



Sicherheitsmanagement

StorageGRID

NetApp

November 04, 2025

Inhalt

Sicherheitsmanagement	1
Sicherheit managen: Übersicht	1
Verschlüsselung managen	1
Verwalten von Zertifikaten	1
Konfigurieren von Verschlüsselungsmanagement-Servern	1
Proxy-Einstellungen verwalten	1
Kontrollieren Sie Firewalls	1
Prüfen Sie die StorageGRID Verschlüsselungsmethoden	1
Verwendung mehrerer Verschlüsselungsmethoden	4
Verwalten von Zertifikaten	4
Sicherheitszertifikate verwalten: Übersicht	5
Konfigurieren Sie Serverzertifikate	17
Konfigurieren Sie Client-Zertifikate	30
Konfigurieren Sie die Sicherheitseinstellungen	38
Verwalten Sie die TLS- und SSH-Richtlinie	38
Konfigurieren Sie die Netzwerk- und Objektsicherheit	41
Zeitlimit für Inaktivität des Browsers ändern	42
Konfigurieren von Verschlüsselungsmanagement-Servern	43
Key Management-Server konfigurieren: Übersicht	43
Überblick über die KMS- und Appliance-Konfiguration	44
Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers	47
Überlegungen für das Ändern des KMS für einen Standort	50
Konfigurieren Sie StorageGRID als Client im KMS	53
Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)	54
KMS-Details anzeigen	61
Verschlüsselte Nodes anzeigen	63
Bearbeiten eines Verschlüsselungsmanagement-Servers (KMS)	64
Entfernen eines Verschlüsselungsmanagement-Servers (KMS)	66
Proxy-Einstellungen verwalten	67
Konfigurieren Sie Speicher-Proxy-Einstellungen	67
Konfigurieren Sie die Administrator-Proxy-Einstellungen	69
Kontrollieren Sie Firewalls	70
Kontrolle des Zugriffs über externe Firewall	70
Interne Firewall-Kontrollen verwalten	71
Konfigurieren Sie die interne Firewall	75

Sicherheitsmanagement

Sicherheit managen: Übersicht

Sie können verschiedene Sicherheitseinstellungen über den Grid-Manager konfigurieren, um das StorageGRID-System zu sichern.

Verschlüsselung managen

StorageGRID bietet verschiedene Optionen zur Datenverschlüsselung. Sollten Sie ["Überprüfen Sie die verfügbaren Verschlüsselungsmethoden"](#) Ermitteln, welche die Anforderungen für die Datensicherung erfüllen

Verwalten von Zertifikaten

Das können Sie ["Konfigurieren und verwalten Sie die Serverzertifikate"](#) Wird für HTTP-Verbindungen oder die Clientzertifikate verwendet, mit denen eine Client- oder Benutzeridentität beim Server authentifiziert wird.

Konfigurieren von Verschlüsselungsmanagement-Servern

Mit einem ["Verschlüsselungsmanagement-Server"](#) Damit können Sie StorageGRID Daten selbst dann sichern, wenn eine Appliance aus dem Datacenter entfernt wird. Nachdem die Appliance-Volumes verschlüsselt wurden, können Sie nur auf Daten auf der Appliance zugreifen, wenn der Node mit dem KMS kommunizieren kann.



Um die Verschlüsselungsschlüsselverwaltung zu verwenden, müssen Sie während der Installation die Einstellung **Node Encryption** für jedes Gerät aktivieren, bevor das Gerät zum Grid hinzugefügt wird.

Proxy-Einstellungen verwalten

Wenn Sie S3-Platformservices oder Cloud Storage Pools verwenden, können Sie ein konfigurieren ["Storage-Proxyserver"](#) Zwischen Storage-Nodes und den externen S3 -Endpunkten. Wenn Sie AutoSupport Meldungen mit HTTPS oder HTTP senden, können Sie ein konfigurieren ["Admin-Proxyserver"](#) Zwischen Admin-Knoten und technischem Support.


Kontrollieren Sie Firewalls

Um die Sicherheit Ihres Systems zu erhöhen, können Sie den Zugriff auf StorageGRID-Administratorknoten steuern, indem Sie bestimmte Ports am öffnen oder schließen ["Externe Firewall"](#). Sie können auch den Netzwerkzugriff auf jeden Node steuern, indem Sie dessen konfigurieren ["Interne Firewall"](#). Sie können den Zugriff auf alle Ports außer den für Ihre Bereitstellung benötigten verhindern.

Prüfen Sie die StorageGRID Verschlüsselungsmethoden

StorageGRID bietet verschiedene Optionen zur Datenverschlüsselung. Anhand der verfügbaren Methoden können Sie ermitteln, welche Methoden Ihre Datensicherungsanforderungen erfüllen.

Die Tabelle bietet eine allgemeine Zusammenfassung der in StorageGRID verfügbaren

Verschlüsselungsoption	So funktioniert es	Gilt für
Verschlüsselungsmanagement-Server (KMS) in Grid Manager	Du " Konfigurieren eines Verschlüsselungsmanagement-Servers " Auf der StorageGRID-Website und " Aktivieren Sie die Node-Verschlüsselung für die Appliance ". Anschließend stellt ein Appliance-Node eine Verbindung mit dem KMS her, um einen Schlüsselverschlüsselungsschlüssel (KEK) anzufordern. Dieser Schlüssel verschlüsselt und entschlüsselt den Datenverschlüsselungsschlüssel (DEK) auf jedem Volume.	<p>Appliance-Knoten, deren Node Encryption während der Installation aktiviert ist. Alle Daten auf der Appliance sind gegen physischen Verlust oder aus dem Datacenter geschützt.</p> <div data-bbox="1075 575 1133 630">  </div> <p>Das Management von Verschlüsselungen mit einem KMS wird nur für Storage Nodes und Service-Appliances unterstützt.</p>
Laufwerkssicherheit in SANtricity System Manager	Wenn die Laufwerkssicherheitsfunktion für eine SG5700- oder SG6000-Speicheranwendung aktiviert ist, können Sie diese verwenden " SANtricity System Manager " So erstellen und verwalten Sie den Sicherheitsschlüssel. Der Schlüssel ist erforderlich, um auf die Daten auf den gesicherten Laufwerken zuzugreifen.	Storage-Appliances mit Full Disk Encryption (FDE)-Laufwerken oder FIPS-Laufwerken. Alle Daten auf den gesicherten Laufwerken sind vor physischem Verlust oder Entfernung aus dem Datacenter geschützt. Kann nicht mit Storage Appliances oder Service-Appliances verwendet werden.
Verschlüsselung gespeicherter Objekte	Sie aktivieren die " Verschlüsselung gespeicherter Objekte " Im Grid-Manager. Wenn diese Option aktiviert ist, werden alle neuen Objekte, die nicht auf Bucket-Ebene oder Objektebene verschlüsselt sind, bei der Aufnahme verschlüsselt.	<p>Neu aufgenommene S3- und Swift-Objektdaten</p> <p>Vorhandene gespeicherte Objekte werden nicht verschlüsselt. Objektmetadaten und andere sensible Daten werden nicht verschlüsselt.</p>

Verschlüsselungsoption	So funktioniert es	Gilt für
S3-Bucket-Verschlüsselung	Sie stellen eine PUT-Bucket-Verschlüsselungsanforderung bereit, um die Verschlüsselung für den Bucket zu aktivieren. Alle neuen Objekte, die nicht auf Objektebene verschlüsselt werden, werden bei der Aufnahme verschlüsselt.	<p>Nur neu aufgenommene S3-Objektdaten</p> <p>Für den Bucket muss eine Verschlüsselung angegeben werden. Vorhandene Bucket-Objekte werden nicht verschlüsselt. Objektmetadaten und andere sensible Daten werden nicht verschlüsselt.</p> <p>"Operationen auf Buckets"</p>
S3-Objektserverseitige Verschlüsselung (SSE)	Sie geben eine S3-Anforderung zum Speichern eines Objekts aus und schließen das ein <code>x-amz-server-side-encryption</code> Kopfzeile der Anfrage.	<p>Nur neu aufgenommene S3-Objektdaten</p> <p>Für das Objekt muss eine Verschlüsselung angegeben werden. Objektmetadaten und andere sensible Daten werden nicht verschlüsselt.</p> <p>StorageGRID verwaltet die Schlüssel.</p> <p>"Serverseitige Verschlüsselung"</p>
S3 Objektserverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln (SSE-C)	<p>Sie geben eine S3-Anforderung zum Speichern eines Objekts aus und enthalten drei Anfrageheader.</p> <ul style="list-style-type: none"> <code>x-amz-server-side-encryption-customer-algorithm</code> <code>x-amz-server-side-encryption-customer-key</code> <code>x-amz-server-side-encryption-customer-key-MD5</code> 	<p>Nur neu aufgenommene S3-Objektdaten</p> <p>Für das Objekt muss eine Verschlüsselung angegeben werden. Objektmetadaten und andere sensible Daten werden nicht verschlüsselt.</p> <p>Schlüssel werden außerhalb von StorageGRID gemanagt.</p> <p>"Serverseitige Verschlüsselung"</p>

Verschlüsselungsoption	So funktioniert es	Gilt für
Externe Volume- oder Datastore-Verschlüsselung	Sofern die Implementierungsplattform sie unterstützt, verwenden Sie eine Verschlüsselungsmethode außerhalb von StorageGRID, um ein gesamtes Volume oder Datastore zu verschlüsseln.	<p>Alle Objektdaten, Metadaten und Systemkonfigurationsdaten, wobei jedes Volume oder jeder Datastore verschlüsselt ist</p> <p>Eine externe Verschlüsselungsmethode bietet eine engere Kontrolle über Verschlüsselungsalgorithmen und -Schlüssel. Kann mit den anderen aufgeführten Methoden kombiniert werden.</p>
Objektverschlüsselung außerhalb von StorageGRID	Dabei kommt eine Verschlüsselungsmethode außerhalb von StorageGRID zum Einsatz, um Objektdaten und Metadaten zu verschlüsseln, bevor sie in StorageGRID aufgenommen werden.	<p>Nur Objektdaten und Metadaten (Systemkonfigurationsdaten sind nicht verschlüsselt).</p> <p>Eine externe Verschlüsselungsmethode bietet eine engere Kontrolle über Verschlüsselungsalgorithmen und -Schlüssel. Kann mit den anderen aufgeführten Methoden kombiniert werden.</p> <p>"Amazon Simple Storage Service – Developer Guide: Schutz von Daten mit Client-seitiger Verschlüsselung"</p>

Verwendung mehrerer Verschlüsselungsmethoden

Je nach Ihren Anforderungen können Sie mehrere Verschlüsselungsmethoden gleichzeitig verwenden.
Beispiel:

- Mit einem KMS können Appliance-Nodes geschützt werden. Außerdem kann mithilfe der Laufwerks sicherheitsfunktion in SANtricity System Manager die Daten „double verschlüsselte“ auf den Self-Encrypting Drives in denselben Appliances verschlüsselt werden.
- Sie können ein KMS verwenden, um Daten auf Appliance-Nodes zu sichern, und die Option gespeicherte Objektverschlüsselung verwenden, um alle Objekte bei der Aufnahme zu verschlüsseln.

Wenn nur ein kleiner Teil Ihrer Objekte eine Verschlüsselung erfordern, sollten Sie stattdessen die Verschlüsselung auf Bucket- oder Objektebene kontrollieren. Durch die Aktivierung diverser Verschlüsselungsstufen entstehen zusätzliche Performance-Kosten.

Verwalten von Zertifikaten

Sicherheitszertifikate verwalten: Übersicht

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, 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 **CONFIGURATION > Security > Certificates**.

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- 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 oder laden Sie das Zertifikat der Grid-Zertifizierungsstelle herunter"**, Aber man kann 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](#) Sichern der Verbindungen zwischen S3 und Swift Clients und dem StorageGRID Load Balancer-Service auf Gateway-Nodes und Admin-Nodes

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:

- ["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- 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:

- [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 nur Informationen zu anderen Zertifikaten anzeigen und darauf zugreifen, wenn Sie über die entsprechende Berechtigung verfügen.

Ihre Vorteile:

- ["Festlegen eines Cloud-Storage-Pool-Zertifikats für S3, C2S S3 oder Azure"](#)
- ["Legen Sie ein Zertifikat für Benachrichtigungen per E-Mail fest"](#)
- ["Geben Sie ein externes Syslog-Serverzertifikat an"](#)
- ["Verbindungszertifikate für Netzverbund 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 wählen Sie dann Management Interface Certificate aus	"Konfigurieren Sie Zertifikate für die Managementoberfläche"

S3- und Swift-API-Zertifikat

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	<p>Authentifizierung von sicheren S3- oder Swift-Client-Verbindungen zu einem Storage Node und Load Balancer-Endpunkten (optional)</p>	KONFIGURATION > Sicherheit > Zertifikate , wählen Sie die Registerkarte Global und wählen Sie dann S3 und Swift API Zertifikat aus	"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	<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 dann die Registerkarte Client wählen	"Konfigurieren Sie Client-Zertifikate"

Endpunkt-Zertifikat für Load Balancer

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	<p>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.</p> <p>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 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"

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"

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.	ALARME > 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 und dann externen Syslog-Server konfigurieren wählen	"Konfigurieren 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 Federation	<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 > Zugangskontrolle > Identitätsverbund	"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 > Zugangskontrolle > 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- 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.



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 dies tun ["Vorübergehendes Zurücksetzen auf die Standard-Sicherheitsrichtlinie"](#).

Weitere Informationen darüber, wie StorageGRID Client-Verbindungen für die REST-API sichert, finden Sie unter ["Sicherheit für S3-REST-API konfigurieren"](#) Oder ["Konfigurieren Sie die Sicherheit für Swift REST API"](#).

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 Warnmeldung **Ablauf des Serverzertifikats für die Managementoberfläche** ausgelöst, wenn dieses Serverzertifikat abläuft. Wenn erforderlich, können Sie anzeigen, wann das aktuelle Zertifikat abläuft, indem Sie **KONFIGURATION > Sicherheit > Zertifikate** auswählen und das Ablaufdatum für das Zertifikat der Verwaltungsschnittstelle auf der Registerkarte Global anzeigen.



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:

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 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 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 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 ersetzen oder wiederherstellen, das für S3- oder Swift-Clientverbindungen zu Storage Nodes oder zu Load Balancer-Endpunkten verwendet wird. 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 der Betrieb nicht durch ein fehlerhaftes Serverzertifikat unterbrochen wird, wird die Warnung **Ablauf des globalen Serverzertifikats für S3 und Swift API** ausgelöst, wenn das Stammserverzertifikat 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:

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 **Zertifikatdetails** 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 Wiederherstellung auf die Verwendung des standardmäßigen S3- und Swift-API-Zertifikats für S3- und Swift-Client-Verbindungen zu Storage Nodes durchführen. Sie können jedoch nicht das standardmäßige S3- und Swift-API-Zertifikat für einen Load Balancer-Endpoint 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 Serverzertifikatdateien gelöscht und können nicht vom System wiederhergestellt werden. Das standardmäßige S3- und Swift-API-Zertifikat wird für nachfolgende neue S3- und Swift-Client-Verbindungen zu Storage-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-REST-API VERWENDEN"](#)
- ["Nutzen Sie die Swift REST API"](#)
- ["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 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 das Zertifikat im Abschnitt **Zertifikat PEM** 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

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 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"](#).

Schritte

1. Konfigurieren Sie optional eine HA-Gruppe (High Availability, Hochverfügbarkeit) für die Verwendung von FabricPool.

2. Einen S3-Load-Balancer-Endpoint für FabricPool erstellen.

Wenn Sie einen HTTPS-Load-Balancer-Endpoint 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 von Client-Zertifikaten, die auf der Seite Zertifikate konfiguriert ist** ausgelöst, wenn dieses 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"](#).

