Configurazione dei certificati del server

StorageGRID 11.5

NetApp
April 11, 2024

Sommario

Configurazione dei certificati del server

È possibile personalizzare i certificati server utilizzati dal sistema StorageGRID.

Il sistema StorageGRID utilizza certificati di sicurezza per diversi scopi distinti:

- Management Interface Server Certificates: Utilizzato per proteggere l'accesso a Grid Manager, tenant Manager, Grid Management API e tenant Management API.
- Storage API Server Certificates: Utilizzato per proteggere l'accesso ai nodi di storage e ai nodi gateway, le applicazioni client API utilizzate per caricare e scaricare i dati degli oggetti.

È possibile utilizzare i certificati predefiniti creati durante l'installazione oppure sostituire uno o entrambi i tipi di certificati predefiniti con certificati personalizzati.

Tipi supportati di certificati server personalizzati

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

Per ulteriori informazioni su come StorageGRID protegge le connessioni client per l'API REST, consultare le guide all'implementazione di S3 o Swift.

Certificati per gli endpoint del bilanciamento del carico

StorageGRID gestisce separatamente i certificati utilizzati per gli endpoint del bilanciamento del carico. Per configurare i certificati di bilanciamento del carico, consultare le istruzioni per la configurazione degli endpoint di bilanciamento del carico.

Informazioni correlate

"Utilizzare S3"

"USA Swift"

"Configurazione degli endpoint del bilanciamento del carico"

Configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager

È possibile sostituire il certificato del server StorageGRID predefinito con un singolo certificato server personalizzato che consente agli utenti di accedere a Grid Manager e a Tenant Manager senza incontrare avvisi di sicurezza.

A proposito di questa attività

Per impostazione predefinita, ogni nodo amministrativo riceve un certificato firmato dalla CA della griglia. Questi certificati firmati dalla CA possono essere sostituiti da un singolo certificato server personalizzato comune e dalla chiave privata corrispondente.

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

modo che corrisponda a tutti i nodi Admin nella griglia.

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

> Per garantire che le operazioni non vengano interrotte da un certificato del server guasto, l'avviso **scadenza del certificato del server per l'interfaccia di gestione** e l'allarme MCEP (Management Interface Certificate Expiry) legacy vengono attivati quando il certificato del server sta per scadere. In base alle esigenze, è possibile visualizzare il numero di giorni che devono essere trascorsi prima della scadenza del certificato di servizio corrente selezionando **supporto Strumenti topologia griglia**. Quindi, selezionare ***Primary Admin Node* CMN Resources**.

> Se si accede a Grid Manager o Tenant Manager utilizzando un nome di dominio invece di un indirizzo IP, il browser mostra un errore di certificato senza l'opzione di ignorare se si verifica una delle seguenti condizioni:
>
> - Il certificato del server dell'interfaccia di gestione personalizzata scade.
> - Viene ripristinato il certificato del server di un'interfaccia di gestione personalizzata al certificato del server predefinito.

Fasi

1. Selezionare **Configurazione Impostazioni di rete certificati server**.
2. Nella sezione Management Interface Server Certificate (certificato server interfaccia di gestione), fare clic su **Install Custom Certificate** (Installa certificato personalizzato).
3. Caricare i file dei certificati del server richiesti:
   - **Server Certificate**: Il file di certificato del server personalizzato (`.crt`).
   - **Server Certificate Private Key** (chiave privata certificato server): Il file di chiave privata del certificato del server personalizzato (`.key`).

     > Le chiavi private EC devono essere 224 bit o superiori. Le chiavi private RSA devono essere 2048 bit o superiori.

   - **Bundle CA**: Un singolo file contenente i certificati di ciascuna CA intermedia. Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.
4. Fare clic su **Save** (Salva).

   I certificati server personalizzati vengono utilizzati per tutte le nuove connessioni client successive.

   Selezionare una scheda per visualizzare informazioni dettagliate sul certificato del server StorageGRID predefinito o su un certificato firmato dalla CA caricato.

   > Dopo aver caricato un nuovo certificato, attendere fino a un giorno per eliminare eventuali avvisi relativi alla scadenza del certificato (o allarmi legacy).

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

Ripristino dei certificati server predefiniti per Grid Manager e Tenant Manager

È possibile ripristinare l'utilizzo dei certificati server predefiniti per Grid Manager e Tenant Manager.

Fasi

1. Selezionare **Configurazione Impostazioni di rete certificati server**.
2. Nella sezione Manage Interface Server Certificate (Gestisci certificato server interfaccia), fare clic su **Use Default Certificates** (Usa certificati predefiniti)
3. Fare clic su **OK** nella finestra di dialogo di conferma.

   Quando si ripristinano i certificati del server predefiniti, i file dei certificati del server personalizzati configurati vengono cancellati e non possono essere ripristinati dal sistema. I certificati server predefiniti vengono utilizzati per tutte le nuove connessioni client successive.

