Zertifikate verwalten

StorageGRID software

NetApp
October 21, 2025

Inhalt

Zertifikate verwalten

Sicherheitszertifikate verwalten

Sicherheitszertifikate sind kleine Datendateien, die zum Erstellen sicherer, vertrauenswürdiger Verbindungen zwischen StorageGRID Komponenten sowie zwischen StorageGRID Komponenten und externen Systemen verwendet werden.

StorageGRID verwendet zwei Arten von Sicherheitszertifikaten:

- **Serverzertifikate** sind erforderlich, wenn Sie HTTPS-Verbindungen verwenden. Serverzertifikate werden verwendet, um sichere Verbindungen zwischen Clients und Servern herzustellen, die Identität eines Servers gegenüber seinen Clients zu authentifizieren und einen sicheren Kommunikationspfad für Daten bereitzustellen. Sowohl der Server als auch der Client verfügen über eine Kopie des Zertifikats.
- **Client-Zertifikate** authentifizieren die Identität eines Clients oder Benutzers gegenüber dem Server und bieten eine sicherere Authentifizierung als Passwörter allein. Client-Zertifikate verschlüsseln keine Daten.

Wenn ein Client über HTTPS eine Verbindung zum Server herstellt, antwortet der Server mit dem Serverzertifikat, das einen öffentlichen Schlüssel enthält. Der Client überprüft dieses Zertifikat, indem er die Serversignatur mit der Signatur auf seiner Kopie des Zertifikats vergleicht. Wenn die Signaturen übereinstimmen, startet der Client eine Sitzung mit dem Server unter Verwendung desselben öffentlichen Schlüssels.

StorageGRID fungiert als Server für einige Verbindungen (z. B. den Load Balancer-Endpunkt) oder als Client für andere Verbindungen (z. B. den CloudMirror-Replikationsdienst).

Standard-Grid-CA-Zertifikat

StorageGRID enthält eine integrierte Zertifizierungsstelle (CA), die während der Systeminstallation ein internes Grid-CA-Zertifikat generiert. Das Grid-CA-Zertifikat wird standardmäßig verwendet, um den internen StorageGRID -Verkehr zu sichern. Eine externe Zertifizierungsstelle (CA) kann benutzerdefinierte Zertifikate ausstellen, die vollständig mit den Informationssicherheitsrichtlinien Ihres Unternehmens konform sind. Obwohl Sie das Grid-CA-Zertifikat für eine Nicht-Produktionsumgebung verwenden können, besteht die bewährte Vorgehensweise für eine Produktionsumgebung darin, benutzerdefinierte Zertifikate zu verwenden, die von einer externen Zertifizierungsstelle signiert wurden. Ungesicherte Verbindungen ohne Zertifikat werden ebenfalls unterstützt, aber nicht empfohlen.

- Benutzerdefinierte CA-Zertifikate entfernen die internen Zertifikate nicht. Die benutzerdefinierten Zertifikate sollten jedoch diejenigen sein, die zum Überprüfen von Serververbindungen angegeben sind.
- Alle benutzerdefinierten Zertifikate müssen die"Richtlinien zur Systemhärtung für Serverzertifikate" .
- StorageGRID unterstützt die Bündelung von Zertifikaten einer Zertifizierungsstelle in einer einzigen Datei (bekannt als CA-Zertifikatspaket).

> StorageGRID umfasst auch CA-Zertifikate des Betriebssystems, die auf allen Grids gleich sind. Stellen Sie in Produktionsumgebungen sicher, dass Sie anstelle des CA-Zertifikats des Betriebssystems ein benutzerdefiniertes Zertifikat angeben, das von einer externen Zertifizierungsstelle signiert wurde.

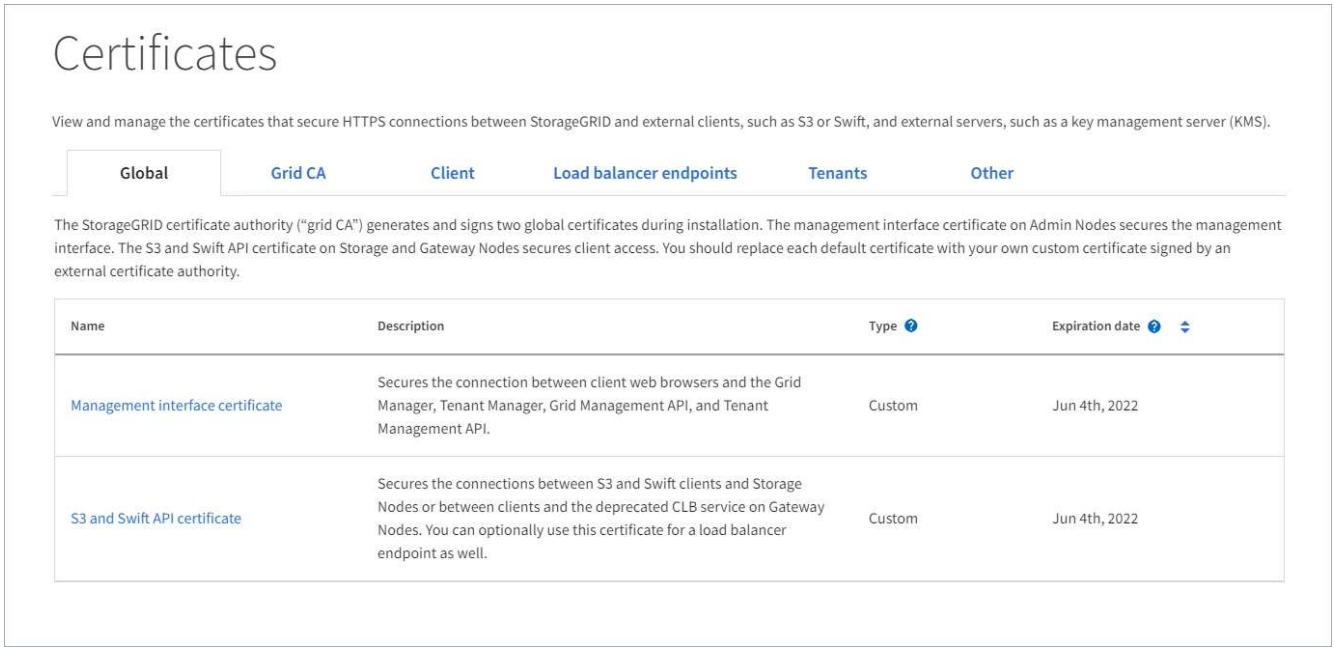
Varianten der Server- und Client-Zertifikattypen werden auf verschiedene Weise implementiert. Sie sollten alle für Ihre spezifische StorageGRID Konfiguration erforderlichen Zertifikate bereithalten, bevor Sie das System konfigurieren.

Zugriff auf Sicherheitszertifikate

Sie können an einem einzigen Ort auf Informationen zu allen StorageGRID -Zertifikaten zugreifen, zusammen mit Links zum Konfigurations-Workflow für jedes Zertifikat.

Schritte

1. Wählen Sie im Grid Manager **KONFIGURATION** > **Sicherheit** > **Zertifikate**.



2. Wählen Sie auf der Seite „Zertifikate“ eine Registerkarte aus, um Informationen zu den einzelnen Zertifikatskategorien zu erhalten und auf die Zertifikatseinstellungen zuzugreifen. Sie können auf eine Registerkarte zugreifen, wenn Sie über die"entsprechende Erlaubnis" .

   - **Global**: Sichert den StorageGRID Zugriff von Webbrowsern und externen API-Clients.
   - **Grid CA**: Sichert den internen StorageGRID Verkehr.
   - **Client**: Sichert Verbindungen zwischen externen Clients und der StorageGRID Prometheus-Datenbank.
   - **Load Balancer-Endpunkte**: Sichert Verbindungen zwischen S3-Clients und dem StorageGRID Load Balancer.
   - **Mandanten**: Sichert Verbindungen zu Identitätsföderationsservern oder von Plattformdienst-Endpunkten zu S3-Speicherressourcen.
   - **Sonstiges**: Sichert StorageGRID Verbindungen, die bestimmte Zertifikate erfordern.

     Jede Registerkarte wird unten mit Links zu weiteren Zertifikatsdetails beschrieben.

Allgemein

Die globalen Zertifikate sichern den StorageGRID Zugriff von Webbrowsern und externen S3-API-Clients. Während der Installation werden zunächst zwei globale Zertifikate von der StorageGRID Zertifizierungsstelle generiert. Die bewährte Vorgehensweise für eine Produktionsumgebung besteht darin, benutzerdefinierte Zertifikate zu verwenden, die von einer externen Zertifizierungsstelle signiert wurden.

- Management-Schnittstellenzertifikat: Sichert Client-Webbrowser-Verbindungen zu StorageGRID Verwaltungsschnittstellen.
- S3-API-Zertifikat: Sichert Client-API-Verbindungen zu Speicherknoten, Admin-Knoten und Gateway-Knoten, die von S3-Clientanwendungen zum Hoch- und Herunterladen von Objektdaten verwendet werden.