Bevor Sie beginnen

- 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

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 die Option **KONFIGURATION > Sicherheit > Zertifikate** und dann die Registerkarte **Client** aus.
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 Zertifikatsdatei der Verwaltungsschnittstelle aus (.pem).
 - 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.

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 zu aus ["Konfigurieren Sie ein Zertifikat für die Managementoberfläche"](#).
2. Wählen Sie im Grid Manager die Option **KONFIGURATION > Sicherheit > Zertifikate** und dann die Registerkarte **Client** aus.
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 aus (.pem).
 - 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 die Option **KONFIGURATION > Sicherheit > Zertifikate** und dann die Registerkarte **Client** aus.
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 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.

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 die Option **KONFIGURATION > Sicherheit > Zertifikate** und wählen Sie dann die Registerkarte **Global** aus.

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 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 Zertifikatsdatei hoch (`.pem`).
- c. Wählen Sie **Erstellen**, um das Zertifikat im Grid Manager zu speichern.

Das neue Zertifikat wird auf der Registerkarte Client 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.

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.

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** 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 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 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.

Konfigurieren Sie die Sicherheitseinstellungen

Verwalten Sie die TLS- und SSH-Richtlinie

Die TLS- und SSH-Richtlinie legt fest, welche Protokolle und Chiffren verwendet werden, um sichere TLS-Verbindungen mit Clientanwendungen und sichere SSH-Verbindungen zu internen StorageGRID-Diensten herzustellen.

Die Sicherheitsrichtlinie steuert, wie TLS und SSH Daten in Bewegung verschlüsseln. Verwenden Sie im Allgemeinen die moderne Kompatibilitätsrichtlinie (Standard), es sei denn, Ihr System muss Common Criteria-konform sein oder Sie müssen andere Chiffren verwenden.



Einige StorageGRID-Dienste wurden nicht aktualisiert, um die Chiffren in diesen Richtlinien zu verwenden.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben die ["Root-Zugriffsberechtigung"](#).

Wählen Sie eine Sicherheitsrichtlinie aus

Schritte

1. Wählen Sie **CONFIGURATION > Security > Security settings**.

Auf der Registerkarte **TLS und SSH Policies** werden die verfügbaren Richtlinien angezeigt. Die derzeit aktive Richtlinie wird durch ein grünes Häkchen auf der Kachel „Richtlinie“ gekennzeichnet.



2. Lesen Sie die Kacheln, um mehr über die verfügbaren Richtlinien zu erfahren.

Richtlinie	Beschreibung
Moderne Kompatibilität (Standard)	Verwenden Sie die Standardrichtlinie, wenn Sie eine starke Verschlüsselung benötigen und wenn Sie keine besonderen Anforderungen haben. Diese Richtlinie ist mit den meisten TLS- und SSH-Clients kompatibel.
Kompatibilität mit älteren Systemen	Verwenden Sie diese Richtlinie, wenn Sie zusätzliche Kompatibilitätsoptionen für ältere Clients benötigen. Die zusätzlichen Optionen in dieser Richtlinie machen sie möglicherweise weniger sicher als die moderne Kompatibilitätsrichtlinie.
Gemeinsame Kriterien	Verwenden Sie diese Richtlinie, wenn Sie eine Common Criteria-Zertifizierung benötigen.
FIPS-strikt	Verwenden Sie diese Richtlinie, wenn Sie eine Common Criteria-Zertifizierung benötigen und das NetApp Cryptographic Security Module 3.0.0 für externe Client-Verbindungen zu Load Balancer-Endpunkten, Tenant Manager und Grid Manager verwenden müssen. Die Verwendung dieser Richtlinie kann die Performance beeinträchtigen.
Individuell	Erstellen Sie eine benutzerdefinierte Richtlinie, wenn Sie Ihre eigenen Chiffren anwenden müssen.

3. Um Details zu den Chiffren, Protokollen und Algorithmen der einzelnen Richtlinien anzuzeigen, wählen Sie **Details anzeigen**.

4. Um die aktuelle Richtlinie zu ändern, wählen Sie **Richtlinie verwenden**.

Ein grünes Häkchen erscheint neben **Aktuelle Richtlinie** auf der Policy-Kachel.

Erstellen Sie eine benutzerdefinierte Sicherheitsrichtlinie

Sie können eine benutzerdefinierte Richtlinie erstellen, wenn Sie Ihre eigenen Chiffren anwenden müssen.

Schritte

1. Wählen Sie auf der Kachel der Richtlinie, die der benutzerdefinierten Richtlinie, die Sie erstellen möchten, am ähnlichsten ist, **Details anzeigen** aus.

2. Wählen Sie **in Zwischenablage kopieren**, und wählen Sie dann **Abbrechen**.



3. Wählen Sie in der Kachel **Benutzerdefinierte Richtlinie** die Option **Konfigurieren und Verwenden** aus.
4. Fügen Sie die JSON ein, die Sie kopiert haben, und nehmen Sie alle erforderlichen Änderungen vor.
5. Wählen Sie **Richtlinie verwenden**.

Auf der Kachel „Benutzerdefinierte Richtlinie“ wird ein grünes Häkchen neben **Aktuelle Richtlinie** angezeigt.

6. Wählen Sie optional **Konfiguration bearbeiten**, um weitere Änderungen an der neuen benutzerdefinierten Richtlinie vorzunehmen.

Vorübergehendes Zurücksetzen auf die Standard-Sicherheitsrichtlinie

Wenn Sie eine benutzerdefinierte Sicherheitsrichtlinie konfiguriert haben, können Sie sich möglicherweise nicht beim Grid Manager anmelden, wenn die konfigurierte TLS-Richtlinie nicht mit dem kompatibel ist ["Serverzertifikat konfiguriert"](#).

Sie können vorübergehend auf die Standard-Sicherheitsrichtlinie zurücksetzen.

Schritte

1. Melden Sie sich bei einem Admin-Knoten an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@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 #.

2. Führen Sie den folgenden Befehl aus:

```
restore-default-cipher-configurations
```

3. Greifen Sie über einen Webbrowser auf den Grid Manager auf demselben Admin-Node zu.

4. Befolgen Sie die Schritte unter [Wählen Sie eine Sicherheitsrichtlinie aus](#) Um die Richtlinie erneut zu konfigurieren.

Konfigurieren Sie die Netzwerk- und Objektsicherheit

Sie können die Netzwerk- und Objektsicherheit so konfigurieren, dass gespeicherte Objekte verschlüsselt, bestimmte S3- und Swift-Anforderungen verhindert oder Client-Verbindungen zu Storage-Nodes HTTP anstelle von HTTPS verwenden.

Verschlüsselung gespeicherter Objekte

Die gespeicherte Objektverschlüsselung ermöglicht die Verschlüsselung aller Objektdaten bei der Aufnahme über S3. Gespeicherte Objekte werden standardmäßig nicht verschlüsselt, aber Sie können Objekte mit dem AES-128- oder AES-256-Verschlüsselungsalgorithmus verschlüsseln. Wenn Sie die Einstellung aktivieren, werden alle neu aufgenommenen Objekte verschlüsselt, aber es werden keine Änderungen an vorhandenen gespeicherten Objekten vorgenommen. Wenn Sie die Verschlüsselung deaktivieren, bleiben derzeit verschlüsselte Objekte verschlüsselt, neu aufgenommene Objekte werden jedoch nicht verschlüsselt.

Die Einstellung für die Verschlüsselung gespeicherter Objekte ist nur für S3-Objekte anwendbar, die nicht durch Verschlüsselung auf Bucket-Ebene oder Objekt-Ebene verschlüsselt wurden.

Weitere Informationen zu Verschlüsselungsmethoden von StorageGRID finden Sie unter "[Prüfen Sie die StorageGRID Verschlüsselungsmethoden](#)".

Client-Änderung verhindern

Die Einstellung „Client-Änderung verhindern“ ist eine systemweite Einstellung. Wenn die Option **Client-Änderung verhindern** ausgewählt ist, werden die folgenden Anfragen abgelehnt.

S3-REST-API

- Bucket-Anforderungen löschen
- Alle Anforderungen, die das Ändern von Daten eines vorhandenen Objekts, benutzerdefinierter Metadaten oder S3-Objekt-Tagging zum Einsatz kommen

Swift REST API

- Container-Anforderungen löschen
- Anträge zum Ändern vorhandener Objekte. Beispielsweise werden folgende Vorgänge verweigert: Put Overwrite, Delete, Metadata Update usw.

Aktivieren Sie HTTP für Storage Node-Verbindungen

Standardmäßig verwenden Clientanwendungen das HTTPS-Netzwerkprotokoll für alle direkten Verbindungen zu Storage-Nodes. Optional können Sie HTTP für diese Verbindungen aktivieren, z. B. beim Testen eines nicht produktiven Grids.

Verwenden Sie HTTP für Storage-Node-Verbindungen nur, wenn S3- und Swift-Clients HTTP-Verbindungen direkt zu Storage-Nodes herstellen müssen. Sie müssen diese Option nicht für Clients verwenden, die nur HTTPS-Verbindungen verwenden, oder für Clients, die eine Verbindung zum Load Balancer-Dienst herstellen (weil Sie dies können "[Konfigurieren Sie jeden Endpunkt der Lastverteilung](#)" Zur Verwendung von HTTP oder HTTPS).

Siehe "[Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen](#)" Um zu erfahren, welche Ports S3 und Swift-Clients bei der Verbindung zu Storage-Nodes über HTTP oder HTTPS verwenden.

Wählen Sie Optionen aus

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben Root-Zugriffsberechtigung.

Schritte

1. Wählen Sie **CONFIGURATION > Security > Security settings**.
2. Wählen Sie die Registerkarte **Netzwerk und Objekte**.
3. Verwenden Sie für die Verschlüsselung gespeicherter Objekte die Einstellung **None** (Standard), wenn Sie keine Verschlüsselung gespeicherter Objekte wünschen, oder wählen Sie **AES-128** oder **AES-256**, um gespeicherte Objekte zu verschlüsseln.
4. Wählen Sie optional **Client-Änderung verhindern**, wenn Sie S3- und Swift-Clients daran hindern möchten, spezifische Anforderungen zu stellen.



Wenn Sie diese Einstellung ändern, dauert es etwa eine Minute, bis die neue Einstellung angewendet wird. Der konfigurierte Wert wird für Performance und Skalierung zwischengespeichert.

5. Wählen Sie optional **HTTP für Storage Node-Verbindungen aktivieren**, wenn Clients direkt mit Storage Nodes verbunden sind und Sie HTTP-Verbindungen verwenden möchten.



Gehen Sie vorsichtig vor, wenn Sie HTTP für ein Produktions-Grid aktivieren, da die Anforderungen unverschlüsselt gesendet werden.

6. Wählen Sie **Speichern**.

Zeitlimit für Inaktivität des Browsers ändern

Sie können steuern, ob Grid Manager und Tenant Manager-Benutzer abgemeldet werden, wenn sie länger als eine bestimmte Zeit inaktiv sind.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben Root-Zugriffsberechtigung.

Über diese Aufgabe

Das Zeitlimit für die Inaktivität des Browsers beträgt standardmäßig 15 Minuten. Wenn der Browser eines Benutzers für diese Zeit nicht aktiv ist, wird der Benutzer abgemeldet.

Bei Bedarf können Sie die Sperrzeit erhöhen oder verringern, indem Sie die Option * Inaktive Benutzer abmelden nach* einstellen.

Das Zeitlimit für die Inaktivität des Browsers wird auch durch Folgendes gesteuert:

- Ein separater, nicht konfigurierbarer StorageGRID-Timer, der für die Systemsicherheit enthalten ist. Standardmäßig läuft das Authentifizierungs-Token jedes Benutzers 16 Stunden nach der Anmeldung des

Benutzers ab. Wenn die Authentifizierung eines Benutzers abläuft, wird dieser Benutzer automatisch abgemeldet, auch wenn das Zeitlimit für die Inaktivität des Browsers deaktiviert ist oder der Wert für das Browsertimeout nicht erreicht wurde. Um das Token zu erneuern, muss sich der Benutzer erneut anmelden.

- Timeout-Einstellungen für den Identitäts-Provider, vorausgesetzt, Single Sign-On (SSO) ist für StorageGRID aktiviert.

Wenn SSO aktiviert ist und der Browser eines Benutzers eine Zeitdauer ausläuft, muss der Benutzer seine SSO-Anmeldeinformationen erneut eingeben, um erneut auf StorageGRID zuzugreifen. Siehe ["Konfigurieren Sie Single Sign-On"](#).

Schritte

1. Wählen Sie **CONFIGURATION > Security > Security settings**.
2. Wählen Sie die Registerkarte **Browser Inaktivität Timeout**.
3. Geben Sie im Feld **Abmelden inaktiver Benutzer nach** einen Browser-Timeout-Zeitraum zwischen 60 Sekunden und 7 Tagen an.

Sie können die Zeitüberschreitung des Browsers in Sekunden, Minuten, Stunden oder Tagen angeben.

4. Wählen Sie **Speichern**. Wenn ein Browser für die angegebene Zeit inaktiv ist, wird der Benutzer vom Grid Manager oder Tenant Manager abgemeldet.

Die neue Einstellung hat keine Auswirkung auf die derzeit angemeldeten Benutzer. Benutzer müssen sich erneut anmelden oder ihre Browser aktualisieren, damit die neue Timeout-Einstellung wirksam wird.

Konfigurieren von Verschlüsselungsmanagement-Servern

Key Management-Server konfigurieren: Übersicht

Sie können einen oder mehrere externe Verschlüsselungsmanagement-Server (KMS) konfigurieren, um die Daten auf speziell konfigurierten Appliance-Nodes zu schützen.

Was ist ein KMS (Key Management Server)?

Ein Verschlüsselungsmanagement-Server (KMS) ist ein externes Drittanbietersystem, das mithilfe des Key Management Interoperability Protocol (KMIP) Verschlüsselungen für die StorageGRID Appliance-Nodes am zugehörigen StorageGRID Standort bereitstellt.

Sie können einen oder mehrere Schlüsselverwaltungsserver verwenden, um die Knotenverschlüsselungsschlüssel für alle StorageGRID Appliance-Knoten zu verwalten, deren **Node-Verschlüsselung**-Einstellung während der Installation aktiviert ist. Durch den Einsatz von Verschlüsselungsmanagement-Servern mit diesen Appliance-Nodes können Sie Ihre Daten selbst dann schützen, wenn eine Appliance aus dem Datacenter entfernt wird. Nachdem die Appliance-Volumes verschlüsselt wurden, können Sie nur auf Daten auf der Appliance zugreifen, wenn der Node mit dem KMS kommunizieren kann.

