezza

Di seguito sono descritti i tipi di certificato di protezione, con collegamenti alle istruzioni di implementazione.

Certificato dell'interfaccia di gestione

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	<p>Autentica la connessione tra i browser Web client e l'interfaccia di gestione di StorageGRID, consentendo agli utenti di accedere a Grid Manager e Tenant Manager senza avvisi di sicurezza.</p> <p>Questo certificato autentica anche le connessioni API Grid Management e API Tenant Management.</p> <p>È possibile utilizzare il certificato predefinito creato durante l'installazione o caricare un certificato personalizzato.</p>	<p>CONFIGURATION > Security > Certificates, selezionare la scheda Global, quindi selezionare Management interface certificate</p>	<p>"Configurare i certificati dell'interfaccia di gestione"</p>

Certificato API S3

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	<p>Autentica le connessioni client S3 sicure a un nodo di storage e agli endpoint del bilanciamento del carico (opzionale).</p>	<p>CONFIGURAZIONE > sicurezza > certificati, selezionare la scheda Globale, quindi selezionare certificato API S3</p>	<p>"Configurare i certificati API S3"</p>

Certificato Grid CA

Consultare la [Descrizione del certificato Grid CA predefinito](#).

Certificato del client di amministratore

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Client	<p>Installato su ciascun client, consentendo a StorageGRID di autenticare l'accesso client esterno.</p> <ul style="list-style-type: none"> • Consente ai client esterni autorizzati di accedere al database StorageGRID Prometheus. • Consente il monitoraggio sicuro di StorageGRID utilizzando strumenti esterni. 	<p>CONFIGURAZIONE > sicurezza > certificati, quindi selezionare la scheda Client</p>	<p>"Configurare i certificati client"</p>

Certificato endpoint per il bilanciamento del carico

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	<p>Autentica la connessione tra i client S3 e il servizio di bilanciamento del carico StorageGRID sui nodi gateway e i nodi amministrativi. È possibile caricare o generare un certificato di bilanciamento del carico quando si configura un endpoint di bilanciamento del carico. Le applicazioni client utilizzano il certificato di bilanciamento del carico durante la connessione a StorageGRID per salvare e recuperare i dati degli oggetti.</p> <p>È inoltre possibile utilizzare una versione personalizzata del certificato globale Certificato API S3 per autenticare le connessioni al servizio Load Balancer. Se il certificato globale viene utilizzato per autenticare le connessioni del bilanciamento del carico, non è necessario caricare o generare un certificato separato per ciascun endpoint del bilanciamento del carico.</p> <p>Nota: il certificato utilizzato per l'autenticazione del bilanciamento del carico è il certificato più utilizzato durante il normale funzionamento StorageGRID.</p>	<p>CONFIGURAZIONE > rete > endpoint del bilanciamento del carico</p>	<ul style="list-style-type: none"> • "Configurare gli endpoint del bilanciamento del carico" • "Creare un endpoint di bilanciamento del carico per FabricPool"

Certificato endpoint Cloud Storage Pool

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

Certificato di notifica degli avvisi via email

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	<p>Autentica la connessione tra un server e-mail SMTP e StorageGRID utilizzato per le notifiche degli avvisi.</p> <ul style="list-style-type: none"> • Se le comunicazioni con il server SMTP richiedono TLS (Transport Layer Security), è necessario specificare il certificato CA del server di posta elettronica. • Specificare un certificato client solo se il server di posta SMTP richiede certificati client per l'autenticazione. 	ALERTS > email setup	"Imposta le notifiche via email per gli avvisi"

Certificato server syslog esterno

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

certificato di connessione Grid Federation

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	Autenticare e crittografare le informazioni inviate tra il sistema StorageGRID corrente e un'altra griglia in una connessione a federazione di griglie.	CONFIGURAZIONE > sistema > federazione griglia	<ul style="list-style-type: none"> • "Creare connessioni di federazione di griglie" • "Ruotare i certificati di connessione"