Zu den installierten globalen Zertifikaten gehören:

- **Name**: Zertifikatsname mit Link zur Verwaltung des Zertifikats.
- **Beschreibung**
- **Typ**: Benutzerdefiniert oder Standard. + Sie sollten für eine verbesserte Grid-Sicherheit immer ein benutzerdefiniertes Zertifikat verwenden.
- **Ablaufdatum**: Bei Verwendung des Standardzertifikats wird kein Ablaufdatum angezeigt.

Du kannst:

- Ersetzen Sie die Standardzertifikate durch benutzerdefinierte Zertifikate, die von einer externen Zertifizierungsstelle signiert wurden, um die Grid-Sicherheit zu verbessern:
  - "Ersetzen Sie das standardmäßige, von StorageGRID generierte Management-Schnittstellenzertifikat"Wird für Grid Manager- und Tenant Manager-Verbindungen verwendet.
  - "Ersetzen des S3-API-Zertifikats"Wird für Verbindungen zu Speicherknoten und Lastenausgleichsendpunkten (optional) verwendet.
- "Wiederherstellen des Standardzertifikats der Verwaltungsschnittstelle" .
- "Wiederherstellen des Standard-S3-API-Zertifikats" .
- "Verwenden Sie ein Skript, um ein neues selbstsigniertes Management-Schnittstellenzertifikat zu generieren" .
- Kopieren oder herunterladen Sie die"Management-Schnittstellenzertifikat" oder"S3-API-Zertifikat" .

Grid CA

DerGrid-CA-Zertifikat , das von der StorageGRID Zertifizierungsstelle während der StorageGRID Installation generiert wird, sichert den gesamten internen StorageGRID Verkehr.

Zu den Zertifikatsinformationen gehören das Ablaufdatum des Zertifikats und der Zertifikatsinhalt.

Du kannst"Kopieren oder laden Sie das Grid CA-Zertifikat herunter" , aber Sie können es nicht ändern.

Kunde

Client-Zertifikate, die von einer externen Zertifizierungsstelle generiert werden, sichern die Verbindungen zwischen externen Überwachungstools und der StorageGRID Prometheus-Datenbank.

Die Zertifikatstabelle enthält eine Zeile für jedes konfigurierte Client-Zertifikat und gibt an, ob das Zertifikat für den Zugriff auf die Prometheus-Datenbank verwendet werden kann, sowie das Ablaufdatum des Zertifikats.

Du kannst:

- "Laden Sie ein neues Client-Zertifikat hoch oder generieren Sie ein neues."
- Wählen Sie einen Zertifikatsnamen aus, um die Zertifikatsdetails anzuzeigen. Dort können Sie:
  - "Ändern Sie den Namen des Client-Zertifikats."
  - "Legen Sie die Prometheus-Zugriffsberechtigung fest."
  - "Laden Sie das Client-Zertifikat hoch und ersetzen Sie es."
  - "Kopieren oder laden Sie das Client-Zertifikat herunter."
  - "Entfernen Sie das Client-Zertifikat."
- Wählen Sie **Aktionen**, um schnell"bearbeiten" ,"befestigen" , oder"entfernen" ein Client-Zertifikat. Sie können bis zu 10 Client-Zertifikate auswählen und diese gleichzeitig über **Aktionen** > **Entfernen** entfernen.

Load Balancer-Endpunkte

Load Balancer-EndpunktzertifikateSichern Sie die Verbindungen zwischen S3-Clients und dem StorageGRID Load Balancer-Dienst auf Gateway-Knoten und Admin-Knoten.

Die Load Balancer-Endpunkttabelle enthält eine Zeile für jeden konfigurierten Load Balancer-Endpunkt und gibt an, ob für den Endpunkt das globale S3-API-Zertifikat oder ein benutzerdefiniertes Load Balancer-Endpunktzertifikat verwendet wird. Außerdem wird das Ablaufdatum jedes Zertifikats angezeigt.

> Es kann bis zu 15 Minuten dauern, bis Änderungen an einem Endpunktzertifikat auf alle Knoten angewendet werden.

Du kannst:

- "Einen Load Balancer-Endpunkt anzeigen", einschließlich der Zertifikatsdetails.
- "Geben Sie ein Load Balancer-Endpunktzertifikat für FabricPool an."
- "Verwenden Sie das globale S3-API-Zertifikat"anstatt ein neues Load Balancer-Endpunktzertifikat zu generieren.

Mieter

Mieter könnenIdentity Federation Server-Zertifikate oderPlattformdienst-Endpunktzertifikate um ihre Verbindungen mit StorageGRID zu sichern.

Die Mandantentabelle enthält für jeden Mandanten eine Zeile und gibt an, ob jeder Mandant die Berechtigung hat, seine eigene Identitätsquelle oder Plattformdienste zu verwenden.

Du kannst:

- "Wählen Sie einen Mandantennamen aus, um sich beim Mandantenmanager anzumelden"
- "Wählen Sie einen Mandantennamen aus, um die Details zur Mandantenidentitätsföderation anzuzeigen."
- "Wählen Sie einen Mandantennamen aus, um Details zu den Mandantenplattformdiensten

anzuzeigen"

- "Geben Sie während der Endpunkterstellung ein Plattformdienstendpunktzertifikat an"

Sonstige

StorageGRID verwendet für bestimmte Zwecke andere Sicherheitszertifikate. Diese Zertifikate werden nach ihrem Funktionsnamen aufgelistet. Weitere Sicherheitszertifikate sind:

- Cloud Storage Pool-Zertifikate
- Zertifikate für E-Mail-Benachrichtigungen
- Externe Syslog-Server-Zertifikate
- Netzverbund-Anschlusszertifikate
- Identitätsverbundzertifikate
- Schlüsselverwaltungsserver-Zertifikate (KMS)
- Single Sign-On-Zertifikate

Die Informationen geben den Zertifikatstyp an, den eine Funktion verwendet, sowie gegebenenfalls die Ablaufdaten des Server- und Client-Zertifikats. Wenn Sie einen Funktionsnamen auswählen, wird eine Browserregisterkarte geöffnet, in der Sie die Zertifikatsdetails anzeigen und bearbeiten können.

Informationen zu anderen Zertifikaten können Sie nur einsehen und abrufen, wenn Sie über die Berechtigung"entsprechende Erlaubnis" .

Du kannst:

- "Geben Sie ein Cloud Storage Pool-Zertifikat für S3, C2S S3 oder Azure an"
- "Geben Sie ein Zertifikat für E-Mail-Benachrichtigungen an"
- "Verwenden Sie ein Zertifikat für einen externen Syslog-Server"
- "Rotieren von Grid-Föderation-Verbindungszertifikaten"
- "Anzeigen und Bearbeiten eines Identitätsverbundzertifikats"
- "Hochladen von KMS-Server- und Client-Zertifikaten (Key Management Server)"
- "Manuelles Angeben eines SSO-Zertifikats für eine Vertrauensstellung der vertrauenden Seite"

Details zum Sicherheitszertifikat

Nachfolgend wird jeder Typ von Sicherheitszertifikat beschrieben, mit Links zu den Implementierungsanweisungen.

Management-Schnittstellenzertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server	Authentifiziert die Verbindung zwischen Client-Webbrowsern und der StorageGRID Verwaltungsschnittstelle, sodass Benutzer ohne Sicherheitswarnungen auf den Grid Manager und den Tenant Manager zugreifen können. Dieses Zertifikat authentifiziert auch Grid Management API- und Tenant Management API-Verbindungen. Sie können das während der Installation erstellte Standardzertifikat verwenden oder ein benutzerdefiniertes Zertifikat hochladen.	**KONFIGURATION** > **Sicherheit** > **Zertifikate**, wählen Sie die Registerkarte **Global** und dann **Management-Schnittstellenzertifikat**	"Konfigurieren von Management-Schnittstellenzertifikaten"

S3-API-Zertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server	Authentifiziert sichere S3-Clientverbindungen zu einem Speicherknoten und zu Load Balancer-Endpunkten (optional).	**KONFIGURATION** > **Sicherheit** > **Zertifikate**, wählen Sie die Registerkarte **Global** und dann **S3-API-Zertifikat**	"Konfigurieren von S3-API-Zertifikaten"

Grid-CA-Zertifikat

Siehe dieBeschreibung des Standard-Grid-CA-Zertifikats .