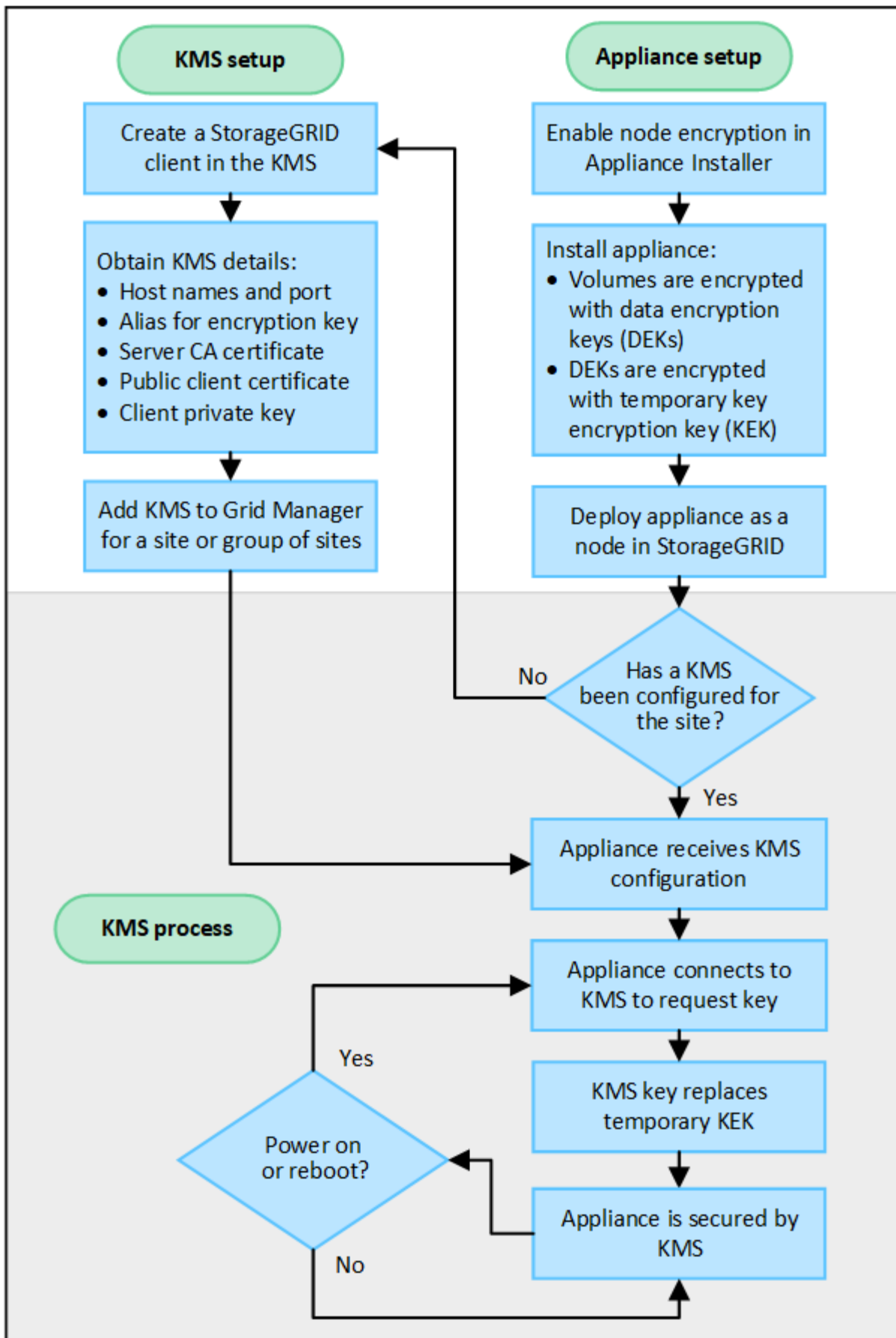


StorageGRID erstellt oder verwaltet keine externen Schlüssel, die zur Verschlüsselung und Entschlüsselung von Appliance-Nodes verwendet werden. Wenn Sie Vorhaben, einen externen Verschlüsselungsmanagementserver zum Schutz von StorageGRID-Daten zu verwenden, müssen Sie wissen, wie Sie diesen Server einrichten, und wissen, wie Sie die Verschlüsselungsschlüssel managen. Die Ausführung wichtiger Managementaufgaben geht über diesen Anweisungen hinaus. Wenn Sie Hilfe benötigen, lesen Sie die Dokumentation für Ihren zentralen Managementserver, oder wenden Sie sich an den technischen Support.

Überblick über die KMS- und Appliance-Konfiguration

Bevor der Verschlüsselungsmanagement-Server (KMS) die StorageGRID-Daten auf Appliance-Nodes sichern kann, müssen zwei Konfigurationsaufgaben durchgeführt werden: Ein oder mehrere KMS-Server einrichten und die Node-Verschlüsselung für die Appliance-Nodes aktivieren. Wenn diese beiden Konfigurationsaufgaben abgeschlossen sind, erfolgt automatisch der Verschlüsselungsmanagementprozess.

Das Flussdiagramm zeigt die grundlegenden Schritte bei der Verwendung eines KMS zur Sicherung von StorageGRID-Daten auf Appliance-Nodes.



Das Flussdiagramm zeigt die parallele Einrichtung von KMS und die Einrichtung der Appliance. Sie können

jedoch die Verschlüsselungsmanagement-Server je nach Ihren Anforderungen vor oder nach Aktivierung der Node-Verschlüsselung für neue Appliance-Nodes einrichten.

Einrichten des Verschlüsselungsmanagement-Servers (KMS)

Die Einrichtung eines Schlüsselverwaltungsservers umfasst die folgenden grundlegenden Schritte.

Schritt	Siehe
Greifen Sie auf die KMS-Software zu und fügen Sie jedem KMS- oder KMS-Cluster einen Client für StorageGRID hinzu.	"Konfigurieren Sie StorageGRID als Client im KMS"
Erhalten Sie die erforderlichen Informationen für den StorageGRID-Client auf dem KMS.	"Konfigurieren Sie StorageGRID als Client im KMS"
Fügen Sie den KMS dem Grid Manager hinzu, weisen Sie ihn einer einzelnen Site oder einer Standardgruppe von Standorten zu, laden Sie die erforderlichen Zertifikate hoch und speichern Sie die KMS-Konfiguration.	"Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)"

Richten Sie das Gerät ein

Die Einrichtung eines Appliance-Nodes für die KMS-Nutzung umfasst die folgenden grundlegenden Schritte.

1. Verwenden Sie während der Hardware-Konfigurationsphase der Appliance-Installation das Installationsprogramm von StorageGRID Appliance, um die Einstellung **Node-Verschlüsselung** für die Appliance zu aktivieren.



Sie können die Einstellung **Node Encryption** nicht aktivieren, nachdem eine Appliance zum Grid hinzugefügt wurde, und Sie können keine externe Schlüsselverwaltung für Geräte verwenden, für die keine Knotenverschlüsselung aktiviert ist.

2. Führen Sie das Installationsprogramm für die StorageGRID-Appliance aus. Während der Installation wird jedem Appliance-Volume ein zufälliger Datenverschlüsselungsschlüssel (random Data Encryption Key, DEK) zugewiesen:
 - Die DEKs werden verwendet, um die Daten auf jedem Volume zu verschlüsseln. Diese Schlüssel werden mit der Linux Unified Key Setup (LUKS)-Festplattenverschlüsselung im Betriebssystem der Appliance generiert und können nicht geändert werden.
 - Jede einzelne DEK wird durch einen Master Key Encryption Key (KEK) verschlüsselt. Bei der ersten KEK handelt es sich um einen temporären Schlüssel, der die DEKs verschlüsselt, bis das Gerät eine Verbindung mit dem KMS herstellen kann.
3. Fügen Sie den Appliance-Node StorageGRID hinzu.

Siehe ["Aktivieren Sie die Node-Verschlüsselung"](#) Entsprechende Details.

Verschlüsselungsmanagementprozess (wird automatisch durchgeführt)

Die Verschlüsselung des Verschlüsselungsmanagement umfasst die folgenden grundlegenden Schritte, die automatisch durchgeführt werden.

1. Wenn Sie eine Appliance installieren, bei der die Node-Verschlüsselung im Grid aktiviert ist, bestimmt StorageGRID, ob für den Standort, der den neuen Node enthält, eine KMS-Konfiguration vorhanden ist.
 - Wenn bereits ein KMS für den Standort konfiguriert wurde, erhält die Appliance die KMS-Konfiguration.
 - Wenn ein KMS für den Standort noch nicht konfiguriert wurde, werden die Daten auf der Appliance weiterhin durch die temporäre KEK verschlüsselt, bis Sie einen KMS für den Standort konfigurieren und die Appliance die KMS-Konfiguration erhält.
2. Die Appliance verwendet die KMS-Konfiguration, um eine Verbindung zum KMS herzustellen und einen Verschlüsselungsschlüssel anzufordern.
3. Der KMS sendet einen Verschlüsselungsschlüssel an die Appliance. Der neue Schlüssel des KMS ersetzt die temporäre KEK und wird nun zur Verschlüsselung und Entschlüsselung der DEKs für die Appliance-Volumes verwendet.



Alle Daten, die vor der Verbindung des verschlüsselten Appliance-Nodes mit dem konfigurierten KMS vorhanden sind, werden mit einem temporären Schlüssel verschlüsselt. Die Appliance-Volumes sollten jedoch erst dann als vor Entfernung aus dem Datacenter geschützt betrachtet werden, wenn der temporäre Schlüssel durch den KMS-Schlüssel ersetzt wird.

4. Wenn die Appliance eingeschaltet oder neu gestartet wird, stellt sie eine Verbindung zum KMS her, um den Schlüssel anzufordern. Der Schlüssel, der im flüchtigen Speicher gespeichert ist, kann einen Stromausfall oder einen Neustart nicht überleben.

Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers

Bevor Sie einen externen KMS (Key Management Server) konfigurieren, müssen Sie die Überlegungen und Anforderungen verstehen.

Was sind die KMIP-Anforderungen?

StorageGRID unterstützt KMIP Version 1.4.

"Spezifikation Des Key Management Interoperability Protocol Version 1.4"

Für die Kommunikation zwischen den Appliance-Nodes und dem konfigurierten KMS werden sichere TLS-Verbindungen verwendet. StorageGRID unterstützt die folgenden TLS v1.2-Chiffren für KMIP:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Sie müssen sicherstellen, dass jeder Appliance-Node, der Node-Verschlüsselung verwendet, Netzwerkzugriff auf den für den Standort konfigurierten KMS- oder KMS-Cluster hat.

Die Netzwerk-Firewall-Einstellungen müssen es jedem Appliance-Node ermöglichen, über den Port zu kommunizieren, der für KMIP-Kommunikation (Key Management Interoperability Protocol) verwendet wird. Der KMIP-Standardport ist 5696.

Welche Appliances werden unterstützt?

Sie können einen Schlüsselverwaltungsserver (KMS) verwenden, um Verschlüsselungsschlüssel für jede StorageGRID-Appliance in Ihrem Grid zu verwalten, auf der die Einstellung **Node-Verschlüsselung** aktiviert

ist. Diese Einstellung kann nur während der Hardware-Konfigurationsphase der Appliance-Installation mithilfe des StorageGRID Appliance Installer aktiviert werden.



Nach dem Hinzufügen einer Appliance zum Grid kann die Node-Verschlüsselung nicht aktiviert werden. Zudem kann kein externes Verschlüsselungsmanagement für Appliances verwendet werden, bei denen die Node-Verschlüsselung nicht aktiviert ist.

Sie können das konfigurierte KMS für StorageGRID-Appliances und Appliance-Nodes verwenden.

Sie können das konfigurierte KMS nicht für softwarebasierte (nicht-Appliance-)Knoten verwenden, einschließlich der folgenden:

- Als Virtual Machines (VMs) implementierte Nodes
- Nodes, die in Container-Engines auf Linux Hosts implementiert sind

Auf diesen anderen Plattformen implementierte Nodes können Verschlüsselung außerhalb von StorageGRID auf Datenspeicher- oder Festplattenebene verwenden.

Wann sollte ich wichtige Management-Server konfigurieren?

Bei einer neuen Installation sollten Sie in der Regel einen oder mehrere Schlüsselverwaltungsserver im Grid Manager einrichten, bevor Sie Mandanten erstellen. Diese Reihenfolge stellt sicher, dass die Nodes geschützt sind, bevor Objektdaten auf ihnen gespeichert werden.

Sie können die Schlüsselverwaltungsserver im Grid Manager vor oder nach der Installation der Appliance-Knoten konfigurieren.

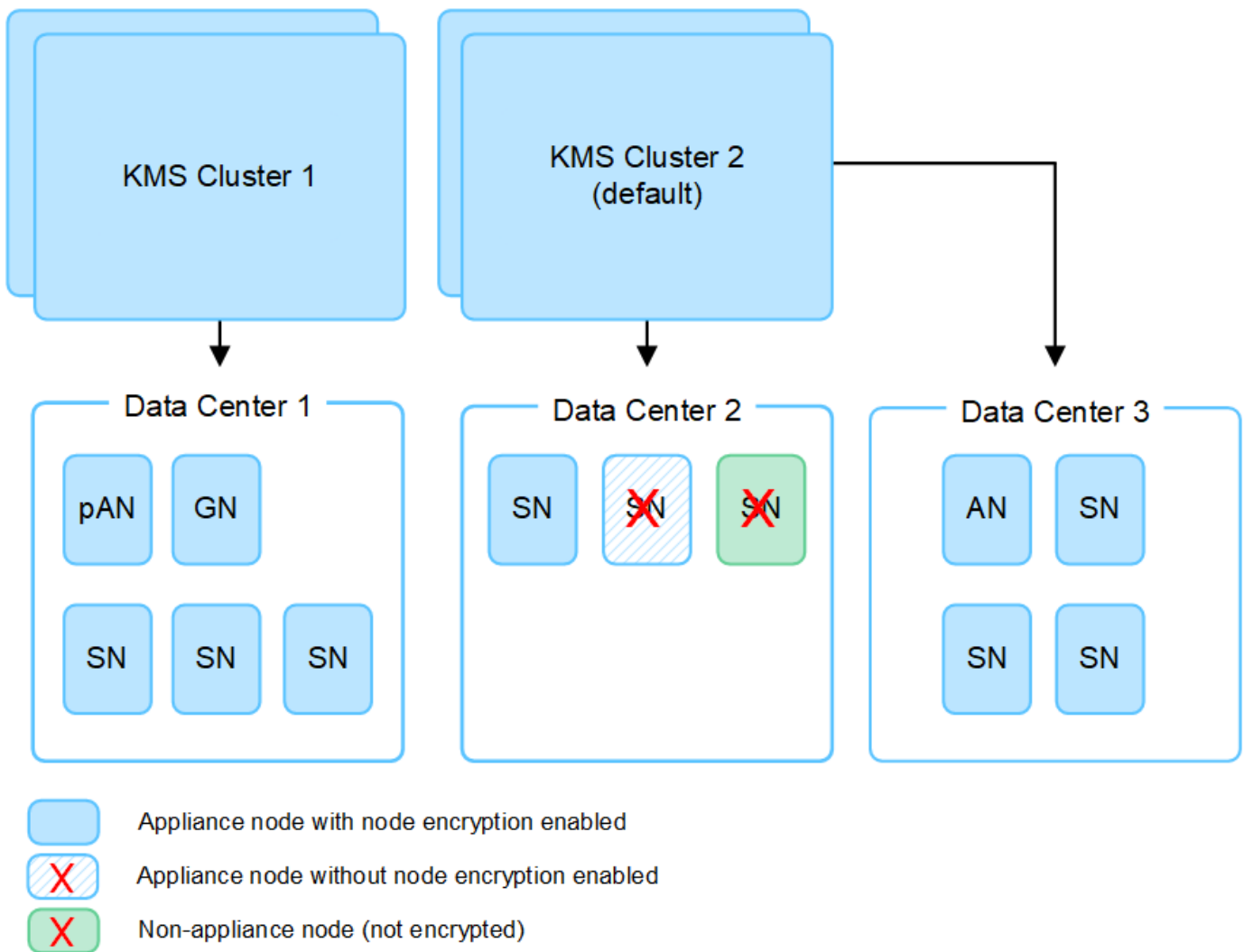
Wie viele wichtige Management Server brauche ich?

Sie können einen oder mehrere externe Verschlüsselungsmanagementserver konfigurieren, um die Appliance-Nodes in Ihrem StorageGRID-System Verschlüsselungen bereitzustellen. Jeder KMS stellt den StorageGRID Appliance-Nodes an einem einzelnen Standort oder einer Gruppe von Standorten einen einzelnen Verschlüsselungsschlüssel zur Verfügung.

