Gestisci i certificati

StorageGRID software

NetApp
July 23, 2026

Sommario

Gestisci i certificati

Gestisci i certificati di sicurezza in StorageGRID

${post_edited_translations.segment}

${post_edited_translations.segment}

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

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

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

${post_edited_translations.segment}

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

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

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

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

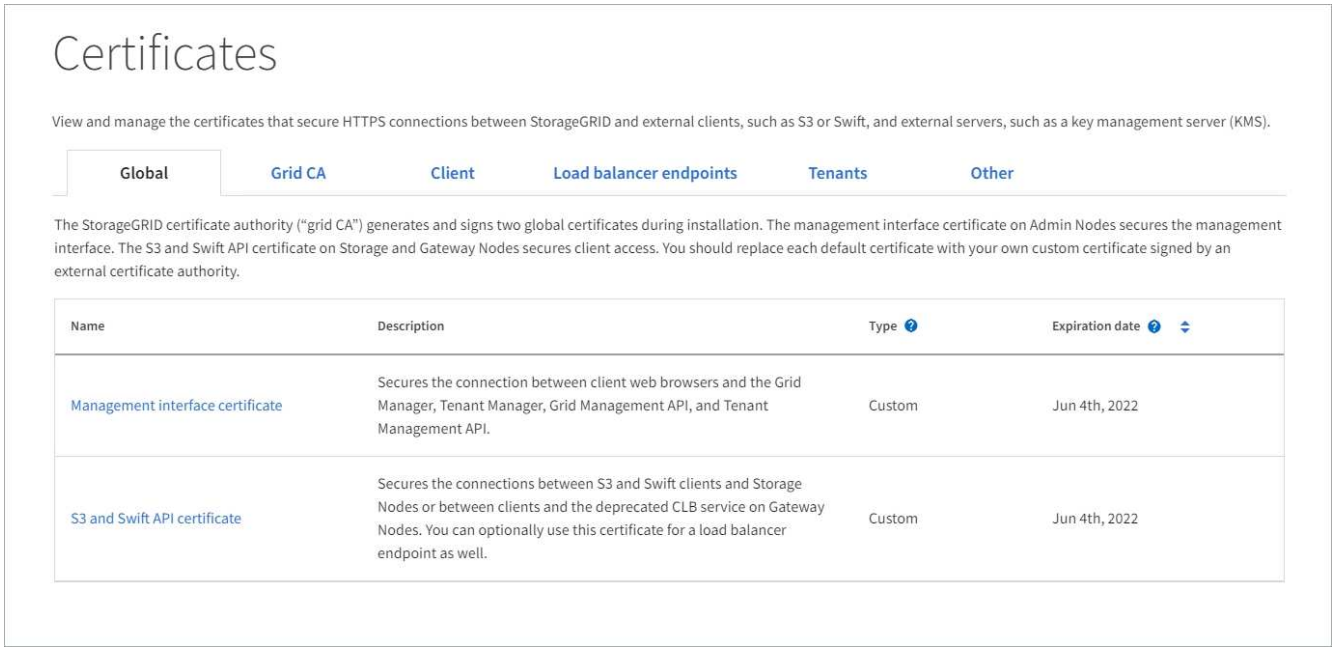
Le varianti dei tipi di certificati server e client vengono implementate in diversi modi. Dovresti avere pronti tutti i certificati necessari per la tua specifica configurazione di StorageGRID prima di configurare il sistema.

Certificati di sicurezza di accesso

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

Passaggi

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



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

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

     ${post_edited_translations.segment}

Globale

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

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

Le informazioni relative ai certificati globali installati includono:

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

Puoi:

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

${post_edited_translations.segment}

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

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

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

${post_edited_translations.segment}

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

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

Puoi:

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

${post_edited_translations.segment}

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

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

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

Puoi:

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

Tenant

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

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

Puoi:

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

Altro

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

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

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

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

Puoi:

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

Dettagli del certificato di sicurezza

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

${post_edited_translations.segment}

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

Certificato API S3

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

Certificato CA Grid

Vedi la Descrizione del certificato CA Grid predefinito.

certificato client amministratore

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

${post_edited_translations.segment}

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

Certificato endpoint di Cloud Storage Pool

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

Certificato di notifica di avviso email

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

Certificato del server syslog esterno

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

${post_edited_translations.segment}

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

Certificato di federazione dell'identità

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

${post_edited_translations.segment}

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

Certificato endpoint dei servizi della piattaforma

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

Certificato di single sign-on (SSO)

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

${post_edited_translations.segment}

Esempio 1: Servizio di bilanciamento del carico

${post_edited_translations.segment}

1. ${post_edited_translations.segment}
2. Configuri una connessione client S3 all'endpoint del bilanciatore di carico e carichi lo stesso certificato sul client.
3. Quando il client vuole salvare o recuperare dati, si connette all'endpoint del bilanciatore di carico tramite HTTPS.
4. ${post_edited_translations.segment}
5. Il client confronta la firma del server con la firma presente sulla sua copia del certificato. Se le firme corrispondono, il client avvia una sessione utilizzando la stessa chiave pubblica.
6. Il client invia i dati dell'oggetto a StorageGRID.

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

In questo esempio, StorageGRID funge da client.

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

4. ${post_edited_translations.segment}
5. Il server KMS risponde utilizzando la connessione validata.

Tipi di certificati server supportati in StorageGRID

${post_edited_translations.segment}

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

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

Configura i certificati dell'interfaccia di gestione in StorageGRID

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

Informazioni su questa attività

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

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

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

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

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

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

Aggiungi un certificato di interfaccia di gestione personalizzato

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

Passaggi

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

Carica il certificato

Carica i file del certificato server richiesti.

a. Seleziona **Carica certificato**.

b. Carica i file del certificato server richiesti:

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

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

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

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

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

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

  Ad esempio: `storagegrid_certificate.pem`

- ${post_edited_translations.segment}

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

Genera certificato

Genera i file del certificato del server.