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

Configurazione di un certificato server personalizzato per le connessioni al nodo di storage o al servizio CLB

È possibile sostituire il certificato del server utilizzato per le connessioni client S3 o Swift al nodo di storage o al servizio CLB (obsoleto) sul nodo gateway. Il certificato del server personalizzato sostitutivo è specifico dell'organizzazione.

A proposito di questa attività

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

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

Una volta completata la configurazione sul server, gli utenti potrebbero anche aver bisogno di installare il certificato CA principale nel client S3 o Swift API che utilizzeranno per accedere al sistema, a seconda dell'autorità di certificazione (CA) root in uso.

> Per garantire che le operazioni non vengano interrotte da un certificato del server guasto, l'avviso **scadenza del certificato del server per gli endpoint API di storage** e l'allarme scadenza del certificato (SCEP) degli endpoint del servizio API di storage legacy vengono attivati quando il certificato del server root sta per scadere. In base alle esigenze, è possibile visualizzare il numero di giorni che devono essere trascorsi prima della scadenza del certificato di servizio corrente selezionando **supporto Strumenti topologia griglia**. Quindi, selezionare ***Primary Admin Node*** **CMN Resources**.

I certificati personalizzati vengono utilizzati solo se i client si connettono a StorageGRID utilizzando il servizio CLB obsoleto sui nodi gateway o se si connettono direttamente ai nodi di storage. I client S3 o Swift che si connettono a StorageGRID utilizzando il servizio bilanciamento del carico sui nodi di amministrazione o

gateway utilizzano il certificato configurato per l'endpoint del bilanciamento del carico.

> L'avviso **scadenza del certificato endpoint del bilanciamento del carico** viene attivato per gli endpoint del bilanciamento del carico che scadranno a breve.

Fasi

1. Selezionare **Configurazione Impostazioni di rete certificati server**.
2. Nella sezione Object Storage API Service Endpoints Server Certificate, fare clic su **Install Custom Certificate** (Installa certificato personalizzato).
3. Caricare i file dei certificati del server richiesti:
   - **Server Certificate**: Il file di certificato del server personalizzato (`.crt`).
   - **Server Certificate Private Key** (chiave privata certificato server): Il file di chiave privata del certificato del server personalizzato (`.key`).

     > Le chiavi private EC devono essere 224 bit o superiori. Le chiavi private RSA devono essere 2048 bit o superiori.

   - **Bundle CA**: Un singolo file contenente i certificati di ciascuna CA intermedia. Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.
4. Fare clic su **Save** (Salva).

   Il certificato del server personalizzato viene utilizzato per tutte le nuove connessioni client API successive.

   Selezionare una scheda per visualizzare informazioni dettagliate sul certificato del server StorageGRID predefinito o su un certificato firmato dalla CA caricato.

   > Dopo aver caricato un nuovo certificato, attendere fino a un giorno per eliminare eventuali avvisi relativi alla scadenza del certificato (o allarmi legacy).

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

Informazioni correlate

"Utilizzare S3"

"USA Swift"

"Configurazione dei nomi di dominio degli endpoint S3 API"

Ripristino dei certificati server predefiniti per gli endpoint S3 e Swift REST API

È possibile ripristinare l'utilizzo dei certificati server predefiniti per gli endpoint S3 e Swift REST API.

Fasi

1. Selezionare **Configurazione Impostazioni di rete certificati server**.
2. Nella sezione Object Storage API Service Endpoints Server Certificate, fare clic su **Use Default Certificates** (Usa certificati predefiniti).

3. Fare clic su **OK** nella finestra di dialogo di conferma.

   Quando si ripristinano i certificati server predefiniti per gli endpoint API dello storage a oggetti, i file di certificato del server personalizzati configurati vengono cancellati e non possono essere ripristinati dal sistema. I certificati server predefiniti vengono utilizzati per tutte le nuove connessioni client API successive.

