Serverzertifikate werden konfiguriert

StorageGRID 11.5

NetApp
April 11, 2024

Inhalt

Serverzertifikate werden konfiguriert . . . 1
- Unterstützte Arten von benutzerdefiniertem Serverzertifikat . . . 1
- Zertifikate für Load Balancer-Endpunkte . . . 1
- Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager . . . 1
- Wiederherstellen der Standard-Serverzertifikate für den Grid Manager und den Tenant Manager . . . 3
- Konfigurieren eines benutzerdefinierten Serverzertifikats für Verbindungen mit dem Speicherknoten oder dem CLB-Dienst . . . 3
- Wiederherstellen der Standard-Serverzertifikate für die S3- und Swift-REST-API-Endpunkte . . . 5
- Das CA-Zertifikat des StorageGRID-Systems wird kopiert . . . 5
- Konfigurieren von StorageGRID-Zertifikaten für FabricPool . . . 6
- Erstellen eines selbstsignierten Serverzertifikats für die Managementoberfläche . . . 7

Serverzertifikate werden konfiguriert

Sie können die vom StorageGRID-System verwendeten Serverzertifikate anpassen.

Das StorageGRID System verwendet Sicherheitszertifikate für mehrere unterschiedliche Zwecke:

- Management Interface Server Certificates: Dient zum sicheren Zugriff auf den Grid Manager, den Tenant Manager, die Grid Management API und die Tenant Management API.
- Storage API Server Certificates: Dient zum sicheren Zugriff auf die Storage Nodes und Gateway Nodes, welche API-Client-Anwendungen zum Hochladen und Herunterladen von Objektdaten verwenden.

Sie können die während der Installation erstellten Standardzertifikate verwenden oder diese Standardtypen durch Ihre eigenen benutzerdefinierten Zertifikate ersetzen.

Unterstützte Arten von benutzerdefiniertem Serverzertifikat

Das StorageGRID-System unterstützt benutzerdefinierte Serverzertifikate, die mit RSA oder ECDSA (Algorithmus für digitale Signaturen der Elliptischen Kurve) verschlüsselt sind.

Weitere Informationen dazu, wie StorageGRID Client-Verbindungen für DIE REST-API sichert, finden Sie in den S3 oder Swift-Implementierungsleitfäden.

Zertifikate für Load Balancer-Endpunkte

StorageGRID managt die für Load Balancer-Endpunkte verwendeten Zertifikate separat. Informationen zum Konfigurieren von Load Balancer-Zertifikaten finden Sie in den Anweisungen zum Konfigurieren von Load Balancer-Endpunkten.

Verwandte Informationen

"S3 verwenden"

"Verwenden Sie Swift"

"Konfigurieren von Load Balancer-Endpunkten"

Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager

Sie können das standardmäßige StorageGRID-Serverzertifikat durch ein einzelnes benutzerdefiniertes Serverzertifikat ersetzen, das Benutzern den Zugriff auf den Grid-Manager und den Tenant-Manager ermöglicht, ohne dass Sicherheitswarnungen ausgegeben werden.

Über diese Aufgabe

Standardmäßig wird jeder Admin-Node ein von der Grid-CA signiertes Zertifikat ausgestellt. Diese CA-signierten Zertifikate können durch ein einziges allgemeines benutzerdefiniertes Serverzertifikat und den entsprechenden privaten Schlüssel ersetzt werden.

Da ein einzelnes benutzerdefiniertes Serverzertifikat für alle Administratorknoten verwendet wird, müssen Sie das Zertifikat als Platzhalter- oder Multi-Domain-Zertifikat angeben, wenn Clients bei der Verbindung mit Grid

Manager und Tenant Manager den Hostnamen überprüfen müssen. Definieren Sie das benutzerdefinierte Zertifikat so, dass es mit allen Admin-Nodes im Raster übereinstimmt.

