



Verwalten von Zertifikaten

StorageGRID software

NetApp
February 12, 2026

Inhalt

Verwalten von Zertifikaten	1
Verwalten von Sicherheitszertifikaten	1
Greifen Sie auf Sicherheitszertifikate zu	2
Details zum Sicherheitszertifikat	5
Beispiele für Zertifikate	12
Unterstützte Serverzertifikatstypen	13
Konfigurieren Sie Zertifikate für die Managementoberfläche	13
Fügen Sie ein Zertifikat für eine benutzerdefinierte Managementoberfläche hinzu	14
Stellen Sie das Standardzertifikat für die Managementoberfläche wieder her	17
Erstellen Sie mit einem Skript ein neues Zertifikat für die selbstsignierte Managementoberfläche	17
Laden Sie das Zertifikat für die Managementoberfläche herunter oder kopieren Sie es	18
Konfigurieren Sie S3-API-Zertifikate	19
Fügen Sie ein benutzerdefiniertes S3-API-Zertifikat hinzu	20
Stellen Sie das standardmäßige S3-API-Zertifikat wieder her	23
Laden Sie das S3-API-Zertifikat herunter oder kopieren Sie es	23
Kopieren Sie das Grid-CA-Zertifikat	24
Konfigurieren Sie StorageGRID-Zertifikate für FabricPool	25
Konfigurieren Sie Client-Zertifikate	26
Fügen Sie Client-Zertifikate hinzu	27
Client-Zertifikate bearbeiten	30
Verbinden Sie das neue Clientzertifikat	31
Herunterladen oder Kopieren von Clientzertifikaten	33
Entfernen Sie Client-Zertifikate	34

Verwalten von Zertifikaten

Verwalten von Sicherheitszertifikaten

Sicherheitszertifikate sind kleine Datendateien, die zur Erstellung sicherer, vertrauenswürdiger Verbindungen zwischen StorageGRID-Komponenten und 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 bei seinen Clients zu authentifizieren und einen sicheren Kommunikationspfad für Daten bereitzustellen. Der Server und der Client verfügen jeweils über eine Kopie des Zertifikats.
- **Clientzertifikate** authentifizieren eine Client- oder Benutzeridentität auf dem Server und bieten eine sicherere Authentifizierung als Passwörter allein. Clientzertifikate 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 vergleicht die Serversignatur mit der Signatur auf seiner Kopie des Zertifikats. Wenn die Signaturen übereinstimmen, startet der Client eine Sitzung mit dem Server unter Verwendung desselben öffentlichen Schlüssels.

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

Standard Grid CA-Zertifikat

StorageGRID verfügt über 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.

Verwenden Sie das Grid CA-Zertifikat für Nicht-Produktionsumgebungen. Verwenden Sie für die Produktion benutzerdefinierte Zertifikate, die von einer externen Zertifizierungsstelle signiert wurden. Ungesicherte Verbindungen ohne Zertifikat werden unterstützt, aber nicht empfohlen.

- Benutzerdefinierte CA-Zertifikate entfernen die internen Zertifikate nicht, jedoch sollten die benutzerdefinierten Zertifikate für die Überprüfung der Serververbindungen angegeben sein.
- Alle benutzerdefinierten Zertifikate müssen den erfüllen "[Richtlinien für die Systemhärtung von Serverzertifikaten](#)".
- StorageGRID unterstützt das Bündeln von Zertifikaten aus einer Zertifizierungsstelle in einer einzelnen Datei (Bundle als CA-Zertifikat).



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

Varianten der Server- und Client-Zertifikatstypen werden auf verschiedene Weise implementiert. Vor der Konfiguration des Systems sollten Sie alle erforderlichen Zertifikate für Ihre spezifische StorageGRID-Konfiguration bereithaben.

Greifen Sie auf Sicherheitszertifikate zu

Sie haben Zugriff auf Informationen zu allen StorageGRID-Zertifikaten an einer zentralen Stelle, zusammen mit Links zum Konfigurations-Workflow für jedes Zertifikat.

Schritte

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

Certificates

View and manage the certificates that secure HTTPS connections between StorageGRID and external clients, such as S3 or Swift, and external servers, such as a key management server (KMS).

GlobalGrid CAClientLoad balancer endpointsTenantsOther

The StorageGRID certificate authority ("grid CA") generates and signs two global certificates during installation. The management interface certificate on Admin Nodes secures the management interface. The S3 and Swift API certificate on Storage and Gateway Nodes secures client access. You should replace each default certificate with your own custom certificate signed by an external certificate authority.

Name	Description	Type ?	Expiration date ? ↕
Management interface certificate	Secures the connection between client web browsers and the Grid Manager, Tenant Manager, Grid Management API, and Tenant Management API.	Custom	Jun 4th, 2022
S3 and Swift API certificate	Secures the connections between S3 and Swift clients and Storage Nodes or between clients and the deprecated CLB service on Gateway Nodes. You can optionally use this certificate for a load balancer endpoint as well.	Custom	Jun 4th, 2022

2. Wählen Sie auf der Seite Zertifikate eine Registerkarte aus, um Informationen zu den einzelnen Zertifikatkategorien zu erhalten und auf die Zertifikateinstellungen zuzugreifen. Sie können auf eine Registerkarte zugreifen, wenn Sie über die verfügbare ["Entsprechende Berechtigung"](#).

- **Global:** Sichert den StorageGRID-Zugriff von Webbrowsern und externen API-Clients.
- **Raster CA:** Sichert internen StorageGRID-Datenverkehr.
- **Kunde:** 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 Identitäts-Federation-Servern oder von Plattform-Service-Endpunkten zu S3-Storage-Ressourcen.
- **Sonstiges:** Sichert StorageGRID-Verbindungen, die bestimmte Zertifikate erfordern.

Jede Registerkarte wird unten mit Links zu weiteren Zertifikatdetails beschrieben.

Weltweit

Die globalen Zertifikate sichern den StorageGRID-Zugriff über Webbrowser und externe S3-API-Clients. Zwei globale Zertifikate werden zunächst von der StorageGRID-Zertifizierungsstelle während der Installation generiert. Die beste Vorgehensweise für eine Produktionsumgebung besteht darin, benutzerdefinierte Zertifikate zu verwenden, die von einer externen Zertifizierungsstelle signiert wurden.

- [Zertifikat für die Managementoberfläche](#): Sichert Client-Web-Browser-Verbindungen zu StorageGRID-Verwaltungsschnittstellen.
- [S3-API-Zertifikat](#): Sichert Client-API-Verbindungen zu Storage Nodes, Admin-Nodes und Gateway-Nodes, die S3-Client-Anwendungen zum Hochladen und Herunterladen von Objektdaten verwenden.