Administrator-Client-Zertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Kunde	Wird auf jedem Client installiert, sodass StorageGRID den externen Clientzugriff authentifizieren kann. • Ermöglicht autorisierten externen Clients den Zugriff auf die StorageGRID Prometheus-Datenbank. • Ermöglicht die sichere Überwachung von StorageGRID mit externen Tools.	**KONFIGURATION** > **Sicherheit** > **Zertifikate** und wählen Sie dann die Registerkarte **Client**	"Konfigurieren von Clientzertifikaten"

Load Balancer-Endpunktzertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server	Authentifiziert die Verbindung zwischen S3-Clients und dem StorageGRID Load Balancer-Dienst auf Gateway-Knoten und Admin-Knoten. Sie können ein Load Balancer-Zertifikat hochladen oder generieren, wenn Sie einen Load Balancer-Endpunkt konfigurieren. Clientanwendungen verwenden das Load Balancer-Zertifikat beim Herstellen einer Verbindung mit StorageGRID , um Objektdaten zu speichern und abzurufen. Sie können auch eine benutzerdefinierte Version des globalenS3-API-Zertifikat Zertifikat zur Authentifizierung von Verbindungen mit dem Load Balancer-Dienst. Wenn das globale Zertifikat zum Authentifizieren von Load Balancer-Verbindungen verwendet wird, müssen Sie nicht für jeden Load Balancer-Endpunkt ein separates Zertifikat hochladen oder generieren. **Hinweis:** Das für die Load Balancer-Authentifizierung verwendete Zertifikat ist das am häufigsten verwendete Zertifikat während des normalen StorageGRID -Betriebs.	**KONFIGURATION** > **Netzwerk** > **Load Balancer-Endpunkte**	• "Konfigurieren von Load Balancer-Endpunkten" • "Erstellen Sie einen Load Balancer-Endpunkt für FabricPool"

Cloud Storage Pool-Endpunktzertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server	Authentifiziert die Verbindung von einem StorageGRID Cloud Storage Pool zu einem externen Speicherort, wie z. B. S3 Glacier oder Microsoft Azure Blob Storage. Für jeden Cloud-Anbietertyp ist ein anderes Zertifikat erforderlich.	**ILM** > **Speicherpools**	"Erstellen Sie einen Cloud-Speicherpool"

Zertifikat für E-Mail-Benachrichtigungen

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server und Client	Authentifiziert die Verbindung zwischen einem SMTP-E-Mail-Server und StorageGRID , die für Warnbenachrichtigungen verwendet wird. • Wenn für die Kommunikation mit dem SMTP-Server Transport Layer Security (TLS) erforderlich ist, müssen Sie das CA-Zertifikat des E-Mail-Servers angeben. • Geben Sie nur dann ein Client-Zertifikat an, wenn der SMTP-E-Mail-Server Client-Zertifikate zur Authentifizierung erfordert.	**WARNUNGEN** > **E-Mail-Einrichtung**	"E-Mail-Benachrichtigungen für Warnmeldungen einrichten"

Externes Syslog-Server-Zertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server	Authentifiziert die TLS- oder RELP/TLS-Verbindung zwischen einem externen Syslog-Server, der Ereignisse in StorageGRID protokolliert. **Hinweis:** Für TCP-, RELP/TCP- und UDP-Verbindungen zu einem externen Syslog-Server ist kein externes Syslog-Serverzertifikat erforderlich.	**KONFIGURATION** > **Überwachung** > **Audit- und Syslog-Server**	"Verwenden Sie einen externen Syslog-Server"

Grid-Föderation-Verbindungszertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server und Client	Authentifizieren und verschlüsseln Sie Informationen, die zwischen dem aktuellen StorageGRID -System und einem anderen Grid in einer Grid-Föderationsverbindung gesendet werden.	**KONFIGURATION** > **System** > **Grid-Föderation**	• "Erstellen von Grid-Föderationsverbindungen" • "Verbindungszertifikate rotieren"

Identitätsverbundzertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server	Authentifiziert die Verbindung zwischen StorageGRID und einem externen Identitätsanbieter wie Active Directory, OpenLDAP oder Oracle Directory Server. Wird für die Identitätsföderation verwendet, wodurch Administratorgruppen und Benutzer von einem externen System verwaltet werden können.	**KONFIGURATION** > **Zugriffskontrolle** > **Identitätsföderation**	"Verwenden der Identitätsföderation"

Schlüsselverwaltungsserver-Zertifikat (KMS)

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server und Client	Authentifiziert die Verbindung zwischen StorageGRID und einem externen Schlüsselverwaltungsserver (KMS), der Verschlüsselungsschlüssel für StorageGRID Appliance-Knoten bereitstellt.	**KONFIGURATION** > **Sicherheit** > **Schlüsselverwaltungsserver**	"Schlüsselverwaltungsserver (KMS) hinzufügen"

Plattformdienste-Endpunktzertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server	Authentifiziert die Verbindung vom StorageGRID -Plattformdienst zu einer S3-Speicherressource.	**Mandantenmanager** > **SPEICHER (S3)** > **Plattformdienst-Endpunkte**	"Plattformdienst-Endpunkt erstellen" "Plattformdienst-Endpunkt bearbeiten"

Single Sign-On (SSO)-Zertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server	Authentifiziert die Verbindung zwischen Identitätsföderationsdiensten wie Active Directory Federation Services (AD FS) und StorageGRID , die für Single Sign-On (SSO)-Anfragen verwendet werden.	**KONFIGURATION** > **Zugriffskontrolle** > **Single Sign-On**	"Konfigurieren der einmaligen Anmeldung"

Zertifikatbeispiele

Beispiel 1: Load Balancer-Dienst

In diesem Beispiel fungiert StorageGRID als Server.

1. Sie konfigurieren einen Load Balancer-Endpunkt und laden ein Serverzertifikat in StorageGRID hoch oder generieren es.
2. Sie konfigurieren eine S3-Client-Verbindung zum Load Balancer-Endpunkt und laden dasselbe Zertifikat auf den Client hoch.
3. Wenn der Client Daten speichern oder abrufen möchte, stellt er über HTTPS eine Verbindung zum Load

Balancer-Endpunkt her.

4. StorageGRID antwortet mit dem Serverzertifikat, das einen öffentlichen Schlüssel enthält, und mit einer Signatur, die auf dem privaten Schlüssel basiert.
5. Der Client überprüft dieses Zertifikat, indem er die Serversignatur mit der Signatur auf seiner Kopie des Zertifikats vergleicht. Wenn die Signaturen übereinstimmen, startet der Client eine Sitzung mit demselben öffentlichen Schlüssel.
6. Der Client sendet Objektdaten an StorageGRID.

Beispiel 2: Externer Schlüsselverwaltungsserver (KMS)

In diesem Beispiel fungiert StorageGRID als Client.

1. Mithilfe externer Key Management Server-Software konfigurieren Sie StorageGRID als KMS-Client und erhalten ein von einer Zertifizierungsstelle signiertes Serverzertifikat, ein öffentliches Client-Zertifikat und den privaten Schlüssel für das Client-Zertifikat.
2. Mithilfe des Grid Managers konfigurieren Sie einen KMS-Server und laden die Server- und Client-Zertifikate sowie den privaten Client-Schlüssel hoch.
3. Wenn ein StorageGRID Knoten einen Verschlüsselungsschlüssel benötigt, sendet er eine Anfrage an den KMS-Server, die Daten aus dem Zertifikat und eine auf dem privaten Schlüssel basierende Signatur enthält.
4. Der KMS-Server validiert die Zertifikatssignatur und entscheidet, dass er StorageGRID vertrauen kann.
5. Der KMS-Server antwortet über die validierte Verbindung.

Unterstützte Serverzertifikattypen

Das StorageGRID -System unterstützt benutzerdefinierte Zertifikate, die mit RSA oder ECDSA (Elliptic Curve Digital Signature Algorithm) verschlüsselt sind.

> Der Verschlüsselungstyp für die Sicherheitsrichtlinie muss mit dem Serverzertifikatstyp übereinstimmen. Beispielsweise erfordern RSA-Chiffren RSA-Zertifikate und ECDSA-Chiffren ECDSA-Zertifikate. Sehen "Sicherheitszertifikate verwalten" . Wenn Sie eine benutzerdefinierte Sicherheitsrichtlinie konfigurieren, die nicht mit dem Serverzertifikat kompatibel ist, können Sie"vorübergehend zur Standardsicherheitsrichtlinie zurückkehren" .

Weitere Informationen dazu, wie StorageGRID Clientverbindungen sichert, finden Sie unter"Sicherheit für S3-Clients" .

Konfigurieren von Management-Schnittstellenzertifikaten

Sie können das Standardzertifikat der Verwaltungsschnittstelle durch ein einzelnes benutzerdefiniertes Zertifikat ersetzen, das Benutzern den Zugriff auf den Grid Manager und den Tenant Manager ermöglicht, ohne dass Sicherheitswarnungen angezeigt werden. Sie können auch zum Standardzertifikat der Verwaltungsschnittstelle zurückkehren oder ein neues generieren.

Informationen zu diesem Vorgang

Standardmäßig wird jedem Admin-Knoten ein von der Grid-CA signiertes Zertifikat ausgestellt. Diese von der Zertifizierungsstelle signierten Zertifikate können durch ein einzelnes gemeinsames benutzerdefiniertes

Verwaltungsschnittstellenzertifikat und den entsprechenden privaten Schlüssel ersetzt werden.

Da für alle Admin-Knoten ein einziges benutzerdefiniertes Verwaltungsschnittstellenzertifikat verwendet wird, müssen Sie das Zertifikat als Platzhalter- oder Multidomänenzertifikat angeben, wenn Clients den Hostnamen beim Herstellen einer Verbindung mit dem Grid Manager und Tenant Manager überprüfen müssen. Definieren Sie das benutzerdefinierte Zertifikat so, dass es mit allen Admin-Knoten im Raster übereinstimmt.