Sie müssen die Konfiguration auf dem Server abschließen, und je nach der von Ihnen verwendeten Root Certificate Authority (CA) müssen Benutzer möglicherweise auch das Root CA-Zertifikat im Webbrowser installieren, mit dem sie auf den Grid Manager und den Tenant Manager zugreifen.

> Um sicherzustellen, dass die Vorgänge nicht durch ein Serverzertifikat unterbrochen werden, werden die Warnung **Ablauf des Serverzertifikats für die Managementoberfläche** und der Alarm Legacy Management Interface Certificate Expiry (MCEP) ausgelöst, wenn dieses Serverzertifikat abläuft. Nach Bedarf können Sie die Anzahl der Tage anzeigen, bis das aktuelle Service-Zertifikat abläuft, indem Sie **Support** > **Tools** > **Grid Topology** auswählen. Wählen Sie dann ***primary Admin Node*** > **CMN** > **Ressourcen** aus.

> Wenn Sie mit einem Domänennamen anstelle einer IP-Adresse auf den Grid Manager oder den Tenant Manager zugreifen, zeigt der Browser einen Zertifikatfehler ohne eine Option zum Umgehen an, wenn eine der folgenden Fälle auftritt:
>
> - Ihr Zertifikat für den benutzerdefinierten Verwaltungsserver läuft ab.
> - Sie werden von einem Server-Zertifikat der benutzerdefinierten Managementoberfläche auf das Standardserverzertifikat zurückgesetzt.

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Server-Zertifikate**.
2. Klicken Sie im Abschnitt Management Interface Server Certificate auf **Benutzerdefiniertes Zertifikat installieren**.
3. Laden Sie die erforderlichen Serverzertifikatdateien hoch:
   - **Server-Zertifikat**: Die benutzerdefinierte Server-Zertifikatdatei (`.crt`).
   - **Server Certificate Private Key**: Die benutzerdefinierte Server Zertifikat private Schlüssel Datei (`.key`).

     > Private EC-Schlüssel müssen 224 Bit oder größer sein. RSA Private Keys müssen mindestens 2048 Bit groß sein.

   - **CA Bundle**: Eine einzelne Datei, die die Zertifikate jeder Intermediate Emission Certificate Authority (CA) enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatdateien enthalten, die in der Reihenfolge der Zertifikatskette verkettet sind.
4. Klicken Sie Auf **Speichern**.

   Die benutzerdefinierten Serverzertifikate werden für alle nachfolgenden neuen Clientverbindungen verwendet.

   Wählen Sie eine Registerkarte aus, um detaillierte Informationen zum StorageGRID-Standardserverzertifikat oder zum hochgeladenen Zertifikat einer Zertifizierungsstelle anzuzeigen.

   > Nachdem Sie ein neues Zertifikat hochgeladen haben, lassen Sie bis zu einem Tag, bis alle zugehörigen Alarme zum Ablauf des Zertifikats (oder ältere Alarme) gelöscht werden können.

5. Aktualisieren Sie die Seite, um sicherzustellen, dass der Webbrowser aktualisiert wird.

Wiederherstellen der Standard-Serverzertifikate für den Grid Manager und den Tenant Manager

Sie können auf die Verwendung der Standard-Serverzertifikate für den Grid Manager und den Tenant Manager zurücksetzen.

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Server-Zertifikate**.
2. Klicken Sie im Abschnitt Schnittstellenserverzertifikat verwalten auf **Standardzertifikate verwenden**.
3. Klicken Sie im Bestätigungsdialogfeld auf **OK**.

   Wenn Sie die Standardserverzertifikate wiederherstellen, werden die von Ihnen konfigurierten benutzerdefinierten Serverzertifikatdateien gelöscht und können nicht vom System wiederhergestellt werden. Die Standard-Serverzertifikate werden für alle nachfolgenden neuen Clientverbindungen verwendet.