Informationen zu den installierten globalen Zertifikaten umfassen:

- **Name**: Zertifikatsname mit Link zur Verwaltung des Zertifikats.
- **Beschreibung**
- **Typ**: Benutzerdefiniert oder Standard. + Sie sollten immer ein benutzerdefiniertes Zertifikat verwenden, um die Netzsicherheit zu verbessern.
- **Ablaufdatum**: Bei Verwendung des Standardzertifikats wird kein Ablaufdatum angezeigt.

Ihre Vorteile:

- Ersetzen Sie die Standardzertifikate durch benutzerdefinierte Zertifikate, die von einer externen Zertifizierungsstelle signiert wurden, um eine verbesserte Grid-Sicherheit zu gewährleisten:
 - ["Ersetzen Sie das von StorageGRID generierte Standardzertifikat für die Managementoberfläche"](#) Wird für Verbindungen zwischen Grid Manager und Tenant Manager verwendet.
 - ["Ersetzen Sie das S3-API-Zertifikat"](#) Wird für Storage-Node- und Load Balancer-Endpunktverbindungen (optional) verwendet.
- ["Stellen Sie das Standardzertifikat für die Managementoberfläche wieder her"](#).
- ["Stellen Sie das standardmäßige S3-API-Zertifikat wieder her"](#).
- ["Erstellen Sie mit einem Skript ein neues Zertifikat für die selbstsignierte Managementoberfläche"](#).
- Kopieren oder laden Sie die oder herunter["Zertifikat für die Managementoberfläche"](#)["S3-API-Zertifikat"](#).

Grid CA

Der [Grid-CA-Zertifikat](#), der während der StorageGRID-Installation von der StorageGRID-Zertifizierungsstelle generiert wird, sichert den gesamten internen StorageGRID-Datenverkehr.

Zertifikatsinformationen umfassen das Ablaufdatum des Zertifikats und den Zertifikatsinhalt.

Sie können ["Kopieren oder laden Sie das Zertifikat der Grid-Zertifizierungsstelle herunter"](#), aber Sie können es nicht ändern.

Client

[Client-Zertifikate](#), Von einer externen Zertifizierungsstelle generiert, sichern Sie die Verbindungen zwischen externen Überwachungstools und der StorageGRID Prometheus Datenbank.

Die Zertifikatstabelle verfügt über eine Zeile für jedes konfigurierte Clientzertifikat und gibt an, ob das Zertifikat zusammen mit dem Ablaufdatum des Zertifikats für den Zugriff auf die Prometheus-Datenbank verwendet werden kann.

Ihre Vorteile:

- ["Hochladen oder Generieren eines neuen Clientzertifikats"](#)
- Wählen Sie einen Zertifikatnamen aus, um die Zertifikatdetails anzuzeigen, in denen Sie:
 - ["Ändern Sie den Namen des Client-Zertifikats."](#)
 - ["Legen Sie die Zugriffsberechtigung für Prometheus fest."](#)
 - ["Laden Sie das Clientzertifikat hoch, und ersetzen Sie es."](#)
 - ["Kopieren Sie das Client-Zertifikat, oder laden Sie es herunter."](#)
 - ["Entfernen Sie das Clientzertifikat."](#)
- Wählen Sie **actions**, um schnell ["Bearbeiten"](#), ["Anhängen"](#) oder ["Entfernen"](#) ein Client-Zertifikat auszuwählen. Sie können bis zu 10 Clientzertifikate auswählen und gleichzeitig mit **Actions > Remove** entfernen.

Load Balancer-Endpunkte

[Load Balancer-Endpunktzertifikate](#) Sichern der Verbindungen zwischen S3-Clients und dem StorageGRID Load Balancer-Service auf Gateway-Nodes und Admin-Nodes

Die Endpunktstabelle des Load Balancers verfügt über eine Zeile für jeden konfigurierten Load Balancer-Endpunkt und gibt an, ob das globale S3-API-Zertifikat oder ein benutzerdefiniertes Endpunktzertifikat des Load Balancer für den Endpunkt verwendet wird. Es wird auch das Ablaufdatum für jedes Zertifikat angezeigt.



Änderungen an einem Endpunktzertifikat können bis zu 15 Minuten dauern, bis sie auf alle Knoten angewendet werden können.

Ihre Vorteile:

- ["Anzeigen eines Endpunkts für die Lastverteilung"](#), Einschließlich der Zertifikatdetails.
- ["Geben Sie ein Endpoint-Zertifikat für den Load Balancer für FabricPool an."](#)
- ["Verwenden Sie das globale S3-API-Zertifikat"](#) Statt ein neues Endpunktzertifikat für den Load Balancer zu erzeugen.

Mandanten

Mandanten können ihre Verbindungen zu StorageGRID nutzen [Identity Federation Server-Zertifikate](#) oder [Endpoint-Zertifikate für Plattformservices](#) sichern.

Die Mandantentabelle verfügt über eine Zeile für jeden Mandanten und gibt an, ob jeder Mandant die Berechtigung hat, seine eigenen Identitätsquellen- oder Plattform-Services zu nutzen.

Ihre Vorteile:

- ["Wählen Sie einen Mandantennamen aus, um sich beim Mandanten-Manager anzumelden"](#)
- ["Wählen Sie einen Mandantennamen aus, um Details zur Identitätsföderation des Mandanten anzuzeigen"](#)
- ["Wählen Sie einen Mandantennamen aus, um Details zu den Services der Mandantenplattform"](#)

anzuzeigen"

- ["Festlegen eines Endpunktzertifikats für den Plattformservice während der Endpunkterstellung"](#)

Sonstiges

StorageGRID verwendet andere Sicherheitszertifikate zu bestimmten Zwecken. Diese Zertifikate werden nach ihrem Funktionsnamen aufgelistet. Weitere Sicherheitszertifikate:

- [Cloud Storage Pool-Zertifikate](#)
- [Benachrichtigungszertifikate per E-Mail senden](#)
- [Externe Syslog-Server-Zertifikate](#)
- [Verbindungszertifikate für Grid Federation](#)
- [Zertifikate für Identitätsföderation](#)
- [KMS-Zertifikate \(Key Management Server\)](#)
- [Einzelanmelde-Zertifikate](#)

Informationen geben den Zertifikattyp an, den eine Funktion verwendet, sowie die Gültigkeitsdaten des Server- und Clientzertifikats. Wenn Sie einen Funktionsnamen auswählen, wird eine Browserregisterkarte geöffnet, auf der Sie die Zertifikatdetails anzeigen und bearbeiten können.



Sie können Informationen für andere Zertifikate nur anzeigen und darauf zugreifen, wenn Sie über die verfügen ["Entsprechende Berechtigung"](#).