StorageGRID unterstützt die Verwendung von KMS-Clustern. Jeder KMS-Cluster enthält mehrere replizierte Verschlüsselungsmanagement-Server, die Konfigurationseinstellungen und Verschlüsselungen teilen. Die Verwendung von KMS-Clustern für das Verschlüsselungsmanagement wird empfohlen, da dadurch die Failover-Funktionen einer Hochverfügbarkeitskonfiguration verbessert werden.

Nehmen Sie beispielsweise an, Ihr StorageGRID System verfügt über drei Datacenter-Standorte. Sie können ein KMS-Cluster konfigurieren, um allen Appliance-Nodes in Datacenter 1 und einem zweiten KMS-Cluster einen Schlüssel für alle Appliance-Nodes an allen anderen Standorten bereitzustellen. Wenn Sie den zweiten KMS-Cluster hinzufügen, können Sie einen Standard-KMS für Datacenter 2 und Datacenter 3 konfigurieren.

Beachten Sie, dass Sie kein KMS für nicht-Appliance-Knoten oder für alle Appliance-Knoten verwenden können, für die die Einstellung **Node Encryption** während der Installation nicht aktiviert war.



Was passiert, wenn eine Taste gedreht wird?

Als bewährte Sicherheitsmethode sollten Sie den Verschlüsselungsschlüssel, der von jedem konfigurierten KMS verwendet wird, regelmäßig drehen.

Wenn Sie den Verschlüsselungsschlüssel drehen, verwenden Sie die KMS-Software, um von der letzten verwendeten Version des Schlüssels auf eine neue Version desselben Schlüssels zu drehen. Drehen Sie nicht zu einer ganz anderen Taste.



Versuchen Sie niemals, einen Schlüssel zu drehen, indem Sie den Schlüsselnamen (Alias) für den KMS im Grid Manager ändern. Drehen Sie stattdessen den Schlüssel, indem Sie die Schlüsselversion in der KMS-Software aktualisieren. Verwenden Sie denselben Schlüssel-Alias für neue Schlüssel, wie sie für vorherige Schlüssel verwendet wurden. Wenn Sie den Schlüssel-Alias für einen konfigurierten KMS ändern, kann StorageGRID Ihre Daten möglicherweise nicht entschlüsseln.

Wenn die neue Schlüsselversion verfügbar ist:

- Die Appliance wird automatisch auf die verschlüsselten Appliance-Nodes am Standort oder an den dem KMS zugeordneten Standorten verteilt. Die Verteilung sollte innerhalb einer Stunde erfolgen, wenn der Schlüssel gedreht wird.

- Wenn der Node der verschlüsselten Appliance offline ist, wenn die neue Schlüsselversion verteilt ist, erhält der Node den neuen Schlüssel, sobald er neu gebootet wird.
- Wenn die neue Schlüsselversion aus irgendeinem Grund nicht zur Verschlüsselung von Appliance-Volumes verwendet werden kann, wird der Alarm **KMS-Schlüsselrotation fehlgeschlagen** für den Appliance-Knoten ausgelöst. Möglicherweise müssen Sie sich an den technischen Support wenden, um Hilfe bei der Lösung dieses Alarms zu erhalten.

Kann ich einen Appliance-Knoten nach der Verschlüsselung wiederverwenden?

Wenn Sie eine verschlüsselte Appliance in einem anderen StorageGRID System installieren müssen, müssen Sie zuerst den Grid-Node außer Betrieb nehmen, um Objektdaten auf einen anderen Node zu verschieben. Anschließend können Sie das Installationsprogramm der StorageGRID-Appliance für verwenden "[Löschen Sie die KMS-Konfiguration](#)". Durch das Löschen der KMS-Konfiguration wird die **Node Encryption**-Einstellung deaktiviert und die Zuordnung zwischen dem Appliance-Knoten und der KMS-Konfiguration für den StorageGRID-Standort wird aufgehoben.



Der Zugriff auf den KMS-Verschlüsselungsschlüssel ist ausgeschlossen, dass alle Daten, die auf der Appliance verbleiben, nicht mehr zugänglich sind und dauerhaft gesperrt werden.

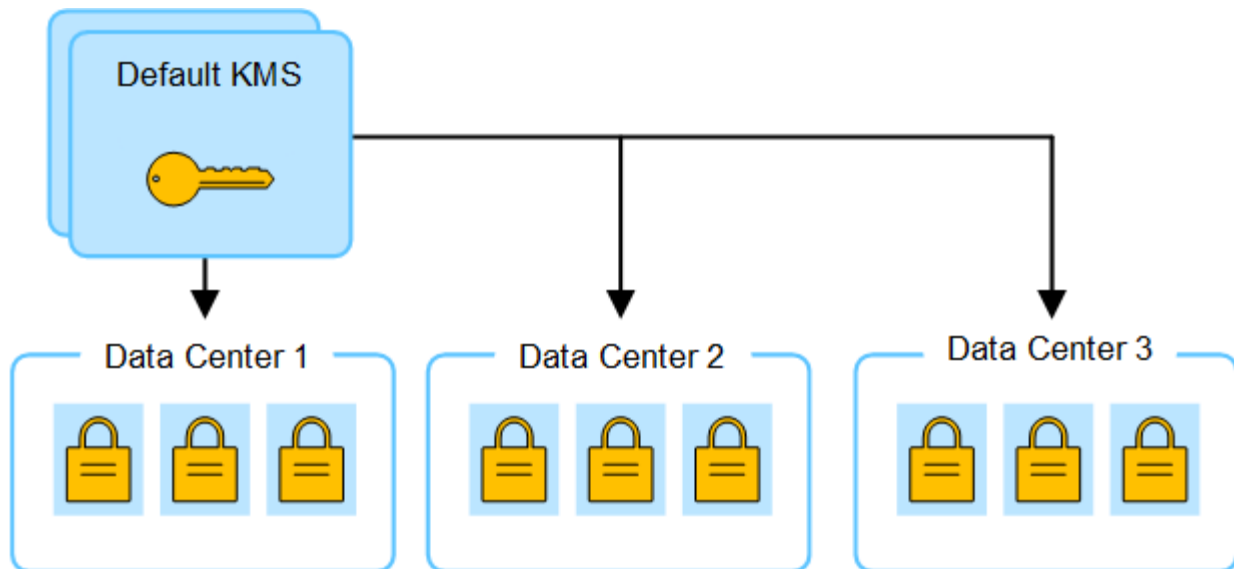
Überlegungen für das Ändern des KMS für einen Standort

Jeder Verschlüsselungsmanagement-Server (KMS) oder KMS-Cluster gewährt allen Appliance-Nodes an einem einzelnen Standort oder einer Gruppe von Standorten einen Verschlüsselungsschlüssel. Wenn Sie ändern müssen, welcher KMS für einen Standort verwendet wird, müssen Sie den Verschlüsselungsschlüssel möglicherweise von einem KMS auf einen anderen kopieren.

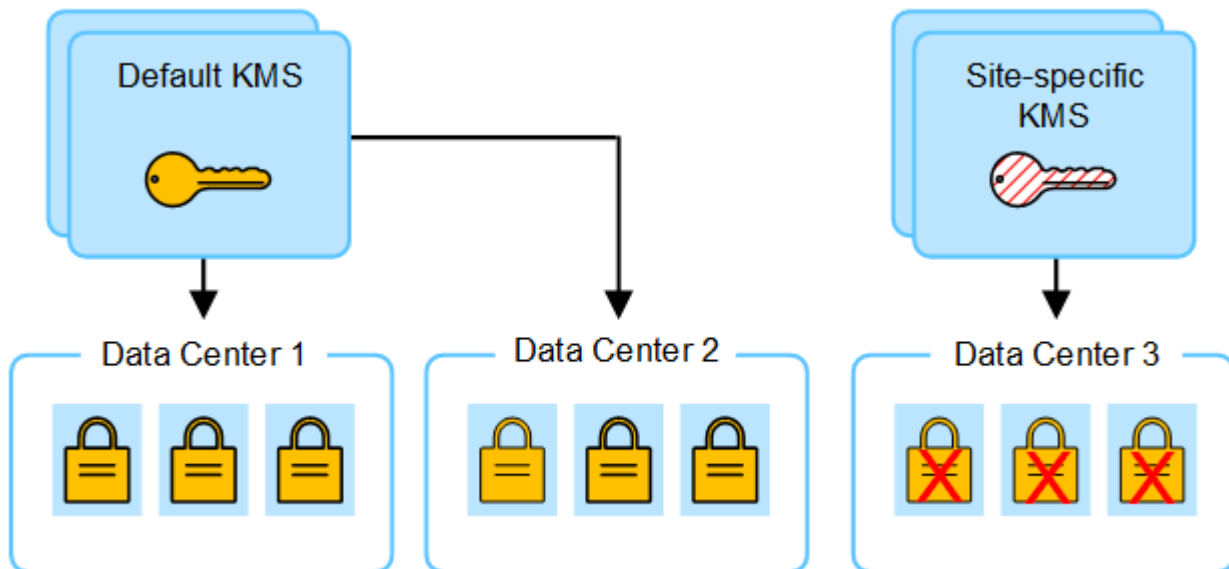
Wenn Sie den KMS ändern, der für einen Standort verwendet wird, müssen Sie sicherstellen, dass die zuvor verschlüsselten Appliance-Nodes an diesem Standort mit dem auf dem neuen KMS gespeicherten Schlüssel entschlüsselt werden können. In einigen Fällen müssen Sie möglicherweise die aktuelle Version des Verschlüsselungsschlüssels vom ursprünglichen KMS auf den neuen KMS kopieren. Sie müssen sicherstellen, dass der KMS über den richtigen Schlüssel verfügt, um die verschlüsselten Appliance-Nodes am Standort zu entschlüsseln.

Beispiel:

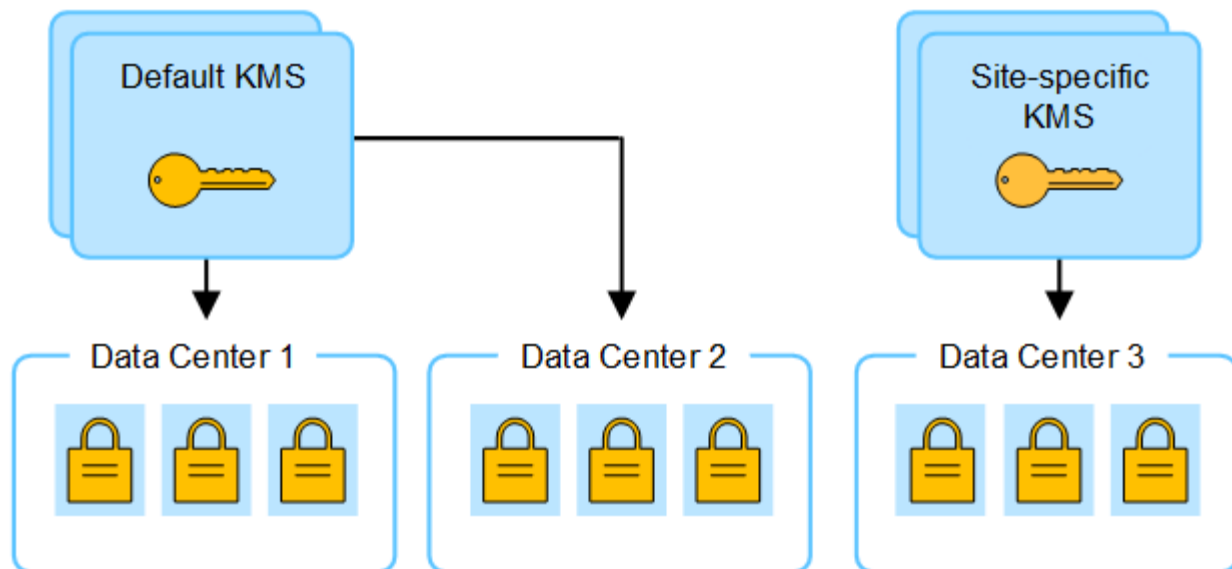
1. Sie konfigurieren zunächst ein Standard-KMS, das für alle Standorte gilt, die kein dediziertes KMS haben.
2. Wenn der KMS gespeichert wird, stellen alle Appliance-Nodes, deren **Node Encryption**-Einstellung aktiviert ist, eine Verbindung zum KMS her und fordern den Verschlüsselungsschlüssel an. Dieser Schlüssel wird verwendet, um die Appliance-Nodes an allen Standorten zu verschlüsseln. Dieser Schlüssel muss auch verwendet werden, um diese Geräte zu entschlüsseln.



3. Sie entscheiden, einen standortspezifischen KMS für einen Standort hinzuzufügen (Datacenter 3 in der Abbildung). Da die Appliance-Nodes jedoch bereits verschlüsselt sind, tritt ein Validierungsfehler auf, wenn Sie versuchen, die Konfiguration für den standortspezifischen KMS zu speichern. Der Fehler tritt auf, weil der standortspezifische KMS nicht über den korrekten Schlüssel verfügt, um die Knoten an diesem Standort zu entschlüsseln.



4. Um das Problem zu beheben, kopieren Sie die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS auf den neuen KMS. (Technisch kopieren Sie den Originalschlüssel in einen neuen Schlüssel mit dem gleichen Alias. Der ursprüngliche Schlüssel wird zu einer früheren Version des neuen Schlüssels.) Der standortspezifische KMS hat jetzt den richtigen Schlüssel zur Entschlüsselung der Appliance-Nodes in Datacenter 3, sodass er in StorageGRID gespeichert werden kann.



Anwendungsfälle für die Änderung, welcher KMS für eine Site verwendet wird

Die Tabelle fasst die erforderlichen Schritte für die häufigsten Fälle zur Änderung des KMS für einen Standort zusammen.

Anwendungsfall zum Ändern des KMS einer Site	Erforderliche Schritte
Sie haben einen oder mehrere Site-spezifische KMS-Einträge, und Sie möchten einen von ihnen als Standard-KMS verwenden.	<p>Bearbeiten Sie den Site-spezifischen KMS. Wählen Sie im Feld verwaltet Schlüssel für die Option Sites, die nicht von einem anderen KMS verwaltet werden (Standard KMS). Der Site-spezifische KMS wird jetzt als Standard-KMS verwendet. Sie gilt für alle Standorte, die kein dediziertes KMS haben.</p> <p>"Bearbeiten eines Verschlüsselungsmanagement-Servers (KMS)"</p>
Sie haben einen Standard-KMS, und Sie fügen eine neue Site in einer Erweiterung hinzu. Sie möchten nicht das Standard-KMS für den neuen Standort verwenden.	<ol style="list-style-type: none"> 1. Wenn die Appliance-Nodes auf dem neuen Standort bereits durch den Standard-KMS verschlüsselt wurden, kopieren Sie mithilfe der KMS-Software die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS auf einen neuen KMS. 2. Fügen Sie mithilfe des Grid-Managers den neuen KMS hinzu und wählen Sie die Site aus. <p>"Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)"</p>
Sie möchten, dass der KMS für eine Site einen anderen Server verwendet.	<ol style="list-style-type: none"> 1. Wenn die Appliance-Nodes am Standort bereits durch den vorhandenen KMS verschlüsselt wurden, kopieren Sie mithilfe der KMS-Software die aktuelle Version des Verschlüsselungsschlüssels vom bestehenden KMS auf den neuen KMS. 2. Bearbeiten Sie mithilfe des Grid Manager die bestehende KMS-Konfiguration und geben Sie den neuen Hostnamen oder die neue IP-Adresse ein. <p>"Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)"</p>

Konfigurieren Sie StorageGRID als Client im KMS

Sie müssen StorageGRID als Client für jeden externen Verschlüsselungsmanagement-Server oder KMS-Cluster konfigurieren, bevor Sie den KMS StorageGRID hinzufügen können.

Über diese Aufgabe

Diese Anweisungen gelten für Thales CipherTrust Manager. Eine Liste der unterstützten Versionen finden Sie unter "[NetApp Interoperabilitäts-Matrix-Tool \(IMT\)](#)".