4. Aktualisieren Sie die Seite, um sicherzustellen, dass der Webbrowser aktualisiert wird.

Konfigurieren eines benutzerdefinierten Serverzertifikats für Verbindungen mit dem Speicherknoten oder dem CLB-Dienst

Sie können das Serverzertifikat, das für S3- oder Swift-Client-Verbindungen zum Storage-Node oder zum CLB-Service (veraltet) auf Gateway-Node verwendet wird, ersetzen. Das benutzerdefinierte Ersatzserverzertifikat ist speziell für Ihr Unternehmen bestimmt.

Über diese Aufgabe

Standardmäßig wird jeder Speicherknoten ein X.509-Serverzertifikat ausgestellt, das von der Grid-CA signiert wurde. Diese CA-signierten Zertifikate können durch ein einziges allgemeines benutzerdefiniertes Serverzertifikat und den entsprechenden privaten Schlüssel ersetzt werden.

Für alle Speicherknoten wird ein einzelnes benutzerdefiniertes Serverzertifikat verwendet. Sie müssen daher das Zertifikat als Platzhalter- oder Multidomain-Zertifikat angeben, wenn Clients den Hostnamen bei der Verbindung mit dem Speicherendpunkt überprüfen müssen. Definieren Sie das benutzerdefinierte Zertifikat, sodass es mit allen Speicherknoten im Raster übereinstimmt.

Nach Abschluss der Konfiguration auf dem Server müssen Benutzer möglicherweise auch das Root-CA-Zertifikat im S3- oder Swift-API-Client installieren, den sie für den Zugriff auf das System verwenden, abhängig von der Root Certificate Authority (CA), die Sie verwenden.

Um sicherzustellen, dass die Vorgänge nicht durch ein ausgefallenes Serverzertifikat unterbrochen werden, wird der Alarm **Ablauf des Serverzertifikats für Storage API Endpunkte** und der Alarm Legacy Storage API Service Endpoints Certificate Expiry (SCEP) ausgelöst, wenn das Root-Server-Zertifikat abläuft. Nach Bedarf können Sie die Anzahl der Tage anzeigen, bis das aktuelle Service-Zertifikat abläuft, indem Sie **Support** > **Tools** > **Grid Topology** auswählen. Wählen Sie dann ***primary Admin Node*** > **CMN** > **Ressourcen** aus.

Die benutzerdefinierten Zertifikate werden nur verwendet, wenn Clients über den veralteten CLB-Dienst auf Gateway-Nodes eine Verbindung zu StorageGRID herstellen oder eine direkte Verbindung zu Storage-Nodes herstellen. S3- oder Swift-Clients, die über den Load Balancer Service am Admin-Nodes oder Gateway-Nodes eine Verbindung zu StorageGRID herstellen, verwenden das für den Load Balancer-Endpunkt konfigurierte Zertifikat.

Die Warnung **Ablauf des Load Balancer-Endpunktzertifikats** wird für Load Balancer-Endpunkte ausgelöst, die bald ablaufen.

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Server-Zertifikate**.
2. Klicken Sie im Abschnitt Serverzertifikat für Objekt-Storage-API-Service-Endpunkte auf **Benutzerdefiniertes Zertifikat installieren**.
3. Laden Sie die erforderlichen Serverzertifikatdateien hoch:
   - **Server-Zertifikat**: Die benutzerdefinierte Server-Zertifikatdatei (`.crt`).
   - **Server Certificate Private Key**: Die benutzerdefinierte Server Zertifikat private Schlüssel Datei (`.key`).

     Private EC-Schlüssel müssen 224 Bit oder größer sein. RSA Private Keys müssen mindestens 2048 Bit groß sein.

   - **CA Bundle**: Eine einzelne Datei, die die Zertifikate jeder Intermediate Emission Certificate Authority (CA) enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatdateien enthalten, die in der Reihenfolge der Zertifikatskette verkettet sind.
4. Klicken Sie Auf **Speichern**.

   Das benutzerdefinierte Serverzertifikat wird für alle nachfolgenden neuen API-Client-Verbindungen verwendet.