Ihre Vorteile:

- ["Festlegen eines Cloud-Storage-Pool-Zertifikats für S3, C2S S3 oder Azure"](#)
- ["Legen Sie ein Zertifikat für Benachrichtigungen per E-Mail fest"](#)
- ["Verwenden Sie ein Zertifikat für einen externen Syslog-Server"](#)
- ["Verbindungszertifikate für Netzwerk drehen"](#)
- ["Anzeigen und Bearbeiten eines Zertifikats für die Identitätsföderation"](#)
- ["Laden Sie den KMS-Server \(Key Management Server\) und die Clientzertifikate hoch"](#)
- ["Geben Sie manuell ein SSO-Zertifikat für eine vertrauenswürdige Partei an"](#)

Details zum Sicherheitszertifikat

Jede Art von Sicherheitszertifikat wird unten beschrieben, mit Links zu den Implementierungsanleitungen.

Zertifikat für die Managementoberfläche

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	<p>Authentifiziert die Verbindung zwischen Client-Webbrowsern und der StorageGRID-Managementoberfläche, sodass Benutzer ohne Sicherheitswarnungen auf Grid-Manager und Mandantenmanager zugreifen können.</p> <p>Dieses Zertifikat authentifiziert auch Grid Management-API- und Mandantenmanagement-API-Verbindungen.</p> <p>Sie können das bei der Installation erstellte Standardzertifikat verwenden oder ein benutzerdefiniertes Zertifikat hochladen.</p>	Konfiguration > Sicherheit > Zertifikate , wählen Sie die Registerkarte Global und dann Management-Schnittstellenzertifikat	"Konfigurieren Sie Zertifikate für die Managementoberfläche"

S3-API-Zertifikat

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	Authentifiziert sichere S3-Clientverbindungen zu einem Storage-Node und zu Endpunkten für den Load Balancer (optional).	Konfiguration > Sicherheit > Zertifikate , wählen Sie die Registerkarte Global und dann S3-API-Zertifikat	"Konfigurieren Sie S3-API-Zertifikate"

Grid-CA-Zertifikat

Siehe [Beschreibung des Standard Grid CA-Zertifikats](#).

Administrator-Client-Zertifikat

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Client	<p>Wird auf jedem Client installiert, sodass StorageGRID den externen Client-Zugriff authentifizieren kann.</p> <ul style="list-style-type: none"> • 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 Sie Client-Zertifikate"

Endpunkt-Zertifikat für Load Balancer

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	<p>Authentifiziert die Verbindung zwischen S3 Clients und dem StorageGRID Load Balancer auf Gateway-Nodes und Admin-Nodes. Sie können ein Load Balancer-Zertifikat hochladen oder generieren, wenn Sie einen Load Balancer-Endpunkt konfigurieren. Client-Applikationen verwenden das Load Balancer-Zertifikat, wenn Sie eine Verbindung zu StorageGRID herstellen, um Objektdaten zu speichern und abzurufen.</p> <p>Sie können auch eine benutzerdefinierte Version des globalen Zertifikats verwenden S3-API-Zertifikat, um Verbindungen zum Load Balancer-Dienst zu authentifizieren. Wenn das globale Zertifikat zur Authentifizierung von Load Balancer-Verbindungen verwendet wird, müssen Sie kein separates Zertifikat für jeden Load Balancer-Endpunkt hochladen oder generieren.</p> <p>Hinweis: das Zertifikat, das für die Load Balancer Authentifizierung verwendet wird, ist das am häufigsten verwendete Zertifikat während des normalen StorageGRID-Betriebs.</p>	Konfiguration > Netzwerk > Load Balancer-Endpunkte	<ul style="list-style-type: none"> • "Konfigurieren von Load Balancer-Endpunkten" • "Erstellen eines Load Balancer-Endpunkts für FabricPool"

Endpunkt-Zertifikat für Cloud Storage Pool

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	Authentifiziert die Verbindung von einem StorageGRID Cloud Storage Pool auf einem externen Storage-Standort wie S3 Glacier oder Microsoft Azure Blob Storage. Für jeden Cloud-Provider-Typ ist ein anderes Zertifikat erforderlich.	ILM > Speicherpools	"Erstellen Sie einen Cloud-Storage-Pool"

Zertifikat für eine E-Mail-Benachrichtigung

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server und Client	<p>Authentifiziert die Verbindung zwischen einem SMTP-E-Mail-Server und StorageGRID, die für Benachrichtigungen verwendet werden.</p> <ul style="list-style-type: none"> • Wenn die Kommunikation mit dem SMTP-Server TLS (Transport Layer Security) erfordert, müssen Sie das CA-Zertifikat für den E-Mail-Server angeben. • Geben Sie ein Clientzertifikat nur an, wenn für den SMTP-E-Mail-Server Clientzertifikate zur Authentifizierung erforderlich sind. 	Benachrichtigungen > E-Mail-Einrichtung	"Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein"

Externes Syslog-Serverzertifikat

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

Verbindungszertifikat für Grid Federation

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server und Client	Authentifizieren und verschlüsseln Sie Informationen, die zwischen dem aktuellen StorageGRID-System und einem anderen Grid in einer Grid-Verbundverbindung gesendet werden.	Konfiguration > System > Grid-Föderation	<ul style="list-style-type: none"> • "Erstellen von Grid Federation-Verbindungen" • "Verbindungszertifikate drehen"

Zertifikat für Identitätsföderation

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	Authentifiziert die Verbindung zwischen StorageGRID und einem externen Identitäts-Provider, z. B. Active Directory, OpenLDAP oder Oracle Directory Server. Wird für Identitätsföderation verwendet, durch die Administratoren und Benutzer von einem externen System gemanagt werden können.	Konfiguration > Zugriffskontrolle > Identitätsföderation	"Verwenden Sie den Identitätsverbund"

KMS-Zertifikat (Key Management Server)

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server und Client	Authentifiziert die Verbindung zwischen StorageGRID und einem externen Verschlüsselungsmanagement-Server (KMS), der Verschlüsselungsschlüssel für die StorageGRID Appliance-Nodes bereitstellt.	Konfiguration > Sicherheit > Schlüsselverwaltungsserver	"Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)"

Endpoint-Zertifikat für Plattform-Services

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	Authentifiziert die Verbindung vom StorageGRID Plattform-Service zu einer S3-Storage-Ressource.	Tenant Manager > STORAGE (S3) > Plattform-Services-Endpunkte	"Endpunkt für Plattformservices erstellen" "Endpunkt der Plattformdienste bearbeiten"

SSO-Zertifikat (Single Sign On)

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	Authentifiziert die Verbindung zwischen Services der Identitätsföderation, z. B. Active Directory Federation Services (AD FS) und StorageGRID, die für SSO-Anforderungen (Single Sign On) verwendet werden.	Konfiguration > Zugriffskontrolle > Single Sign-On	"Konfigurieren Sie Single Sign-On"

Beispiele für Zertifikate

Beispiel 1: Load Balancer Service

In diesem Beispiel fungiert StorageGRID als Server.