Certificato di federazione delle identità

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	<p>Autentica la connessione tra StorageGRID e un provider di identità esterno, ad esempio Active Directory, OpenLDAP o Oracle Directory Server.</p> <p>Utilizzato per la federazione delle identità, che consente ai gruppi di amministrazione e agli utenti di essere gestiti da un sistema esterno.</p>	CONFIGURAZIONE > controllo accessi > federazione identità	"USA la federazione delle identità"

Certificato del Key Management Server (KMS)

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	Autentica la connessione tra StorageGRID e un KMS (Key Management Server) esterno, che fornisce chiavi di crittografia ai nodi appliance StorageGRID.	CONFIGURAZIONE > sicurezza > Server di gestione delle chiavi	" Aggiunta del 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 storage S3.	Tenant Manager > STORAGE (S3) > endpoint dei servizi della piattaforma	" Creare endpoint di servizi di piattaforma " " Modifica dell'endpoint dei servizi della piattaforma "

Certificato SSO (Single Sign-on)

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra i servizi di federazione delle identità, come ad FS (Active Directory Federation Services) e StorageGRID, utilizzati per le richieste SSO (Single Sign-on).	CONFIGURAZIONE > controllo di accesso > Single Sign-on	" Configurare il single sign-on "

Esempi di certificati

Esempio 1: Servizio di bilanciamento del carico

In questo esempio, StorageGRID agisce come server.

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

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

Esempio 2: Server KMS (Key Management Server) esterno

In questo esempio, StorageGRID agisce come client.

1. Utilizzando il software del server di gestione delle chiavi esterno, è possibile configurare StorageGRID come client KMS e ottenere un certificato server con firma CA, un certificato client pubblico e la chiave privata per il certificato client.
2. Utilizzando Grid Manager, è possibile configurare un server KMS e caricare i certificati server e client e la chiave privata del client.
3. Quando un nodo StorageGRID necessita di una chiave di crittografia, effettua una richiesta al server KMS che include i dati del certificato e una firma basata sulla chiave privata.
4. Il server KMS convalida la firma del certificato e decide che può fidarsi di StorageGRID.
5. Il server KMS risponde utilizzando la connessione validata.

Tipi di certificato server supportati

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



Il tipo di crittografia per il criterio di protezione deve corrispondere al tipo di certificato del server. Ad esempio, le crittografie RSA richiedono certificati RSA e le crittografie ECDSA richiedono certificati ECDSA. Vedere "[Gestire i certificati di sicurezza](#)". Se si configura un criterio di protezione personalizzato non compatibile con il certificato del server, è possibile "[ripristinare temporaneamente il criterio di protezione predefinito](#)".

Per ulteriori informazioni su come StorageGRID protegge le connessioni client, vedere "[Sicurezza per S3 client](#)".

Configurare i certificati dell'interfaccia di gestione

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

A proposito di questa attività

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

Poiché per tutti i nodi di amministrazione viene utilizzato un singolo certificato di interfaccia di gestione personalizzata, è necessario specificare il certificato come carattere jolly o certificato multidominio se i client devono verificare il nome host durante la connessione a Grid Manager e Tenant Manager. Definire il certificato personalizzato in modo che corrisponda a tutti i nodi Admin nella griglia.

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



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



Se si accede a Grid Manager o Tenant Manager utilizzando un nome di dominio invece di un indirizzo IP, il browser mostra un errore di certificato senza l'opzione di ignorare se si verifica una delle seguenti condizioni:

- Il certificato dell'interfaccia di gestione personalizzata scade.
- Voi [ripristinare da un certificato dell'interfaccia di gestione personalizzata al certificato server predefinito](#).

Aggiungere un certificato di interfaccia di gestione personalizzata

Per aggiungere un certificato di interfaccia di gestione personalizzato, è possibile fornire un certificato personalizzato o generarne uno utilizzando Grid Manager.

