Verwalten eines StorageGRID-Systems

StorageGRID

NetApp
October 03, 2025

Inhalt

Verwalten eines StorageGRID-Systems

Verwenden Sie diese Anweisungen, um ein StorageGRID System zu konfigurieren und zu verwalten.

In diesen Anweisungen wird beschrieben, wie Sie mit dem Grid Manager Gruppen und Benutzer einrichten, Mandantenkonten erstellen, damit S3- und Swift-Client-Applikationen Objekte speichern und abrufen können, StorageGRID-Netzwerke konfigurieren und managen, AutoSupport konfigurieren, Node-Einstellungen verwalten und vieles mehr.

Die Anweisungen zum Management von Objekten mit Regeln und Richtlinien für das Information Lifecycle Management (ILM) wurden in verschoben"Objektmanagement mit ILM".

Diese Anweisungen richtet sich an technische Mitarbeiter, die nach der Installation ein StorageGRID System konfigurieren, verwalten und unterstützen.

Was Sie benötigen

- Sie verfügen über allgemeine Kenntnisse des StorageGRID Systems.
- Sie verfügen über ziemlich detaillierte Kenntnisse über Linux-Befehlssells, das Netzwerk und die Einrichtung und Konfiguration von Serverhardware.

Anforderungen an einen Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	Unterstützte Mindestversion
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Sie sollten das Browserfenster auf eine empfohlene Breite einstellen.

Browserbreite	Pixel
Minimum	1024
Optimal	1280

Melden Sie sich beim Grid Manager an

Sie greifen auf die Anmeldeseite des Grid Manager zu, indem Sie den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse eines Admin-Knotens in die Adressleiste eines unterstützten Webbrowsers eingeben.

Was Sie benötigen

- Sie müssen über Ihre Anmeldedaten verfügen.
- Sie müssen über die URL für den Grid Manager verfügen.
- Sie müssen einen unterstützten Webbrowser verwenden.
- Cookies müssen in Ihrem Webbrowser aktiviert sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Jedes StorageGRID System umfasst einen primären Admin-Node und eine beliebige Anzahl nicht primärer Admin-Nodes. Sie können sich bei einem beliebigen Admin-Knoten beim Grid-Manager anmelden, um das StorageGRID-System zu verwalten. Die Admin-Nodes sind jedoch nicht genau die gleichen:

- Die auf einem Admin-Knoten ausgemachten Alarmbestätigungen (Legacy-System) werden nicht auf andere Admin-Knoten kopiert. Aus diesem Grund sehen die für Alarme angezeigten Informationen auf jedem Administratorknoten möglicherweise nicht gleich aus.
- Einige Wartungsvorgänge können nur vom primären Admin-Node ausgeführt werden.

Wenn Admin-Nodes in einer HA-Gruppe (High Availability, Hochverfügbarkeit) enthalten sind, stellen Sie eine Verbindung über die virtuelle IP-Adresse der HA-Gruppe oder einen vollständig qualifizierten Domänennamen her, der der der virtuellen IP-Adresse zugeordnet ist. Der primäre Admin-Node sollte als bevorzugter Master der Gruppe ausgewählt werden, sodass Sie beim Zugriff auf den Grid-Manager auf den primären Admin-Node zugreifen können, wenn der primäre Admin-Node nicht verfügbar ist.

Schritte

1. Starten Sie einen unterstützten Webbrowser.
2. Geben Sie in der Adressleiste des Browsers die URL für den Grid Manager ein:

   `https://FQDN_or_Admin_Node_IP/`

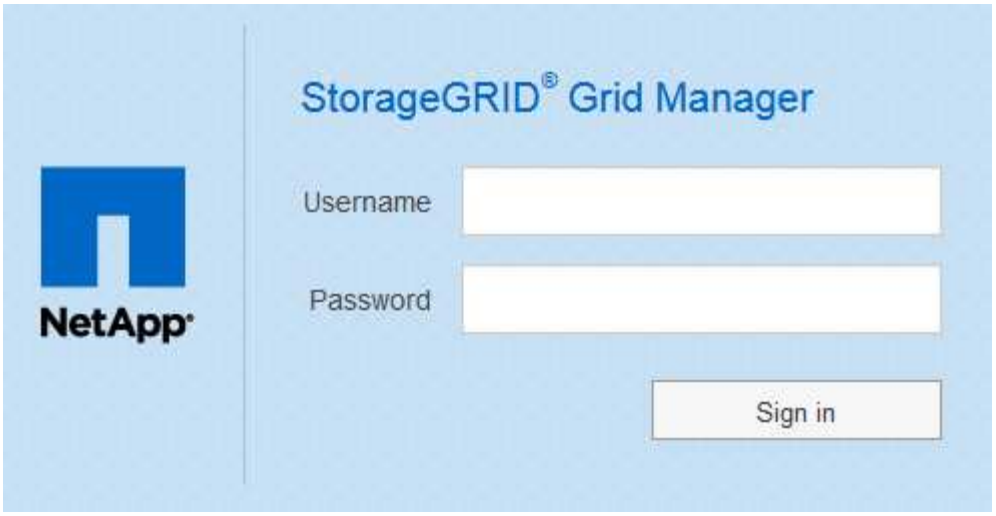
   Wo *`FQDN_or_Admin_Node_IP`* Ist ein vollständig qualifizierter Domain-Name oder die IP-Adresse eines Admin-Knotens oder die virtuelle IP-Adresse einer HA-Gruppe von Admin-Nodes.

   Wenn Sie auf den Grid Manager auf einem anderen Port als dem Standard-Port für HTTPS (443) zugreifen müssen, geben Sie Folgendes ein, wobei *`FQDN_or_Admin_Node_IP`* Ist ein vollständig qualifizierter Domain-Name oder IP-Adresse und Port ist die Port-Nummer:

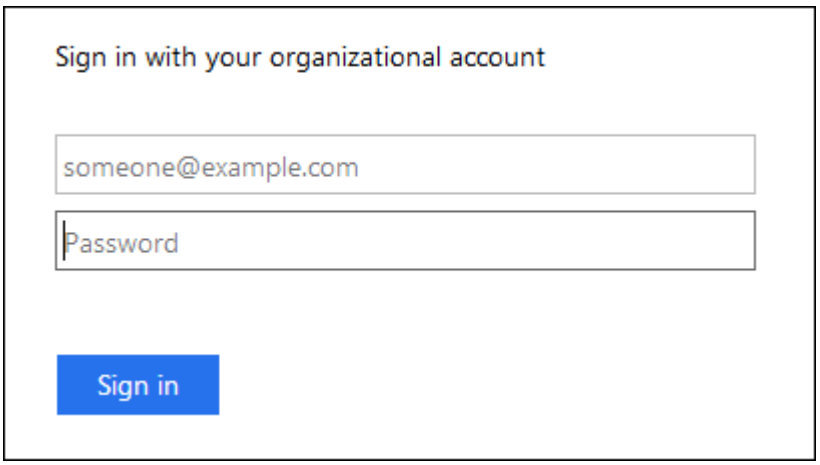
   `https://FQDN_or_Admin_Node_IP:port/`

3. Wenn Sie aufgefordert werden, eine Sicherheitswarnung zu erhalten, installieren Sie das Zertifikat mithilfe des Browser-Installationsassistenten.
4. Melden Sie sich beim Grid Manager an:

   - Wenn Single Sign On (SSO) nicht für Ihr StorageGRID-System verwendet wird:
     i. Geben Sie Ihren Benutzernamen und Ihr Kennwort für den Grid Manager ein.
     ii. Klicken Sie Auf **Anmelden**.