Schritte

1. Erstellen Sie von der KMS-Software einen StorageGRID-Client für jeden KMS- oder KMS-Cluster, den Sie verwenden möchten.

Jeder KMS managt einen einzelnen Verschlüsselungsschlüssel für die Nodes der StorageGRID Appliances an einem einzelnen Standort oder einer Gruppe von Standorten.

2. Erstellen Sie von der KMS-Software einen AES-Verschlüsselungsschlüssel für jedes KMS- oder KMS-Cluster.

Der Verschlüsselungsschlüssel muss mindestens 2,048 Bit haben und exportierbar sein.

3. Notieren Sie die folgenden Informationen für jeden KMS- oder KMS-Cluster.

Diese Informationen benötigen Sie, wenn Sie den KMS StorageGRID hinzufügen.

- Host-Name oder IP-Adresse für jeden Server.
- Der vom KMS verwendete KMIP-Port.
- Schlüsselalias für den Verschlüsselungsschlüssel im KMS.



Der Verschlüsselungsschlüssel muss bereits im KMS vorhanden sein. StorageGRID erstellt oder managt keine KMS-Schlüssel.

4. Beziehen Sie für jeden KMS- oder KMS-Cluster ein Serverzertifikat, das von einer Zertifizierungsstelle (CA) signiert wurde, oder ein Zertifikatbündel, das jede der PEM-kodierten CA-Zertifikatdateien enthält, die in der Reihenfolge der Zertifikatskette verkettet sind.

Das Serverzertifikat ermöglicht es dem externen KMS, sich bei StorageGRID zu authentifizieren.

- Das Zertifikat muss das mit Privacy Enhanced Mail (PEM) Base-64 codierte X.509-Format verwenden.
- Das Feld für alternativen Servernamen (SAN) in jedem Serverzertifikat muss den vollständig qualifizierten Domännennamen (FQDN) oder die IP-Adresse enthalten, mit der StorageGRID eine Verbindung herstellt.



Wenn Sie den KMS in StorageGRID konfigurieren, müssen Sie dieselben FQDNs oder IP-Adressen im Feld **Hostname** eingeben.

- Das Serverzertifikat muss mit dem Zertifikat übereinstimmen, das von der KMIP-Schnittstelle des KMS verwendet wird. In der Regel wird Port 5696 verwendet.
5. Holen Sie sich das öffentliche Clientzertifikat, das vom externen KMS an StorageGRID ausgestellt wurde, und den privaten Schlüssel für das Clientzertifikat.

Das Client-Zertifikat ermöglicht StorageGRID, sich am KMS zu authentifizieren.

Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)

Mithilfe des Assistenten für den StorageGRID-Verschlüsselungsmanagement-Server können Sie jeden KMS- oder KMS-Cluster hinzufügen.

Bevor Sie beginnen

- Sie haben die geprüft ["Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers"](#).
- Das ist schon ["StorageGRID wurde als Client im KMS konfiguriert"](#), Und Sie haben die erforderlichen Informationen für jeden KMS- oder KMS-Cluster.
- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben die Root-Zugriffsberechtigung.

Über diese Aufgabe

Konfigurieren Sie, falls möglich, Site-spezifische Verschlüsselungsmanagement-Server, bevor Sie einen Standard-KMS konfigurieren, der für alle Standorte gilt, die nicht von einem anderen KMS gemanagt werden. Wenn Sie zuerst den Standard-KMS erstellen, werden alle Node-verschlüsselten Appliances im Grid durch den Standard-KMS verschlüsselt. Wenn Sie später einen Site-spezifischen KMS erstellen möchten, müssen Sie zuerst die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS auf den neuen KMS kopieren. Siehe ["Überlegungen für das Ändern des KMS für einen Standort"](#) Entsprechende Details.

Schritt 1: KM Details

In Schritt 1 (KMS-Details) des Assistenten zum Hinzufügen eines Schlüsselverwaltungsservers geben Sie Details zum KMS- oder KMS-Cluster an.

Schritte

1. Wählen Sie **KONFIGURATION > Sicherheit > Schlüsselverwaltungsserver** aus.

Die Seite Key Management Server wird angezeigt, und die Registerkarte Configuration Details ist ausgewählt.

Key management server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID data at rest.

Configuration details

Encrypted nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [Configure key management servers](#).

[Create](#) [Actions](#)

Displaying one result

<input type="checkbox"/>	KMS name	Key name	Manages keys for	Hostname	Certificate expiration
<input type="checkbox"/>	KMS	SG-Global	nmakmipdc1	thales1.vtc.englab.netapp.com and 2 others	All certificates are valid

[← Previous](#) **1** [Next →](#)

2. Wählen Sie **Erstellen**.

Schritt 1 (KMS-Details) des Assistenten zum Hinzufügen eines Schlüsselverwaltungsservers wird angezeigt.

×

Add a Key Management Server

1 KMS Details
 2 Upload server certificate
 3 Upload client certificates

KMS details

Enter information about the external key management server (KMS) and the StorageGRID client you configured in that KMS. If you are configuring a KMS cluster select **Add another hostname** to add a hostname for each server in the cluster.

KMS name ?

Key name ?

Manages keys for ?

Port ?

Hostname ?

[Add another hostname](#)

Cancel
Continue

3. Geben Sie die folgenden Informationen für den KMS und den StorageGRID-Client ein, den Sie in diesem KMS konfiguriert haben.

Feld	Beschreibung
KMS-Name	Einen beschreibenden Namen, der Ihnen bei der Identifizierung dieses KMS hilft. Muss zwischen 1 und 64 Zeichen liegen.
Schlüsselname	Der exakte Schlüssel-Alias für den StorageGRID-Client im KMS. Muss zwischen 1 und 255 Zeichen liegen.

Feld	Beschreibung
Verwaltet Schlüssel für	<p>Der StorageGRID-Site, die diesem KMS zugeordnet wird. Wenn möglich, sollten Sie alle standortspezifischen Verschlüsselungsmanagement-Server konfigurieren, bevor Sie einen Standard-KMS konfigurieren, der für alle Standorte gilt, die nicht von einem anderen KMS verwaltet werden.</p> <ul style="list-style-type: none"> Wählen Sie einen Standort aus, wenn dieser KMS Verschlüsselungen für die Appliance-Nodes an einem bestimmten Standort managt. Wählen Sie Sites Not Managed by another KMS (default KMS) aus, um ein Standard-KMS zu konfigurieren, das für alle Sites gilt, die kein dediziertes KMS haben, und für alle Sites, die Sie in nachfolgenden Erweiterungen hinzufügen. <p>Hinweis: beim Speichern der KMS-Konfiguration tritt Ein Validierungsfehler auf, wenn Sie eine Site auswählen, die zuvor durch den Standard-KMS verschlüsselt wurde, aber Sie haben die aktuelle Version des ursprünglichen Verschlüsselungsschlüssels nicht dem neuen KMS zur Verfügung gestellt.</p>
Port	<p>Der Port, den der KMS-Server für die KMIP-Kommunikation (Key Management Interoperability Protocol) verwendet. Die Standardeinstellung ist 5696, d. h. der KMIP-Standardport.</p>
Hostname	<p>Der vollständig qualifizierte Domänenname oder die IP-Adresse für den KMS.</p> <p>Hinweis: das Feld Subject Alternative Name (SAN) des Serverzertifikats muss den FQDN oder die IP-Adresse enthalten, die Sie hier eingeben. Andernfalls kann StorageGRID keine Verbindung zum KMS oder zu allen Servern eines KMS-Clusters herstellen.</p>

- Wenn Sie einen KMS-Cluster konfigurieren, wählen Sie **Add another hostname**, um einen Hostnamen für jeden Server im Cluster hinzuzufügen.
- Wählen Sie **Weiter**.

Schritt 2: Serverzertifikat hochladen

In Schritt 2 (Serverzertifikat hochladen) des Assistenten zum Hinzufügen eines Schlüsselmanagementservers laden Sie das Serverzertifikat (oder Zertifikatpaket) für das KMS hoch. Das Serverzertifikat ermöglicht es dem externen KMS, sich bei StorageGRID zu authentifizieren.

Schritte

- Navigieren Sie aus **Schritt 2 (Serverzertifikat hochladen)** zum Speicherort des gespeicherten Serverzertifikats oder Zertifikatbündels.

Add a Key Management Server

1
KMS Details

2
Upload server certificate

3
Upload client certificates

Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server certificate

Browse

Previous
Continue

2. Laden Sie die Zertifikatdatei hoch.

Die Metadaten des Serverzertifikats werden angezeigt.

Add a Key Management Server

1
KMS Details

2
Upload server certificate

3
Upload client certificates

Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server certificate

Browse

Cert.pem

Server certificate details

Uploaded successfully

Download certificate
Copy certificate PEM

Metadata

Subject DN:
/CN=1bdd91b0-3f9e-4934-8b85-83d949e0a43f/UID=nmanohar

Serial number:
F8:4C:34:24:2C:CD:22:77:39:1A:BD:07:62:B1:32:D9

Issuer DN:
/C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA

Issued on:
2022-05-23T16:15:24.000Z

Expires on:
2024-05-22T16:15:24.000Z

SHA-1 fingerprint:
DF:AF:A8:33:34:69:54:C6:F3:7A:07:DD:17:54:88:DD:11:BB:38:E8

SHA-256 fingerprint:
75:E0:8D:7B:C7:CF:28:87:62:BA:82:4A:46:6F:CD:94:69:C7:B7:82:58:26:8F:58:95:B2:B6:FB:94:70:2B:81

Alternative names:

Previous
Continue



Wenn Sie ein Zertifikatbündel hochgeladen haben, werden die Metadaten für jedes Zertifikat auf der eigenen Registerkarte angezeigt.

3. Wählen Sie **Weiter**.

Schritt 3: Laden Sie Clientzertifikate hoch

In Schritt 3 (Clientzertifikate hochladen) des Assistenten zum Hinzufügen eines Schlüsselverwaltungsservers laden Sie das Clientzertifikat und den privaten Schlüssel des Clientzertifikats hoch. Das Client-Zertifikat ermöglicht StorageGRID, sich am KMS zu authentifizieren.

Schritte

1. Navigieren Sie unter **Schritt 3 (Client-Zertifikate hochladen)** zum Speicherort des Client-Zertifikats.

The screenshot shows a web-based wizard titled "Add a Key Management Server". The wizard has three steps: "KMS Details", "Upload server certificate", and "3 Upload client certificates". The third step is currently active. Below the step indicators, there is a text block explaining the purpose: "Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS." Below this text, there are two sections: "Client certificate" and "Client certificate private key", each with a "Browse" button. At the bottom right, there are two buttons: "Previous" and "Test and save".

2. Laden Sie die Clientzertifikatdatei hoch.

Die Metadaten des Client-Zertifikats werden angezeigt.

3. Navigieren Sie zum Speicherort des privaten Schlüssels für das Clientzertifikat.

4. Laden Sie die Datei mit dem privaten Schlüssel hoch.

×

Add a Key Management Server

✓ KMS Details

✓ Upload server certificate

3 Upload client certificates

Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client certificate ?

Browse

✓ Cert.pem

Client certificate details

Uploaded successfully

^

Download certificate

Copy certificate PEM

Metadata

Subject DN:	/CN=1bdd91b0-3f9e-4934-8b85-83d949e0a43f/UID=nmanohar
Serial number:	F8:4C:34:24:2C:CD:22:77:39:1A:BD:D7:62:B1:32:D9
Issuer DN:	/C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued on:	2022-05-23T16:15:24.000Z
Expires on:	2024-05-22T16:15:24.000Z
SHA-1 fingerprint:	DF:AF:A8:33:34:69:54:C6:F3:7A:07:0D:17:54:88:DD:11:BB:38:E8
SHA-256 fingerprint:	75:E0:8D:7B:C7:CF:28:87:62:BA:82:4A:46:6F:CD:94:69:C7:B7:82:58:26:8F:58:95:B2:B6:FB:94:70:2B:B1
Alternative names:	

Client certificate private key ?

Browse

✓ Key.pem

Previous

Test and save

 KMS Details
  Upload server certificate
  Upload client certificates

Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client certificate

☒ Cert.pem

Client certificate details

Uploaded successfully

[Download certificate](#)

Copy certificate PEM

Metadata

```
Subject DN: /CN=1bdd91b0-3f9e-4934-8b85-83d942e0a43f/UID=nmanohar
Serial number: F8:4C:34:24:2C:CD:22:77:39:1A:BD:07:62:B1:32:D9
Issuer DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued on: 2022-05-23T16:15:24.000Z
Expires on: 2024-05-22T16:15:24.000Z
SHA-1 fingerprint: DF:AF:A8:33:34:69:54:C6:F3:7A:07:0D:17:54:88:DD:11:BB:38:E8
SHA-256 fingerprint: 75:E0:8D:7B:C7:CF:28:87:62:BA:82:4A:46:6F:CD:94:69:C7:87:82:58:26:8F:58:95:B2:B6:FB:94:70:2B:B1
Alternative names:
```

Client certificate private key

Browse ✓ Key.pem

[Previous](#)

Test and save

5. Wählen Sie **Test und Speichern**.

Die Verbindungen zwischen dem Verschlüsselungsmanagement-Server und den Appliance-Nodes werden getestet. Wenn alle Verbindungen gültig sind und der korrekte Schlüssel auf dem KMS gefunden wird, wird der neue Schlüsselverwaltungsserver der Tabelle auf der Seite des Key Management Servers hinzugefügt.



Unmittelbar nach dem Hinzufügen eines KMS wird der Zertifikatsstatus auf der Seite Key Management Server als Unbekannt angezeigt. Es kann StorageGRID bis zu 30 Minuten dauern, bis der aktuelle Status eines jeden Zertifikats angezeigt wird. Sie müssen Ihren Webbrowser aktualisieren, um den aktuellen Status anzuzeigen.

6. Wenn bei der Auswahl von **Test und Speichern** eine Fehlermeldung angezeigt wird, überprüfen Sie die Nachrichtendetails und wählen Sie dann **OK** aus.

Beispiel: Wenn ein Verbindungstest fehlgeschlagen ist, können Sie einen Fehler bei unbearbeitbarer Einheit mit 422: Nicht verarbeitbarer Einheit erhalten.

7. Wenn Sie die aktuelle Konfiguration speichern müssen, ohne die externe Verbindung zu testen, wählen Sie **Speichern erzwingen**.



Wenn Sie **Force save** auswählen, wird die KMS-Konfiguration gespeichert, aber die externe Verbindung von jedem Gerät zu diesem KMS wird nicht getestet. Wenn Probleme mit der Konfiguration bestehen, können Sie Appliance-Nodes, für die die Node-Verschlüsselung am betroffenen Standort aktiviert ist, möglicherweise nicht neu starten. Wenn der Zugriff auf Ihre Daten nicht mehr vollständig ist, können Sie diese Probleme beheben.

- Überprüfen Sie die Bestätigungswarnung, und wählen Sie **OK**, wenn Sie sicher sind, dass Sie das Speichern der Konfiguration erzwingen möchten.

Die KMS-Konfiguration wird gespeichert, die Verbindung zum KMS wird jedoch nicht getestet.

KMS-Details anzeigen

Sie können Informationen zu jedem Schlüsselverwaltungsserver (KMS) in Ihrem StorageGRID-System anzeigen, einschließlich des aktuellen Status des Servers und der Clientzertifikate.

Schritte

- Wählen Sie **KONFIGURATION > Sicherheit > Schlüsselverwaltungsserver** aus.

Die Seite Key Management Server wird angezeigt. Auf der Registerkarte Konfigurationsdetails werden alle konfigurierten Schlüsselverwaltungsserver angezeigt.

- Überprüfen Sie die Informationen in der Tabelle für jeden KMS.

