



Verwalten von Zertifikaten

StorageGRID

NetApp
October 03, 2025

Inhalt

Verwalten von Zertifikaten	1
Informationen zu Sicherheitszertifikaten	1
Greifen Sie auf Sicherheitszertifikate zu	2
Details zum Sicherheitszertifikat	5
Beispiele für Zertifikate	11
Konfigurieren Sie Serverzertifikate	12
Unterstützte Serverzertifikatstypen	12
Konfigurieren Sie Zertifikate für die Managementoberfläche	12
Konfigurieren von S3- und Swift-API-Zertifikaten	17
Kopieren Sie das Grid-CA-Zertifikat	22
Konfigurieren Sie StorageGRID-Zertifikate für FabricPool	22
Konfigurieren Sie Client-Zertifikate	23
Fügen Sie Client-Zertifikate hinzu	24
Client-Zertifikate bearbeiten	28
Verbinden Sie das neue Clientzertifikat	29
Herunterladen oder Kopieren von Clientzertifikaten	31
Entfernen Sie Client-Zertifikate	31

Verwalten von Zertifikaten

Informationen zu 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 überprüft dieses Zertifikat, indem er die Serversignatur mit der Signatur seiner Kopie des Zertifikats vergleicht. Wenn die Signaturen übereinstimmen, startet der Client eine Sitzung mit dem Server, der denselben öffentlichen Schlüssel verwendet.

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 enthält eine integrierte Zertifizierungsstelle (CA), die während der Systeminstallation ein internes Grid CA-Zertifikat generiert. Das Grid-CA-Zertifikat wird standardmäßig zum Schutz des internen StorageGRID-Datenverkehrs verwendet. Eine externe Zertifizierungsstelle (CA) kann benutzerdefinierte Zertifikate ausstellen, die vollständig den Informationssicherheitsrichtlinien Ihres Unternehmens entsprechen. Sie können das Grid-CA-Zertifikat zwar für eine nicht-Produktionsumgebungen verwenden, jedoch empfiehlt es sich, benutzerdefinierte Zertifikate zu verwenden, die von einer externen Zertifizierungsstelle signiert sind. Ungesicherte Verbindungen ohne Zertifikat werden ebenfalls unterstützt, werden jedoch nicht empfohlen.

- Benutzerdefinierte CA-Zertifikate entfernen die internen Zertifikate nicht. Die benutzerdefinierten Zertifikate sollten jedoch die für die Überprüfung der Serververbindungen angegebenen Zertifikate sein.
- Alle benutzerdefinierten Zertifikate müssen den erfüllen [Richtlinien zur Systemhärtung](#) Für Serverzertifikate.
- 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.

1. Wählen Sie im Grid Manager **CONFIGURATON Security Certificates** aus.

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 nur auf eine Registerkarte zugreifen, wenn Sie über die entsprechende Berechtigung verfügen.

- **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- und Swift-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 und Swift 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-Management-Schnittstellen.
- [S3- und Swift-API-Zertifikat](#): Sichert Client-API-Verbindungen zu Storage-Nodes, Admin-Nodes und Gateway-Nodes, über die S3- und Swift-Client-Applikationen Objektdaten hochladen und herunterladen.

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 Grid Manager- und Tenant Manager-Verbindungen verwendet.
 - [Das S3- und Swift-API-Zertifikat ersetzen](#) Wird für Storage-Node-, CLB-Service (veraltet) und Load Balancer-Endpunktverbindungen (optional) verwendet.
- [Stellen Sie das Standardzertifikat für die Managementoberfläche wieder her.](#)
- [Stellen Sie das S3- und Swift-API-Standardzertifikat wieder her.](#)
- [Erstellen Sie mit einem Skript ein neues Zertifikat für die selbstsignierte Managementoberfläche.](#)
- Kopieren Sie die, oder laden Sie sie herunter [Zertifikat für die Managementoberfläche](#) Oder [S3- und Swift-API-Zertifikat](#).

Grid CA

Der [Grid-CA-Zertifikat](#), Von der StorageGRID-Zertifizierungsstelle während der StorageGRID-Installation erzeugt, sichert den gesamten internen StorageGRID-Verkehr.

Zertifikatsinformationen umfassen das Ablaufdatum des Zertifikats und den Zertifikatsinhalt.