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

Copia del certificato CA del sistema StorageGRID

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

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

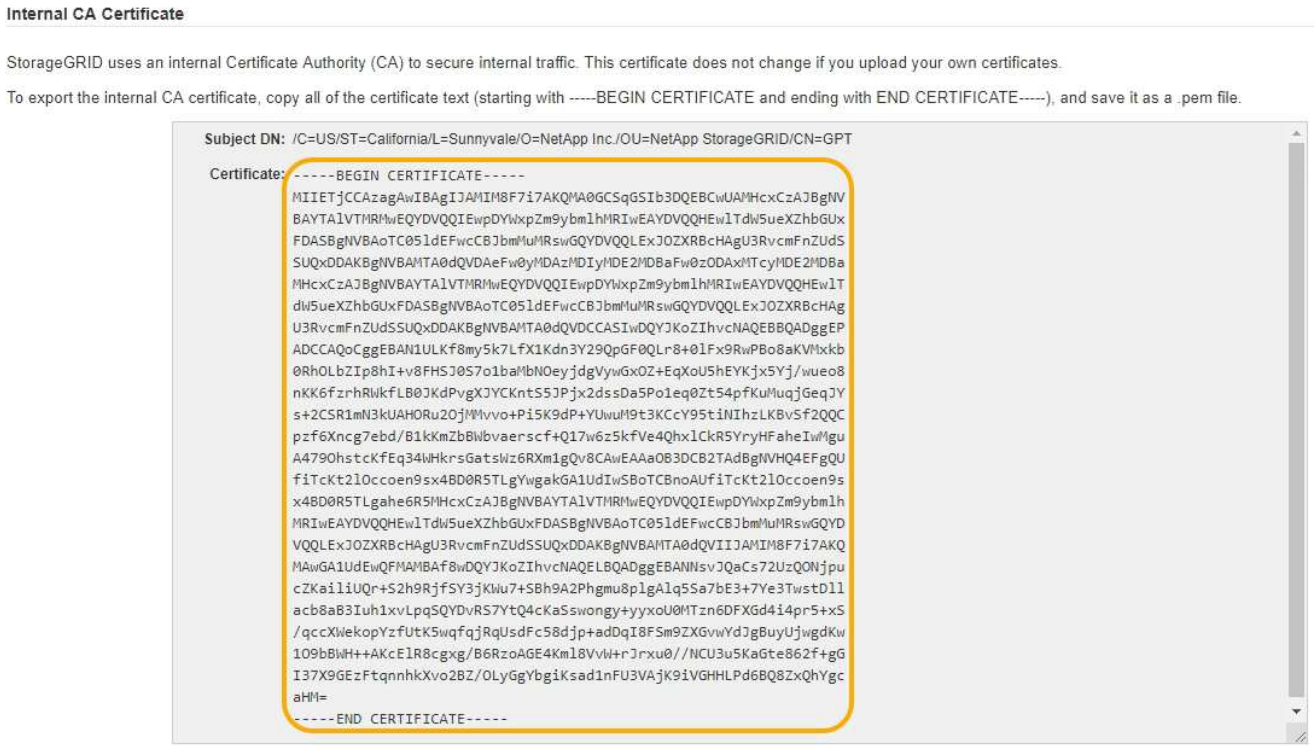
A proposito di questa attività

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

Fasi

1. Selezionare **Configurazione Impostazioni di rete certificati server**.
2. Nella sezione **certificato CA interno**, selezionare tutto il testo del certificato.

   È necessario includere `-----BEGIN CERTIFICATE-----` e. `-----END CERTIFICATE-----` nella selezione.



3. Fare clic con il pulsante destro del mouse sul testo selezionato e selezionare **Copia**.
4. Incollare il certificato copiato in un editor di testo.
5. Salvare il file con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Configurazione dei certificati StorageGRID per FabricPool

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

Di cosa hai bisogno

- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario accedere a Grid Manager utilizzando un browser supportato.

A proposito di questa attività

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

La procedura riportata di seguito fornisce linee guida generali per i client S3 che utilizzano FabricPool. Per informazioni e procedure più dettagliate, consultare le istruzioni per la configurazione di StorageGRID per FabricPool.

> Il servizio separato di bilanciamento del carico di connessione (CLB) sui nodi gateway è obsoleto e non è più consigliato per l'utilizzo con FabricPool.

Fasi

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

   Quando si crea un endpoint di bilanciamento del carico HTTPS, viene richiesto di caricare il certificato del server, la chiave privata del certificato e il bundle CA.

3. Collega StorageGRID come Tier cloud in ONTAP.

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

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

Informazioni correlate

Creazione di un certificato server autofirmato per l'interfaccia di gestione

È possibile utilizzare uno script per generare un certificato server autofirmato per i client API di gestione che richiedono una convalida rigorosa del nome host.

Di cosa hai bisogno

- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario disporre di `Passwords.txt` file.

A proposito di questa attività

Negli ambienti di produzione, è necessario utilizzare un certificato firmato da un'autorità di certificazione nota (CA). I certificati firmati da una CA possono essere ruotati senza interruzioni. Sono inoltre più sicuri perché offrono una migliore protezione contro gli attacchi man-in-the-middle.

Fasi

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

      Una volta effettuato l'accesso 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. Ad esempio, `*.ui.storagegrid.example.com` utilizza il carattere jolly * per rappresentare `admin1.ui.storagegrid.example.com` e. `admin2.ui.storagegrid.example.com`.
   - Impostare `--type` a. `management` Per configurare il certificato utilizzato da Grid Manager e Tenant Manager.
   - Per impostazione predefinita, i certificati generati sono validi per un anno (365 giorni) e devono essere ricreati prima della scadenza. È possibile utilizzare `--days` argomento per eseguire l'override del periodo di validità predefinito.

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

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 365
```

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

4. Selezionare e copiare il certificato.

   Includere i tag BEGIN e END nella selezione.

5. Disconnettersi dalla shell dei comandi. `$ exit`
6. Verificare che il certificato sia stato configurato:
   a. Accedere a Grid Manager.
   b. Selezionare **Configuration Server Certificates Management Interface Server Certificate**.
7. Configurare il client API di gestione in modo che utilizzi il certificato pubblico copiato. Includere i tag inizio e FINE.