Fasi

1. Selezionare **CONFIGURAZIONE > sicurezza > certificati**.
2. Nella scheda **Global**, selezionare **Management interface certificate**.
3. Selezionare **Usa certificato personalizzato**.
4. Caricare o generare il certificato.

Carica certificato

Caricare i file dei certificati del server richiesti.

- a. Selezionare **carica certificato**.
- b. Caricare i file dei certificati del server richiesti:
 - **Server certificate**: Il file di certificato del server personalizzato (con codifica PEM).
 - **Chiave privata del certificato**: Il file della chiave privata del certificato del server personalizzato (.key).



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

- **Bundle CA**: Un singolo file opzionale contenente i certificati di ogni autorità di certificazione di emissione intermedia (CA). Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.
- c. Espandere **Dettagli certificato** per visualizzare i metadati di ciascun certificato caricato. Se è stato caricato un bundle CA opzionale, ciascun certificato viene visualizzato nella propria scheda.
 - Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato oppure selezionare **Download CA bundle** (Scarica pacchetto CA) per salvare il bundle del certificato.

Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione .pem.

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy certificate PEM** or **Copy CA bundle PEM** per copiare il contenuto del certificato e incollarlo altrove.
- d. Selezionare **Salva**. Il certificato dell'interfaccia di gestione personalizzata viene utilizzato per tutte le nuove connessioni successive a Grid Manager, Tenant Manager, Grid Manager API o tenant Manager API.

Generare un certificato

Generare i file dei certificati del server.



La procedura consigliata per un ambiente di produzione consiste nell'utilizzare un certificato dell'interfaccia di gestione personalizzata firmato da un'autorità di certificazione esterna.

- a. Selezionare **genera certificato**.
- b. Specificare le informazioni del certificato:

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

Campo	Descrizione
IP	Uno o più indirizzi IP da includere nel certificato.
Soggetto (facoltativo)	X.509 nome soggetto o nome distinto (DN) del proprietario del certificato. Se in questo campo non viene immesso alcun valore, il certificato generato utilizza il primo nome di dominio o indirizzo IP come nome comune (CN) del soggetto.
Giorni di validità	Numero di giorni successivi alla creazione della scadenza del certificato.
Aggiungere estensioni di utilizzo chiave	Se selezionata (impostazione predefinita e consigliata), l'utilizzo delle chiavi e le estensioni estese dell'utilizzo delle chiavi vengono aggiunte al certificato generato. Queste estensioni definiscono lo scopo della chiave contenuta nel certificato. Nota: Lasciare questa casella di controllo selezionata a meno che non si verifichino problemi di connessione con client meno recenti quando i certificati includono queste estensioni.

c. Selezionare **generate**.

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

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

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

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.

e. Selezionare **Salva**. Il certificato dell'interfaccia di gestione personalizzata viene utilizzato per tutte le nuove connessioni successive a Grid Manager, Tenant Manager, Grid Manager API o tenant Manager API.

5. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.



Dopo aver caricato o generato un nuovo certificato, attendere fino a un giorno per la cancellazione degli avvisi relativi alla scadenza del certificato.

6. Dopo aver aggiunto un certificato dell'interfaccia di gestione personalizzata, la pagina del certificato dell'interfaccia di gestione visualizza informazioni dettagliate sul certificato per i certificati in uso. + è possibile scaricare o copiare il PEM del certificato secondo necessità.

Ripristinare il certificato dell'interfaccia di gestione predefinita

È possibile ripristinare l'utilizzo del certificato dell'interfaccia di gestione predefinita per Grid Manager e Tenant Manager Connections.

Fasi

1. Selezionare **CONFIGURAZIONE > sicurezza > certificati**.
2. Nella scheda **Global**, selezionare **Management interface certificate**.
3. Selezionare **Usa certificato predefinito**.

Quando si ripristina il certificato dell'interfaccia di gestione predefinita, i file di certificato del server personalizzati configurati vengono cancellati e non possono essere ripristinati dal sistema. Il certificato predefinito dell'interfaccia di gestione viene utilizzato per tutte le nuove connessioni client successive.

4. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

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

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

Prima di iniziare

- Si dispone di "[autorizzazioni di accesso specifiche](#)".
- Si dispone del `Passwords.txt` file.

A proposito di questa attività

La procedura consigliata per un ambiente di produzione consiste nell'utilizzare un certificato firmato da un'autorità di certificazione esterna.

Fasi

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

Quando si è collegati 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 Admin. Ad esempio, `*.ui.storagegrid.example.com` utilizza il carattere jolly `*` per rappresentare `admin1.ui.storagegrid.example.com` e `admin2.ui.storagegrid.example.com`.
- Impostare `--type` su `management` per configurare il certificato dell'interfaccia di gestione, utilizzato

da Grid Manager e Tenant Manager.

- Per impostazione predefinita, i certificati generati sono validi per un anno (365 giorni) e devono essere ricreati prima della scadenza. È possibile utilizzare l' `--days` argomento per sovrascrivere il periodo di validità predefinito.



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

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

L'output risultante contiene il certificato pubblico necessario al client API di gestione.

4. Selezionare e copiare il certificato.

Includere i tag BEGIN e END nella selezione.

5. Disconnettersi dalla shell dei comandi. `$ exit`

6. Verificare che il certificato sia stato configurato:

- Accedere a Grid Manager.
- Selezionare **CONFIGURAZIONE > sicurezza > certificati**
- Nella scheda **Global**, selezionare **Management interface certificate**.

7. Configurare il client di gestione in modo che utilizzi il certificato pubblico copiato. Includere i tag inizio e FINE.

Scaricare o copiare il certificato dell'interfaccia di gestione

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

Fasi

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

Scaricare il file di certificato o il bundle CA

Scaricare il certificato o il file bundle CA .pem. Se si utilizza un bundle CA opzionale, ciascun certificato del bundle viene visualizzato nella propria sottoscheda.

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

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

b. Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione .pem.

Ad esempio: `storagegrid_certificate.pem`

Copia certificato o pacchetto CA PEM

Copiare il testo del certificato per incollarlo altrove. Se si utilizza un bundle CA opzionale, ciascun certificato del bundle viene visualizzato nella propria sottoscheda.

a. Selezionare **Copy certificate PEM** or **Copy CA bundle PEM**.

Se si copia un bundle CA, tutti i certificati contenuti nelle schede secondarie del bundle CA vengono copiati insieme.

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

c. Salvare il file di testo con l'estensione .pem.

Ad esempio: `storagegrid_certificate.pem`

Configurare i certificati API S3

È possibile sostituire o ripristinare il certificato del server utilizzato per le connessioni client S3 ai nodi di storage o agli endpoint di bilanciamento del carico. Il certificato del server personalizzato sostitutivo è specifico dell'organizzazione.



I dettagli Swift sono stati rimossi da questa versione del sito della documentazione. Vedere ["StorageGRID 11,8: Configurazione dei certificati API S3 e Swift"](#).

A proposito di questa attività

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

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

Dopo aver completato la configurazione sul server, potrebbe essere necessario installare anche il certificato

CA Grid nel client API S3 da utilizzare per accedere al sistema, a seconda dell'autorità di certificazione principale (CA) in uso.



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

È possibile caricare o generare un certificato API S3 personalizzato.

Aggiungere un certificato API S3 personalizzato

Fasi

1. Selezionare **CONFIGURAZIONE > sicurezza > certificati**.
2. Nella scheda **Globale**, selezionare **S3 certificato API**.
3. Selezionare **Usa certificato personalizzato**.
4. Caricare o generare il certificato.

Carica certificato

Caricare i file dei certificati del server richiesti.

a. Selezionare **carica certificato**.

b. Caricare i file dei certificati del server richiesti:

- **Server certificate:** Il file di certificato del server personalizzato (con codifica PEM).
- **Chiave privata del certificato:** Il file della chiave privata del certificato del server personalizzato (.key).