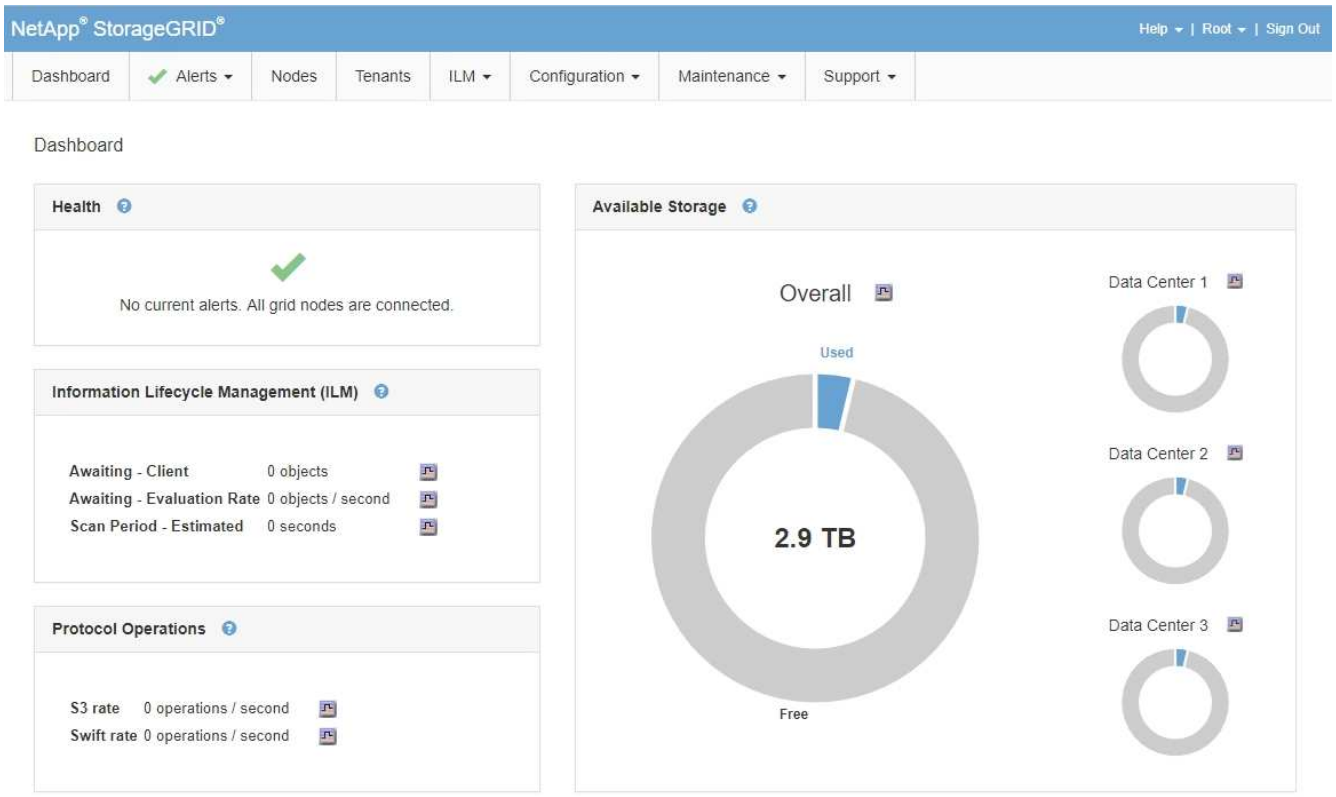


- Wenn SSO für Ihr StorageGRID-System aktiviert ist und Sie in diesem Browser zum ersten Mal auf die URL zugreifen:
  i. Klicken Sie auf **Anmelden**. Sie können das Feld Konto-ID leer lassen.
  ii. Geben Sie auf der SSO-Anmeldeseite Ihres Unternehmens Ihre Standard-SSO-Anmeldedaten ein. Beispiel:



- Wenn SSO für Ihr StorageGRID-System aktiviert ist und Sie zuvor auf den Grid Manager oder ein Mandantenkonto zugegriffen haben:
  i. Führen Sie einen der folgenden Schritte aus:
    - Geben Sie **0** (die Konto-ID für den Grid Manager) ein, und klicken Sie auf **Anmelden**.
    - Wählen Sie **Grid Manager** aus, wenn er in der Liste der letzten Konten angezeigt wird, und klicken Sie auf **Anmelden**.

ii. Melden Sie sich mit Ihren Standard-SSO-Anmeldedaten auf der SSO-Anmeldeseite Ihres Unternehmens an. Wenn Sie sich angemeldet haben, wird die Startseite des Grid Managers angezeigt, die das Dashboard enthält. Informationen zu den bereitgestellten Informationen finden Sie unter „`Viewing the Dashboard`“ in den Monitoring- und Fehlerbehebungsanweisungen für StorageGRID.



5. Wenn Sie sich bei einem anderen Admin-Knoten anmelden möchten:

Option	Schritte
SSO ist nicht aktiviert	a. Geben Sie in der Adressleiste des Browsers den vollständig qualifizierten Domänennamen oder die IP-Adresse des anderen Admin-Knotens ein. Geben Sie die Portnummer nach Bedarf an. b. Geben Sie Ihren Benutzernamen und Ihr Kennwort für den Grid Manager ein. c. Klicken Sie Auf **Anmelden**.
SSO aktiviert	Geben Sie in der Adressleiste des Browsers den vollständig qualifizierten Domänennamen oder die IP-Adresse des anderen Admin-Knotens ein. Wenn Sie sich bei einem Admin-Knoten angemeldet haben, können Sie auf andere Admin-Knoten zugreifen, ohne sich erneut anmelden zu müssen. Wenn Ihre SSO-Sitzung jedoch abläuft, werden Sie erneut zur Eingabe Ihrer Anmeldedaten aufgefordert. **Hinweis:** SSO ist auf dem Port des eingeschränkten Grid Manager nicht verfügbar. Sie müssen den Standard-HTTPS-Port (443) verwenden, wenn Benutzer sich mit Single Sign-On authentifizieren möchten.