   Wählen Sie eine Registerkarte aus, um detaillierte Informationen zum StorageGRID-Standardserverzertifikat oder zum hochgeladenen Zertifikat einer Zertifizierungsstelle anzuzeigen.

   Nachdem Sie ein neues Zertifikat hochgeladen haben, lassen Sie bis zu einem Tag, bis alle zugehörigen Alarme zum Ablauf des Zertifikats (oder ältere Alarme) gelöscht werden können.

5. Aktualisieren Sie die Seite, um sicherzustellen, dass der Webbrowser aktualisiert wird.

Verwandte Informationen

"S3 verwenden"

"Verwenden Sie Swift"

"Konfigurieren von S3-API-Endpunkt-Domain-Namen"

Wiederherstellen der Standard-Serverzertifikate für die S3- und Swift-REST-API-Endpunkte

Sie können die Standardeinstellungen für die S3- und Swift-REST-API-Endpunkte verwenden.

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Server-Zertifikate**.
2. Klicken Sie im Abschnitt Serverzertifikat für Objekt-Storage-API-Service-Endpunkte auf **Standardzertifikate verwenden**.
3. Klicken Sie im Bestätigungsdialogfeld auf **OK**.

   Wenn Sie die Standard-Serverzertifikate für die Endpunkte der Objekt-Storage-API wiederherstellen, werden die von Ihnen konfigurierten benutzerdefinierten Serverzertifikatdateien gelöscht und können nicht vom System wiederhergestellt werden. Die Standard-Serverzertifikate werden für alle nachfolgenden neuen API-Client-Verbindungen verwendet.

4. Aktualisieren Sie die Seite, um sicherzustellen, dass der Webbrowser aktualisiert wird.

Das CA-Zertifikat des StorageGRID-Systems wird kopiert

StorageGRID verwendet eine interne Zertifizierungsstelle (Certificate Authority, CA) zur Sicherung des internen Datenverkehrs. Dieses Zertifikat ändert sich nicht, wenn Sie Ihre eigenen Zertifikate hochladen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

