Gestisci i certificati

StorageGRID software

NetApp
December 03, 2025

Sommario

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.

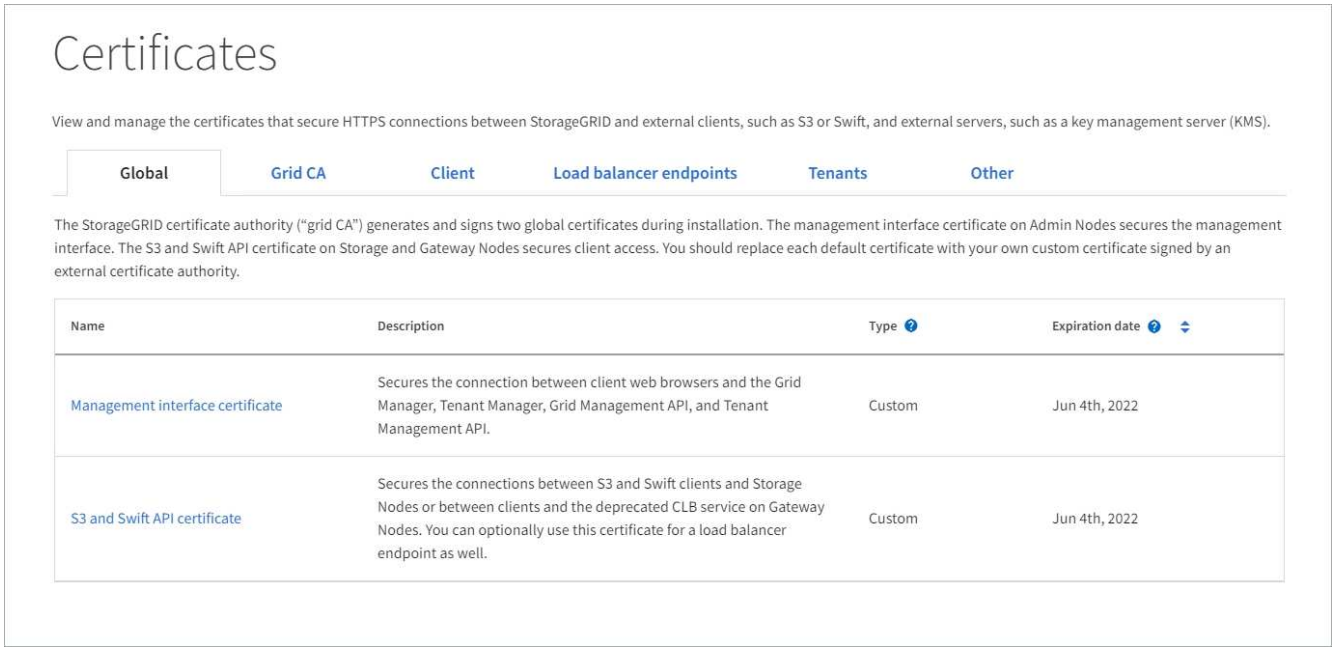
Le varianti dei tipi di certificato server e client vengono implementate in diversi modi. Prima di configurare il sistema, è necessario disporre di tutti i certificati necessari per la configurazione specifica StorageGRID .

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.

Informazioni sul copyright

Informazioni sul marchio commerciale