Verwandte Informationen

"Anforderungen an einen Webbrowser"

"Zugriffskontrolle durch Firewalls"

"Serverzertifikate werden konfiguriert"

"Konfigurieren der Single Sign-On-Konfiguration"

"Verwalten von Admin-Gruppen"

"Verwalten von Hochverfügbarkeitsgruppen"

"Verwenden Sie ein Mandantenkonto"

"Monitor Fehlerbehebung"

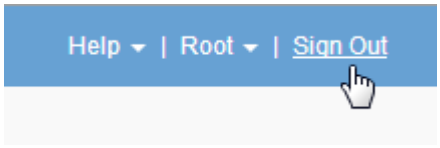
Vom Grid Manager abmelden

Wenn Sie mit dem Grid-Manager arbeiten, müssen Sie sich anmelden, um sicherzustellen, dass nicht autorisierte Benutzer nicht auf das StorageGRID-System zugreifen können. Wenn Sie Ihren Browser schließen, werden Sie möglicherweise

aufgrund der Cookie-Einstellungen des Browsers nicht aus dem System abgesendet.

Schritte

1. Klicken Sie oben rechts auf der Benutzeroberfläche auf den Link **Abmelden**.



2. Klicken Sie Auf **Abmelden**.

Option	Beschreibung
SSO wird nicht verwendet	Sie sind vom Admin-Knoten abgemeldet. Die Anmeldeseite des Grid Manager wird angezeigt. **Hinweis:** Wenn Sie sich bei mehr als einem Admin-Knoten angemeldet haben, müssen Sie sich von jedem Knoten abmelden.
SSO aktiviert	Sie sind von allen Admin-Knoten abgemeldet, auf die Sie zugreifen konnten. Die Seite StorageGRID-Anmeldung wird angezeigt. **Grid Manager** wird standardmäßig im Dropdown-Menü **Letzte Konten** aufgeführt, und im Feld **Konto-ID** wird 0 angezeigt. **Hinweis:** Wenn SSO aktiviert ist und Sie auch beim Mandantenmanager angemeldet sind, müssen Sie sich ebenfalls vom Mandantenkonto abzeichnen, um sich von SSO abzumelden.

Verwandte Informationen

"Konfigurieren der Single Sign-On-Konfiguration"

"Verwenden Sie ein Mandantenkonto"

Ihr Passwort wird geändert

Wenn Sie ein lokaler Benutzer des Grid Managers sind, können Sie Ihr eigenes Passwort ändern.

Was Sie benötigen

Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

Über diese Aufgabe

Wenn Sie sich bei StorageGRID als föderierten Benutzer anmelden oder SSO (Single Sign On) aktiviert ist, können Sie Ihr Kennwort im Grid Manager nicht ändern. Stattdessen müssen Sie Ihr Passwort in der externen Identitätsquelle ändern, z. B. Active Directory oder OpenLDAP.

Schritte

1. Wählen Sie in der Kopfzeile des Grid Managers ***your Name* > Passwort ändern**.
2. Geben Sie Ihr aktuelles Kennwort ein.
3. Geben Sie ein neues Passwort ein.

   Ihr Kennwort muss mindestens 8 und höchstens 32 Zeichen enthalten. Bei Passwörtern wird die Groß-/Kleinschreibung berücksichtigt.

4. Geben Sie das neue Passwort erneut ein.
5. Klicken Sie Auf **Speichern**.

Ändern der Provisionierungs-Passphrase

Verwenden Sie dieses Verfahren, um die StorageGRID-Provisionierungs-Passphrase zu ändern. Die Passphrase ist für Recovery-, Erweiterungs- und Wartungsvorgänge erforderlich. Die Passphrase ist außerdem erforderlich, um Backups im Recovery-Paket herunterzuladen, die Grid-Topologiedaten und Verschlüsselungen für das StorageGRID-System enthalten.

Was Sie benötigen

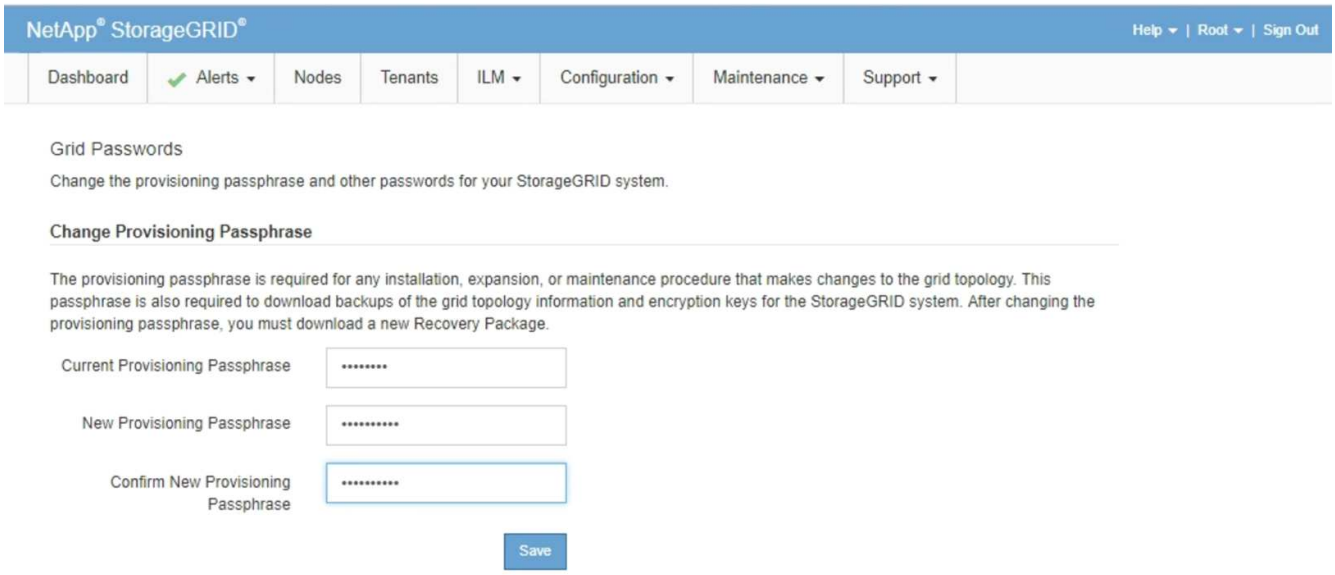
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über Wartungs- oder Root-Zugriffsberechtigungen verfügen.
- Sie müssen über die aktuelle Passphrase für die Bereitstellung verfügen.