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

- **Bundle CA:** Un singolo file opzionale contenente i certificati di ciascuna autorità di certificazione di emissione intermedia. Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.

c. Selezionare i dettagli del certificato per visualizzare i metadati e PEM per ogni certificato API S3 personalizzato caricato. Se è stato caricato un bundle CA opzionale, ciascun certificato viene visualizzato nella propria scheda.

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato oppure selezionare **Download CA bundle** (Scarica pacchetto CA) per salvare il bundle del certificato.

Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione .pem.

Ad esempio: storagegrid_certificate.pem

- Selezionare **Copy certificate PEM** or **Copy CA bundle PEM** per copiare il contenuto del certificato e incollarlo altrove.

d. Selezionare **Salva**.

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

Generare un certificato

Generare i file dei certificati del server.

a. Selezionare **genera certificato**.

b. Specificare le informazioni del certificato:

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

Campo	Descrizione
Soggetto (facoltativo)	X.509 nome soggetto o nome distinto (DN) del proprietario del certificato. Se in questo campo non viene immesso alcun valore, il certificato generato utilizza il primo nome di dominio o indirizzo IP come nome comune (CN) del soggetto.
Giorni di validità	Numero di giorni successivi alla creazione della scadenza del certificato.
Aggiungere estensioni di utilizzo chiave	Se selezionata (impostazione predefinita e consigliata), l'utilizzo delle chiavi e le estensioni estese dell'utilizzo delle chiavi vengono aggiunte al certificato generato. Queste estensioni definiscono lo scopo della chiave contenuta nel certificato. Nota: Lasciare questa casella di controllo selezionata a meno che non si verifichino problemi di connessione con client meno recenti quando i certificati includono queste estensioni.

c. Selezionare **generate**.

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

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

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

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.

e. Selezionare **Salva**.

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

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



Dopo aver caricato o generato un nuovo certificato, attendere fino a un giorno per la cancellazione degli avvisi relativi alla scadenza del certificato.

6. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

7. Dopo aver aggiunto un certificato API S3 personalizzato, la pagina del certificato API S3 visualizza informazioni dettagliate sul certificato API S3 personalizzato in uso. + è possibile scaricare o copiare il PEM del certificato secondo necessità.

Ripristinare il certificato API S3 predefinito

È possibile ripristinare l'utilizzo del 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 di bilanciamento del carico.

Fasi

1. Selezionare **CONFIGURAZIONE > sicurezza > certificati**.
2. Nella scheda **Globale**, selezionare **S3 certificato API**.
3. Selezionare **Usa certificato predefinito**.

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

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

Se si dispone dell'autorizzazione di accesso root e il certificato API S3 personalizzato è stato utilizzato per le connessioni endpoint del bilanciamento del carico, viene visualizzato un elenco degli endpoint del bilanciamento del carico che non saranno più accessibili utilizzando il certificato API S3 predefinito. Accedere a "[Configurare gli endpoint del bilanciamento del carico](#)" per modificare o rimuovere gli endpoint interessati.

5. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

Scaricare o copiare il certificato API S3

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

Fasi

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

Scaricare il file di certificato o il bundle CA

Scaricare il certificato o il file bundle CA .pem. Se si utilizza un bundle CA opzionale, ciascun certificato del bundle viene visualizzato nella propria sottoscheda.

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

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

b. Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione .pem.

Ad esempio: `storagegrid_certificate.pem`

Copia certificato o pacchetto CA PEM

Copiare il testo del certificato per incollarlo altrove. Se si utilizza un bundle CA opzionale, ciascun certificato del bundle viene visualizzato nella propria sottoscheda.

a. Selezionare **Copy certificate PEM** or **Copy CA bundle PEM**.

Se si copia un bundle CA, tutti i certificati contenuti nelle schede secondarie del bundle CA vengono copiati insieme.

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

c. Salvare il file di testo con l'estensione .pem.