1. Sie konfigurieren einen Load Balancer-Endpunkt und laden ein Serverzertifikat in StorageGRID hoch oder erstellen.
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 auf Grundlage des privaten Schlüssels.
5. Der Client vergleicht die Serversignatur mit der Signatur auf seiner Kopie des Zertifikats. Wenn die Signaturen übereinstimmen, startet der Client eine Sitzung mit demselben öffentlichen Schlüssel.
6. Der Client sendet Objektdaten an StorageGRID.

Beispiel 2: Externer KMS (Key Management Server)

In diesem Beispiel fungiert StorageGRID als Client.

1. Mithilfe der Software für den externen Verschlüsselungsmanagement-Server konfigurieren Sie StorageGRID als KMS-Client und erhalten ein von einer Zertifizierungsstelle signiertes Serverzertifikat, ein öffentliches Clientzertifikat und den privaten Schlüssel für das Clientzertifikat.
2. Mit dem Grid Manager konfigurieren Sie einen KMS-Server und laden die Server- und Client-Zertifikate sowie den privaten Client-Schlüssel hoch.
3. Wenn ein StorageGRID-Node einen Verschlüsselungsschlüssel benötigt, fordert er den KMS-Server an, der Daten des Zertifikats enthält und eine auf dem privaten Schlüssel basierende Signatur.
4. Der KMS-Server validiert die Zertifikatsignatur und entscheidet, dass er StorageGRID vertrauen kann.
5. Der KMS-Server antwortet über die validierte Verbindung.

Unterstützte Serverzertifikatstypen

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



Der Verschlüsselungstyp für die Sicherheitsrichtlinie muss mit dem Serverzertifikattyp übereinstimmen. RSA-Chiffren erfordern beispielsweise RSA-Zertifikate, und ECDSA-Chiffren erfordern ECDSA-Zertifikate. Siehe ["Verwalten von Sicherheitszertifikaten"](#). Wenn Sie eine benutzerdefinierte Sicherheitsrichtlinie konfigurieren, die nicht mit dem Serverzertifikat kompatibel ist, können Sie ["Vorübergehendes Zurücksetzen auf die Standard-Sicherheitsrichtlinie"](#).

Weitere Informationen darüber, wie StorageGRID Clientverbindungen sichert, finden Sie unter ["Sicherheit für S3-Clients"](#).

Konfigurieren Sie Zertifikate für die Managementoberfläche

Sie können das Standardzertifikat für die Verwaltungsschnittstelle durch ein einzelnes benutzerdefiniertes Zertifikat ersetzen, das Benutzern den Zugriff auf den Grid Manager und den Tenant Manager ermöglicht, ohne dass Sicherheitswarnungen auftreten. Sie können auch das Standard-Zertifikat für die Managementoberfläche zurücksetzen oder ein neues erstellen.

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 Zertifikat für benutzerdefinierte Verwaltungsschnittstellen und einen entsprechenden privaten Schlüssel ersetzt werden.

Da für alle Admin-Nodes ein einzelnes Zertifikat für eine benutzerdefinierte Managementoberfläche verwendet wird, müssen Sie das Zertifikat als Platzhalter- oder Multi-Domain-Zertifikat angeben, wenn Clients den Hostnamen bei der Verbindung mit Grid Manager und Tenant Manager 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. Je nach der von Ihnen verwendeten Root Certificate Authority (CA) müssen Benutzer möglicherweise auch das Grid CA-Zertifikat in den Webbrowser installieren, mit dem sie auf den Grid Manager und den Tenant Manager zugreifen können.



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 prüfen.



Wenn Sie mit einem Domännennamen anstelle einer IP-Adresse auf den Grid Manager oder den Tenant Manager zugreifen, zeigt der Browser einen Zertifikatsfehler ohne eine Option zum Umgehen an, wenn eine der folgenden Fälle auftritt:

- Ihr Zertifikat für die benutzerdefinierte Managementoberfläche läuft ab.
- Sie [Zurücksetzen von einem Zertifikat der benutzerdefinierten Managementoberfläche auf das Standard-Serverzertifikat](#).

Fügen Sie ein Zertifikat für eine benutzerdefinierte Managementoberfläche hinzu

Zum Hinzufügen eines Zertifikats einer benutzerdefinierten Managementoberfläche können Sie Ihr eigenes Zertifikat bereitstellen oder mit dem Grid Manager ein Zertifikat erstellen.

Schritte

1. Wählen Sie **Konfiguration > Sicherheit > Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global** die Option **Management Interface Certificate** aus.
3. Wählen Sie **Benutzerdefiniertes Zertifikat verwenden**.
4. Hochladen oder Generieren des Zertifikats

Zertifikat hochladen

Laden Sie die erforderlichen Serverzertifikatdateien hoch.

a. Wählen Sie **Zertifikat hochladen**.

b. Laden Sie die erforderlichen Serverzertifikatdateien hoch:

- **Server-Zertifikat:** Die benutzerdefinierte Server-Zertifikatdatei (PEM-codiert).
- **Zertifikat privater Schlüssel:** Die benutzerdefinierte Server Zertifikat private Schlüsseldatei (.key).



EC Private Keys müssen mindestens 224 Bit groß sein. RSA Private Keys müssen mindestens 2048 Bit groß sein.

- **CA-Paket:** Eine einzelne optionale Datei, die die Zertifikate jeder Intermediate-Zertifizierungsstelle (CA) enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatdateien enthalten, die in der Reihenfolge der Zertifikatskette verkettet sind.

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

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

Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Endung .pem.

Beispiel: storagegrid_certificate.pem

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

d. Wählen Sie **Speichern**. + das Zertifikat der benutzerdefinierten Managementoberfläche wird für alle nachfolgenden neuen Verbindungen mit Grid Manager, Tenant Manager, Grid Manager API oder Tenant Manager API verwendet.

Zertifikat wird generiert

Erstellen Sie die Serverzertifikatdateien.



Die beste Vorgehensweise für eine Produktionsumgebung ist die Verwendung eines Zertifikats der benutzerdefinierten Management-Schnittstelle, das von einer externen Zertifizierungsstelle signiert wurde.

a. Wählen Sie **Zertifikat erstellen**.

b. Geben Sie die Zertifikatsinformationen an:

Feld	Beschreibung
Domain-Name	Mindestens ein vollständig qualifizierter Domänenname, der in das Zertifikat aufgenommen werden soll. Verwenden Sie ein * als Platzhalter, um mehrere Domain-Namen darzustellen.