Über diese Aufgabe

Die Provisionierungs-Passphrase ist für viele Installations- und Wartungsverfahren und für das Herunterladen des Recovery Package erforderlich. Die Provisionierungs-Passphrase wird im nicht aufgeführt `Passwords.txt` Datei: Achten Sie darauf, die Provisionierungs-Passphrase zu dokumentieren und an einem sicheren Ort zu halten.

Schritte

1. Wählen Sie **Konfiguration** > **Zugangskontrolle** > **Grid-Passwörter**.

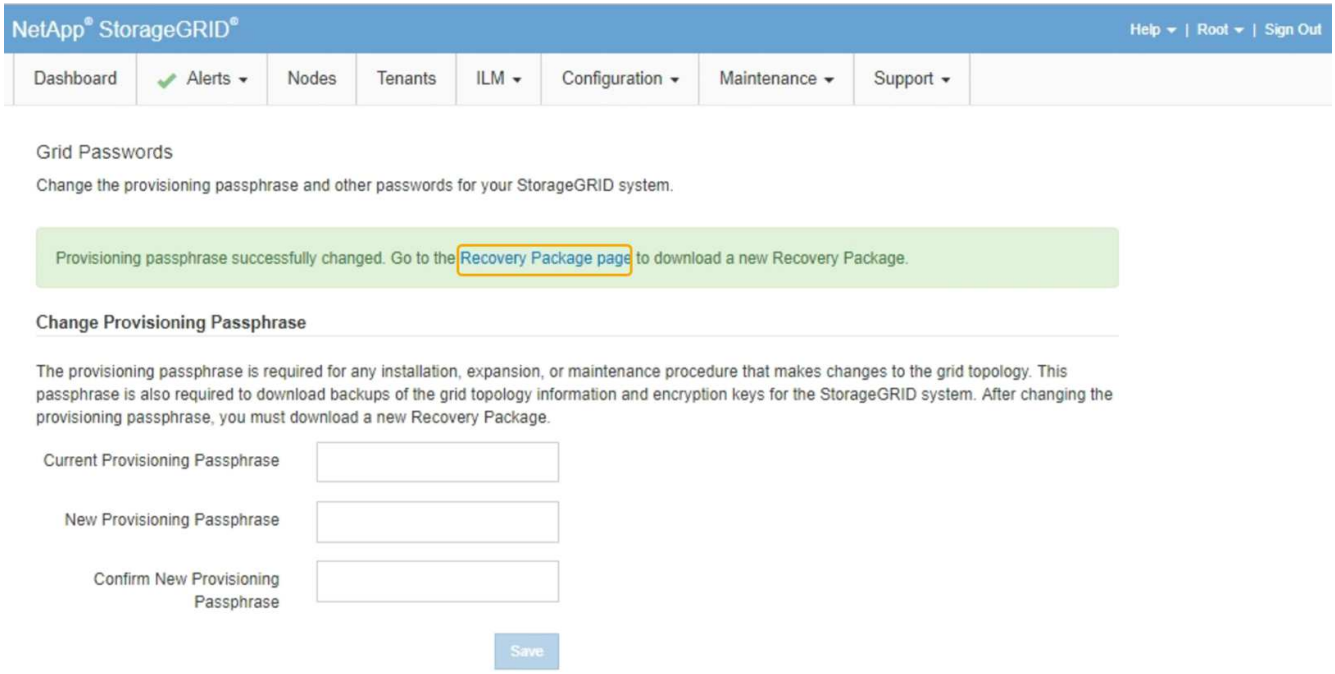


2. Geben Sie Ihre aktuelle Provisionierungs-Passphrase ein.
3. Geben Sie die neue Passphrase ein.die Passphrase muss mindestens 8 und nicht mehr als 32 Zeichen enthalten. Passphrases sind Groß-/Kleinschreibung.

> Speichern Sie die neue Provisionierungs-Passphrase an einem sicheren Ort. Sie ist für Installations-, Erweiterungs- und Wartungsverfahren erforderlich.

4. Geben Sie die neue Passphrase erneut ein, und klicken Sie auf **Speichern**.

   Das System zeigt ein grünes Erfolgsbanner an, wenn die Änderung der Provisionierungs-Passphrase abgeschlossen ist. Die Änderung sollte weniger als eine Minute dauern.



5. Wählen Sie den Link * Wiederherstellungspaket Seite* im Erfolgsbanner aus.
6. Laden Sie das neue Wiederherstellungspaket aus dem Grid Manager herunter. Wählen Sie **Wartung** >

Wiederherstellungspaket und geben Sie die neue Provisioning-Passphrase ein.

> Nachdem Sie die Provisionierungs-Passphrase geändert haben, müssen Sie sofort ein neues Wiederherstellungspaket herunterladen. Die Recovery Package-Datei ermöglicht es Ihnen, das System wiederherzustellen, wenn ein Fehler auftritt.

Ändern der Zeitüberschreitung der Browser-Sitzung

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

Was Sie benötigen

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

Über diese Aufgabe

Das Timeout für die GUI-Inaktivität ist standardmäßig auf 900 Sekunden (15 Minuten) eingestellt. Wenn die Browser-Sitzung eines Benutzers für diesen Zeitraum nicht aktiv ist, wird die Sitzung beendet.

Nach Bedarf können Sie den Timeout-Zeitraum vergrößern oder verkleinern, indem Sie die Anzeigeoption GUI Inaktivität Timeout einstellen.

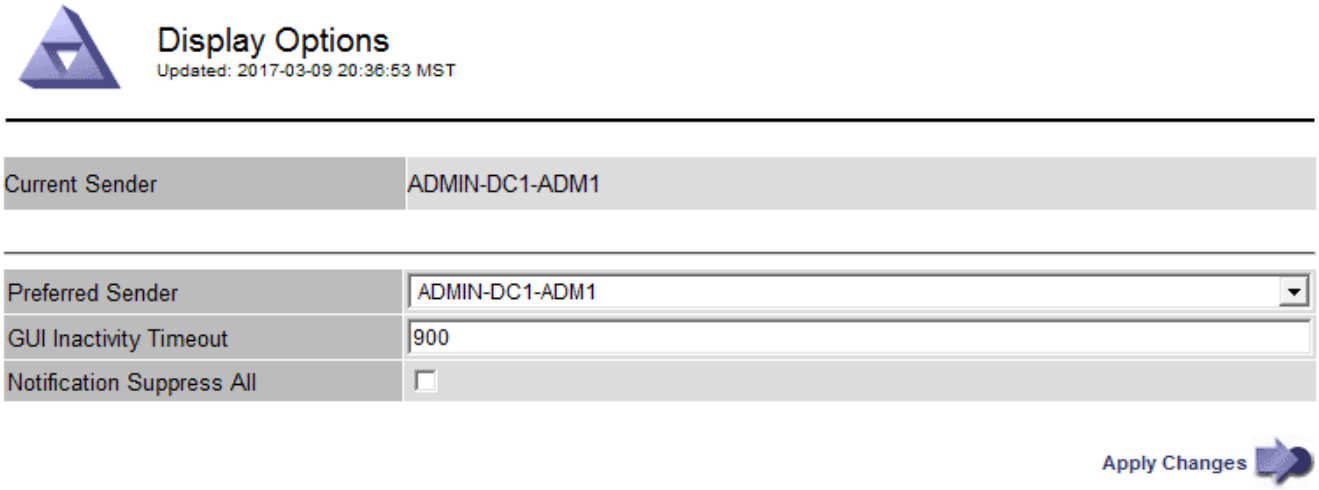
Wenn Single Sign-On (SSO) aktiviert ist und die Browsersitzung eines Benutzers beendet wird, verhält sich das System so, als ob der Benutzer manuell auf **Abmelden** geklickt hat. Der Benutzer muss seine SSO-Anmeldedaten erneut eingeben, um wieder auf StorageGRID zugreifen zu können.