Das können Sie [Kopieren Sie das Grid-CA-Zertifikat, oder laden Sie es herunter](#), Aber Sie können es nicht ändern.

Client

[Client-Zertifikate](#), Generiert von einer externen Zertifizierungsstelle, sichern Sie die Verbindungen zwischen externen Monitoring-Tools 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 zu reagieren [Bearbeiten](#), [Anhängen](#), Oder [Entfernen](#) Ein Client-Zertifikat. Sie können bis zu 10 Clientzertifikate auswählen und gleichzeitig mit **Actions Remove** entfernen.

Load Balancer-Endpunkte

[Load Balancer-Endpunktzertifikate](#), Dass Sie die Verbindungen zwischen S3 und Swift Clients und dem StorageGRID Load Balancer Service auf Gateway Nodes und Admin Nodes hochladen oder generieren.

Die Endpunktstabelle für Load Balancer verfügt über eine Reihe für jeden konfigurierten Load Balancer-Endpunkt und gibt an, ob das globale S3- und Swift-API-Zertifikat oder ein benutzerdefiniertes Load Balancer-Endpoint-Zertifikat 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:

- [Wählen Sie einen Endpunkt-Namen aus, um eine Browserregisterkarte mit Informationen zum Load Balancer-Endpunkt einschließlich der Zertifikatdetails zu öffnen.](#)
- [Geben Sie ein Endpoint-Zertifikat für den Load Balancer für FabricPool an.](#)
- [Verwenden Sie das globale S3- und Swift-API-Zertifikat](#) Statt ein neues Load Balancer-Endpoint-Zertifikat zu erstellen.

Mandanten

Die Mandanten nutzen können [Identity Federation Server-Zertifikate](#) Oder [Endpoint-Zertifikate für Plattformservice](#) Um ihre Verbindungen mit StorageGRID zu 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](#)

Andere

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

- [Zertifikate für Identitätsföderation](#)
- [Cloud Storage Pool-Zertifikate](#)
- [KMS-Zertifikate \(Key Management Server\)](#)
- [Einzelanmelde-Zertifikate](#)
- [Benachrichtigungszertifikate per E-Mail senden](#)
- [Externe Syslog-Server-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 nur Informationen zu anderen Zertifikaten anzeigen und darauf zugreifen, wenn Sie über die entsprechende Berechtigung verfügen.

Ihre Vorteile:

- [Anzeigen und Bearbeiten eines Zertifikats für die Identitätsföderation](#)
- [Laden Sie den KMS-Server \(Key Management Server\) und die Clientzertifikate hoch](#)
- [Festlegen eines Cloud-Storage-Pool-Zertifikats für S3, C2S S3 oder Azure](#)
- [Geben Sie manuell ein SSO-Zertifikat für das Vertrauen der Vertrauenssteller an](#)
- [Legen Sie ein Zertifikat für Benachrichtigungen per E-Mail fest](#)
- [Geben Sie ein externes Syslog-Serverzertifikat an](#)

Details zum Sicherheitszertifikat

Jeder Typ von Sicherheitszertifikat ist unten beschrieben, mit Links zu Artikeln, die Implementierungsanweisungen enthalten.

Zertifikat für die Managementoberfläche

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

S3- und Swift-API-Zertifikat

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	Authentifiziert sichere S3- oder Swift-Client-Verbindungen zu einem Storage-Node, zum veralteten Connection Load Balancer (CLB)-Service auf einem Gateway-Node und den Load Balancer-Endpunkten (optional).	KONFIGURATION Sicherheit Zertifikate , wählen Sie die Registerkarte Global und wählen Sie dann S3 und Swift API Zertifikat	Konfigurieren von S3- und Swift-API-Zertifikaten

Grid-CA-Zertifikat

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

Administrator-Client-Zertifikat

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Client	Wird auf jedem Client installiert, sodass StorageGRID den externen Client-Zugriff 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 dann die Registerkarte Client wählen	Konfigurieren Sie Client-Zertifikate