Ad esempio: `storagegrid_certificate.pem`

Informazioni correlate

- ["UTILIZZARE L'API REST S3"](#)
- ["Configurare i nomi di dominio degli endpoint S3"](#)

Copiare il certificato Grid CA

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

Prima di iniziare

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

A proposito di questa attività

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

Fasi

1. Selezionare **CONFIGURATION > Security > Certificates**, quindi selezionare la scheda **Grid CA**.

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

Scaricare il file del certificato

Scaricare il file del certificato `.pem`.

- a. Selezionare **Scarica certificato**.
- b. Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

Copia certificato PEM

Copiare il testo del certificato per incollarlo altrove.

- a. Selezionare **Copy certificate PEM** (Copia certificato PEM).
- b. Incollare il certificato copiato in un editor di testo.
- c. Salvare il file di testo con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

Configurare i certificati StorageGRID per FabricPool

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

Prima di iniziare

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

A proposito di questa attività

Quando si crea un endpoint di bilanciamento del carico, è possibile generare un certificato server autofirmato o caricare un certificato firmato da un'autorità di certificazione (CA) nota. Negli ambienti di produzione, è necessario utilizzare un certificato firmato da una CA nota. I certificati firmati da una CA possono essere ruotati senza interruzioni. Sono inoltre più sicuri perché offrono una migliore protezione contro gli attacchi man-in-the-middle.

La procedura riportata di seguito fornisce linee guida generali per i client S3 che utilizzano FabricPool. Per informazioni e procedure più dettagliate, vedere ["Configurare StorageGRID per FabricPool"](#).

Fasi

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

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

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

3. Collega StorageGRID come Tier cloud in ONTAP.

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



Se una CA intermedia ha emesso il certificato StorageGRID, è necessario fornire il certificato CA intermedio. Se il certificato StorageGRID è stato emesso direttamente dalla CA principale, è necessario fornire il certificato della CA principale.

Configurare i certificati client

I certificati client consentono ai client esterni autorizzati di accedere al database StorageGRID Prometheus, fornendo un modo sicuro per i tool esterni di monitorare StorageGRID.

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

Vedere ["Gestire i certificati di sicurezza"](#) e ["Configurare certificati server personalizzati"](#).



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



Se si utilizza un server di gestione delle chiavi (KMS) per proteggere i dati su nodi di appliance appositamente configurati, vedere le informazioni specifiche su ["Caricamento di un certificato del client KMS"](#).

Prima di iniziare

- Si dispone dell'autorizzazione di accesso root.
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Per configurare un certificato client:
 - Si dispone dell'indirizzo IP o del nome di dominio del nodo di amministrazione.
 - Se è stato configurato il certificato dell'interfaccia di gestione StorageGRID, si dispone della CA, del certificato client e della chiave privata utilizzati per configurare il certificato dell'interfaccia di gestione.
 - Per caricare il certificato, la chiave privata del certificato è disponibile sul computer locale.
 - La chiave privata deve essere stata salvata o registrata al momento della creazione. Se non si dispone della chiave privata originale, è necessario crearne una nuova.
- Per modificare un certificato client:
 - Si dispone dell'indirizzo IP o del nome di dominio del nodo di amministrazione.
 - Per caricare il proprio certificato o un nuovo certificato, la chiave privata, il certificato client e la CA (se utilizzata) sono disponibili sul computer locale.

Aggiungere certificati client

Per aggiungere il certificato client, attenersi a una delle seguenti procedure:

- [Certificato dell'interfaccia di gestione già configurato](#)
- [CERTIFICATO client emesso DALLA CA](#)
- [Certificato generato da Grid Manager](#)

Certificato dell'interfaccia di gestione già configurato

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

Fasi

1. In Grid Manager, selezionare **CONFIGURATION > Security > Certificates**, quindi selezionare la scheda **Client**.
2. Selezionare **Aggiungi**.
3. Immettere un nome per il certificato.
4. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow prometheus** (Consenti prometheus).
5. Selezionare **continua**.
6. Per il passo **Allega certificati**, caricare il certificato dell'interfaccia di gestione.
 - a. Selezionare **carica certificato**.
 - b. Selezionare **Sfoglia** e selezionare il file di certificato dell'interfaccia di gestione (.pem).
 - Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.
 - Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.
 - c. Selezionare **Crea** per salvare il certificato in Grid Manager.