> Das Timeout der Benutzersitzung kann auch durch Folgendes gesteuert werden:
>
> - 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 der Wert für das Timeout der GUI nicht erreicht wurde. Um das Token zu erneuern, muss sich der Benutzer erneut anmelden.
> - Zeitüberschreitungseinstellungen für den Identitäts-Provider, vorausgesetzt, SSO ist für StorageGRID aktiviert.

Schritte

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Anzeigeoptionen**.
2. Geben Sie für **GUI Inaktivität Timeout** einen Timeout-Zeitraum von mindestens 60 Sekunden ein.

   Setzen Sie dieses Feld auf 0, wenn Sie diese Funktion nicht verwenden möchten. Benutzer werden 16 Stunden nach ihrer Anmeldung bei Ablauf ihrer Authentifizierungs-Tokens abgemeldet.



3. Klicken Sie Auf **Änderungen Übernehmen**.

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

Verwandte Informationen

"Funktionsweise von Single Sign-On"

"Verwenden Sie ein Mandantenkonto"

Anzeigen von StorageGRID-Lizenzinformationen

Sie können die Lizenzinformationen für Ihr StorageGRID-System anzeigen, z. B. die maximale Storage-Kapazität eines Grids, wann immer sie benötigt werden.

Was Sie benötigen

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

Über diese Aufgabe

Wenn ein Problem mit der Softwarelizenz für dieses StorageGRID-System vorliegt, enthält das Bedienfeld „Systemzustand“ auf dem Dashboard ein Symbol für den Lizenzstatus und einen Link mit **Lizenz**. Die Nummer gibt an, wie viele Probleme mit Lizenzen es gibt.

Schritt

Um die Lizenz anzuzeigen, führen Sie einen der folgenden Schritte aus:

- Klicken Sie im Bedienfeld „Systemzustand“ des Dashboards auf das Symbol Lizenzstatus oder den Link **Lizenz**. Dieser Link wird nur angezeigt, wenn ein Problem mit der Lizenz vorliegt.
- Wählen Sie **Wartung** > **System** > **Lizenz**.

Die Lizenzseite wird angezeigt und enthält die folgenden, schreibgeschützten Informationen zur aktuellen Lizenz:

- StorageGRID System-ID. Hierbei handelt es sich um die eindeutige Identifikationsnummer für diese StorageGRID Installation
- Seriennummer der Lizenz
- Lizenzierte Storage-Kapazität des Grid
- Enddatum der Softwarelizenz
- Enddatum des Support-Servicevertrags
- Inhalt der Lizenztext-Datei

Bei Lizenzen, die vor StorageGRID 10.3 ausgestellt wurden, ist die lizenzierte Speicherkapazität nicht in der Lizenzdatei enthalten, und anstelle eines Werts wird eine Meldung „Siehe Lizenzvereinbarung“ angezeigt.

Die StorageGRID-Lizenzinformationen werden aktualisiert

Sie müssen die Lizenzinformationen für Ihr StorageGRID-System jederzeit aktualisieren, wenn sich die Bedingungen Ihrer Lizenz ändern. Sie müssen beispielsweise die Lizenzinformationen aktualisieren, wenn Sie zusätzliche Speicherkapazität für Ihr Grid erwerben.

Was Sie benötigen

- Sie müssen über eine neue Lizenzdatei verfügen, um sich auf Ihr StorageGRID-System bewerben zu können.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen über eine Passphrase für die Bereitstellung verfügen.

Schritte

1. Wählen Sie **Wartung** > **System** > **Lizenz**.
2. Geben Sie die Provisionierungs-Passphrase für Ihr StorageGRID-System im Textfeld **Provisioning-Passphrase** ein.
3. Klicken Sie Auf **Durchsuchen**.
4. Suchen Sie im Dialogfeld Öffnen die neue Lizenzdatei, und wählen Sie sie aus (`.txt`Und klicken Sie auf **Öffnen**.

   Die neue Lizenzdatei wird validiert und angezeigt.

5. Klicken Sie Auf **Speichern**.

Verwenden der Grid-Management-API

Sie können Systemmanagementaufgaben mithilfe der Grid Management REST-API anstelle der Grid Manager-Benutzeroberfläche ausführen. Möglicherweise möchten Sie beispielsweise die API zur Automatisierung von Vorgängen verwenden oder mehrere Einheiten, wie beispielsweise Benutzer, schneller erstellen.

Die Grid Management API verwendet die Swagger Open-Source-API-Plattform. Swagger bietet eine intuitive Benutzeroberfläche, die es Entwicklern und nicht-Entwicklern ermöglicht, mit der API Echtzeit-Operationen in StorageGRID durchzuführen.

Allgemeine Ressourcen

Die Grid Management API bietet die folgenden Ressourcen auf oberster Ebene:

- `/grid`: Der Zugriff ist auf Grid Manager-Benutzer beschränkt und basiert auf den konfigurierten Gruppenberechtigungen.
- `/org`: Der Zugriff ist auf Benutzer beschränkt, die zu einer lokalen oder föderierten LDAP-Gruppe für ein Mandantenkonto gehören. Details finden Sie in den Informationen zur Verwendung von Mandantenkonten.
- `/private`: Der Zugriff ist auf Grid Manager-Benutzer beschränkt und basiert auf den konfigurierten Gruppenberechtigungen. Diese APIs sind nur zur internen Verwendung bestimmt und nicht öffentlich dokumentiert. Diese APIs können auch ohne vorherige Ankündigung geändert werden.

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

"Prometheus: Grundlagen der Abfrage"

Grid-Management-API-Vorgänge

Die Grid Management API organisiert die verfügbaren API-Vorgänge in die folgenden Abschnitte.