Sie müssen die Konfiguration auf dem Server abschließen. Je nach der von Ihnen verwendeten Stammzertifizierungsstelle (CA) müssen Benutzer möglicherweise auch das Grid-CA-Zertifikat in dem Webbrowser installieren, den sie für den Zugriff auf den Grid Manager und den Tenant Manager verwenden.

Um sicherzustellen, dass der Betrieb nicht durch ein fehlerhaftes Serverzertifikat unterbrochen wird, wird die Warnung **Ablauf des Serverzertifikats für die Verwaltungsschnittstelle** ausgelöst, wenn dieses Serverzertifikat bald abläuft. Bei Bedarf können Sie das Ablaufdatum des aktuellen Zertifikats anzeigen, indem Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate** auswählen und auf der Registerkarte „Global“ das Ablaufdatum für das Management-Schnittstellenzertifikat anzeigen.

Wenn Sie auf den Grid Manager oder Tenant Manager über einen Domänennamen statt einer IP-Adresse zugreifen, zeigt der Browser einen Zertifikatsfehler ohne Umgehungsoption an, wenn einer der folgenden Fälle eintritt:

- Ihr benutzerdefiniertes Verwaltungsschnittstellenzertifikat läuft ab.
- Duvon einem benutzerdefinierten Verwaltungsschnittstellenzertifikat auf das Standardserverzertifikat zurücksetzen .

Hinzufügen eines benutzerdefinierten Verwaltungsschnittstellenzertifikats

Um ein benutzerdefiniertes Verwaltungsschnittstellenzertifikat hinzuzufügen, können Sie Ihr eigenes Zertifikat bereitstellen oder mithilfe des Grid Managers eines generieren.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global** die Option **Management-Schnittstellenzertifikat** aus.
3. Wählen Sie **Benutzerdefiniertes Zertifikat verwenden**.
4. Laden Sie das Zertifikat hoch oder generieren Sie es.

Zertifikat hochladen

Laden Sie die erforderlichen Serverzertifikatsdateien hoch.

a. Wählen Sie **Zertifikat hochladen**.

b. Laden Sie die erforderlichen Serverzertifikatsdateien hoch:

- **Serverzertifikat**: Die benutzerdefinierte Serverzertifikatsdatei (PEM-codiert).
- **Privater Zertifikatsschlüssel**: Die benutzerdefinierte private Schlüsseldatei des Serverzertifikats(`.key`).

> Private EC-Schlüssel müssen mindestens 224 Bit lang sein. Private RSA-Schlüssel müssen mindestens 2048 Bit lang sein.

- **CA-Paket**: Eine einzelne optionale Datei, die die Zertifikate jeder zwischengeschalteten ausstellenden Zertifizierungsstelle (CA) enthält. Die Datei sollte alle PEM-codierten CA-Zertifikatsdateien enthalten, die in der Reihenfolge der Zertifikatskette aneinandergereiht sind.

c. Erweitern Sie **Zertifikatdetails**, um die Metadaten für jedes von Ihnen hochgeladene Zertifikat anzuzeigen. Wenn Sie ein optionales CA-Paket hochgeladen haben, wird jedes Zertifikat auf einer eigenen Registerkarte angezeigt.

- Wählen Sie **Zertifikat herunterladen**, um die Zertifikatsdatei zu speichern, oder wählen Sie **CA-Paket herunterladen**, um das Zertifikatspaket zu speichern.

  Geben Sie den Namen der Zertifikatsdatei und den Download-Speicherort an. Speichern Sie die Datei mit der Erweiterung `.pem` .

  Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Zertifikat PEM kopieren** oder **CA-Paket PEM kopieren**, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.

d. Wählen Sie **Speichern**. + Das benutzerdefinierte Verwaltungsschnittstellenzertifikat wird für alle nachfolgenden neuen Verbindungen zum Grid Manager, Tenant Manager, Grid Manager API oder Tenant Manager API verwendet.

Zertifikat generieren

Generieren Sie die Serverzertifikatsdateien.

> Die bewährte Vorgehensweise für eine Produktionsumgebung besteht darin, ein benutzerdefiniertes Verwaltungsschnittstellenzertifikat zu verwenden, das von einer externen Zertifizierungsstelle signiert wurde.

a. Wählen Sie **Zertifikat generieren**.

b. Geben Sie die Zertifikatsinformationen an:

Feld	Beschreibung
Domänenname	Ein oder mehrere vollqualifizierte Domänennamen, die in das Zertifikat aufgenommen werden sollen. Verwenden Sie ein * als Platzhalter, um mehrere Domänennamen darzustellen.

Feld	Beschreibung
IP	Eine oder mehrere IP-Adressen, die in das Zertifikat aufgenommen werden sollen.
Betreff (optional)	X.509-Betreff oder Distinguished Name (DN) des Zertifikatsinhabers. Wenn in dieses Feld kein Wert eingegeben wird, verwendet das generierte Zertifikat den ersten Domänennamen oder die erste IP-Adresse als allgemeinen Namen (CN) des Betreffs.
Gültigkeitstage	Anzahl der Tage nach der Erstellung, bis zu der das Zertifikat abläuft.
Hinzufügen von Schlüsselverwendungserweiterungen	Wenn ausgewählt (Standard und empfohlen), werden dem generierten Zertifikat Schlüsselverwendung und erweiterte Schlüsselverwendungserweiterungen hinzugefügt. Diese Erweiterungen definieren den Zweck des im Zertifikat enthaltenen Schlüssels. **Hinweis**: Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, Sie haben Verbindungsprobleme mit älteren Clients, wenn die Zertifikate diese Erweiterungen enthalten.

c. Wählen Sie **Generieren**.

d. Wählen Sie **Zertifikatdetails** aus, um die Metadaten für das generierte Zertifikat anzuzeigen.

   - Wählen Sie **Zertifikat herunterladen**, um die Zertifikatsdatei zu speichern.

     Geben Sie den Namen der Zertifikatsdatei und den Download-Speicherort an. Speichern Sie die Datei mit der Erweiterung `.pem` .

   Beispiel: `storagegrid_certificate.pem`

   - Wählen Sie **Zertifikat PEM kopieren**, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.

e. Wählen Sie **Speichern**. + Das benutzerdefinierte Verwaltungsschnittstellenzertifikat wird für alle nachfolgenden neuen Verbindungen zum Grid Manager, Tenant Manager, Grid Manager API oder Tenant Manager API verwendet.

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

> Warten Sie nach dem Hochladen oder Generieren eines neuen Zertifikats bis zu einem Tag, bis alle zugehörigen Warnungen zum Ablauf des Zertifikats gelöscht werden.

6. Nachdem Sie ein benutzerdefiniertes Management-Schnittstellenzertifikat hinzugefügt haben, werden auf der Seite „Management-Schnittstellenzertifikat“ detaillierte Zertifikatsinformationen zu den verwendeten Zertifikaten angezeigt. + Sie können das Zertifikat PEM nach Bedarf herunterladen oder kopieren.

Wiederherstellen des Standardzertifikats der Verwaltungsschnittstelle

Sie können für Grid Manager- und Tenant Manager-Verbindungen wieder das Standardzertifikat der Verwaltungsschnittstelle verwenden.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global** die Option **Management-Schnittstellenzertifikat** aus.
3. Wählen Sie **Standardzertifikat verwenden**.

   Wenn Sie das Standardzertifikat der Verwaltungsschnittstelle wiederherstellen, werden die von Ihnen konfigurierten benutzerdefinierten Serverzertifikatdateien gelöscht und können nicht vom System wiederhergestellt werden. Für alle nachfolgenden neuen Clientverbindungen wird das Standardzertifikat der Verwaltungsschnittstelle verwendet.

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

Verwenden Sie ein Skript, um ein neues selbstsigniertes Management-Schnittstellenzertifikat zu generieren

Wenn eine strenge Hostnamenvalidierung erforderlich ist, können Sie ein Skript zum Generieren des Verwaltungsschnittstellenzertifikats verwenden.

Bevor Sie beginnen

- Du hast"spezifische Zugriffsberechtigungen" .
- Sie haben die `Passwords.txt` Datei.

Informationen zu diesem Vorgang

Die bewährte Vorgehensweise für eine Produktionsumgebung besteht darin, ein von einer externen Zertifizierungsstelle signiertes Zertifikat zu verwenden.

Schritte

1. Besorgen Sie sich den vollqualifizierten Domänennamen (FQDN) jedes Admin-Knotens.
2. Melden Sie sich beim primären Admin-Knoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
   b. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

      Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Zu `#` .
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 vollqualifizierten Domänennamen aller Admin-Knoten darzustellen. Zum Beispiel, `*.ui.storagegrid.example.com` verwendet das Platzhalterzeichen * zur Darstellung `admin1.ui.storagegrid.example.com` Und `admin2.ui.storagegrid.example.com` .

- Satz `--type` Zu `management` um das Management-Schnittstellenzertifikat zu konfigurieren, das von Grid Manager und Tenant Manager verwendet wird.
- Standardmäßig sind generierte Zertifikate ein Jahr (365 Tage) gültig und müssen vor ihrem Ablauf neu erstellt werden. Sie können die `--days` Argument, um die Standardgültigkeitsdauer zu überschreiben.