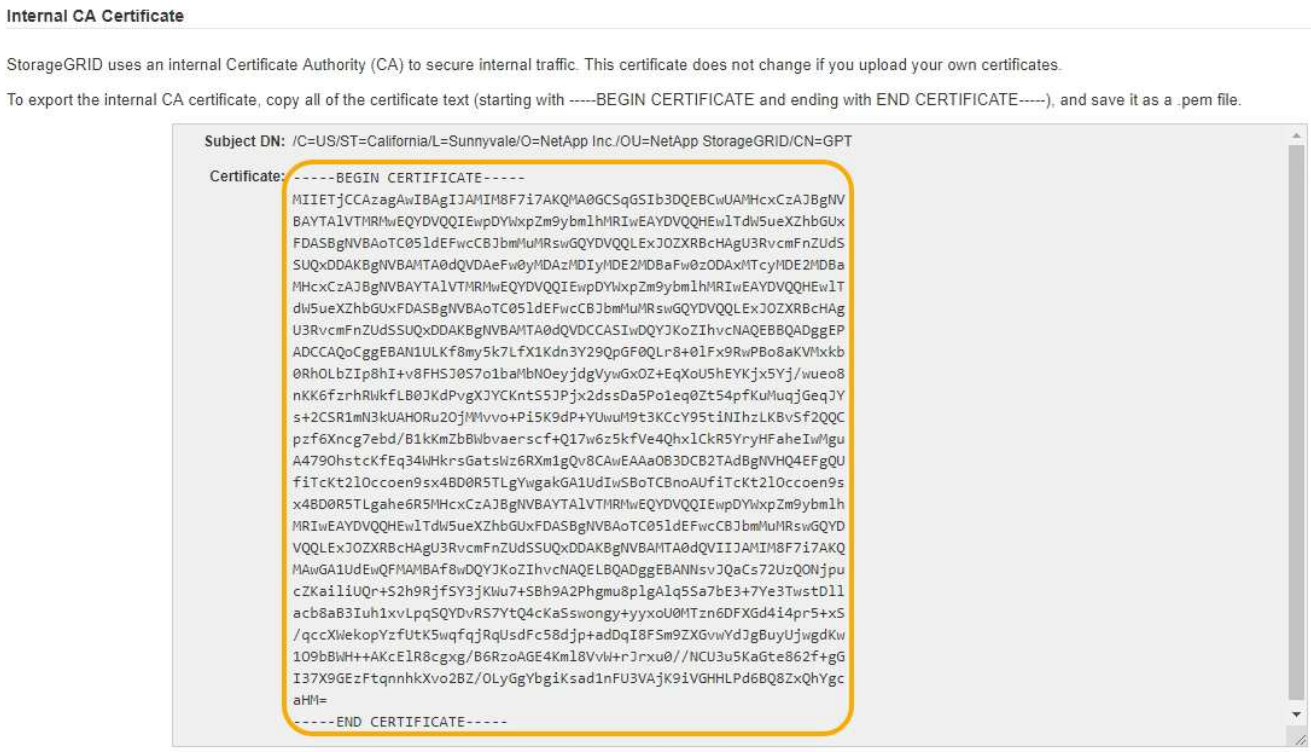
Über diese Aufgabe

Wenn ein benutzerdefiniertes Serverzertifikat konfiguriert wurde, sollten Client-Anwendungen den Server anhand des benutzerdefinierten Serverzertifikats überprüfen. Sie sollten das CA-Zertifikat nicht aus dem StorageGRID-System kopieren.

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerkeinstellungen** > **Server-Zertifikate**.
2. Wählen Sie im Abschnitt * Internes CA-Zertifikat* den gesamten Zertifikatstext aus.

   Sie müssen Folgendes einschließen `-----BEGIN CERTIFICATE-----` Und `-----END CERTIFICATE-----` Wählen Sie aus.



3. Klicken Sie mit der rechten Maustaste auf den ausgewählten Text, und wählen Sie **Kopieren**.
4. Fügen Sie das kopierte Zertifikat in einen Texteditor ein.
5. Speichern Sie die Datei mit der Erweiterung `.pem`.

   Beispiel: `storagegrid_certificate.pem`

Konfigurieren von StorageGRID-Zertifikaten für FabricPool

Bei S3-Clients, die eine strenge Hostname-Validierung durchführen und keine strenge Hostname-Validierung deaktivieren, z. B. ONTAP-Clients, die FabricPool verwenden, können Sie ein Serverzertifikat generieren oder hochladen, wenn Sie den Load Balancer-Endpunkt konfigurieren.

Was Sie benötigen

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Über diese Aufgabe

Wenn Sie einen Load Balancer-Endpunkt erstellen, können Sie ein selbstsigniertes Serverzertifikat generieren oder ein Zertifikat hochladen, das von einer bekannten Zertifizierungsstelle (CA) signiert ist. In Produktionsumgebungen sollten Sie ein Zertifikat verwenden, das von einer bekannten Zertifizierungsstelle signiert ist. Von einer Zertifizierungsstelle signierte Zertifikate können unterbrechungsfrei gedreht werden. Sie sind außerdem sicherer, weil sie einen besseren Schutz vor man-in-the-Middle-Angriffen bieten.

In den folgenden Schritten finden Sie allgemeine Richtlinien für S3-Clients, die FabricPool verwenden. Weitere Informationen und Verfahren finden Sie in den Anweisungen zum Konfigurieren von StorageGRID für FabricPool.

Der separate Connection Load Balancer (CLB)-Service auf Gateway-Nodes ist veraltet und wird nicht mehr für die Verwendung mit FabricPool empfohlen.

Schritte

1. Konfigurieren Sie optional eine HA-Gruppe (High Availability, Hochverfügbarkeit) für die Verwendung von FabricPool.
2. Einen S3-Load-Balancer-Endpunkt für FabricPool erstellen.