Feld	Beschreibung
KMS-Name	Der beschreibende Name des KMS.
Schlüsselname	Der Schlüsselalias für den StorageGRID-Client im KMS.
Verwaltet Schlüssel für	Der dem KMS zugeordnete StorageGRID-Site. Dieses Feld zeigt den Namen einer bestimmten StorageGRID-Site oder Sites an, die nicht von einem anderen KMS verwaltet werden (Standard-KMS) .

Feld	Beschreibung
Hostname	<p>Der vollständig qualifizierte Domänenname oder die IP-Adresse des KMS.</p> <p>Wenn ein Cluster von zwei Schlüsselverwaltungsservern vorhanden ist, werden der vollständig qualifizierte Domänenname oder die IP-Adresse beider Server aufgelistet. Wenn mehr als zwei Schlüsselverwaltungsserver in einem Cluster vorhanden sind, wird der vollständig qualifizierte Domänenname oder die IP-Adresse des ersten KMS zusammen mit der Anzahl der zusätzlichen Schlüsselverwaltungsserver im Cluster aufgelistet.</p> <p>Beispiel: 10.10.10.10 and 10.10.10.11 Oder 10.10.10.10 and 2 others.</p> <p>Um alle Hostnamen in einem Cluster anzuzeigen, öffnen Sie ein KMS und wählen Bearbeiten oder Aktionen > Bearbeiten.</p>
Ablauf des Zertifikats	<p>Aktueller Status des Serverzertifikats, des optionalen CA-Zertifikats und des Client-Zertifikats: Gültig, abgelaufen, bald abgelaufen oder unbekannt.</p> <p>Hinweis: Es kann StorageGRID so lange wie 30 Minuten dauern, bis Updates zum Ablauf des Zertifikats erhalten. Sie müssen Ihren Webbrowser aktualisieren, um die aktuellen Werte anzuzeigen.</p>

3. Wenn der Ablauf des Zertifikats unbekannt ist, warten Sie bis zu 30 Minuten, und aktualisieren Sie dann Ihren Webbrowser.



Unmittelbar nach dem Hinzufügen eines KMS wird der Ablauf des Zertifikats auf der Seite Key Management Server als Unbekannt angezeigt. Es kann StorageGRID bis zu 30 Minuten dauern, bis der aktuelle Status eines jeden Zertifikats angezeigt wird. Sie müssen Ihren Webbrowser aktualisieren, um den aktuellen Status anzuzeigen.

4. Wenn in der Spalte Zertifikatablauf angezeigt wird, dass ein Zertifikat abgelaufen ist oder kurz vor dem Ablaufdatum steht, beheben Sie das Problem so schnell wie möglich.

Wenn die Warnungen **KMS CA Certificate Expiration**, **KMS Client Certificate Expiration** und **KMS Server Certificate Expiration** ausgelöst werden, notieren Sie sich die Beschreibung der einzelnen Warnungen und führen Sie die empfohlenen Aktionen durch.



Sie müssen Probleme mit dem Zertifikat so schnell wie möglich beheben, um den Datenzugriff aufrechtzuerhalten.

5. Um die Zertifikatdetails für dieses KMS anzuzeigen, wählen Sie den KMS-Namen aus der Tabelle aus.
6. Überprüfen Sie auf der KMS-Übersichtsseite die Metadaten und das Zertifikat-PEM sowohl für das Serverzertifikat als auch für das Clientzertifikat. Wählen Sie bei Bedarf **Zertifikat bearbeiten**, um ein Zertifikat durch ein neues zu ersetzen.

Verschlüsselte Nodes anzeigen

Sie können Informationen zu den Appliance-Knoten in Ihrem StorageGRID-System anzeigen, bei denen die Einstellung **Node-Verschlüsselung** aktiviert ist.

Schritte

1. Wählen Sie **KONFIGURATION > Sicherheit > Schlüsselverwaltungsserver** aus.

Die Seite Key Management Server wird angezeigt. Auf der Registerkarte Konfigurationsdetails werden alle konfigurierten Schlüsselverwaltungsserver angezeigt.

2. Wählen Sie oben auf der Seite die Registerkarte **verschlüsselte Knoten** aus.

Auf der Registerkarte Verschlüsselte Knoten werden die Geräteknoten in Ihrem StorageGRID-System aufgelistet, für die die Einstellung **Knotenverschlüsselung** aktiviert ist.

3. Überprüfen Sie die Informationen in der Tabelle für jeden Appliance-Node.

Spalte	Beschreibung
Node-Name	Der Name des Appliance-Node.
Node-Typ	Der Node-Typ: Storage, Admin oder Gateway.
Standort	Der Name der StorageGRID-Site, auf der der Node installiert ist.
KMS-Name	<p>Der beschreibende Name des für den Knoten verwendeten KMS.</p> <p>Wenn kein KMS aufgeführt ist, wählen Sie die Registerkarte Konfigurationsdetails aus, um ein KMS hinzuzufügen.</p> <p>"Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)"</p>
Schlüssel-UID	<p>Die eindeutige ID des Verschlüsselungsschlüssels, der zur Verschlüsselung und Entschlüsselung von Daten auf dem Appliance-Node verwendet wird. Um eine gesamte Schlüssel-UID anzuzeigen, setzen Sie den Cursor über die Zelle.</p> <p>Ein Bindestrich (-) gibt an, dass die Schlüssel-UID unbekannt ist, möglicherweise wegen eines Verbindungsproblem zwischen dem Appliance-Node und dem KMS.</p>
Status	<p>Der Status der Verbindung zwischen dem KMS und dem Appliance-Node. Wenn der Knoten verbunden ist, wird der Zeitstempel alle 30 Minuten aktualisiert. Nach einer Änderung der KMS-Konfiguration kann es mehrere Minuten dauern, bis der Verbindungsstatus aktualisiert wird.</p> <p>Hinweis: Sie müssen Ihren Webbrowser aktualisieren, um die neuen Werte zu sehen.</p>

4. Wenn in der Spalte Status ein KMS-Problem angezeigt wird, beheben Sie das Problem sofort.

Während normaler KMS-Vorgänge wird der Status **mit KMS** verbunden. Wenn ein Knoten von der Tabelle getrennt wird, wird der Verbindungsstatus des Knotens angezeigt (administrativ ausgefallen oder unbekannt).

Andere Statusmeldungen entsprechen StorageGRID Meldungen mit denselben Namen:

- KMS-Konfiguration konnte nicht geladen werden
- KMS-Verbindungsfehler
- DER VERSCHLÜSSELUNGSSCHLÜSSELNAME VON KMS wurde nicht gefunden
- DIE Drehung des VERSCHLÜSSELUNGSSCHLÜSSELS ist fehlgeschlagen
- KMS-Schlüssel konnte ein Appliance-Volume nicht entschlüsseln
- KM ist nicht konfiguriert

Führen Sie die empfohlenen Aktionen für diese Warnmeldungen aus.



Sämtliche Probleme müssen sofort behoben werden, um einen vollständigen Schutz Ihrer Daten zu gewährleisten.

Bearbeiten eines Verschlüsselungsmanagement-Servers (KMS)

Möglicherweise müssen Sie die Konfiguration eines Schlüsselverwaltungsservers bearbeiten, z. B. wenn ein Zertifikat kurz vor dem Ablauf steht.

Bevor Sie beginnen

- Sie haben die geprüft ["Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers"](#).
- Wenn Sie die für einen KMS ausgewählte Site aktualisieren möchten, haben Sie die geprüft ["Überlegungen für das Ändern des KMS für einen Standort"](#).
- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Sie haben die Root-Zugriffsberechtigung.

Schritte


1. Wählen Sie **KONFIGURATION > Sicherheit > Schlüsselverwaltungsserver** aus.

Die Seite Key Management Server wird angezeigt und zeigt alle konfigurierten Key Management Server an.

2. Wählen Sie den KMS aus, den Sie bearbeiten möchten, und wählen Sie **actions > Edit**.

Sie können einen KMS auch bearbeiten, indem Sie den KMS-Namen in der Tabelle auswählen und auf der KMS-Detailseite **Bearbeiten** auswählen.

3. Aktualisieren Sie optional die Details in **Schritt 1 (KMS-Details)** des Assistenten zum Bearbeiten eines Schlüsselverwaltungsservers.

Feld	Beschreibung
KMS-Name	Einen beschreibenden Namen, der Ihnen bei der Identifizierung dieses KMS hilft. Muss zwischen 1 und 64 Zeichen liegen.
Schlüsselname	<p>Der exakte Schlüssel-Alias für den StorageGRID-Client im KMS. Muss zwischen 1 und 255 Zeichen liegen.</p> <p>In seltenen Fällen müssen Sie nur den Schlüsselnamen bearbeiten. Sie müssen beispielsweise den Schlüsselnamen bearbeiten, wenn der Alias im KMS umbenannt wird oder alle Versionen des vorherigen Schlüssels in die Versionsgeschichte des neuen Alias kopiert wurden.</p> <div>  <p>Versuchen Sie niemals, einen Schlüssel zu drehen, indem Sie den Schlüsselnamen (Alias) für den KMS ändern. Drehen Sie stattdessen den Schlüssel, indem Sie die Schlüsselversion in der KMS-Software aktualisieren. Für StorageGRID müssen alle zuvor verwendeten Schlüsselversionen (sowie zukünftige Versionen) vom KMS mit demselben Schlüsselalias zugänglich sein. Wenn Sie den Schlüssel-Alias für einen konfigurierten KMS ändern, kann StorageGRID Ihre Daten möglicherweise nicht entschlüsseln.</p> <p>"Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers"</p> </div>
Verwaltet Schlüssel für	<p>Wenn Sie ein standortspezifisches KMS bearbeiten und noch kein Standard-KMS haben, wählen Sie optional Sites Not Managed by another KMS (default KMS) aus. Diese Auswahl konvertiert ein standortspezifisches KMS in das Standard-KMS, das für alle Standorte gilt, die kein dediziertes KMS haben, und für alle Sites, die in einer Erweiterung hinzugefügt wurden.</p> <p>Hinweis: Wenn Sie eine Site-spezifische KMS bearbeiten, können Sie keine andere Site auswählen. Wenn Sie das Standard-KMS bearbeiten, können Sie keine bestimmte Site auswählen.</p>
Port	Der Port, den der KMS-Server für die KMIP-Kommunikation (Key Management Interoperability Protocol) verwendet. Die Standardeinstellung ist 5696, d. h. der KMIP-Standardport.
Hostname	<p>Der vollständig qualifizierte Domänenname oder die IP-Adresse für den KMS.</p> <p>Hinweis: das Feld Subject Alternative Name (SAN) des Serverzertifikats muss den FQDN oder die IP-Adresse enthalten, die Sie hier eingeben. Andernfalls kann StorageGRID keine Verbindung zum KMS oder zu allen Servern eines KMS-Clusters herstellen.</p>

- Wenn Sie einen KMS-Cluster konfigurieren, wählen Sie **Add another hostname**, um einen Hostnamen für jeden Server im Cluster hinzuzufügen.
- Wählen Sie **Weiter**.

Schritt 2 (Serverzertifikat hochladen) des Assistenten zum Bearbeiten eines Schlüsselverwaltungsservers wird angezeigt.

6. Wenn Sie das Serverzertifikat ersetzen müssen, wählen Sie **Durchsuchen** und laden Sie die neue Datei hoch.
7. Wählen Sie **Weiter**.

Schritt 3 (Client-Zertifikate hochladen) des Assistenten zum Bearbeiten eines Schlüsselverwaltungsservers wird angezeigt.

8. Wenn Sie das Clientzertifikat und den privaten Schlüssel des Clientzertifikats ersetzen müssen, wählen Sie **Durchsuchen** und laden Sie die neuen Dateien hoch.
9. Wählen Sie **Test und Speichern**.

Die Verbindungen zwischen dem Verschlüsselungsmanagement-Server und allen Node-verschlüsselten Appliance-Nodes an den betroffenen Standorten werden getestet. Wenn alle Knotenverbindungen gültig sind und der korrekte Schlüssel auf dem KMS gefunden wird, wird der Schlüsselverwaltungsserver der Tabelle auf der Seite des Key Management Servers hinzugefügt.

10. Wenn eine Fehlermeldung angezeigt wird, überprüfen Sie die Nachrichtendetails, und wählen Sie **OK**.

Sie können beispielsweise einen Fehler bei der nicht verarbeitbaren Einheit von 422 erhalten, wenn die für diesen KMS ausgewählte Site bereits von einem anderen KMS verwaltet wird oder wenn ein Verbindungstest fehlgeschlagen ist.

11. Wenn Sie die aktuelle Konfiguration speichern müssen, bevor Sie die Verbindungsfehler beheben, wählen Sie **Speichern erzwingen**.



Wenn Sie **Force save** auswählen, wird die KMS-Konfiguration gespeichert, aber die externe Verbindung von jedem Gerät zu diesem KMS wird nicht getestet. Wenn Probleme mit der Konfiguration bestehen, können Sie Appliance-Nodes, für die die Node-Verschlüsselung am betroffenen Standort aktiviert ist, möglicherweise nicht neu starten. Wenn der Zugriff auf Ihre Daten nicht mehr vollständig ist, können Sie diese Probleme beheben.

Die KMS-Konfiguration wird gespeichert.

12. Überprüfen Sie die Bestätigungswarnung, und wählen Sie **OK**, wenn Sie sicher sind, dass Sie das Speichern der Konfiguration erzwingen möchten.

Die KMS-Konfiguration wird gespeichert, die Verbindung zum KMS wird jedoch nicht getestet.

Entfernen eines Verschlüsselungsmanagement-Servers (KMS)

In einigen Fällen möchten Sie einen Schlüsselverwaltungsserver entfernen. Sie können beispielsweise einen standortspezifischen KMS entfernen, wenn Sie den Standort deaktiviert haben.

Bevor Sie beginnen

- Sie haben die geprüft ["Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers"](#).
- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).

- Sie haben die Root-Zugriffsberechtigung.

Über diese Aufgabe

In diesen Fällen können Sie einen KMS entfernen:

- Wenn der Standort außer Betrieb genommen wurde oder wenn der Standort keine Appliance-Nodes mit aktivierter Node-Verschlüsselung enthält, können Sie einen standortspezifischen KMS entfernen.
- Der Standard-KMS kann entfernt werden, wenn für jeden Standort bereits ein standortspezifischer KMS vorhanden ist, bei dem Appliance-Nodes mit aktivierter Node-Verschlüsselung vorhanden sind.

Schritte

1. Wählen Sie **KONFIGURATION > Sicherheit > Schlüsselverwaltungsserver** aus.

Die Seite Key Management Server wird angezeigt und zeigt alle konfigurierten Key Management Server an.

2. Wählen Sie den KMS aus, den Sie entfernen möchten, und wählen Sie **Aktionen > Entfernen**.

Sie können KMS auch entfernen, indem Sie den KMS-Namen in der Tabelle auswählen und auf der KMS-Detailseite **Entfernen** auswählen.

3. Bestätigen Sie, dass Folgendes zutrifft:

- Sie entfernen ein standortspezifisches KMS für einen Standort, der keinen Appliance-Knoten mit aktivierter Knotenverschlüsselung hat.
- Sie entfernen den Standard-KMS, aber für jeden Standort mit Knotenverschlüsselung ist bereits ein standortspezifisches KMS vorhanden.

4. Wählen Sie **Ja**.

Die KMS-Konfiguration wurde entfernt.

Proxy-Einstellungen verwalten

Konfigurieren Sie Speicher-Proxy-Einstellungen

Wenn Sie Plattform-Services oder Cloud Storage-Pools verwenden, können Sie einen nicht transparenten Proxy zwischen Storage Nodes und den externen S3-Endpunkten konfigurieren. Beispielsweise benötigen Sie einen nicht transparenten Proxy, um Meldungen von Plattformdiensten an externe Endpunkte, z. B. einen Endpunkt im Internet, zu senden.