Feld	Beschreibung
IP	Mindestens eine IP-Adresse, die in das Zertifikat aufgenommen werden soll.
Betreff (optional)	X.509 Subject oder Distinguished Name (DN) des Zertifikateigentümers. Wenn in diesem Feld kein Wert eingegeben wird, verwendet das generierte Zertifikat den ersten Domännennamen oder die IP-Adresse als allgemeinen Studienteilnehmer (CN).
Tage gültig	Anzahl der Tage nach Erstellung, nach denen das Zertifikat abläuft.
Fügen Sie wichtige Nutzungserweiterungen hinzu	Wenn diese Option ausgewählt ist (Standard und empfohlen), werden die Schlüsselnutzung und die erweiterten Schlüsselnutzungserweiterungen dem generierten Zertifikat hinzugefügt. Diese Erweiterungen definieren den Zweck des Schlüssels, der im Zertifikat enthalten ist. Hinweis: Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, Sie haben Verbindungsprobleme mit älteren Clients, wenn Zertifikate diese Erweiterungen enthalten.

c. Wählen Sie **Erzeugen**.

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

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

Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an.
Speichern Sie die Datei mit der Endung `.pem`.

Beispiel: `storagegrid_certificate.pem`

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

e. Wählen Sie **Speichern**. + das Zertifikat der benutzerdefinierten Managementoberfläche wird für alle nachfolgenden neuen Verbindungen mit Grid Manager, Tenant Manager, Grid Manager API oder Tenant Manager API verwendet.

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



Nachdem Sie ein Zertifikat hochgeladen oder generiert haben, lassen Sie sich bis zu einen Tag lang alle damit verbundenen Warnmeldungen zum Ablauf des Zertifikats löschen.

6. Nachdem Sie ein Zertifikat für eine benutzerdefinierte Managementoberfläche hinzugefügt haben, werden auf der Seite Zertifikat der Verwaltungsschnittstelle detaillierte Zertifikatsinformationen für die verwendeten Zertifikate angezeigt. + Sie können das PEM-Zertifikat nach Bedarf herunterladen oder kopieren.

Stellen Sie das Standardzertifikat für die Managementoberfläche wieder her

Sie können das Standardzertifikat zur Managementoberfläche für Grid Manager- und Tenant-Manager-Verbindungen wiederherstellen.

Schritte

1. Wählen Sie **Konfiguration > Sicherheit > Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global** die Option **Management Interface Certificate** aus.
3. Wählen Sie **Standard-Zertifikat verwenden**.

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

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

Erstellen Sie mit einem Skript ein neues Zertifikat für die selbstsignierte Managementoberfläche

Wenn eine strikte Host-Validierung erforderlich ist, können Sie das Zertifikat der Managementoberfläche mithilfe eines Skripts generieren.

Bevor Sie beginnen

- Sie haben "[Bestimmte Zugriffsberechtigungen](#)".
- Sie haben die `Passwords.txt` Datei.

Über diese Aufgabe

Die beste Vorgehensweise für eine Produktionsumgebung ist die Verwendung eines Zertifikats, das von einer externen Zertifizierungsstelle signiert wurde.

Schritte

1. Ermitteln Sie den vollständig qualifizierten Domännennamen (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 in der Datei aufgeführte Passwort ein `Passwords.txt`.
 - c. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
 - d. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.

Wenn Sie als root angemeldet sind, wechselt 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 vollständig qualifizierten Domännennamen aller Admin-Knoten darzustellen. Zum Beispiel `*.ui.storagegrid.example.com` verwendet den Platzhalter `*` für `admin1.ui.storagegrid.example.com` und `admin2.ui.storagegrid.example.com`.

- Legen Sie fest `--type management`, um das Zertifikat für die Managementoberfläche zu konfigurieren, 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 Argument verwenden `--days`, um die Standardgültigkeitsdauer zu überschreiben.