- **Accounts** — Operationen für das Management von Speicher-Mandantenkonten, einschließlich der Erstellung neuer Konten und der Abruf der Speichernutzung für ein bestimmtes Konto.
- **Alarms** — Operationen zur Auflistung aktueller Alarme (Legacy-System) und zur Ausgabe von Informationen über den Systemzustand des Rasters, einschließlich der aktuellen Warnungen und einer Zusammenfassung der Knoten Verbindungsstatus.
- **Alarmverlauf** — Betrieb bei gelösten Warnmeldungen.
- **Alarm-Empfänger** — Betrieb bei Alarmbenachrichtigungen Empfänger (E-Mail).
- **Alert-rules** — Operationen für Alarmregeln.
- **Alarm-Stille** — Operationen bei Alarmgeräuschen.
- **Alerts** — Betrieb bei Warnungen.
- **Audit** — Operationen zur Auflistung und Aktualisierung der Audit-Konfiguration.
- **Auth** — Operationen zur Authentifizierung der Benutzersitzung.

  Die Grid Management API unterstützt das Authentifizierungsschema für das Inhabertoken. Zur Anmeldung

geben Sie im JSON-Text der Authentifizierungsanforderung einen Benutzernamen und ein Passwort an (d. h. `POST /api/v3/authorize`). Wenn der Benutzer erfolgreich authentifiziert wurde, wird ein Sicherheitstoken zurückgegeben. Dieses Token muss in der Kopfzeile der nachfolgenden API-Anforderungen ("Authorization: Bearer_Token_") angegeben werden.

> Wenn Single Sign-On für das StorageGRID-System aktiviert ist, müssen Sie zur Authentifizierung verschiedene Schritte durchführen. Weitere Informationen finden Sie unter „`Authentifizierung bei aktivierter Einzelanmelde-Aktivierung bei der API.`“

Informationen zur Verbesserung der Authentifizierungssicherheit finden Sie unter „`Protecting Against Cross-Site Request Forgery`“.

- **Client-Zertifikate** — Betrieb zum Konfigurieren von Client-Zertifikaten, sodass mit externen Monitoring-Tools sicher auf StorageGRID zugegriffen werden kann.
- **Config** — Operationen bezogen auf die Produktversion und Versionen der Grid Management API. Sie können die Produktversion und die Hauptversionen der von dieser Version unterstützten Grid Management API auflisten und veraltete Versionen der API deaktivieren.
- **Deaktivierte Funktionen** — Funktionen zum Anzeigen von Funktionen, die möglicherweise deaktiviert wurden.
- **dns-Server** — Operationen, um konfigurierte externe DNS-Server aufzulisten und zu ändern.
- **Endpunkt-Domain-Namen** — Operationen zum Auflisten und Ändern von Endpunkt-Domain-Namen.
- **Erasure-Coding** — Operationen auf Erasure Coding-Profilen.
- **Erweiterung** — Betrieb bei Erweiterung (Verfahrensebene).
- **Erweiterungsknoten** — Betrieb auf Erweiterung (Knotenebene).
- **Erweiterungsstandorte** — Betrieb auf Erweiterungsebene (Standort-Ebene).
- **Grid-Networks** — Operationen zur Auflistung und Änderung der Grid-Netzwerkliste.
- **Grid-passwords** — Operationen für das Grid-Passwort-Management.
- **Groups** — Operationen zur Verwaltung lokaler Grid-Administratorgruppen und zum Abrufen von föderierten Grid-Administratorgruppen von einem externen LDAP-Server.
- **Identity-Source** — Operationen, um eine externe Identitätsquelle zu konfigurieren und föderierte Gruppen- und Benutzerinformationen manuell zu synchronisieren.
- **ilm** — Operationen zum Information Lifecycle Management (ILM).
- **Lizenz** — Operationen zum Abrufen und Aktualisieren der StorageGRID-Lizenz.
- **Logs** — Operationen zum Sammeln und Herunterladen von Protokolldateien.
- **Metriken** — Betrieb auf StorageGRID-Kennzahlen einschließlich sofortiger metrischer Abfragen zu einem einzelnen Zeitpunkt und metrischen Bereichsabfragen über einen bestimmten Zeitraum. Die Grid Management API verwendet das Prometheus Systems Monitoring Tool als Backend-Datenquelle. Informationen zum Erstellen von Prometheus-Abfragen finden Sie auf der Prometheus-Website.

  > Metriken, die enthalten*`private`* In ihren Namen sind nur für den internen Gebrauch bestimmt. Diese Kennzahlen können sich ohne Ankündigung zwischen StorageGRID Versionen ändern.

- **Node-Health** — Operationen auf Node-Status.

- **ntp-Server** — Operationen zum Auflisten oder Aktualisieren von NTP-Servern (External Network Time Protocol).
- **Objects** — Operationen an Objekten und Objektmetadaten.
- **Recovery** — Operationen für den Wiederherstellungsvorgang.
- **Recovery-Paket** — Operationen, um das Recovery-Paket herunterzuladen.
- **Regionen** — Operationen zum Anzeigen und Erstellen von Regionen.
- **s3-Object-Lock** — Operationen auf globalen S3 Object Lock Einstellungen.
- **Server-Zertifikat** — Operationen zum Anzeigen und Aktualisieren von Grid Manager-Serverzertifikaten.
- **snmp** — Betrieb auf der aktuellen SNMP-Konfiguration.
- **Verkehrsklassen** — Operationen für Verkehrsklassifizierungen.
- **UnTrusted-Client-Netzwerk** — Operationen auf der nicht vertrauenswürdigen Client-Netzwerk-Konfiguration.
- **Benutzer** — Operationen zum Anzeigen und Verwalten von Grid Manager-Benutzern.

API-Anforderungen werden ausgegeben

Die Swagger-Benutzeroberfläche bietet vollständige Details und Dokumentation für jeden API-Vorgang.