Il nuovo certificato viene visualizzato nella scheda Client.
7. [Configurare uno strumento di monitoraggio esterno](#), Come Grafana.

CERTIFICATO client emesso DALLA CA

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

Fasi

1. Eseguire i passaggi da a ["configurare un certificato dell'interfaccia di gestione"](#).
2. In Grid Manager, selezionare **CONFIGURATION > Security > Certificates**, quindi selezionare la scheda **Client**.
3. Selezionare **Aggiungi**.
4. Immettere un nome per il certificato.

5. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow prometheus** (Consenti prometheus).
6. Selezionare **continua**.
7. Per il passo **Allega certificati**, caricare i file di certificato client, chiave privata e bundle CA:
 - a. Selezionare **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 **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.
 - c. Selezionare **Crea** per salvare il certificato in Grid Manager.

I nuovi certificati vengono visualizzati nella scheda Client.

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 intende aggiungere un certificato client per Prometheus che utilizza la funzione di generazione del certificato in Grid Manager.

Fasi

1. In Grid Manager, selezionare **CONFIGURATION > Security > Certificates**, quindi selezionare la scheda **Client**.
2. Selezionare **Aggiungi**.
3. Immettere un nome per il certificato.
4. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow prometheus** (Consenti prometheus).
5. Selezionare **continua**.
6. Per il passo **Allega certificati**, selezionare **genera certificato**.
7. Specificare le informazioni del certificato:
 - **Oggetto** (opzionale): Nome distinto (DN) o oggetto X.509 del proprietario del certificato.
 - **Giorni validi**: Il numero di giorni in cui il certificato generato è valido, a partire dal momento in cui viene generato.
 - **Add key usage Extensions** (Aggiungi estensioni utilizzo chiave): Se selezionata (impostazione predefinita e consigliata), l'utilizzo della chiave e le estensioni estese dell'utilizzo della chiave vengono aggiunte al certificato generato.

Queste estensioni definiscono lo scopo della chiave contenuta nel certificato.



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

8. Selezionare **generate**.

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



Non sarà possibile visualizzare la chiave privata del certificato dopo aver chiuso la finestra di dialogo. Copiare o scaricare la chiave in un luogo sicuro.

- Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.
- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

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

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy private key** (Copia chiave privata) per copiare la chiave privata del certificato e incollarla altrove.
- Selezionare **Download private key** (Scarica chiave privata) per salvare la chiave privata come file.

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

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

Il nuovo certificato viene visualizzato nella scheda Client.

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

12. Selezionare **certificato interfaccia di gestione**.

13. Selezionare **Usa certificato personalizzato**.

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

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

Il nuovo certificato viene visualizzato nella pagina Management Interface certificate (certificato interfaccia di gestione).

15. [Configurare uno strumento di monitoraggio esterno](#), Come Grafana.

Configura uno strumento di monitoraggio esterno

Fasi

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

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

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

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

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

c. Abilitare **TLS Client Auth** e con **CA Certate**.

d. In TLS/SSL Auth Details (Dettagli autorizzazione TLS/SSL), copiare e incollare:

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

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

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

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

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

Per informazioni sulle metriche, vedere "[Istruzioni per il monitoraggio di StorageGRID](#)".

Modificare i certificati client

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

Fasi

1. Selezionare **CONFIGURATION > Security > Certificates**, quindi selezionare la scheda **Client**.

Le date di scadenza del certificato e le autorizzazioni di accesso Prometheus sono elencate nella tabella. Se un certificato scade presto o è già scaduto, viene visualizzato un messaggio nella tabella e viene attivato un avviso.