Die Gültigkeitsdauer eines Zertifikats beginnt, wenn `make-certificate` ausgeführt wird. Sie müssen sicherstellen, dass der Management-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 720
```

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 Befehls-Shell 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 Interface Certificate** aus.
7. Konfigurieren Sie den Management-Client so, dass er das öffentliche Zertifikat verwendet, das Sie kopiert haben. Geben Sie DIE START- und END-Tags an.

Laden Sie das Zertifikat für die Managementoberfläche herunter oder kopieren Sie es

Sie können den Inhalt des Zertifikats der Managementoberfläche speichern oder kopieren, um ihn an einer anderen Stelle zu verwenden.

Schritte

1. Wählen Sie **Konfiguration > Sicherheit > Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global** die Option **Management Interface Certificate** aus.
3. Wählen Sie die Registerkarte **Server** oder **CA Bundle** aus und laden Sie das Zertifikat herunter oder kopieren Sie es.

Laden Sie die Zertifikatdatei oder das CA-Paket herunter

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

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

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

- b. Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Endung `.pem`.

Beispiel: `storagegrid_certificate.pem`

Zertifikat oder CA-Bundle-PEM kopieren

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

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

Wenn Sie ein CA-Bundle kopieren, kopieren alle Zertifikate in den sekundären Registerkarten des CA-Bundles zusammen.

- b. Fügen Sie das kopierte Zertifikat in einen Texteditor ein.
- c. Speichern Sie die Textdatei mit der Endung `.pem`.

Beispiel: `storagegrid_certificate.pem`

Konfigurieren Sie S3-API-Zertifikate

Sie können das Serverzertifikat ersetzen oder wiederherstellen, das für S3-Clientverbindungen zu Storage Nodes oder zu Load Balancer-Endpunkten verwendet wird. Das benutzerdefinierte Ersatzserverzertifikat ist speziell für Ihr Unternehmen bestimmt.



Swift-Details wurden aus dieser Version der doc-Site entfernt. Siehe ["StorageGRID 11.8: Konfigurieren Sie S3- und Swift-API-Zertifikate"](#).

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 Sie möglicherweise auch das Grid-CA-Zertifikat in dem S3-API-Client installieren, den Sie für den Zugriff auf das System verwenden, je nachdem, welche Root-Zertifizierungsstelle Sie 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. Hochladen oder Generieren des Zertifikats

Zertifikat hochladen

Laden Sie die erforderlichen Serverzertifikatdateien hoch.

a. Wählen Sie **Zertifikat hochladen**.

b. Laden Sie die erforderlichen Serverzertifikatdateien hoch:

- **Server-Zertifikat:** Die benutzerdefinierte Server-Zertifikatdatei (PEM-codiert).
- **Zertifikat privater Schlüssel:** Die benutzerdefinierte Server Zertifikat private Schlüsseldatei (.key).



EC Private Keys müssen mindestens 224 Bit groß sein. RSA Private Keys müssen mindestens 2048 Bit groß sein.

- **CA-Paket:** Eine einzelne optionale Datei, die die Zertifikate jeder Intermediate-Zertifizierungsstelle enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatdateien enthalten, die in der Reihenfolge der Zertifikatskette verkettet sind.

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

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

Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Endung .pem.

Beispiel: storagegrid_certificate.pem

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

d. Wählen Sie **Speichern**.

Das benutzerdefinierte Serverzertifikat wird für nachfolgende neue S3-Client-Verbindungen verwendet.

Zertifikat wird generiert

Erstellen Sie die Serverzertifikatdateien.

a. Wählen Sie **Zertifikat erstellen**.

b. Geben Sie die Zertifikatsinformationen an:

Feld	Beschreibung
Domain-Name	Mindestens ein vollständig qualifizierter Domänenname, der in das Zertifikat aufgenommen werden soll. Verwenden Sie ein * als Platzhalter, um mehrere Domain-Namen darzustellen.
IP	Mindestens eine IP-Adresse, die in das Zertifikat aufgenommen werden soll.

Feld	Beschreibung
Betreff (optional)	X.509 Subject oder Distinguished Name (DN) des Zertifikateigentümers. Wenn in diesem Feld kein Wert eingegeben wird, verwendet das generierte Zertifikat den ersten Domännennamen oder die IP-Adresse als allgemeinen Studienteilnehmer (CN).
Tage gültig	Anzahl der Tage nach Erstellung, nach denen das Zertifikat abläuft.
Fügen Sie wichtige Nutzungserweiterungen hinzu	Wenn diese Option ausgewählt ist (Standard und empfohlen), werden die Schlüsselnutzung und die erweiterten Schlüsselnutzungserweiterungen dem generierten Zertifikat hinzugefügt. Diese Erweiterungen definieren den Zweck des Schlüssels, der im Zertifikat enthalten ist. Hinweis: Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, Sie haben Verbindungsprobleme mit älteren Clients, wenn Zertifikate diese Erweiterungen enthalten.

c. Wählen Sie **Erzeugen**.

d. Wählen Sie **Certificate Details**, um die Metadaten und PEM für das erzeugte benutzerdefinierte S3 API-Zertifikat anzuzeigen.

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

Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an.
Speichern Sie die Datei mit der Endung `.pem`.

Beispiel: `storagegrid_certificate.pem`

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

e. Wählen Sie **Speichern**.

Das benutzerdefinierte Serverzertifikat wird für nachfolgende neue S3-Client-Verbindungen verwendet.

5. Wählen Sie eine Registerkarte aus, um Metadaten für das Standard-StorageGRID-Serverzertifikat, ein Zertifikat mit einer Zertifizierungsstelle, das hochgeladen wurde, oder ein benutzerdefiniertes Zertifikat anzuzeigen, das erstellt wurde.



Nachdem Sie ein Zertifikat hochgeladen oder generiert haben, lassen Sie sich bis zu einen Tag lang alle damit verbundenen Warnmeldungen zum Ablauf des Zertifikats löschen.

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

7. Nach dem Hinzufügen eines benutzerdefinierten S3-API-Zertifikats zeigt die Seite mit dem S3-API-Zertifikat detaillierte Zertifikatsinformationen für das verwendete benutzerdefinierte S3-API-Zertifikat an. +

Sie können das PEM-Zertifikat nach Bedarf herunterladen oder kopieren.

Stellen Sie das standardmäßige S3-API-Zertifikat wieder her

Sie können auf die Verwendung des standardmäßigen S3-API-Zertifikats für S3-Client-Verbindungen zu Storage-Nodes zurücksetzen. Sie können jedoch das S3-API-Standardzertifikat 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 **Standard-Zertifikat verwenden**.

Wenn Sie die Standardversion des globalen S3-API-Zertifikats wiederherstellen, werden die von Ihnen konfigurierten benutzerdefinierten Serverzertifikatdateien gelöscht und können nicht vom System wiederhergestellt werden. Das S3-API-Standardzertifikat wird für nachfolgende neue S3-Client-Verbindungen zu Storage-Nodes verwendet.

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

Wenn Sie über Root-Zugriffsberechtigungen verfügen und das benutzerdefinierte S3-API-Zertifikat für Load Balancer-Endpunktverbindungen verwendet wurde, wird eine Liste der Load Balancer-Endpunkte angezeigt, auf die über das standardmäßige S3-API-Zertifikat nicht mehr zugegriffen werden kann. Gehen Sie zu, um die betroffenen Endpunkte zu ["Konfigurieren von Load Balancer-Endpunkten"](#) bearbeiten oder zu entfernen.

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

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

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

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 Bundle** aus und laden Sie das Zertifikat herunter oder kopieren Sie es.

Laden Sie die Zertifikatdatei oder das CA-Paket herunter