Endpunkt-Zertifikat für Load Balancer

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	Authentifiziert die Verbindung zwischen S3- oder Swift-Clients und dem StorageGRID Load Balancer-Service 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. Sie können auch eine benutzerdefinierte Version des globalen verwenden S3- und Swift-API-Zertifikat Zertifikat zur Authentifizierung von Verbindungen zum Lastverteilungsservice. Wenn das globale Zertifikat zur Authentifizierung von Load Balancer-Verbindungen verwendet wird, müssen Sie für jeden Load Balancer-Endpunkt kein separates Zertifikat hochladen oder generieren. Hinweis: das Zertifikat, das für die Load Balancer Authentifizierung verwendet wird, ist das am häufigsten verwendete Zertifikat während des normalen StorageGRID-Betriebs.	KONFIGURATION Netzwerk Load Balancer-Endpunkte	• Konfigurieren von Load Balancer-Endpunkten • Erstellen eines Load Balancer-Endpunkts für FabricPool

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 Zugangskontrolle Identitätsverbund	Verwenden Sie den Identitätsverbund

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	Endpoint für Plattformservices erstellen Endpoint der Plattfordienste bearbeiten

Endpoint-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

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 Schlüsselverwaltungs- server	Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)

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 Zugangskontrolle Single Sign-On	Konfigurieren Sie Single Sign-On

Zertifikat für eine E-Mail-Benachrichtigung

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server und Client	Authentifiziert die Verbindung zwischen einem SMTP-E-Mail-Server und StorageGRID, die für Benachrichtigungen verwendet werden. • 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.	WARNUNGEN E-Mail-Einrichtung	Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein

Externes Syslog-Serverzertifikat

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	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 und dann externen Syslog-Server konfigurieren	Konfigurieren Sie einen externen Syslog-Server

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- oder Swift-Client-Verbindung zum Endpunkt des Load Balancer 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 überprüft dieses Zertifikat, indem er die Serversignatur mit der Signatur 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 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.

Konfigurieren Sie Serverzertifikate

Unterstützte Serverzertifikatstypen

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

Weitere Informationen dazu, wie StorageGRID Clientverbindungen für DIE REST-API sichert, finden Sie unter [S3 verwenden](#) Oder [Verwenden Sie Swift](#).

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 die Vorgänge durch ein Serverzertifikat nicht unterbrochen werden, wird die Warnung **Ablauf des Serverzertifikats für die Managementoberfläche** ausgelöst, wenn dieses Serverzertifikat bald abläuft. Wenn erforderlich, können Sie anzeigen, wann das aktuelle Zertifikat abläuft, indem Sie **KONFIGURATION Sicherheit Zertifikate** und das Ablaufdatum für das Zertifikat der Verwaltungsschnittstelle auf der Registerkarte Global auswählen.



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.
- Du [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 Schlüssel Datei (.key).



Private EC-Schlüssel müssen 224 Bit oder größer 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 Erweiterung `.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:

- **Domain-Name:** Ein oder mehrere vollqualifizierte Domain-Namen, die in das Zertifikat enthalten sind. Verwenden Sie ein * als Platzhalter, um mehrere Domain-Namen darzustellen.
- **IP:** Eine oder mehrere IP-Adressen, die in das Zertifikat enthalten sind.
- **Betreff:** X.509 Betreff oder Distinguished Name (DN) des Zertifikatsbesitzers.
- **Tage gültig:** Anzahl der Tage nach der Erstellung, dass das Zertifikat abläuft.

c. Wählen Sie **Erzeugen**.

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 Speicherort für den Download an.
Speichern Sie die Datei mit der Erweiterung `.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 einem 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 für die Verwaltungsschnittstelle wiederherstellen, werden die von Ihnen konfigurierten benutzerdefinierten Serverzertifikatsdateien 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.

Was Sie benötigen

- Sie haben spezifische 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 im aufgeführte Passwort ein `Passwords.txt` Datei:
- c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
- d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

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

3. Konfigurieren Sie StorageGRID mit einem neuen selbstsignierten Zertifikat.

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

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



Die Gültigkeitsdauer eines Zertifikats beginnt, wenn `make-certificate` Wird ausgeführt. Sie müssen sicherstellen, dass der Management-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 Eingabeaufforderung-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 das CA-Paket herunter .pem Datei: 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 Erweiterung .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 Erweiterung .pem.

Beispiel: `storagegrid_certificate.pem`

Konfigurieren von S3- und Swift-API-Zertifikaten

Sie können das Serverzertifikat, das für S3- oder Swift-Client-Verbindungen zu Storage-

Nodes verwendet wird, ersetzen oder wiederherstellen, den veralteten Connection Load Balancer (CLB)-Service auf Gateway-Nodes oder zum Laden von Balancer-Endpunkten. Das benutzerdefinierte Ersatzserverzertifikat ist speziell für Ihr Unternehmen bestimmt.