> ⓘ Die Gültigkeitsdauer eines Zertifikats beginnt, wenn `make-certificate` wird ausgeführt. Sie müssen sicherstellen, dass der Verwaltungsclient mit derselben Zeitquelle wie StorageGRID synchronisiert ist. Andernfalls kann es sein, dass der Client das Zertifikat ablehnt.

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

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

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

   Schließen Sie die Tags BEGIN und END in Ihre Auswahl ein.

5. Melden Sie sich von der Befehlsshell ab. `$ exit`
6. Bestätigen Sie, dass das Zertifikat konfiguriert wurde:
   a. Greifen Sie auf den Grid Manager zu.
   b. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate**
   c. Wählen Sie auf der Registerkarte **Global** die Option **Management-Schnittstellenzertifikat** aus.
7. Konfigurieren Sie Ihren Verwaltungsclient so, dass er das von Ihnen kopierte öffentliche Zertifikat verwendet. Fügen Sie die Tags BEGIN und END ein.

Laden Sie das Management-Interface-Zertifikat herunter oder kopieren Sie es

Sie können den Inhalt des Management-Schnittstellenzertifikats zur Verwendung an anderer Stelle speichern oder kopieren.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global** die Option **Management-Schnittstellenzertifikat** aus.
3. Wählen Sie die Registerkarte **Server** oder **CA-Paket** und laden Sie anschließend das Zertifikat herunter oder kopieren Sie es.

Zertifikatsdatei oder CA-Paket herunterladen

Laden Sie das Zertifikat oder CA-Paket herunter `.pem` Datei. Wenn Sie ein optionales CA-Paket verwenden, wird jedes Zertifikat im Paket auf einer eigenen Unterregisterkarte angezeigt.

a. Wählen Sie **Zertifikat herunterladen** oder **CA-Paket herunterladen**.

   Wenn Sie ein CA-Paket herunterladen, werden alle Zertifikate in den sekundären Registerkarten des CA-Pakets als einzelne Datei heruntergeladen.

b. Geben Sie den Namen der Zertifikatsdatei und den Download-Speicherort an. Speichern Sie die Datei mit der Erweiterung `.pem` .

   Beispiel: `storagegrid_certificate.pem`

Zertifikat oder CA-Bundle PEM kopieren

Kopieren Sie den Zertifikatstext, um ihn an anderer Stelle einzufügen. Wenn Sie ein optionales CA-Paket verwenden, wird jedes Zertifikat im Paket auf einer eigenen Unterregisterkarte angezeigt.

a. Wählen Sie **Zertifikat PEM kopieren** oder **CA-Paket PEM kopieren**.

   Wenn Sie ein CA-Paket kopieren, werden alle Zertifikate in den sekundären Registerkarten des CA-Pakets zusammen kopiert.

b. Fügen Sie das kopierte Zertifikat in einen Texteditor ein.

c. Speichern Sie die Textdatei mit der Erweiterung `.pem` .

   Beispiel: `storagegrid_certificate.pem`

Konfigurieren von S3-API-Zertifikaten

Sie können das Serverzertifikat ersetzen oder wiederherstellen, das für S3-Clientverbindungen zu Speicherknoten oder Load Balancer-Endpunkten verwendet wird. Das benutzerdefinierte Ersatzserverzertifikat ist spezifisch für Ihre Organisation.

Swift-Details wurden aus dieser Version der Dokumentationssite entfernt. Sehen "StorageGRID 11.8: Konfigurieren von S3- und Swift-API-Zertifikaten" .

Informationen zu diesem Vorgang

Standardmäßig wird jedem Speicherknoten ein von der Grid-CA signiertes X.509-Serverzertifikat ausgestellt. Diese von einer Zertifizierungsstelle signierten Zertifikate können durch ein einzelnes gemeinsames benutzerdefiniertes Serverzertifikat und den entsprechenden privaten Schlüssel ersetzt werden.

Für alle Speicherknoten wird ein einzelnes benutzerdefiniertes Serverzertifikat verwendet. Sie müssen das Zertifikat daher als Platzhalter- oder Multidomänenzertifikat angeben, wenn Clients beim Herstellen einer Verbindung mit dem Speicherendpunkt den Hostnamen überprüfen müssen. Definieren Sie das benutzerdefinierte Zertifikat so, dass es mit allen Speicherknoten im Raster übereinstimmt.

Nachdem Sie die Konfiguration auf dem Server abgeschlossen haben, müssen Sie je nach der von Ihnen

verwendeten Stammzertifizierungsstelle (CA) möglicherweise auch das Grid-CA-Zertifikat im S3-API-Client installieren, den Sie für den Zugriff auf das System verwenden.

> Um sicherzustellen, dass der Betrieb nicht durch ein fehlerhaftes Serverzertifikat unterbrochen wird, wird die Warnung **Ablauf des globalen Serverzertifikats für S3-API** ausgelöst, wenn das Stammserverzertifikat bald abläuft. Bei Bedarf können Sie das Ablaufdatum des aktuellen Zertifikats anzeigen, indem Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate** auswählen und auf der Registerkarte „Global“ das Ablaufdatum für das S3-API-Zertifikat anzeigen.

Sie können ein benutzerdefiniertes S3-API-Zertifikat hochladen oder generieren.

Fügen Sie ein benutzerdefiniertes S3-API-Zertifikat hinzu

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global S3-API-Zertifikat** aus.
3. Wählen Sie **Benutzerdefiniertes Zertifikat verwenden**.
4. Laden Sie das Zertifikat hoch oder generieren Sie es.

Zertifikat hochladen

Laden Sie die erforderlichen Serverzertifikatsdateien hoch.

a. Wählen Sie **Zertifikat hochladen**.

b. Laden Sie die erforderlichen Serverzertifikatsdateien hoch:

- **Serverzertifikat**: Die benutzerdefinierte Serverzertifikatsdatei (PEM-codiert).
- **Privater Zertifikatsschlüssel**: Die benutzerdefinierte private Schlüsseldatei des Serverzertifikats(`.key`).

> Private EC-Schlüssel müssen mindestens 224 Bit lang sein. Private RSA-Schlüssel müssen mindestens 2048 Bit lang sein.

- **CA-Paket**: Eine einzelne optionale Datei, die die Zertifikate aller ausstellenden Zwischenzertifizierungsstellen enthält. Die Datei sollte alle PEM-codierten CA-Zertifikatsdateien enthalten, die in der Reihenfolge der Zertifikatskette aneinandergereiht sind.

c. Wählen Sie die Zertifikatsdetails aus, um die Metadaten und PEM für jedes hochgeladene benutzerdefinierte S3-API-Zertifikat anzuzeigen. Wenn Sie ein optionales CA-Paket hochgeladen haben, wird jedes Zertifikat auf einer eigenen Registerkarte angezeigt.

- Wählen Sie **Zertifikat herunterladen**, um die Zertifikatsdatei zu speichern, oder wählen Sie **CA-Paket herunterladen**, um das Zertifikatspaket zu speichern.

  Geben Sie den Namen der Zertifikatsdatei und den Download-Speicherort an. Speichern Sie die Datei mit der Erweiterung `.pem` .

  Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Zertifikat PEM kopieren** oder **CA-Paket PEM kopieren**, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.

d. Wählen Sie **Speichern**.

  Das benutzerdefinierte Serverzertifikat wird für nachfolgende neue S3-Clientverbindungen verwendet.

Zertifikat generieren

Generieren Sie die Serverzertifikatsdateien.

a. Wählen Sie **Zertifikat generieren**.

b. Geben Sie die Zertifikatsinformationen an:

Feld	Beschreibung
Domänenname	Ein oder mehrere vollqualifizierte Domänennamen, die in das Zertifikat aufgenommen werden sollen. Verwenden Sie ein * als Platzhalter, um mehrere Domänennamen darzustellen.
IP	Eine oder mehrere IP-Adressen, die in das Zertifikat aufgenommen werden sollen.

Feld	Beschreibung
Betreff (optional)	X.509-Betreff oder Distinguished Name (DN) des Zertifikatsinhabers. Wenn in dieses Feld kein Wert eingegeben wird, verwendet das generierte Zertifikat den ersten Domänennamen oder die erste IP-Adresse als allgemeinen Namen (CN) des Betreffs.
Gültigkeitstage	Anzahl der Tage nach der Erstellung, bis zu der das Zertifikat abläuft.
Hinzufügen von Schlüsselverwendungserweiterungen	Wenn ausgewählt (Standard und empfohlen), werden dem generierten Zertifikat Schlüsselverwendung und erweiterte Schlüsselverwendungserweiterungen hinzugefügt. Diese Erweiterungen definieren den Zweck des im Zertifikat enthaltenen Schlüssels. **Hinweis**: Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, Sie haben Verbindungsprobleme mit älteren Clients, wenn die Zertifikate diese Erweiterungen enthalten.

c. Wählen Sie **Generieren**.

d. Wählen Sie **Zertifikatdetails** aus, um die Metadaten und PEM für das generierte benutzerdefinierte S3-API-Zertifikat anzuzeigen.

   - Wählen Sie **Zertifikat herunterladen**, um die Zertifikatsdatei zu speichern.