Bevor Sie beginnen

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

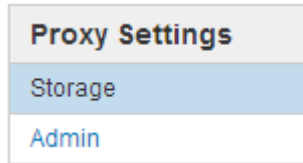
Über diese Aufgabe

Sie können die Einstellungen für einen einzelnen Speicherproxy konfigurieren.

Schritte

1. Wählen Sie **KONFIGURATION > Sicherheit > Proxy-Einstellungen**.

Die Seite Speicher-Proxy-Einstellungen wird angezeigt. Standardmäßig ist **Storage** im Sidebar-Menü ausgewählt.



2. Aktivieren Sie das Kontrollkästchen **Speicher-Proxy aktivieren**.

Die Felder zum Konfigurieren eines Speicher-Proxys werden angezeigt.

Storage Proxy Settings

If you are using platform services or Cloud Storage Pools, you can configure a non-transparent proxy server between Storage Nodes and the external S3 endpoints.

Enable Storage Proxy ☒

Protocol ☒ HTTP ☐ SOCKS5

Hostname

Port (optional)

3. Wählen Sie das Protokoll für den nicht-transparenten Speicher-Proxy aus.
4. Geben Sie den Hostnamen oder die IP-Adresse des Proxy-Servers ein.
5. Geben Sie optional den Port ein, der für die Verbindung mit dem Proxyserver verwendet wird.

Sie können dieses Feld leer lassen, wenn Sie den Standardport für das Protokoll verwenden: 80 für HTTP oder 1080 für SOCKS5.

6. Wählen Sie **Speichern**.

Nach dem Speichern des Storage-Proxy können neue Endpunkte für Plattformservices oder Cloud-Storage-Pools konfiguriert und getestet werden.



Änderungen an Proxy können bis zu 10 Minuten in Anspruch nehmen.

7. Überprüfen Sie die Einstellungen Ihres Proxy-Servers, um sicherzustellen, dass für den Plattformdienst bezogene Nachrichten von StorageGRID nicht blockiert werden.

Nachdem Sie fertig sind

Wenn Sie einen Speicher-Proxy deaktivieren müssen, deaktivieren Sie das Kontrollkästchen **Speicher-Proxy aktivieren**, und wählen Sie **Speichern** aus.

Verwandte Informationen

- ["Netzwerk und Ports für Plattformservices"](#)
- ["Objektmanagement mit ILM"](#)

Konfigurieren Sie die Administrator-Proxy-Einstellungen

Wenn Sie AutoSupport-Meldungen über HTTP oder HTTPS senden (siehe "[Konfigurieren Sie AutoSupport](#)") Können Sie einen nicht transparenten Proxy-Server zwischen Admin-Knoten und technischem Support (AutoSupport) konfigurieren.

Bevor Sie beginnen

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

Über diese Aufgabe

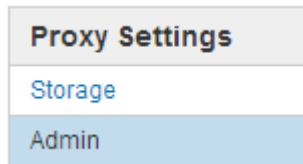
Sie können die Einstellungen für einen einzigen Admin-Proxy konfigurieren.

Schritte

1. Wählen Sie **KONFIGURATION > Sicherheit > Proxy-Einstellungen**.

Die Seite Admin Proxy Settings wird angezeigt. Standardmäßig ist **Storage** im Sidebar-Menü ausgewählt.

2. Wählen Sie im Sidebar-Menü die Option **Admin**.



3. Aktivieren Sie das Kontrollkästchen **Admin-Proxy aktivieren**.

Admin Proxy Settings

If you send AutoSupport messages using HTTPS or HTTP, you can configure a non-transparent proxy server between Admin Nodes and technical support.

Enable Admin Proxy	<input checked="" type="checkbox"/>
Hostname	<input type="text" value="myproxy.example.com"/>
Port	<input type="text" value="8080"/>
Username (optional)	<input type="text" value="root"/>
Password (optional)	<input type="password" value="••••••••"/>
<input type="button" value="Save"/>	

4. Geben Sie den Hostnamen oder die IP-Adresse des Proxy-Servers ein.
5. Geben Sie den Port ein, der für die Verbindung mit dem Proxy-Server verwendet wird.
6. Geben Sie optional den Proxy-Benutzernamen ein.

Lassen Sie dieses Feld leer, wenn Ihr Proxy-Server keinen Benutzernamen benötigt.

7. Geben Sie optional das Proxy-Kennwort ein.

Lassen Sie dieses Feld leer, wenn Ihr Proxy-Server kein Passwort benötigt.

8. Wählen Sie **Speichern**.

Nachdem der Admin-Proxy gespeichert wurde, wird der Proxy-Server zwischen Admin-Nodes und dem technischen Support konfiguriert.



Änderungen an Proxy können bis zu 10 Minuten in Anspruch nehmen.

9. Wenn Sie den Proxy deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Admin Proxy aktivieren**, und wählen Sie **Save** aus.

Kontrollieren Sie Firewalls

Kontrolle des Zugriffs über externe Firewall

Sie können bestimmte Ports an der externen Firewall öffnen oder schließen.

Sie können den Zugriff auf die Benutzeroberflächen und APIs auf StorageGRID-Administratorknoten steuern, indem Sie bestimmte Ports an der externen Firewall öffnen oder schließen. Beispielsweise möchten Sie verhindern, dass Mandanten sich an der Firewall mit dem Grid Manager verbinden können, und zwar zusätzlich über andere Methoden zur Steuerung des Systemzugriffs.

Informationen zum Konfigurieren der internen StorageGRID-Firewall finden Sie unter "[Konfigurieren Sie die interne Firewall](#)".

Port	Beschreibung	Port offen...
443	Standard-HTTPS-Port für Admin-Nodes	Webbrowser und Management-API-Clients können auf den Grid Manager, die Grid Management API, den Mandanten-Manager und die Mandanten-Management-API zugreifen. Hinweis: Port 443 wird auch für einen internen Verkehr genutzt.
8443	Eingeschränkter Grid Manager-Port an Admin-Nodes	<ul style="list-style-type: none">• Webbrowser und Management-API-Clients können mithilfe von HTTPS auf den Grid Manager und die Grid Management API zugreifen.• Webbrowser und Management-API-Clients können nicht auf den Tenant Manager oder die Mandanten-Management-API zugreifen.• Anfragen nach internen Inhalten werden abgelehnt.

Port	Beschreibung	Port offen...
9443	Eingeschränkter Mandantenmanager-Port an Admin-Nodes	<ul style="list-style-type: none"> • Webbrowser und Management-API-Clients können mithilfe von HTTPS auf den Mandanten-Manager und die Mandanten-Management-API zugreifen. • Webbrowser und Management-API-Clients können nicht auf den Grid Manager oder die Grid-Management-API zugreifen. • Anfragen nach internen Inhalten werden abgelehnt.



Single Sign-On (SSO) ist auf den Ports Restricted Grid Manager oder Tenant Manager nicht verfügbar. Sie müssen den Standard-HTTPS-Port (443) verwenden, wenn Benutzer sich mit Single Sign-On authentifizieren möchten.

Verwandte Informationen

- ["Melden Sie sich beim Grid Manager an"](#)
- ["Erstellen eines Mandantenkontos"](#)
- ["Externe Kommunikation"](#)

Interne Firewall-Kontrollen verwalten

StorageGRID verfügt über eine interne Firewall auf jedem Node, die die Sicherheit Ihres Grids erhöht, indem Sie den Netzwerkzugriff auf den Node kontrollieren können. Verwenden Sie die Firewall, um den Netzwerkzugriff auf allen Ports zu verhindern, außer den für Ihre spezifische Grid-Bereitstellung erforderlichen Ports. Die Konfigurationsänderungen, die Sie auf der Seite Firewall-Steuerung vornehmen, werden für jeden Knoten bereitgestellt.

Verwenden Sie die drei Registerkarten auf der Seite „Firewall-Steuerung“, um den für Ihr Raster erforderlichen Zugriff anzupassen.

- **Privilegierte Adressliste:** Verwenden Sie diese Registerkarte, um ausgewählten Zugriff auf geschlossene Ports zu ermöglichen. Sie können IP-Adressen oder Subnetze in CIDR-Notation hinzufügen, die über die Registerkarte externen Zugriff managen auf geschlossene Ports zugreifen können.
- **Externen Zugriff verwalten:** Verwenden Sie diese Registerkarte, um Ports zu schließen, die standardmäßig geöffnet sind, oder um zuvor geschlossene Ports wieder zu öffnen.
- **Nicht vertrauenswürdiges Client-Netzwerk:** Verwenden Sie diese Registerkarte, um anzugeben, ob ein Knoten eingehenden Datenverkehr vom Client-Netzwerk anvertraut.

Auf dieser Registerkarte können Sie auch zusätzliche Ports angeben, die geöffnet werden sollen, wenn das nicht vertrauenswürdige Clientnetzwerk konfiguriert ist. Diese Ports können Zugriff auf den Grid Manager, den Tenant Manager oder beide ermöglichen.

Die Einstellungen auf dieser Registerkarte überschreiben die Einstellungen auf der Registerkarte externen Zugriff verwalten.

- Ein Knoten mit einem nicht vertrauenswürdigen Client-Netzwerk akzeptiert nur Verbindungen auf den an diesem Knoten konfigurierten Load-Balancer-Endpunktports (global, Knotenschnittstelle und Knotentyp gebundene Endpunkte).
- Zusätzliche Ports, die auf der Registerkarte nicht vertrauenswürdiger Client-Netzwerk geöffnet werden, sind in allen nicht vertrauenswürdigen Client-Netzwerken geöffnet, auch wenn keine Load Balancer-Endpunkte konfiguriert sind.
- Load Balancer-Endpunkt-Ports und ausgewählte zusätzliche Ports *sind die einzigen offenen Ports* in nicht vertrauenswürdigen Client-Netzwerken, unabhängig von den Einstellungen auf der Registerkarte Externe Netzwerke verwalten.
- Wenn vertrauenswürdig, sind alle Ports, die auf der Registerkarte externen Zugriff managen geöffnet sind, sowie alle im Client-Netzwerk geöffneten Load Balancer-Endpunkte zugänglich.



Die Einstellungen, die Sie auf einer Registerkarte vornehmen, können sich auf die Zugriffsänderungen auswirken, die Sie auf einer anderen Registerkarte vornehmen. Überprüfen Sie die Einstellungen auf allen Registerkarten, um sicherzustellen, dass sich Ihr Netzwerk wie erwartet verhält.

Informationen zum Konfigurieren der internen Firewall-Steuerelemente finden Sie unter ["Konfigurieren Sie die Firewall-Steuerelemente"](#).

Weitere Informationen zu externen Firewalls und Netzwerksicherheit finden Sie unter ["Kontrolle des Zugriffs über externe Firewall"](#).

Liste privilegierter Adressen und Verwaltung externer Zugriffsregisterkarten

Auf der Registerkarte Liste der privilegierten Adressen können Sie eine oder mehrere IP-Adressen registrieren, denen Zugriff auf geschlossene Grid-Ports gewährt wird. Auf der Registerkarte externen Zugriff verwalten können Sie den externen Zugriff auf ausgewählte externe Ports oder alle offenen externen Ports schließen (externe Ports sind Ports, auf die standardmäßig nicht-Grid-Nodes zugreifen können). Diese beiden Registerkarten können häufig zusammen verwendet werden, um den genauen Netzwerkzugriff anzupassen, den Sie für Ihr Raster benötigen.



Privilegierte IP-Adressen haben standardmäßig keinen internen Grid-Port-Zugriff.

Beispiel 1: Verwenden Sie einen Jump-Host für Wartungsaufgaben

Angenommen, Sie möchten einen Jump-Host (einen sicherheitsgesicherten Host) für die Netzwerkadministration verwenden. Sie können die folgenden allgemeinen Schritte verwenden:

1. Verwenden Sie die Registerkarte Liste der privilegierten Adressen, um die IP-Adresse des Jump-Hosts hinzuzufügen.
2. Verwenden Sie die Registerkarte externen Zugriff verwalten, um alle Ports zu blockieren.



Fügen Sie die privilegierte IP-Adresse hinzu, bevor Sie die Ports 443 und 8443 blockieren. Alle Benutzer, die derzeit mit einem blockierten Port verbunden sind, einschließlich Ihnen, verlieren den Zugriff auf Grid Manager, es sei denn, ihre IP-Adresse wurde der Liste der privilegierten Adressen hinzugefügt.

Nachdem Sie Ihre Konfiguration gespeichert haben, werden alle externen Ports auf dem Admin-Knoten in Ihrem Grid für alle Hosts außer dem Jump-Host gesperrt. Sie können dann den Jump-Host verwenden, um Wartungsarbeiten am Grid sicherer durchzuführen.

Beispiel 2: Beschränken Sie den Zugriff auf den Grid-Manager und den Tenant Manager

Angenommen, Sie möchten den Zugriff auf den Grid-Manager und den Mandantenmanager aus Sicherheitsgründen einschränken. Sie können die folgenden allgemeinen Schritte verwenden:

1. Verwenden Sie den Umschalter auf der Registerkarte externen Zugriff verwalten, um Port 443 zu blockieren.
2. Verwenden Sie die Umschalttaste auf der Registerkarte externen Zugriff verwalten, um den Zugriff auf Port 8443 zu ermöglichen.
3. Verwenden Sie die Umschalttaste auf der Registerkarte externen Zugriff verwalten, um den Zugriff auf Port 9443 zu ermöglichen.

Nachdem Sie Ihre Konfiguration gespeichert haben, können Hosts nicht auf Port 443 zugreifen, aber sie können dennoch über Port 8443 und den Tenant Manager über Port 9443 auf den Grid Manager zugreifen.

Beispiel 3: Sperren sensibler Ports

Angenommen, Sie möchten sensible Ports und den Dienst auf diesem Port sperren (z. B. SSH an Port 22). Sie können die folgenden allgemeinen Schritte verwenden:

1. Verwenden Sie die Registerkarte Liste der privilegierten Adressen, um nur den Hosts Zugriff zu gewähren, die Zugriff auf den Dienst benötigen.
2. Verwenden Sie die Registerkarte externen Zugriff verwalten, um alle Ports zu blockieren.



Fügen Sie die privilegierte IP-Adresse hinzu, bevor Sie die Ports 443 und 8443 blockieren. Alle Benutzer, die derzeit mit einem blockierten Port verbunden sind, einschließlich Ihnen, verlieren den Zugriff auf Grid Manager, es sei denn, ihre IP-Adresse wurde der Liste der privilegierten Adressen hinzugefügt.

Nachdem Sie die Konfiguration gespeichert haben, stehen den Hosts auf der Liste der privilegierten Adressen Port 22 und SSH-Dienst zur Verfügung. Allen anderen Hosts wird der Zugriff auf den Dienst verweigert, unabhängig davon, von welcher Schnittstelle die Anforderung stammt.

Beispiel 4: Deaktivieren Sie den Zugriff auf nicht verwendete Dienste

Auf Netzwerkebene können Sie einige Dienste deaktivieren, die Sie nicht verwenden möchten. Wenn Sie beispielsweise keinen Swift-Zugriff bereitstellen, führen Sie die folgenden allgemeinen Schritte aus:

1. Verwenden Sie den Umschalter auf der Registerkarte externen Zugriff verwalten, um Port 18083 zu blockieren.
2. Verwenden Sie den Umschalter auf der Registerkarte externen Zugriff verwalten, um Port 18085 zu blockieren.

Nachdem Sie die Konfiguration gespeichert haben, lässt der Storage Node die Swift-Konnektivität nicht mehr zu, erlaubt aber weiterhin den Zugriff auf andere Dienste auf nicht blockierten Ports.