Über diese Aufgabe

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

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

Nach Abschluss der Konfiguration auf dem Server müssen Sie möglicherweise auch das Grid CA-Zertifikat im S3- oder Swift-API-Client installieren, über den Sie je nach der von Ihnen verwendeten Root-Zertifizierungsstelle (CA) auf das System zugreifen können.



Um sicherzustellen, dass die Vorgänge nicht durch ein ausgefallenes Serverzertifikat unterbrochen werden, wird die Meldung **Ablauf des globalen Serverzertifikats für S3 und Swift API** ausgelöst, sobald das Zertifikat für den Stammserver abläuft. Wenn erforderlich, können Sie anzeigen, wann das aktuelle Zertifikat abläuft, indem Sie **KONFIGURATION Sicherheit Zertifikate** und das Ablaufdatum für das S3- und Swift-API-Zertifikat auf der Registerkarte Global auswählen.

Sie können ein benutzerdefiniertes S3- und Swift-API-Zertifikat hochladen oder erstellen.

Fügen Sie ein benutzerdefiniertes S3- und Swift-API-Zertifikat hinzu

Schritte

1. Wählen Sie **KONFIGURATION Sicherheit Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global S3 und Swift API Zertifikat**.
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 Schlüssel Datei (.key).



Private EC-Schlüssel müssen 224 Bit oder größer 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 Zertifikatsdetails aus, um die Metadaten und PEM für jedes benutzerdefinierte S3- und Swift-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 Erweiterung .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- und Swift-Client-Verbindungen verwendet.

Zertifikat wird generiert

Erstellen Sie die Serverzertifikatdateien.

a. Wählen Sie **Zertifikat erstellen**.

b. Geben Sie die Zertifikatsinformationen an:

- **Domain-Name:** Ein oder mehrere vollqualifizierte Domain-Namen, die in das Zertifikat enthalten sind. Verwenden Sie ein * als Platzhalter, um mehrere Domain-Namen darzustellen.
- **IP:** Eine oder mehrere IP-Adressen, die in das Zertifikat enthalten sind.
- **Betreff:** X.509 Betreff oder Distinguished Name (DN) des Zertifikatbesitzers.
- **Tage gültig:** Anzahl der Tage nach der Erstellung, dass das Zertifikat abläuft.

c. Wählen Sie **Erzeugen**.

d. Wählen Sie **Zertifikatsdetails** aus, um die Metadaten und das PEM für das benutzerdefinierte S3- und Swift-API-Zertifikat anzuzeigen, das erstellt wurde.

- 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 Erweiterung `.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- und Swift-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 einem Tag lang alle damit verbundenen Warnmeldungen zum Ablauf des Zertifikats löschen.

6. Aktualisieren Sie die Seite, um sicherzustellen, dass der Webbrowser aktualisiert wird.
7. Nachdem Sie ein benutzerdefiniertes S3- und Swift-API-Zertifikat hinzugefügt haben, zeigt die S3- und Swift-API-Zertifikatsseite detaillierte Zertifikatsinformationen für das verwendete S3- und Swift-API-Zertifikat an. + Sie können das PEM-Zertifikat nach Bedarf herunterladen oder kopieren.

Stellen Sie das S3- und Swift-API-Standardzertifikat wieder her

Sie können die Standardeinstellung für S3- und Swift-API-Zertifikat für S3- und Swift-Client-Verbindungen zu Storage-Nodes sowie zum veralteten CLB-Service auf Gateway-Nodes zurücksetzen. Sie können jedoch das S3- und Swift-API-Standardzertifikat für einen Load Balancer-Endpunkt nicht verwenden.

Schritte

1. Wählen Sie **KONFIGURATION Sicherheit Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global S3 und Swift API Zertifikat**.
3. Wählen Sie **Standard-Zertifikat verwenden**.

Wenn Sie die Standardversion des globalen S3- und Swift-API-Zertifikats wiederherstellen, werden die von Ihnen konfigurierten benutzerdefinierten Serverzertifikatsdateien gelöscht und können nicht aus dem System wiederhergestellt werden. Das S3- und Swift-API-Standardzertifikat wird für nachfolgende neue S3- und Swift-Client-Verbindungen zu Storage-Nodes und zum veralteten CLB-Service auf Gateway-Nodes verwendet.