     Geben Sie den Namen der Zertifikatsdatei und den Download-Speicherort an. Speichern Sie die Datei mit der Erweiterung `.pem` .

     Beispiel: `storagegrid_certificate.pem`

   - Wählen Sie **Zertifikat PEM kopieren**, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.

e. Wählen Sie **Speichern**.

   Das benutzerdefinierte Serverzertifikat wird für nachfolgende neue S3-Clientverbindungen verwendet.

5. Wählen Sie eine Registerkarte aus, um Metadaten für das Standard StorageGRID Serverzertifikat, ein hochgeladenes, von einer Zertifizierungsstelle signiertes Zertifikat oder ein generiertes benutzerdefiniertes Zertifikat anzuzeigen.

   Warten Sie nach dem Hochladen oder Generieren eines neuen Zertifikats bis zu einem Tag, bis alle zugehörigen Warnungen zum Ablauf des Zertifikats gelöscht werden.

6. Aktualisieren Sie die Seite, um sicherzustellen, dass der Webbrowser aktualisiert ist.

7. Nachdem Sie ein benutzerdefiniertes S3-API-Zertifikat hinzugefügt haben, werden auf der S3-API-Zertifikatseite detaillierte Zertifikatsinformationen für das verwendete benutzerdefinierte S3-API-Zertifikat angezeigt. + Sie können das Zertifikat PEM nach Bedarf herunterladen oder kopieren.

Wiederherstellen des Standard-S3-API-Zertifikats

Sie können für S3-Clientverbindungen zu Speicherknoten wieder das standardmäßige S3-API-Zertifikat verwenden. Sie können das Standard-S3-API-Zertifikat jedoch nicht für einen Load Balancer-Endpunkt verwenden.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global S3-API-Zertifikat** aus.
3. Wählen Sie **Standardzertifikat verwenden**.

   Wenn Sie die Standardversion des globalen S3-API-Zertifikats wiederherstellen, werden die von Ihnen konfigurierten benutzerdefinierten Serverzertifikatsdateien gelöscht und können nicht vom System wiederhergestellt werden. Das standardmäßige S3-API-Zertifikat wird für nachfolgende neue S3-Clientverbindungen zu Speicherknoten verwendet.

4. Wählen Sie **OK**, um die Warnung zu bestätigen und das Standard-S3-API-Zertifikat wiederherzustellen.

   Wenn Sie über Root-Zugriffsberechtigung verfügen und das benutzerdefinierte S3-API-Zertifikat für Verbindungen mit Load Balancer-Endpunkten verwendet wurde, wird eine Liste der Load Balancer-Endpunkte angezeigt, auf die mit dem standardmäßigen S3-API-Zertifikat nicht mehr zugegriffen werden kann. Gehe zu"Konfigurieren von Load Balancer-Endpunkten" um die betroffenen Endpunkte zu bearbeiten oder zu entfernen.

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

Laden Sie das S3-API-Zertifikat herunter oder kopieren Sie es

Sie können den Inhalt des S3-API-Zertifikats zur Verwendung an anderer Stelle speichern oder kopieren.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global S3-API-Zertifikat** aus.
3. Wählen Sie die Registerkarte **Server** oder **CA-Paket** und laden Sie anschließend das Zertifikat herunter oder kopieren Sie es.

Zertifikatsdatei oder CA-Paket herunterladen

Laden Sie das Zertifikat oder CA-Paket herunter `.pem` Datei. Wenn Sie ein optionales CA-Paket verwenden, wird jedes Zertifikat im Paket auf einer eigenen Unterregisterkarte angezeigt.

a. Wählen Sie **Zertifikat herunterladen** oder **CA-Paket herunterladen**.

   Wenn Sie ein CA-Paket herunterladen, werden alle Zertifikate in den sekundären Registerkarten des CA-Pakets als einzelne Datei heruntergeladen.

b. Geben Sie den Namen der Zertifikatsdatei und den Download-Speicherort an. Speichern Sie die Datei mit der Erweiterung `.pem` .

   Beispiel: `storagegrid_certificate.pem`

Zertifikat oder CA-Bundle PEM kopieren

Kopieren Sie den Zertifikatstext, um ihn an anderer Stelle einzufügen. Wenn Sie ein optionales CA-Paket verwenden, wird jedes Zertifikat im Paket auf einer eigenen Unterregisterkarte angezeigt.

a. Wählen Sie **Zertifikat PEM kopieren** oder **CA-Paket PEM kopieren**.

   Wenn Sie ein CA-Paket kopieren, werden alle Zertifikate in den sekundären Registerkarten des CA-Pakets zusammen kopiert.

b. Fügen Sie das kopierte Zertifikat in einen Texteditor ein.

c. Speichern Sie die Textdatei mit der Erweiterung `.pem` .

   Beispiel: `storagegrid_certificate.pem`

Ähnliche Informationen

- "Verwenden Sie die S3 REST-API"
- "Konfigurieren von S3-Endpunktdomänennamen"

Kopieren Sie das Grid CA-Zertifikat

StorageGRID verwendet eine interne Zertifizierungsstelle (CA), um den internen Datenverkehr zu sichern. Dieses Zertifikat ändert sich nicht, wenn Sie eigene Zertifikate hochladen.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .

Informationen zu diesem Vorgang

Wenn ein benutzerdefiniertes Serverzertifikat konfiguriert wurde, sollten Clientanwendungen den Server mithilfe des benutzerdefinierten Serverzertifikats überprüfen. Sie sollten das CA-Zertifikat nicht vom StorageGRID -System kopieren.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Grid CA**.
2. Laden Sie im Abschnitt **Zertifikat PEM** das Zertifikat herunter oder kopieren Sie es.

Zertifikatsdatei herunterladen

Laden Sie das Zertifikat herunter `.pem` Datei.

a. Wählen Sie **Zertifikat herunterladen**.
b. Geben Sie den Namen der Zertifikatsdatei und den Download-Speicherort an. Speichern Sie die Datei mit der Erweiterung `.pem` .

   Beispiel: `storagegrid_certificate.pem`

Kopie des Zertifikats PEM

Kopieren Sie den Zertifikatstext, um ihn an anderer Stelle einzufügen.

a. Wählen Sie **Zertifikat PEM kopieren**.
b. Fügen Sie das kopierte Zertifikat in einen Texteditor ein.
c. Speichern Sie die Textdatei mit der Erweiterung `.pem` .

   Beispiel: `storagegrid_certificate.pem`

Konfigurieren Sie StorageGRID -Zertifikate für FabricPool

Für S3-Clients, die eine strenge Hostnamenvalidierung durchführen und die Deaktivierung der strengen Hostnamenvalidierung nicht unterstützen, wie z. B. ONTAP Clients, die FabricPool verwenden, können Sie beim Konfigurieren des Load Balancer-Endpunkts ein Serverzertifikat generieren oder hochladen.

Bevor Sie beginnen

- Du hast"spezifische Zugriffsberechtigungen" .
- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .

Informationen zu diesem Vorgang

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 rotiert werden. Sie sind außerdem sicherer, da sie einen besseren Schutz vor Man-in-the-Middle-Angriffen bieten.

Die folgenden Schritte bieten allgemeine Richtlinien für S3-Clients, die FabricPool verwenden. Ausführlichere Informationen und Vorgehensweisen finden Sie unter"Konfigurieren von StorageGRID für FabricPool" .

Schritte

1. Konfigurieren Sie optional eine Hochverfügbarkeitsgruppe (HA) für die Verwendung durch FabricPool .

2. Erstellen Sie einen S3-Load Balancer-Endpunkt für die Verwendung durch FabricPool .

   Wenn Sie einen HTTPS-Load Balancer-Endpunkt erstellen, werden Sie aufgefordert, Ihr Serverzertifikat, Ihren privaten Zertifikatsschlüssel und das optionale CA-Paket hochzuladen.

3. Hängen Sie StorageGRID als Cloud-Ebene in ONTAP an.

   Geben Sie den Endpunktport des Lastenausgleichs und den vollqualifizierten Domänennamen an, der im von Ihnen hochgeladenen CA-Zertifikat verwendet wird. Geben Sie dann das CA-Zertifikat an.

> Wenn das StorageGRID -Zertifikat von einer Zwischenzertifizierungsstelle ausgestellt wurde, müssen Sie das Zwischenzertifizierungsstellenzertifikat angeben. Wenn das StorageGRID -Zertifikat direkt von der Root-CA ausgestellt wurde, müssen Sie das Root-CA-Zertifikat angeben.

Konfigurieren von Clientzertifikaten

Client-Zertifikate ermöglichen autorisierten externen Clients den Zugriff auf die StorageGRID Prometheus-Datenbank und bieten externen Tools eine sichere Möglichkeit, StorageGRID zu überwachen.

Wenn Sie über ein externes Überwachungstool auf StorageGRID zugreifen müssen, müssen Sie mithilfe des Grid Managers ein Client-Zertifikat hochladen oder generieren und die Zertifikatsinformationen in das externe Tool kopieren.

Sehen"Sicherheitszertifikate verwalten" Und"Konfigurieren benutzerdefinierter Serverzertifikate" .