Was Sie benötigen

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

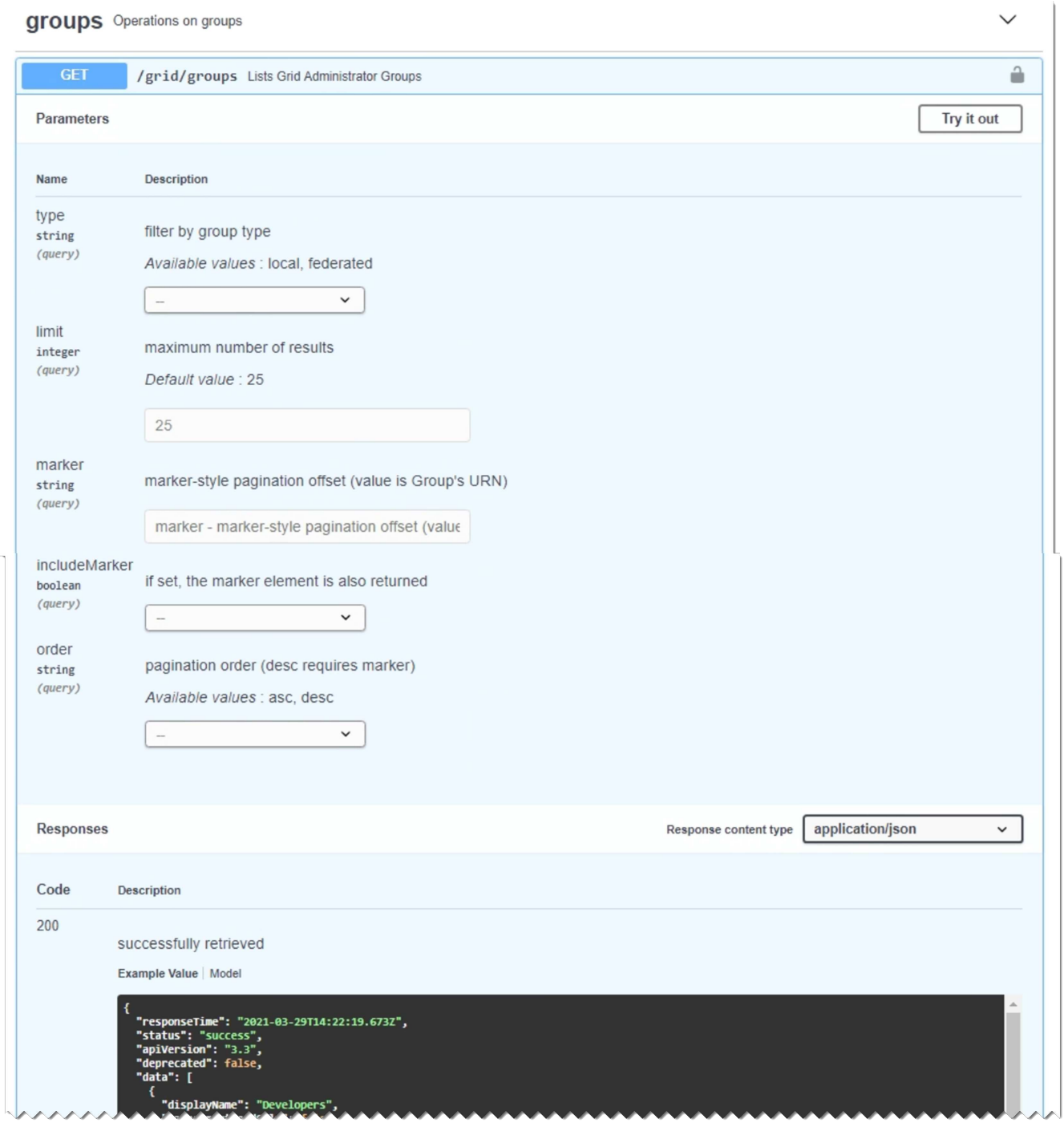
> Alle API-Operationen, die Sie mit der API Docs Webseite durchführen, sind Live-Operationen. Achten Sie darauf, dass Konfigurationsdaten oder andere Daten nicht versehentlich erstellt, aktualisiert oder gelöscht werden.

Schritte

1. Wählen Sie in der Kopfzeile des Grid Managers die Option **Hilfe** > **API-Dokumentation** aus.
2. Wählen Sie den gewünschten Vorgang aus.

   Wenn Sie einen API-Vorgang erweitern, werden die verfügbaren HTTP-Aktionen angezeigt, z. B. GET, PUT, UPDATE und DELETE.

3. Wählen Sie eine HTTP-Aktion aus, um die Anforderungsdetails anzuzeigen, einschließlich der Endpunkt-URL, einer Liste aller erforderlichen oder optionalen Parameter, einem Beispiel für den Anforderungskörper (falls erforderlich) und den möglichen Antworten.



4. Stellen Sie fest, ob für die Anforderung zusätzliche Parameter erforderlich sind, z. B. eine Gruppe oder eine Benutzer-ID. Dann erhalten Sie diese Werte. Sie müssen möglicherweise zuerst eine andere API-Anfrage stellen, um die Informationen zu erhalten, die Sie benötigen.
5. Bestimmen Sie, ob Sie den Text für die Beispielanforderung ändern müssen. In diesem Fall können Sie auf **Modell** klicken, um die Anforderungen für jedes Feld zu erfahren.
6. Klicken Sie auf **Probieren Sie es aus**.
7. Geben Sie alle erforderlichen Parameter ein, oder ändern Sie den Anforderungskörper nach Bedarf.
8. Klicken Sie Auf **Ausführen**.
9. Überprüfen Sie den Antwortcode, um festzustellen, ob die Anfrage erfolgreich war.

Die Grid Management API-Versionierung

Die Grid Management API verwendet Versionierung zur Unterstützung unterbrechungsfreier Upgrades.

Diese Anforderungs-URL gibt beispielsweise Version 3 der API an.

`https://hostname_or_ip_address/api/v3/authorize`

Die Hauptversion der Mandantenmanagement-API wird angestoßen, wenn Änderungen vorgenommen werden, die mit älteren Versionen ***nicht kompatibel*** sind. Die Nebenversion der Mandantenmanagement-API wird angestoßen, wenn Änderungen vorgenommen werden, dass ***kompatibel*** mit älteren Versionen sind. Zu den kompatiblen Änderungen gehört das Hinzufügen neuer Endpunkte oder neuer Eigenschaften. Das folgende Beispiel zeigt, wie die API-Version basierend auf dem Typ der vorgenommenen Änderungen angestoßen wird.

Typ der Änderung in API	Alte Version	Neue Version
Kompatibel mit älteren Versionen	2.1	2.2
Nicht kompatibel mit älteren Versionen	2.1	3.0

Wenn Sie die StorageGRID-Software zum ersten Mal installieren, ist nur die neueste Version der Grid-Management-API aktiviert. Wenn Sie jedoch ein Upgrade auf eine neue Funktionsversion von StorageGRID durchführen, haben Sie weiterhin Zugriff auf die ältere API-Version für mindestens eine StorageGRID-Funktionsversion.

> Sie können die Grid Management API verwenden, um die unterstützten Versionen zu konfigurieren. Weitere Informationen finden Sie im Abschnitt „`config`“ der Dokumentation der Swagger API. Sie sollten die Unterstützung für die ältere Version deaktivieren, nachdem Sie alle Grid Management API-Clients aktualisiert haben, um die neuere Version zu verwenden.