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

Wenn Sie über Root-Zugriffsberechtigungen verfügen und das benutzerdefinierte S3- und Swift-API-Zertifikat für Endpoint-Verbindungen für den Load Balancer verwendet wurde, wird eine Liste mit Endpunkten für Load Balancer angezeigt, auf die über das Standard-S3- und Swift-API-Zertifikat nicht mehr zugegriffen werden kann. Gehen Sie zu [Konfigurieren von Load Balancer-Endpunkten](#) Zum Bearbeiten oder Entfernen der betroffenen Endpunkte.

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

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

Sie können Inhalte des S3- und Swift-API-Zertifikats zur anderen Verwendung speichern oder kopieren.

Schritte

1. Wählen Sie **KONFIGURATION Sicherheit Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global S3 und Swift API Zertifikat**.
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 das CA-Paket herunter .pem Datei: 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 Erweiterung .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 Erweiterung .pem.

Beispiel: `storagegrid_certificate.pem`

Verwandte Informationen

- [S3 verwenden](#)
- [Verwenden Sie Swift](#)
- [Konfigurieren von S3-API-Endpunkt-Domain-Namen](#)

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.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet [Unterstützter Webbrowser](#).
- Sie haben spezifische 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 **Raster CA** aus.
2. Laden Sie im Abschnitt **Zertifikat PEM** das Zertifikat herunter oder kopieren Sie es.

Laden Sie die Zertifikatdatei herunter

Laden Sie das Zertifikat herunter .pem Datei:

- 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 Erweiterung .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 Erweiterung .pem.

Beispiel: `storagegrid_certificate.pem`

Konfigurieren Sie StorageGRID-Zertifikate für FabricPool

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

Was Sie benötigen

- Sie haben spezifische Zugriffsberechtigungen.
- Sie sind mit einem bei Grid Manager 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](#).



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

Schritte

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

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

Weitere Informationen finden Sie unter [Allgemeine Verwendung des Sicherheitszertifikats](#) Und [Konfigurieren von benutzerdefinierten Serverzertifikaten](#).



Um sicherzustellen, dass die Vorgänge durch ein Serverzertifikat nicht unterbrochen werden, wird die Meldung **Ablauf der auf der Seite Zertifikate** konfigurierten Clientzertifikate ausgelöst, sobald das Serverzertifikat abläuft. Wenn erforderlich, können Sie anzeigen, wann das aktuelle Zertifikat abläuft, indem Sie **KONFIGURATION Sicherheit Zertifikate** und das Ablaufdatum des Clientzertifikats auf der Registerkarte Client auswählen.



Wenn Sie zum Schutz der Daten auf speziell konfigurierten Appliance-Nodes einen Verschlüsselungsmanagement-Server (KMS) verwenden, lesen Sie die spezifischen Informationen zu [Hochladen eines KMS-Clientzertifikats](#).

Was Sie benötigen

- Sie haben Root-Zugriffsberechtigung.
- Sie sind mit einem bei Grid Manager 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 Schlüssel 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

Befolgen Sie die Vorgehensweise für Ihr Szenario, um ein 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 die Option **KONFIGURATION Sicherheit Zertifikate** und wählen Sie dann die Registerkarte **Client** aus.
2. Wählen Sie **Hinzufügen**.

3. Geben Sie einen Zertifikatnamen ein, der mindestens 1 und nicht mehr als 32 Zeichen enthält.
4. Um mit Ihrem externen Monitoring-Tool auf die Prometheus-Kennzahlen zuzugreifen, wählen Sie **Prometheus erlauben**.
5. Laden Sie im Abschnitt **Zertifikatstyp** das Zertifikat der Verwaltungsschnittstelle hoch (.pem Datei):
 - a. Wählen Sie **Zertifikat hochladen** und dann **Weiter**.
 - b. Laden Sie die Zertifikatdatei der Managementoberfläche hoch (.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.

6. 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.

- f. 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.