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

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

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

- b. Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Endung `.pem`.

Beispiel: `storagegrid_certificate.pem`

Zertifikat oder CA-Bundle-PEM kopieren

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

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

Wenn Sie ein CA-Bundle kopieren, kopieren alle Zertifikate in den sekundären Registerkarten des CA-Bundles zusammen.

- b. Fügen Sie das kopierte Zertifikat in einen Texteditor ein.
- c. Speichern Sie die Textdatei mit der Endung `.pem`.

Beispiel: `storagegrid_certificate.pem`

Verwandte Informationen

- ["S3-REST-API VERWENDEN"](#)
- ["Konfigurieren Sie die Domännennamen des S3-Endpunkts"](#)

Kopieren Sie das Grid-CA-Zertifikat

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

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben ["Bestimmte Zugriffsberechtigungen"](#).

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

Laden Sie die Zertifikatdatei herunter

Laden Sie die Zertifikatdatei herunter `.pem`.

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

Beispiel: `storagegrid_certificate.pem`

Zertifikat PEM kopieren

Kopieren Sie den Zertifikatstext, um ihn an eine andere Stelle einzufügen.

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

Beispiel: `storagegrid_certificate.pem`

Konfigurieren Sie StorageGRID-Zertifikate für FabricPool

Für S3-Clients, die strenge Hostnamen-Validierungen durchführen und die eine strikte Hostname-Validierung nicht unterstützen, z. B. ONTAP-Clients mit FabricPool, können Sie beim Konfigurieren des Load Balancer-Endpunkts ein Serverzertifikat generieren oder hochladen.

Bevor Sie beginnen

- Sie haben ["Bestimmte Zugriffsberechtigungen"](#).
- Sie sind im Grid Manager mit einem angemeldet ["Unterstützter Webbrowser"](#).

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 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 unter ["Konfigurieren Sie StorageGRID für FabricPool"](#).

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 optionale 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 Domännennamen 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.

Konfigurieren Sie Client-Zertifikate

Mit Clientzertifikaten können autorisierte externe Clients auf die StorageGRID Prometheus-Datenbank zugreifen und externe Tools zur Überwachung von StorageGRID sicher einsetzen.

Wenn Sie mit einem externen Monitoring-Tool auf StorageGRID zugreifen müssen, müssen Sie mithilfe des Grid Managers ein Clientzertifikat hochladen oder generieren und die Zertifikatsinformationen in das externe Tool kopieren.

Siehe "[Verwalten von Sicherheitszertifikaten](#)" und "[Konfigurieren Sie benutzerdefinierte 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 Geräteknoten verwenden, lesen Sie die spezifischen Informationen zu "[Hochladen eines KMS-Clientzertifikats](#)".

Bevor Sie beginnen

- Sie haben Root-Zugriffsberechtigung.
- Sie sind im Grid Manager mit einem angemeldet "[Unterstützter Webbrowser](#)".
- So konfigurieren Sie ein Clientzertifikat:
 - Sie haben die IP-Adresse oder den Domännennamen des Admin-Knotens.
 - Wenn Sie das Zertifikat für die StorageGRID-Managementoberfläche konfiguriert haben, verfügen Sie über die CA, das Client-Zertifikat und den privaten Schlüssel, mit dem Sie das Zertifikat für die Managementoberfläche konfigurieren können.
 - Um Ihr eigenes Zertifikat hochzuladen, steht der private Schlüssel für das Zertifikat auf Ihrem lokalen Computer zur Verfügung.
 - Der private Schlüssel muss zum Zeitpunkt der Erstellung gespeichert oder aufgezeichnet worden sein.

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

- So bearbeiten Sie ein Clientzertifikat:
 - Sie haben die IP-Adresse oder den Domännennamen des Admin-Knotens.
 - Um Ihr eigenes Zertifikat oder ein neues Zertifikat hochzuladen, sind der private Schlüssel, das Clientzertifikat und die CA (sofern verwendet) auf Ihrem lokalen Computer verfügbar.

Fügen Sie Client-Zertifikate hinzu

Gehen Sie wie folgt vor, um das Clientzertifikat hinzuzufügen:

- [Das Zertifikat der Managementoberfläche ist bereits konfiguriert](#)
- [KANN Client-Zertifikat AUSGESTELLT haben](#)
- [Zertifikat vom Grid Manager generiert](#)

Das Zertifikat der Managementoberfläche ist bereits konfiguriert

Verwenden Sie diese Vorgehensweise, um ein Clientzertifikat hinzuzufügen, wenn bereits ein Zertifikat für eine Managementoberfläche mit einer vom Kunden bereitgestellten CA, einem Clientzertifikat und einem privaten Schlüssel konfiguriert wurde.

Schritte

1. Wählen Sie im Grid Manager **Konfiguration > Sicherheit > Zertifikate** und dann die Registerkarte **Client**.
2. Wählen Sie **Hinzufügen**.
3. Geben Sie einen Zertifikatnamen ein.
4. Um über Ihr externes Monitoring-Tool auf Prometheus-Kennzahlen zuzugreifen, wählen Sie **prometheus zulassen**.
5. Wählen Sie **Weiter**.
6. Laden Sie für den Schritt **Attach certificates** das Management Interface Zertifikat hoch.
 - a. Wählen Sie **Zertifikat hochladen**.
 - b. Wählen Sie **Browse** und wählen Sie die Zertifikatdatei der Verwaltungsschnittstelle (.pem).
 - Wählen Sie **Client Certificate Details** aus, um die Zertifikatmetadaten und das Zertifikat PEM anzuzeigen.
 - Wählen Sie **Zertifikat kopieren PEM** aus, um den Zertifikatinhalt zum Einfügen an eine andere 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. [Konfiguration eines externen Überwachungstools](#), Wie Grafana.

KANN Client-Zertifikat AUSGESTELLT haben

Verwenden Sie dieses Verfahren, um ein Administrator-Client-Zertifikat hinzuzufügen, wenn ein Zertifikat der Verwaltungsschnittstelle nicht konfiguriert wurde und Sie planen, ein Client-Zertifikat für Prometheus hinzuzufügen, das ein vom Zertifizierungsstellen ausgestelltes Clientzertifikat und einen privaten Schlüssel verwendet.

Schritte

1. Führen Sie die Schritte bis "[Konfigurieren Sie ein Zertifikat für die Managementoberfläche](#)" aus.
2. Wählen Sie im Grid Manager **Konfiguration > Sicherheit > Zertifikate** und dann die Registerkarte **Client**.
3. Wählen Sie **Hinzufügen**.
4. Geben Sie einen Zertifikatnamen ein.
5. Um über Ihr externes Monitoring-Tool auf Prometheus-Kennzahlen zuzugreifen, wählen Sie **prometheus zulassen**.
6. Wählen Sie **Weiter**.
7. Laden Sie für den Schritt **Attach certificates** das Clientzertifikat, den privaten Schlüssel und die CA-Bundle-Dateien hoch:
 - a. Wählen Sie **Zertifikat hochladen**.
 - b. Wählen Sie **Browse** aus und wählen Sie das Clientzertifikat, den privaten Schlüssel und die CA-Paketdateien (.pem) aus.
 - Wählen Sie **Client Certificate Details** aus, um die Zertifikatmetadaten und das Zertifikat PEM anzuzeigen.
 - Wählen Sie **Zertifikat kopieren PEM** aus, um den Zertifikatsinhalt zum Einfügen an eine andere 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. [Konfiguration eines externen Überwachungstools](#), Wie Grafana.

Zertifikat vom Grid Manager generiert

Verwenden Sie dieses Verfahren, um ein Administrator-Client-Zertifikat hinzuzufügen, wenn ein Zertifikat der Verwaltungsschnittstelle nicht konfiguriert wurde und Sie planen, ein Clientzertifikat für Prometheus hinzuzufügen, das die Funktion Zertifikat generieren 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 Zertifikatnamen ein.
4. Um über Ihr externes Monitoring-Tool auf Prometheus-Kennzahlen zuzugreifen, wählen Sie **prometheus zulassen**.
5. Wählen Sie **Weiter**.
6. Wählen Sie für den Schritt **Zertifikate anhängen** **Zertifikat generieren** aus.
7. Geben Sie die Zertifikatsinformationen an:
 - **Subject** (optional): X.509 Subject oder Distinguished Name (DN) des Zertifikateigentümers.