> Um sicherzustellen, dass der Betrieb nicht durch ein fehlerhaftes Serverzertifikat unterbrochen wird, wird die Warnung **Ablauf der auf der Seite „Zertifikate“ konfigurierten Clientzertifikate** ausgelöst, wenn dieses Serverzertifikat bald abläuft. Bei Bedarf können Sie das Ablaufdatum des aktuellen Zertifikats anzeigen, indem Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate** auswählen und auf der Registerkarte „Client“ das Ablaufdatum für das Client-Zertifikat anzeigen.

> Wenn Sie einen Schlüsselverwaltungsserver (KMS) zum Schutz der Daten auf speziell konfigurierten Appliance-Knoten verwenden, lesen Sie die spezifischen Informationen zu"Hochladen eines KMS-Client-Zertifikats" .

Bevor Sie beginnen

- Sie verfügen über Root-Zugriffsberechtigung.
- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- So konfigurieren Sie ein Client-Zertifikat:
  - Sie haben die IP-Adresse oder den Domänennamen des Admin-Knotens.
  - Wenn Sie das Zertifikat der StorageGRID -Verwaltungsschnittstelle konfiguriert haben, verfügen Sie über die Zertifizierungsstelle, das Client-Zertifikat und den privaten Schlüssel, die zum Konfigurieren des Zertifikats der Verwaltungsschnittstelle verwendet werden.
  - Um Ihr eigenes Zertifikat hochzuladen, steht Ihnen der private Schlüssel für das Zertifikat auf Ihrem lokalen Computer zur Verfügung.
  - Der private Schlüssel muss zum Zeitpunkt seiner Erstellung gespeichert oder aufgezeichnet worden

sein. Wenn Sie nicht über den ursprünglichen privaten Schlüssel verfügen, müssen Sie einen neuen erstellen.

- So bearbeiten Sie ein Client-Zertifikat:
  - Sie haben die IP-Adresse oder den Domänennamen des Admin-Knotens.
  - Um Ihr eigenes Zertifikat oder ein neues Zertifikat hochzuladen, stehen Ihnen der private Schlüssel, das Client-Zertifikat und die CA (sofern verwendet) auf Ihrem lokalen Computer zur Verfügung.

Client-Zertifikate hinzufügen

Um das Client-Zertifikat hinzuzufügen, verwenden Sie eines der folgenden Verfahren:

- Management-Schnittstellenzertifikat bereits konfiguriert
- Von der Zertifizierungsstelle ausgestelltes Client-Zertifikat
- Generiertes Zertifikat vom Grid Manager

Management-Schnittstellenzertifikat bereits konfiguriert

Verwenden Sie dieses Verfahren, um ein Client-Zertifikat hinzuzufügen, wenn bereits ein Management-Schnittstellenzertifikat mit einer vom Kunden bereitgestellten Zertifizierungsstelle, einem Client-Zertifikat und einem privaten Schlüssel konfiguriert ist.

Schritte

1. Wählen Sie im Grid Manager **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Client**.
2. Wählen Sie **Hinzufügen**.
3. Geben Sie einen Zertifikatsnamen ein.
4. Um mit Ihrem externen Überwachungstool auf Prometheus-Metriken zuzugreifen, wählen Sie **Prometheus zulassen**.
5. Wählen Sie **Weiter**.
6. Laden Sie für den Schritt **Zertifikate anhängen** das Verwaltungsschnittstellenzertifikat hoch.
   a. Wählen Sie **Zertifikat hochladen**.
   b. Wählen Sie **Durchsuchen** und wählen Sie die Zertifikatsdatei der Verwaltungsschnittstelle aus(`.pem`).
      - Wählen Sie **Client-Zertifikatdetails** aus, um die Zertifikatmetadaten und das Zertifikat-PEM anzuzeigen.
      - Wählen Sie **Zertifikat PEM kopieren**, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.
   c. Wählen Sie **Erstellen**, um das Zertifikat im Grid Manager zu speichern.

      Das neue Zertifikat wird auf der Registerkarte „Client“ angezeigt.
7. Konfigurieren eines externen Überwachungstools, wie Grafana.

Von der Zertifizierungsstelle ausgestelltes Client-Zertifikat

Verwenden Sie dieses Verfahren, um ein Administrator-Client-Zertifikat hinzuzufügen, wenn kein Management-Schnittstellenzertifikat konfiguriert wurde und Sie ein Client-Zertifikat für Prometheus hinzufügen möchten, das ein von einer Zertifizierungsstelle ausgestelltes Client-Zertifikat und einen privaten Schlüssel verwendet.

Schritte

1. Führen Sie die Schritte aus, um"Konfigurieren eines Management-Schnittstellenzertifikats" .
2. Wählen Sie im Grid Manager **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Client**.
3. Wählen Sie **Hinzufügen**.
4. Geben Sie einen Zertifikatsnamen ein.
5. Um mit Ihrem externen Überwachungstool auf Prometheus-Metriken zuzugreifen, wählen Sie **Prometheus zulassen**.
6. Wählen Sie **Weiter**.
7. Laden Sie für den Schritt **Zertifikate anhängen** das Client-Zertifikat, den privaten Schlüssel und die CA-Bundle-Dateien hoch:
   a. Wählen Sie **Zertifikat hochladen**.
   b. Wählen Sie **Durchsuchen** und wählen Sie das Client-Zertifikat, den privaten Schlüssel und die CA-Bundle-Dateien aus(`.pem`).
      - Wählen Sie **Client-Zertifikatdetails** aus, um die Zertifikatmetadaten und das Zertifikat-PEM anzuzeigen.
      - Wählen Sie **Zertifikat PEM kopieren**, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.
   c. Wählen Sie **Erstellen**, um das Zertifikat im Grid Manager zu speichern.

      Die neuen Zertifikate werden auf der Registerkarte „Client“ angezeigt.
8. Konfigurieren eines externen Überwachungstools, wie Grafana.

Generiertes Zertifikat vom Grid Manager

Verwenden Sie dieses Verfahren, um ein Administrator-Client-Zertifikat hinzuzufügen, wenn kein Management-Schnittstellenzertifikat konfiguriert wurde und Sie ein Client-Zertifikat für Prometheus hinzufügen möchten, das die Funktion zum Generieren von Zertifikaten in Grid Manager verwendet.

Schritte

1. Wählen Sie im Grid Manager **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Client**.
2. Wählen Sie **Hinzufügen**.
3. Geben Sie einen Zertifikatsnamen ein.
4. Um mit Ihrem externen Überwachungstool auf Prometheus-Metriken zuzugreifen, wählen Sie **Prometheus zulassen**.
5. Wählen Sie **Weiter**.
6. Wählen Sie für den Schritt **Zertifikate anhängen** die Option **Zertifikat generieren** aus.
7. Geben Sie die Zertifikatsinformationen an:
   - **Betreff** (optional): X.509-Betreff oder Distinguished Name (DN) des Zertifikatsinhabers.
   - **Gültigkeitstage**: Die Anzahl der Tage, die das generierte Zertifikat gültig ist, beginnend mit dem Zeitpunkt der Generierung.
   - **Schlüsselverwendungserweiterungen hinzufügen**: Wenn ausgewählt (Standard und empfohlen),

werden dem generierten Zertifikat Schlüsselverwendungs- und erweiterte Schlüsselverwendungserweiterungen hinzugefügt.

Diese Erweiterungen definieren den Zweck des im Zertifikat enthaltenen Schlüssels.

> Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, Sie haben Verbindungsprobleme mit älteren Clients, wenn die Zertifikate diese Erweiterungen enthalten.

8. Wählen Sie **Generieren**.
9. Wählen Sie **Client-Zertifikatdetails**, um die Zertifikatmetadaten und das Zertifikat-PEM anzuzeigen.

> Nachdem Sie das Dialogfeld geschlossen haben, können Sie den privaten Schlüssel des Zertifikats nicht mehr anzeigen. Kopieren oder laden Sie den Schlüssel an einen sicheren Ort herunter.

   - Wählen Sie **Zertifikat PEM kopieren**, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.
   - Wählen Sie **Zertifikat herunterladen**, um die Zertifikatsdatei zu speichern.

     Geben Sie den Namen der Zertifikatsdatei und den Download-Speicherort an. Speichern Sie die Datei mit der Erweiterung `.pem`.

     Beispiel: `storagegrid_certificate.pem`

   - Wählen Sie **Privaten Schlüssel kopieren**, um den privaten Schlüssel des Zertifikats zum Einfügen an anderer Stelle zu kopieren.
   - Wählen Sie **Privaten Schlüssel herunterladen**, um den privaten Schlüssel als Datei zu speichern.

     Geben Sie den Dateinamen des privaten Schlüssels und den Download-Speicherort an.

10. Wählen Sie **Erstellen**, um das Zertifikat im Grid Manager zu speichern.

    Das neue Zertifikat wird auf der Registerkarte „Client“ angezeigt.