   Wenn Sie einen HTTPS-Load-Balancer-Endpunkt erstellen, werden Sie aufgefordert, Ihr Serverzertifikat, den privaten Zertifikatschlüssel und das CA-Bundle hochzuladen.

3. Fügen Sie StorageGRID als Cloud-Tier in ONTAP bei.

   Geben Sie den Endpunkt-Port des Load Balancer und den vollständig qualifizierten Domänennamen an, der im hochgeladenen CA-Zertifikat verwendet wird. Geben Sie dann das CA-Zertifikat ein.

   Wenn eine Zwischenzertifizierungsstelle das StorageGRID-Zertifikat ausgestellt hat, müssen Sie das Zertifikat der Zwischenzertifizierungsstelle vorlegen. Wenn das StorageGRID-Zertifikat direkt von der Root-CA ausgestellt wurde, müssen Sie das Root-CA-Zertifikat bereitstellen.

Verwandte Informationen

"Konfigurieren Sie StorageGRID für FabricPool"

Erstellen eines selbstsignierten Serverzertifikats für die Managementoberfläche

Sie können ein Skript verwenden, um ein selbstsigniertes Serverzertifikat für Management-API-Clients zu generieren, die eine strenge Hostnamen-Validierung erfordern.

Was Sie benötigen

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die haben `Passwords.txt` Datei:

Über diese Aufgabe

In Produktionsumgebungen sollten Sie ein Zertifikat verwenden, das von einer bekannten Zertifizierungsstelle (CA) signiert ist. Von einer Zertifizierungsstelle signierte Zertifikate können unterbrechungsfrei gedreht werden. Sie sind außerdem sicherer, weil sie einen besseren Schutz vor man-in-the-Middle-Angriffen bieten.

Schritte

1. Ermitteln Sie den vollständig qualifizierten Domänennamen (FQDN) jedes Admin-Knotens.
2. Melden Sie sich beim primären Admin-Node an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

   Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

3. Konfigurieren Sie StorageGRID mit einem neuen selbstsignierten Zertifikat.

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

   - Für `--domains`, Verwenden Sie Platzhalter, um die vollständig qualifizierten Domänennamen aller Admin-Knoten darzustellen. Beispiel: `*.ui.storagegrid.example.com` Verwendet den Platzhalter * für die Darstellung `admin1.ui.storagegrid.example.com` Und `admin2.ui.storagegrid.example.com`.
   - Einstellen `--type` Bis `management` Zum Konfigurieren des Zertifikats, das von Grid Manager und Tenant Manager verwendet wird.
   - Die erstellten Zertifikate sind standardmäßig für ein Jahr (365 Tage) gültig und müssen vor Ablauf neu erstellt werden. Sie können das verwenden `--days` Argument zum Überschreiben des standardmäßigen Gültigkeitszeitraums.

     > ⓘ Die Gültigkeitsdauer eines Zertifikats beginnt, wenn `make-certificate` Wird ausgeführt. Sie müssen sicherstellen, dass der Management-API-Client mit der gleichen Datenquelle wie StorageGRID synchronisiert wird. Andernfalls kann der Client das Zertifikat ablehnen.

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

     Die resultierende Ausgabe enthält das öffentliche Zertifikat, das vom Management-API-Client benötigt wird.

4. Wählen Sie das Zertifikat aus, und kopieren Sie es.

   Geben Sie DIE START- und DAS ENDE-Tags in Ihre Auswahl ein.

5. Melden Sie sich von der Eingabeaufforderung-Shell ab. `$ exit`
6. Bestätigen Sie, dass das Zertifikat konfiguriert wurde:
   a. Greifen Sie auf den Grid Manager zu.
   b. Wählen Sie **Konfiguration** > **Server Certificates** > **Management Interface Server Certificate** Aus.
7. Konfigurieren Sie den Management-API-Client so, dass er das öffentliche Zertifikat verwendet, das Sie kopiert haben. Geben Sie DIE START- und END-Tags an.