2. Selezionare il certificato che si desidera modificare.

3. Selezionare **Modifica**, quindi selezionare **Modifica nome e permesso**

4. Immettere un nome per il certificato.

5. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow prometheus** (Consenti prometheus).

6. Selezionare **continua** per salvare il certificato in Grid Manager.

Il certificato aggiornato viene visualizzato nella scheda Client.

Allegare un nuovo certificato client

È possibile caricare un nuovo certificato una volta scaduto il certificato corrente.

Fasi

1. Selezionare **CONFIGURATION > Security > Certificates**, quindi selezionare la scheda **Client**.

Le date di scadenza del certificato e le autorizzazioni di accesso Prometheus sono elencate nella tabella. Se un certificato scade presto o è già scaduto, viene visualizzato un messaggio nella tabella e viene attivato un avviso.

2. Selezionare il certificato che si desidera modificare.
3. Selezionare **Edit** (Modifica), quindi un'opzione di modifica.

Carica certificato

Copiare il testo del certificato per incollarlo altrove.

- a. Selezionare **carica certificato**, quindi selezionare **continua**.
- b. Caricare il nome del certificato client (.pem).

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

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione .pem.

Ad esempio: storagegrid_certificate.pem

- Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.
- c. Selezionare **Crea** per salvare il certificato in Grid Manager.

Il certificato aggiornato viene visualizzato nella scheda Client.

Generare un certificato

Generare il testo del certificato da incollare altrove.

- a. Selezionare **genera certificato**.
- b. Specificare le informazioni del certificato:
 - **Oggetto** (opzionale): Nome distinto (DN) o oggetto X.509 del proprietario del certificato.
 - **Giorni validi**: Il numero di giorni in cui il certificato generato è valido, a partire dal momento in cui viene generato.
 - **Add key usage Extensions** (Aggiungi estensioni utilizzo chiave): Se selezionata (impostazione predefinita e consigliata), l'utilizzo della chiave e le estensioni estese dell'utilizzo della chiave vengono aggiunte al certificato generato.

Queste estensioni definiscono lo scopo della chiave contenuta nel certificato.



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

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



Non sarà possibile visualizzare la chiave privata del certificato dopo aver chiuso la finestra di dialogo. Copiare o scaricare la chiave in un luogo sicuro.

- Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del

certificato e incollarlo altrove.

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

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

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy private key** (Copia chiave privata) per copiare la chiave privata del certificato e incollarla altrove.
- Selezionare **Download private key** (Scarica chiave privata) per salvare la chiave privata come file.

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

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

Il nuovo certificato viene visualizzato nella scheda Client.

Scaricare o copiare i certificati client

È possibile scaricare o copiare un certificato client da utilizzare altrove.

Fasi

1. Selezionare **CONFIGURATION > Security > Certificates**, quindi selezionare la scheda **Client**.
2. Selezionare il certificato che si desidera copiare o scaricare.
3. Scaricare o copiare il certificato.

Scaricare il file del certificato

Scaricare il file del certificato `.pem`.

- a. Selezionare **Scarica certificato**.
- b. Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

Copia certificato

Copiare il testo del certificato per incollarlo altrove.

- a. Selezionare **Copy certificate PEM** (Copia certificato PEM).
- b. Incollare il certificato copiato in un editor di testo.
- c. Salvare il file di testo con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

Rimuovere i certificati client

Se non è più necessario un certificato client amministratore, è possibile rimuoverlo.

Fasi

1. Selezionare **CONFIGURATION > Security > Certificates**, quindi selezionare la scheda **Client**.
2. Selezionare il certificato che si desidera rimuovere.
3. Selezionare **Delete** (Elimina), quindi confermare.



Per rimuovere fino a 10 certificati, selezionare ciascun certificato da rimuovere nella scheda Client, quindi selezionare **azioni > Elimina**.

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

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.