11. Wählen Sie im Grid Manager **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Global**.
12. Wählen Sie **Management Interface-Zertifikat**.
13. Wählen Sie **Benutzerdefiniertes Zertifikat verwenden**.
14. Laden Sie die Dateien certificate.pem und private_key.pem von derClient-Zertifikatdetails Schritt. Es ist nicht erforderlich, ein CA-Paket hochzuladen.
    a. Wählen Sie **Zertifikat hochladen** und dann **Weiter**.
    b. Laden Sie jede Zertifikatsdatei hoch(`.pem`).
    c. Wählen Sie **Speichern**, um das Zertifikat im Grid Manager zu speichern.

       Das neue Zertifikat wird auf der Zertifikatsseite der Verwaltungsschnittstelle angezeigt.

15. Konfigurieren eines externen Überwachungstools, wie Grafana.

Konfigurieren Sie ein externes Überwachungstool

Schritte

1. Konfigurieren Sie die folgenden Einstellungen in Ihrem externen Überwachungstool, z. B. Grafana.
   a. **Name**: Geben Sie einen Namen für die Verbindung ein.

      StorageGRID benötigt diese Informationen nicht, Sie müssen jedoch einen Namen angeben, um die Verbindung zu testen.

   b. **URL**: Geben Sie den Domänennamen oder die IP-Adresse für den Admin-Knoten ein. Geben Sie HTTPS und Port 9091 an.

      Beispiel: `https://admin-node.example.com:9091`

   c. Aktivieren Sie **TLS-Client-Authentifizierung** und **Mit CA-Zertifikat**.
   d. Kopieren und fügen Sie unter TLS/SSL-Authentifizierungsdetails Folgendes ein:
      - Das CA-Zertifikat der Verwaltungsschnittstelle an **CA Cert**
      - Das Client-Zertifikat an **Client Cert**
      - Der private Schlüssel zum **Client-Schlüssel**
   e. **Servername**: Geben Sie den Domänennamen des Admin-Knotens ein.

      Der Servername muss mit dem Domänennamen übereinstimmen, der im Zertifikat der Verwaltungsschnittstelle angezeigt wird.

2. Speichern und testen Sie das Zertifikat und den privaten Schlüssel, die Sie aus StorageGRID oder einer lokalen Datei kopiert haben.

   Sie können jetzt mit Ihrem externen Überwachungstool auf die Prometheus-Metriken von StorageGRID zugreifen.

   Informationen zu den Metriken finden Sie im"Anleitung zur Überwachung von StorageGRID" .

Client-Zertifikate bearbeiten

Sie können ein Administrator-Client-Zertifikat bearbeiten, um seinen Namen zu ändern, den Prometheus-Zugriff zu aktivieren oder zu deaktivieren oder ein neues Zertifikat hochzuladen, wenn das aktuelle abgelaufen ist.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Client**.

   Ablaufdaten der Zertifikate und Zugriffsberechtigungen für Prometheus sind in der Tabelle aufgeführt. Läuft ein Zertifikat bald ab oder ist es bereits abgelaufen, erscheint in der Tabelle eine Meldung und es wird ein Alarm ausgelöst.

2. Wählen Sie das Zertifikat aus, das Sie bearbeiten möchten.
3. Wählen Sie **Bearbeiten** und dann **Name und Berechtigung bearbeiten**
4. Geben Sie einen Zertifikatsnamen ein.
5. Um mit Ihrem externen Überwachungstool auf Prometheus-Metriken zuzugreifen, wählen Sie **Prometheus zulassen**.

6. Wählen Sie **Weiter**, um das Zertifikat im Grid Manager zu speichern.

   Das aktualisierte Zertifikat wird auf der Registerkarte „Client“ angezeigt.

Neues Client-Zertifikat anhängen

Sie können ein neues Zertifikat hochladen, wenn das aktuelle abgelaufen ist.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Client**.

   Ablaufdaten der Zertifikate und Zugriffsberechtigungen für Prometheus sind in der Tabelle aufgeführt. Läuft ein Zertifikat bald ab oder ist es bereits abgelaufen, erscheint in der Tabelle eine Meldung und es wird ein Alarm ausgelöst.

2. Wählen Sie das Zertifikat aus, das Sie bearbeiten möchten.
3. Wählen Sie **Bearbeiten** und dann eine Bearbeitungsoption.

Zertifikat hochladen

Kopieren Sie den Zertifikatstext, um ihn an anderer Stelle einzufügen.

a. Wählen Sie **Zertifikat hochladen** und dann **Weiter**.

b. Laden Sie den Namen des Client-Zertifikats hoch(`.pem`).

   Wählen Sie **Client-Zertifikatdetails** aus, um die Zertifikatmetadaten und das Zertifikat-PEM anzuzeigen.

   - Wählen Sie **Zertifikat herunterladen**, um die Zertifikatsdatei zu speichern.

     Geben Sie den Namen der Zertifikatsdatei und den Download-Speicherort an. Speichern Sie die Datei mit der Erweiterung `.pem` .

   Beispiel: `storagegrid_certificate.pem`

   - Wählen Sie **Zertifikat PEM kopieren**, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.

c. Wählen Sie **Erstellen**, um das Zertifikat im Grid Manager zu speichern.

   Das aktualisierte Zertifikat wird auf der Registerkarte „Client“ angezeigt.

Zertifikat generieren

Generieren Sie den Zertifikatstext, um ihn an anderer Stelle einzufügen.

a. Wählen Sie **Zertifikat generieren**.

b. Geben Sie die Zertifikatsinformationen an:

   - **Betreff** (optional): X.509-Betreff oder Distinguished Name (DN) des Zertifikatsinhabers.
   - **Gültigkeitstage**: Die Anzahl der Tage, die das generierte Zertifikat gültig ist, beginnend mit dem Zeitpunkt der Generierung.
   - **Schlüsselverwendungserweiterungen hinzufügen**: Wenn ausgewählt (Standard und empfohlen), werden dem generierten Zertifikat Schlüsselverwendungs- und erweiterte Schlüsselverwendungserweiterungen hinzugefügt.

     Diese Erweiterungen definieren den Zweck des im Zertifikat enthaltenen Schlüssels.

     Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, Sie haben Verbindungsprobleme mit älteren Clients, wenn die Zertifikate diese Erweiterungen enthalten.

c. Wählen Sie **Generieren**.

d. Wählen Sie **Client-Zertifikatdetails** aus, um die Zertifikatmetadaten und das Zertifikat-PEM anzuzeigen.

   Nachdem Sie das Dialogfeld geschlossen haben, können Sie den privaten Schlüssel des Zertifikats nicht mehr anzeigen. Kopieren oder laden Sie den Schlüssel an einen sicheren Ort herunter.

- Wählen Sie **Zertifikat PEM kopieren**, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.
- Wählen Sie **Zertifikat herunterladen**, um die Zertifikatsdatei zu speichern.

  Geben Sie den Namen der Zertifikatsdatei und den Download-Speicherort an. Speichern Sie die Datei mit der Erweiterung `.pem` .

  Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Privaten Schlüssel kopieren**, um den privaten Schlüssel des Zertifikats zum Einfügen an anderer Stelle zu kopieren.
- Wählen Sie **Privaten Schlüssel herunterladen**, um den privaten Schlüssel als Datei zu speichern.

  Geben Sie den Dateinamen des privaten Schlüssels und den Download-Speicherort an.

e. Wählen Sie **Erstellen**, um das Zertifikat im Grid Manager zu speichern.

   Das neue Zertifikat wird auf der Registerkarte „Client“ angezeigt.

Herunterladen oder Kopieren von Client-Zertifikaten

Sie können ein Client-Zertifikat zur Verwendung an anderer Stelle herunterladen oder kopieren.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Client**.
2. Wählen Sie das Zertifikat aus, das Sie kopieren oder herunterladen möchten.
3. Laden Sie das Zertifikat herunter oder kopieren Sie es.

Zertifikatsdatei herunterladen

Laden Sie das Zertifikat herunter `.pem` Datei.

a. Wählen Sie **Zertifikat herunterladen**.
b. Geben Sie den Namen der Zertifikatsdatei und den Download-Speicherort an. Speichern Sie die Datei mit der Erweiterung `.pem` .

   Beispiel: `storagegrid_certificate.pem`

Zertifikat kopieren

Kopieren Sie den Zertifikatstext, um ihn an anderer Stelle einzufügen.

a. Wählen Sie **Zertifikat PEM kopieren**.
b. Fügen Sie das kopierte Zertifikat in einen Texteditor ein.
c. Speichern Sie die Textdatei mit der Erweiterung `.pem` .

   Beispiel: `storagegrid_certificate.pem`

Client-Zertifikate entfernen

Wenn Sie ein Administrator-Client-Zertifikat nicht mehr benötigen, können Sie es entfernen.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Client**.
2. Wählen Sie das Zertifikat aus, das Sie entfernen möchten.
3. Wählen Sie **Löschen** und bestätigen Sie anschließend.

> Um bis zu 10 Zertifikate zu entfernen, wählen Sie jedes zu entfernende Zertifikat auf der Registerkarte „Client“ aus und wählen Sie dann **Aktionen** > **Löschen**.

Nachdem ein Zertifikat entfernt wurde, müssen Clients, die das Zertifikat verwendet haben, ein neues Client-Zertifikat angeben, um auf die StorageGRID Prometheus-Datenbank zugreifen zu können.

Copyright-Informationen

Markeninformationen