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

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 zu aus [Konfigurieren Sie ein Zertifikat für die Managementoberfläche](#).
2. Wählen Sie im Grid Manager die Option **KONFIGURATION Sicherheit Zertifikate** und wählen Sie dann die Registerkarte **Client** aus.
3. Wählen Sie **Hinzufügen**.
4. Geben Sie einen Zertifikatnamen ein, der mindestens 1 und nicht mehr als 32 Zeichen enthält.
5. Um mit Ihrem externen Monitoring-Tool auf die Prometheus-Kennzahlen zuzugreifen, wählen Sie **Prometheus erlauben**.
6. Laden Sie im Abschnitt **Zertifikatstyp** das Clientzertifikat, den privaten Schlüssel und das CA-Paket hoch (.pem Dateien):
 - a. Wählen Sie **Zertifikat hochladen** und dann **Weiter**.
 - b. Laden Sie Client-Zertifikat, privaten Schlüssel und CA-Bundle-Dateien hoch (.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.

Die neuen Zertifikate werden auf der Registerkarte Client angezeigt.

7. 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 Domänennamen übereinstimmen, wie er im Zertifikat der Verwaltungsschnittstelle angezeigt wird.

- f. 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.

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

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 die Option **KONFIGURATION Sicherheit Zertifikate** und wählen Sie dann die Registerkarte **Client** aus.
2. Wählen Sie **Hinzufügen**.
3. Geben Sie einen Zertifikatnamen ein, der mindestens 1 und nicht mehr als 32 Zeichen enthält.
4. Um mit Ihrem externen Monitoring-Tool auf die Prometheus-Kennzahlen zuzugreifen, wählen Sie **Prometheus erlauben**.
5. Wählen Sie im Abschnitt **Zertifikatstyp** die Option **Zertifikat erstellen** aus.
6. Geben Sie die Zertifikatsinformationen an:
 - **Domain-Name**: Ein oder mehrere vollständig qualifizierte Domain-Namen des Admin-Knotens, der in das Zertifikat enthalten ist. Verwenden Sie ein * als Platzhalter, um mehrere Domain-Namen darzustellen.
 - **IP**: Eine oder mehrere Admin-Node-IP-Adressen, die in das Zertifikat enthalten sind.
 - **Betreff**: X.509 Betreff oder Distinguished Name (DN) des Zertifikatsbesitzers.
7. Wählen Sie **Erzeugen**.
8. 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 Erweiterung `.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.

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

Das neue Zertifikat wird auf der Registerkarte Client angezeigt.

10. Wählen Sie im Grid Manager die Option **KONFIGURATION Sicherheit Zertifikate** und wählen Sie dann die Registerkarte **Global** aus.
11. Wählen Sie **Management Interface Certificate** aus.
12. Wählen Sie **Benutzerdefiniertes Zertifikat verwenden**.
13. Laden Sie die Dateien Certificate.pem und private_key.pem aus dem hoch [Details zum Clientzertifikat](#) Schritt: Es ist nicht erforderlich, das CA-Paket hochzuladen.
 - a. Wählen Sie **Zertifikat hochladen** und dann **Weiter**.
 - b. Laden Sie jede Zertifikatdatei hoch (.pem).
 - c. Wählen Sie **Erstellen**, um das Zertifikat im Grid Manager zu speichern.

Das neue Zertifikat wird auf der Registerkarte Client angezeigt.

14. 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-Client-Zertifikat für beide ***CA Cert** und **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.

- f. 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.

Weitere 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** aus.

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, der mindestens 1 und nicht mehr als 32 Zeichen enthält.
5. Um mit Ihrem externen Monitoring-Tool auf die Prometheus-Kennzahlen zuzugreifen, wählen Sie **Prometheus erlauben**.
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** aus.

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 Clientzertifikats 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 Erweiterung .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 Zertifikattext, um ihn an anderer Stelle einzufügen.

- a. Wählen Sie **Zertifikat erstellen**.
- b. Geben Sie die Zertifikatsinformationen an:
 - **Domain-Name:** Ein oder mehrere vollqualifizierte Domain-Namen, die in das Zertifikat enthalten sind. Verwenden Sie ein * als Platzhalter, um mehrere Domain-Namen darzustellen.
 - **IP:** Eine oder mehrere IP-Adressen, die in das Zertifikat enthalten sind.
 - **Betreff:** X.509 Betreff oder Distinguished Name (DN) des Zertifikatbesitzers.
 - **Tage gültig:** Anzahl der Tage nach der Erstellung, dass das Zertifikat abläuft.

- 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 Erweiterung .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** aus.
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 das Zertifikat herunter .pem Datei:

- 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 Erweiterung .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 Erweiterung .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** aus.

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 © 2025 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.