 - **Tage gültig**: Die Anzahl der Tage, an denen das generierte Zertifikat gültig ist, beginnend mit dem Zeitpunkt, an dem es generiert wird.
 - **Key-Usage-Erweiterungen hinzufügen**: Wenn ausgewählt (Standard und empfohlen), werden Key-Usage und erweiterte Key-Usage-Erweiterungen zum generierten Zertifikat hinzugefügt.

Diese Erweiterungen definieren den Zweck des Schlüssels, der im Zertifikat enthalten ist.



Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, es treten Verbindungsprobleme mit älteren Clients auf, wenn diese Erweiterungen in Zertifikaten enthalten sind.

8. Wählen Sie **Erzeugen**.

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



Nach dem Schließen des Dialogfelds können Sie den privaten Zertifikatschlüssel nicht anzeigen. Kopieren Sie den Schlüssel an einem sicheren Ort.

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

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

Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Privatschlüssel kopieren**, um den privaten Zertifikatschlüssel zum Einfügen an andere Orte zu kopieren.
- Wählen Sie **privaten Schlüssel herunterladen**, um den privaten Schlüssel als Datei zu speichern.

Geben Sie den Dateinamen des privaten Schlüssels und den Speicherort für den Download 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 wählen Sie dann die Registerkarte **Global**.

12. Wählen Sie **Management Interface Certificate** aus.

13. Wählen Sie **Benutzerdefiniertes Zertifikat verwenden**.

14. Laden Sie die Dateien `Certificate.pem` und `private_key.pem` aus dem Schritt hoch [Details zum Clientzertifikat](#). Es ist nicht erforderlich, das CA-Paket hochzuladen.

- Wählen Sie **Zertifikat hochladen** und dann **Weiter**.
- Laden Sie jede Zertifikatsdatei hoch (`.pem`).
- Wählen Sie **Speichern**, um das Zertifikat im Grid Manager zu speichern.

Das neue Zertifikat wird auf der Zertifikatsseite der Verwaltungsschnittstelle angezeigt.

15. [Konfiguration eines externen Überwachungstools](#), Wie Grafana.

Konfigurieren Sie ein externes Monitoring-Tool

Schritte

1. Konfigurieren Sie die folgenden Einstellungen für Ihr externes Monitoring-Tool, 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 Domain-Namen oder die IP-Adresse für den Admin-Node ein. Geben Sie HTTPS und Port 9091 an.

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

- c. Aktivieren Sie **TLS Client Auth** und **mit CA Cert**.

- d. Kopieren Sie unter TLS/SSL Auth Details und fügen Sie: + ein

- Das Management-Interface-CA-Zertifikat nach **CA-Zertifikat**
- Das Client-Zertifikat an **Client-Zertifikat**
- Der private Schlüssel zu **Client Key**

- e. **ServerName:** Geben Sie den Domainnamen des Admin-Knotens ein.

Servername muss mit dem Domännennamen übereinstimmen, wie er im Zertifikat der Verwaltungsschnittstelle angezeigt wird.

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

Sie können jetzt mit Ihrem externen Monitoring Tool auf die Prometheus Kennzahlen von StorageGRID zugreifen.

Informationen zu den Metriken finden Sie im ["Anweisungen zur Überwachung von StorageGRID"](#).

Client-Zertifikate bearbeiten

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

Schritte

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

In der Tabelle sind die Daten zum Ablauf des Zertifikats und die Zugriffsrechte für Prometheus aufgeführt. Wenn ein Zertifikat bald abläuft oder bereits abgelaufen ist, wird in der Tabelle eine Meldung angezeigt, und eine Warnmeldung wird ausgelöst.

2. Wählen Sie das Zertifikat aus, das Sie bearbeiten möchten.
3. Wählen Sie **Bearbeiten** und dann **Name und Berechtigung bearbeiten** aus
4. Geben Sie einen Zertifikatnamen ein.
5. Um über Ihr externes Monitoring-Tool auf Prometheus-Kennzahlen 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.

Verbinden Sie das neue Clientzertifikat

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

Schritte

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

In der Tabelle sind die Daten zum Ablauf des Zertifikats und die Zugriffsrechte für Prometheus aufgeführt. Wenn ein Zertifikat bald abläuft oder bereits abgelaufen ist, wird in der Tabelle eine Meldung angezeigt, und eine Warnmeldung wird ausgelöst.

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

Zertifikat hochladen

Kopieren Sie den Zertifikatstext, um ihn an eine andere Stelle einzufügen.

- a. Wählen Sie **Zertifikat hochladen** und dann **Weiter**.
- b. Laden Sie den Namen des Client-Zertifikats hoch (.pem).

Wählen Sie **Client Certificate Details** aus, um die Zertifikatmetadaten und das Zertifikat PEM anzuzeigen.

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

Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an.
Speichern Sie die Datei mit der Endung .pem.

Beispiel: storagegrid_certificate.pem

- Wählen Sie **Zertifikat kopieren PEM** aus, um den Zertifikatinhalt zum Einfügen an eine andere 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 wird generiert

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

- a. Wählen Sie **Zertifikat erstellen**.
- b. Geben Sie die Zertifikatsinformationen an:

- **Subject** (optional): X.509 Subject oder Distinguished Name (DN) des Zertifikateigentümers.
- **Tage gültig**: Die Anzahl der Tage, an denen das generierte Zertifikat gültig ist, beginnend mit dem Zeitpunkt, an dem es generiert wird.
- **Key-Usage-Erweiterungen hinzufügen**: Wenn ausgewählt (Standard und empfohlen), werden Key-Usage und erweiterte Key-Usage-Erweiterungen zum generierten Zertifikat hinzugefügt.

Diese Erweiterungen definieren den Zweck des Schlüssels, der im Zertifikat enthalten ist.



Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, es treten Verbindungsprobleme mit älteren Clients auf, wenn diese Erweiterungen in Zertifikaten enthalten sind.

- c. Wählen Sie **Erzeugen**.
- d. Wählen Sie **Client Certificate Details** aus, um die Zertifikatmetadaten und das Zertifikat PEM anzuzeigen.



Nach dem Schließen des Dialogfelds können Sie den privaten Zertifikatschlüssel nicht anzeigen. Kopieren Sie den Schlüssel an einem sicheren Ort.

- Wählen Sie **Zertifikat kopieren PEM** aus, um den Zertifikatinhalt zum Einfügen an eine

andere Stelle zu kopieren.

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

Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an.
Speichern Sie die Datei mit der Endung `.pem`.

Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Privatschlüssel kopieren**, um den privaten Zertifikatschlüssel zum Einfügen an andere Orte zu kopieren.
- Wählen Sie **privaten Schlüssel herunterladen**, um den privaten Schlüssel als Datei zu speichern.

Geben Sie den Dateinamen des privaten Schlüssels und den Speicherort für den Download 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 Clientzertifikaten

Sie können ein Clientzertifikat 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.

Laden Sie die Zertifikatdatei herunter

Laden Sie die Zertifikatdatei herunter .pem.

- a. Wählen Sie **Zertifikat herunterladen**.
- b. Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Endung .pem.

Beispiel: `storagegrid_certificate.pem`

Zertifikat kopieren

Kopieren Sie den Zertifikatstext, um ihn an eine andere Stelle einzufügen.

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

Beispiel: `storagegrid_certificate.pem`

Entfernen Sie Client-Zertifikate

Wenn Sie kein Administrator-Clientzertifikat 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 dann.



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

Nachdem ein Zertifikat entfernt wurde, müssen Clients, die das Zertifikat verwendet haben, ein neues Clientzertifikat angeben, um auf die StorageGRID Prometheus-Datenbank zuzugreifen.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.