Registerkarte nicht vertrauenswürdige Client-Netzwerke

Wenn Sie ein Clientnetzwerk verwenden, können Sie StorageGRID vor feindlichen Angriffen schützen, indem Sie eingehenden Clientverkehr nur an explizit konfigurierten Endpunkten oder zusätzlichen Ports akzeptieren, die Sie auf dieser Registerkarte auswählen.

Standardmäßig ist das Client-Netzwerk auf jedem Grid-Knoten *Trusted*. Das heißt, standardmäßig vertraut

StorageGRID eingehende Verbindungen zu jedem Grid-Knoten auf allen ["Verfügbare externe Ports"](#).

Sie können die Bedrohung durch feindliche Angriffe auf Ihrem StorageGRID-System verringern, indem Sie angeben, dass das Client-Netzwerk auf jedem Knoten *unvertrauenswürdig* ist. Wenn das Client-Netzwerk eines Knotens nicht vertrauenswürdig ist, akzeptiert der Knoten nur eingehende Verbindungen an Ports, die explizit als Load Balancer-Endpunkte konfiguriert sind, und alle zusätzlichen Ports, die Sie über die Registerkarte nicht vertrauenswürdiges Client-Netzwerk auf der Seite Firewall-Steuerung festlegen. Siehe ["Konfigurieren von Load Balancer-Endpunkten"](#) Und ["Konfigurieren Sie die Firewall-Steuererelemente"](#).

Beispiel 1: Der Gateway-Node akzeptiert nur HTTPS-S3-Anforderungen

Angenommen, ein Gateway-Node soll den gesamten eingehenden Datenverkehr im Client-Netzwerk mit Ausnahme von HTTPS S3-Anforderungen ablehnen. Sie würden folgende allgemeine Schritte durchführen:

1. Von ["Load Balancer-Endpunkte"](#) Konfigurieren Sie einen Load Balancer-Endpunkt für S3 über HTTPS an Port 443.
2. Wählen Sie auf der Seite Firewall-Steuerung die Option nicht vertrauenswürdig aus, um anzugeben, dass das Client-Netzwerk auf dem Gateway-Knoten nicht vertrauenswürdig ist.

Nachdem Sie Ihre Konfiguration gespeichert haben, wird der gesamte eingehende Datenverkehr im Client-Netzwerk des Gateway-Knotens außer HTTPS-S3-Anfragen auf Port 443- und ICMP-Echo-(Ping-)Anfragen verworfen.

Beispiel 2: Storage-Node sendet Anforderungen von S3-Plattform-Services

Angenommen, Sie möchten den ausgehenden Datenverkehr der S3-Plattformdienste von einem Storage-Node aktivieren, möchten jedoch eingehende Verbindungen zu diesem Storage-Node im Client-Netzwerk verhindern. Sie würden diesen allgemeinen Schritt durchführen:

- Geben Sie auf der Registerkarte nicht vertrauenswürdige Client-Netzwerke der Seite Firewall-Steuerung an, dass das Client-Netzwerk auf dem Storage Node nicht vertrauenswürdig ist.

Nachdem Sie die Konfiguration gespeichert haben, akzeptiert der Storage Node keinen eingehenden Datenverkehr mehr im Client-Netzwerk, erlaubt jedoch weiterhin ausgehende Anfragen an konfigurierte Plattformdienstziele.

Beispiel 3: Zugriff auf Grid Manager auf ein Subnetz beschränken

Angenommen, Sie möchten den Zugriff des Grid-Managers nur auf ein bestimmtes Subnetz zulassen. Führen Sie die folgenden Schritte aus:

1. Verbinden Sie das Client-Netzwerk Ihrer Admin-Knoten mit dem Subnetz.
2. Verwenden Sie die Registerkarte nicht vertrauenswürdiges Clientnetzwerk, um das Clientnetzwerk als nicht vertrauenswürdig zu konfigurieren.
3. Fügen Sie im Abschnitt **zusätzliche Ports auf nicht vertrauenswürdigem Client-Netzwerk öffnen** der Registerkarte Port 443 oder 8443 hinzu.
4. Verwenden Sie die Registerkarte externen Zugriff verwalten, um alle externen Ports zu blockieren (mit oder ohne privilegierte IP-Adressen für Hosts außerhalb dieses Subnetzes).

Nachdem Sie die Konfiguration gespeichert haben, können nur Hosts in dem von Ihnen angegebenen Subnetz auf den Grid Manager zugreifen. Alle anderen Hosts sind blockiert.

Konfigurieren Sie die interne Firewall

Sie können die StorageGRID Firewall konfigurieren, um den Netzwerkzugriff auf bestimmte Ports auf Ihren StorageGRID Nodes zu steuern.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet ["Unterstützter Webbrowser"](#).
- Das ist schon ["Bestimmte Zugriffsberechtigungen"](#).
- Sie haben die Informationen in geprüft ["Management der Firewall-Kontrollen"](#) Und ["Netzwerkrichtlinien"](#).
- Wenn ein Admin-Node oder Gateway-Node nur eingehenden Datenverkehr auf explizit konfigurierten Endpunkten annehmen soll, haben Sie die Load Balancer-Endpunkte definiert.



Wenn Sie die Konfiguration des Client-Netzwerks ändern, können bestehende Clientverbindungen fehlschlagen, wenn die Load Balancer-Endpunkte nicht konfiguriert wurden.

Über diese Aufgabe

StorageGRID verfügt über eine interne Firewall auf jedem Node, über die Sie einige Ports an den Nodes des Grids öffnen oder schließen können. Sie können die Registerkarten für die Firewall-Steuerung verwenden, um Ports zu öffnen oder zu schließen, die standardmäßig im Grid-Netzwerk, im Admin-Netzwerk und im Client-Netzwerk geöffnet sind. Sie können auch eine Liste mit privilegierten IP-Adressen erstellen, die auf gesperrte Grid-Ports zugreifen können. Wenn Sie ein Client-Netzwerk verwenden, können Sie angeben, ob ein Knoten eingehenden Datenverkehr vom Client-Netzwerk anvertraut, und Sie können den Zugriff bestimmter Ports auf dem Client-Netzwerk konfigurieren.

Die Beschränkung der Anzahl der offenen Ports auf IP-Adressen außerhalb Ihres Grids auf nur die absolut notwendigen Ports erhöht die Sicherheit Ihres Grids. Mithilfe der Einstellungen auf den drei Registerkarten für die Firewall-Steuerung stellen Sie sicher, dass nur die erforderlichen Ports geöffnet sind.

Weitere Informationen zur Verwendung von Firewall-Kontrollen, einschließlich Beispiele, finden Sie unter ["Management der Firewall-Kontrollen"](#).

Weitere Informationen zu externen Firewalls und Netzwerksicherheit finden Sie unter ["Kontrolle des Zugriffs über externe Firewall"](#).

Firewall-Kontrollen für den Zugriff

Schritte

1. Wählen Sie **CONFIGURATION > Security > Firewall Control**.

Die drei Registerkarten auf dieser Seite werden unter beschrieben ["Management der Firewall-Kontrollen"](#).

2. Wählen Sie eine beliebige Registerkarte aus, um die Firewall-Steuerelemente zu konfigurieren.

Sie können diese Registerkarten in beliebiger Reihenfolge verwenden. Die Konfigurationen, die Sie auf einer Registerkarte festlegen, beschränken nicht, was Sie auf den anderen Registerkarten tun können. Konfigurationsänderungen, die Sie auf einer Registerkarte vornehmen, können jedoch das Verhalten der auf anderen Registerkarten konfigurierten Ports ändern.

Liste privilegierter Adressen

Sie verwenden die Registerkarte Liste der privilegierten Adressen, um Hosts Zugriff auf Ports zu gewähren, die standardmäßig geschlossen oder durch Einstellungen auf der Registerkarte externen Zugriff verwalten geschlossen sind.

Privilegierte IP-Adressen und Subnetze haben standardmäßig keinen internen Grid-Zugriff. Zudem sind die Load Balancer-Endpunkte und zusätzliche Ports, die auf der Registerkarte „privilegierte Adressen“ geöffnet wurden, auch dann verfügbar, wenn sie auf der Registerkarte „externen Zugriff verwalten“ gesperrt sind.



Einstellungen auf der Registerkarte „Liste privilegierter Adressen“ können die Einstellungen auf der Registerkarte „nicht vertrauenswürdiges Clientnetzwerk“ nicht außer Kraft setzen.

Schritte

1. Geben Sie auf der Registerkarte Liste der privilegierten Adressen die Adresse oder das IP-Subnetz ein, die Sie Zugriff auf geschlossene Ports gewähren möchten.
2. Wählen Sie optional **Add another IP address or subnet in CIDR Notation** aus, um weitere privilegierte Clients hinzuzufügen.



Fügen Sie so wenig Adressen wie möglich zur Liste der privilegierten Adressen hinzu.

3. Wählen Sie optional **privilegierten IP-Adressen erlauben, auf interne StorageGRID-Ports zuzugreifen**. Siehe "[Interne StorageGRID-Ports](#)".



Diese Option entfernt einige Schutzmaßnahmen für interne Dienste. Lassen Sie sie nach Möglichkeit deaktiviert.

4. Wählen Sie **Speichern**.

Management des externen Zugriffs

Wenn ein Port auf der Registerkarte externen Zugriff verwalten geschlossen wird, kann keine IP-Adresse ohne Grid auf den Port zugegriffen werden, es sei denn, Sie fügen die IP-Adresse der Liste privilegierter Adressen hinzu. Sie können nur Ports schließen, die standardmäßig geöffnet sind, und Sie können nur Ports öffnen, die Sie geschlossen haben.



Einstellungen auf der Registerkarte „externen Zugriff verwalten“ können die Einstellungen auf der Registerkarte „nicht vertrauenswürdiges Clientnetzwerk“ nicht außer Kraft setzen. Wenn ein Knoten beispielsweise nicht vertrauenswürdig ist, wird Port SSH/22 im Client-Netzwerk gesperrt, selbst wenn er auf der Registerkarte externen Zugriff verwalten geöffnet ist. Die Einstellungen auf der Registerkarte nicht vertrauenswürdiger Client-Netzwerk überschreiben geschlossene Ports (z. B. 443, 8443, 9443) im Client-Netzwerk.

Schritte

1. Wählen Sie **externen Zugriff verwalten**. Auf der Registerkarte wird eine Tabelle mit allen externen Ports (Ports, auf die standardmäßig nicht-Grid-Nodes zugreifen können) für die Nodes in Ihrem Grid angezeigt.
2. Konfigurieren Sie die Ports, die geöffnet und geschlossen werden sollen, mithilfe der folgenden Optionen:
 - Verwenden Sie den Umschalter neben jedem Port, um den ausgewählten Port zu öffnen oder zu schließen.
 - Wählen Sie **Alle angezeigten Ports öffnen**, um alle in der Tabelle aufgeführten Ports zu öffnen.

- Wählen Sie **Alle angezeigten Ports schließen**, um alle in der Tabelle aufgeführten Ports zu schließen.



Wenn Sie die Grid-Manager-Ports 443 oder 8443 schließen, verlieren alle Benutzer, die derzeit an einem blockierten Port verbunden sind, einschließlich Ihnen, den Zugriff auf Grid Manager, es sei denn, ihre IP-Adresse wurde der Liste der privilegierten Adressen hinzugefügt.



Verwenden Sie die Bildlaufleiste auf der rechten Seite der Tabelle, um sicherzustellen, dass Sie alle verfügbaren Ports angezeigt haben. Verwenden Sie das Suchfeld, um die Einstellungen für einen externen Port zu finden, indem Sie eine Portnummer eingeben. Sie können einen Teil der Portnummer eingeben. Wenn Sie beispielsweise einen **2** eingeben, werden alle Ports angezeigt, die den String "2" als Teil ihres Namens haben.

3. Wählen Sie **Speichern**

Nicht Vertrauenswürdiges Client-Netzwerk

Wenn das Client-Netzwerk für einen Knoten nicht vertrauenswürdig ist, akzeptiert der Knoten nur eingehenden Datenverkehr an Ports, die als Load Balancer-Endpunkte konfiguriert sind, und optional zusätzliche Ports, die Sie auf dieser Registerkarte auswählen. Auf dieser Registerkarte können Sie auch die Standardeinstellung für neue Knoten festlegen, die in einer Erweiterung hinzugefügt wurden.



Vorhandene Client-Verbindungen können fehlschlagen, wenn die Load Balancer-Endpunkte nicht konfiguriert wurden.

Die Konfigurationsänderungen, die Sie auf der Registerkarte **nicht vertrauenswürdiges Client-Netzwerk** vornehmen, überschreiben die Einstellungen auf der Registerkarte **externen Zugriff verwalten**.

Schritte

1. Wählen Sie **Nicht Vertrauenswürdiges Client-Netzwerk**.
2. Geben Sie im Abschnitt „Standard für neuen Knoten festlegen“ an, welche Standardeinstellung verwendet werden soll, wenn in einem Erweiterungsverfahren neue Knoten zum Raster hinzugefügt werden.
 - **Trusted** (Standard): Wenn ein Knoten in einer Erweiterung hinzugefügt wird, wird sein Client-Netzwerk vertrauenswürdig.
 - **UnTrusted**: Wenn ein Knoten in einer Erweiterung hinzugefügt wird, ist sein Client-Netzwerk nicht vertrauenswürdig.

Bei Bedarf können Sie zu dieser Registerkarte zurückkehren, um die Einstellung für einen bestimmten neuen Knoten zu ändern.



Diese Einstellung hat keine Auswirkung auf die vorhandenen Nodes im StorageGRID System.

3. Verwenden Sie die folgenden Optionen, um die Knoten auszuwählen, die Clientverbindungen nur an explizit konfigurierten Endpunkten des Lastausgleichs oder zusätzlichen ausgewählten Ports zulassen sollen:
 - Wählen Sie **Untrust on displayed Nodes** aus, um alle in der Tabelle angezeigten Knoten zur Liste UnTrusted Client Network hinzuzufügen.
 - Wählen Sie **Trust on displayed Nodes** aus, um alle in der Tabelle angezeigten Knoten aus der Liste

UnTrusted Client Network zu entfernen.

- Verwenden Sie den Umschalter neben den einzelnen Ports, um das Client-Netzwerk für den ausgewählten Knoten als vertrauenswürdig oder nicht vertrauenswürdig festzulegen.

Sie können beispielsweise **Untrust on displayed Nodes** auswählen, um alle Knoten zur Liste UnTrusted Client Network hinzuzufügen, und dann den Umschalter neben einem einzelnen Knoten verwenden, um diesen einzelnen Knoten zur Liste Trusted Client Network hinzuzufügen.



Verwenden Sie die Bildlaufleiste auf der rechten Seite der Tabelle, um sicherzustellen, dass Sie alle verfügbaren Knoten angezeigt haben. Verwenden Sie das Suchfeld, um die Einstellungen für jeden Knoten durch Eingabe des Knotennamens zu suchen. Sie können einen Teilnamen eingeben. Wenn Sie beispielsweise einen **GW** eingeben, werden alle Knoten angezeigt, die den String "GW" als Teil ihres Namens haben.

4. Wählen Sie optional alle zusätzlichen Ports aus, die im nicht vertrauenswürdigen Client-Netzwerk geöffnet werden sollen. Diese Ports können Zugriff auf den Grid Manager, den Tenant Manager oder beide ermöglichen.

Sie können z. B. mit dieser Option sicherstellen, dass der Grid-Manager im Client-Netzwerk zu Wartungszwecken aufgerufen werden kann.



Diese zusätzlichen Ports sind im Client-Netzwerk geöffnet, unabhängig davon, ob sie auf der Registerkarte externen Zugriff verwalten geschlossen sind.

5. Wählen Sie **Speichern**.

Die neuen Firewall-Einstellungen werden sofort angewendet und durchgesetzt. Vorhandene Client-Verbindungen können fehlschlagen, wenn die Load Balancer-Endpunkte nicht konfiguriert wurden.

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.