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

a. Seleziona **Genera certificato**.

b. ${post_edited_translations.segment}

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

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

c. Seleziona **Genera**.

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

- ${post_edited_translations.segment}

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

  Ad esempio: `storagegrid_certificate.pem`

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

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

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

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

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

Ripristina il certificato predefinito dell'interfaccia di gestione

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

Passaggi

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

3. Seleziona **Usa certificato predefinito**.

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

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

${post_edited_translations.segment}

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

Prima di iniziare

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

Informazioni su questa attività

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

Passaggi

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

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

3. ${post_edited_translations.segment}

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

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

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

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

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

4. Seleziona e copia il certificato.

   Includi i tag BEGIN e END nella tua selezione.

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

Scarica o copia il certificato dell'interfaccia di gestione

${post_edited_translations.segment}

Passaggi

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

${post_edited_translations.segment}

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

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

   ${post_edited_translations.segment}

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

   Ad esempio: `storagegrid_certificate.pem`

Copia certificato o bundle CA PEM

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

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

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

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

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

   Ad esempio: `storagegrid_certificate.pem`

Configura i certificati API S3 in StorageGRID

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

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

Informazioni su questa attività

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

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

${post_edited_translations.segment}

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

Puoi caricare o generare un certificato API S3 personalizzato.

${post_edited_translations.segment}

Passaggi

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

Carica il certificato

Carica i file del certificato server richiesti.

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

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

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

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

   Ad esempio: `storagegrid_certificate.pem`

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

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

Genera certificato

Genera i file del certificato del server.

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

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

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

c. Seleziona **Genera**.

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

- ${post_edited_translations.segment}

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

  Ad esempio: `storagegrid_certificate.pem`

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

e. Seleziona **Salva**.

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

5. ${post_edited_translations.segment}

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

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

${post_edited_translations.segment}

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

Passaggi

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

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

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

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

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

${post_edited_translations.segment}

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

Passaggi

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

${post_edited_translations.segment}

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

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

   ${post_edited_translations.segment}

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

   Ad esempio: `storagegrid_certificate.pem`

Copia certificato o bundle CA PEM

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

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

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

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

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

   Ad esempio: `storagegrid_certificate.pem`

Informazioni correlate

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

Copia il certificato CA della griglia StorageGRID

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

Prima di iniziare

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

Informazioni su questa attività

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

Passaggi

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

Scarica il file del certificato

Scarica il file del certificato `.pem`.

a. Seleziona **Scarica certificato**.

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

Ad esempio: `storagegrid_certificate.pem`

Copia certificato PEM

Copia il testo del certificato per incollarlo altrove.

a. Seleziona **Copia certificato PEM**.

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

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

Ad esempio: `storagegrid_certificate.pem`

Configura i certificati StorageGRID per FabricPool

Per i client S3 che eseguono una convalida rigorosa del nome host e non supportano la disabilitazione di tale convalida, come i client ONTAP che utilizzano FabricPool, puoi

generare o caricare un certificato server quando configuri l'endpoint del bilanciatore di carico.

Prima di iniziare

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

Informazioni su questa attività

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

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

Passaggi

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

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

3. Collega StorageGRID come livello cloud in ONTAP.

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

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

Configura i certificati client in StorageGRID

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

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

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

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

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

Prima di iniziare

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

Aggiungi certificati client

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

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

Certificato dell'interfaccia di gestione già configurato

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

Passaggi

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

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

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

Il nuovo certificato viene visualizzato nella scheda Client.

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

Certificato client emesso da CA

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

Passaggi

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

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

${post_edited_translations.segment}

${post_edited_translations.segment}

Passaggi

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

7. ${post_edited_translations.segment}

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

     Queste estensioni definiscono lo scopo della chiave contenuta nel certificato.

   ${post_edited_translations.segment}

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

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

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

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

   Ad esempio: `storagegrid_certificate.pem`

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

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

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

    Il nuovo certificato viene visualizzato nella scheda Client.

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

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

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

${post_edited_translations.segment}

Passaggi

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

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

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

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

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

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

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

   ${post_edited_translations.segment}

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

${post_edited_translations.segment}

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

Passaggi

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

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

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

   Il certificato aggiornato viene visualizzato nella scheda Client.

${post_edited_translations.segment}

Puoi caricare un nuovo certificato quando quello attuale è scaduto.

Passaggi

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

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

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

Carica il certificato

Copia il testo del certificato per incollarlo altrove.

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

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

   - ${post_edited_translations.segment}

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

   Ad esempio: `storagegrid_certificate.pem`

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

   Il certificato aggiornato viene visualizzato nella scheda Client.

Genera certificato

${post_edited_translations.segment}

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

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

     Queste estensioni definiscono lo scopo della chiave contenuta nel certificato.

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

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

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

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

`.pem`.

Ad esempio: `storagegrid_certificate.pem`

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

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

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

Il nuovo certificato viene visualizzato nella scheda Client.

Scarica o copia i certificati client

${post_edited_translations.segment}

Passaggi

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

Scarica il file del certificato

Scarica il file del certificato `.pem`.

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

   Ad esempio: `storagegrid_certificate.pem`

Copia certificato

Copia il testo del certificato per incollarlo altrove.

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

   Ad esempio: `storagegrid_certificate.pem`

${post_edited_translations.segment}

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

Passaggi

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

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

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

Informazioni sul copyright

Informazioni sul marchio commerciale