Veraltete Anfragen werden wie folgt als veraltet markiert:

- Der Antwortkopf ist "Deprecated: True"
- Der JSON-Antwortkörper enthält „veraltet“: Wahr
- Eine veraltete Warnung wird nms.log hinzugefügt. Beispiel:

```
Received call to deprecated v1 API at POST "/api/v1/authorize"
```

Ermitteln, welche API-Versionen in der aktuellen Version unterstützt werden

Verwenden Sie die folgende API-Anforderung, um eine Liste der unterstützten API-Hauptversionen anzuzeigen:

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

Angeben einer API-Version für eine Anforderung

Sie können die API-Version mithilfe eines Pfadparameters angeben (`/api/v3`) Oder eine Kopfzeile (`Api-Version: 3`). Wenn Sie beide Werte angeben, überschreibt der Kopfzeilenwert den Pfadwert.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

Schutz vor standortübergreifenden Anfrageschmieden (CSRF)

Sie können mithilfe von CSRF-Tokens die Authentifizierung verbessern, die Cookies verwendet, um Angriffe auf Cross-Site Request Forgery (CSRF) gegen StorageGRID zu schützen. Grid Manager und Tenant Manager aktivieren diese Sicherheitsfunktion automatisch; andere API-Clients können wählen, ob sie aktiviert werden sollen, wenn sie sich anmelden.

Ein Angreifer, der eine Anfrage an eine andere Website auslösen kann (z. B. mit einem HTTP-FORMULARPOST), kann dazu führen, dass bestimmte Anfragen mithilfe der Cookies des angemelten Benutzers erstellt werden.

StorageGRID schützt mit CSRF-Tokens vor CSRF-Angriffen. Wenn diese Option aktiviert ist, muss der Inhalt eines bestimmten Cookies mit dem Inhalt eines bestimmten Kopfes oder eines bestimmten POST-Body-Parameters übereinstimmen.

Um die Funktion zu aktivieren, stellen Sie die ein `csrfToken` Parameter an `true` Während der Authentifizierung. Die Standardeinstellung lautet `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Wenn wahr, A `GridCsrfToken` Cookies werden mit einem zufälligen Wert für die Anmeldung bei Grid Manager und dem gesetzt `AccountCsrfToken` Cookie wird mit einem zufälligen Wert für die Anmeldung bei Tenant Manager gesetzt.

Wenn das Cookie vorhanden ist, müssen alle Anforderungen, die den Status des Systems (POST, PUT, PATCH, DELETE) ändern können, eine der folgenden Optionen enthalten:

- Der `X-Csrf-Token` Kopfzeile, wobei der Wert der Kopfzeile auf den Wert des CSRF-Token-Cookies gesetzt ist.
- Für Endpunkte, die einen formcodierten Körper annehmen: A `csrfToken` Formularkodierung für den Anforderungskörperparameter.

Weitere Beispiele und Details finden Sie in der Online-API-Dokumentation.

> Anforderungen, die über ein CSRF-Token-Cookie-Set verfügen, werden auch die durchsetzen `"Content-Type: application/json"` Kopfzeile für jede Anfrage, die einen JSON-Anforderungskörper als zusätzlichen Schutz gegen CSRF-Angriffe erwartet.

Verwenden der API, wenn Single Sign-On aktiviert ist

Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert wurde, können Sie sich nicht mit den Standard-Authenticate-API-Anforderungen bei der Grid-Management-API oder der Mandantenmanagement-API anmelden und diese abzeichnen.

Melden Sie sich an der API an, wenn Single Sign-On aktiviert ist

Wenn Single Sign-On (SSO) aktiviert ist, müssen Sie eine Reihe von API-Anforderungen ausstellen, um ein Authentifizierungs-Token von AD FS zu erhalten, das für die Grid Management API oder die Mandantenmanagement-API gültig ist.

Was Sie benötigen

- Sie kennen den SSO-Benutzernamen und das Passwort für einen föderierten Benutzer, der einer StorageGRID-Benutzergruppe angehört.
- Wenn Sie auf die Mandanten-Management-API zugreifen möchten, kennen Sie die Mandanten-Account-ID.

Über diese Aufgabe

Um ein Authentifizierungs-Token zu erhalten, können Sie eines der folgenden Beispiele verwenden:

- Der `storagegrid-ssoauth.py` Python-Skript, das sich im Verzeichnis der Installationsdateien von

StorageGRID befindet (`./rpms` Für Red hat Enterprise Linux oder CentOS, `./debs` Für Ubuntu oder Debian, und `./vsphere` Für VMware).

- Ein Beispielworkflow von Curl-Anforderungen.

  Der Curl-Workflow kann sich aushalten, wenn Sie ihn zu langsam ausführen. Möglicherweise wird der Fehler angezeigt: Eine gültige SubjectConfirmation wurde bei dieser Antwort nicht gefunden.

  Der Beispiel-Curl-Workflow schützt das Passwort nicht vor der Sicht anderer Benutzer.

Falls Sie ein Problem mit der URL-Codierung haben, sehen Sie möglicherweise den Fehler: Nicht unterstützte SAML-Version.

Schritte

1. Wählen Sie eine der folgenden Methoden aus, um ein Authentifizierungs-Token zu erhalten:
   - Verwenden Sie die `storagegrid-ssoauth.py` Python-Skript Fahren Sie mit Schritt 2 fort.
   - Verwenden Sie Curl-Anforderungen. Fahren Sie mit Schritt 3 fort.
2. Wenn Sie den verwenden möchten `storagegrid-ssoauth.py` Skript, übergeben Sie das Skript an den Python-Interpreter und führen Sie das Skript aus.

   Geben Sie bei der entsprechenden Aufforderung Werte für die folgenden Argumente ein:

   - Der SSO-Benutzername
   - Die Domäne, in der StorageGRID installiert ist
   - Die Adresse für StorageGRID
   - Wenn Sie auf die Mandantenmanagement-API zugreifen möchten, geben Sie die Mandantenkontokennung ein.

   +
   ```
   python3 /tmp/storagegrid-ssoauth.py
   saml_user: my-sso-username
   saml_domain: my-domain
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   Das StorageGRID-Autorisierungs-Token wird in der Ausgabe bereitgestellt. Sie können das Token jetzt auch für andere Anforderungen verwenden. Dies entspricht der Verwendung der API, wenn SSO nicht verwendet wurde.

3. Wenn Sie Curl-Anforderungen verwenden möchten, gehen Sie wie folgt vor.

   a. Deklarieren der Variablen, die für die Anmeldung erforderlich sind.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID=’12345’
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```

Um auf die Grid Management API zuzugreifen, verwenden Sie 0 als `TENANTACCOUNTID`.

b. Um eine signierte Authentifizierungs-URL zu erhalten, senden Sie eine POST-Anfrage an `/api/v3/authorize-saml`, Und entfernen Sie die zusätzliche JSON-Kodierung aus der Antwort.

Dieses Beispiel zeigt eine POST-Anforderung für eine signierte Authentifizierungs-URL für `TENANTACCOUNTID`. Die Ergebnisse werden an Python -m json.Tool übergeben, um die JSON-Codierung zu entfernen.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

Die Antwort für dieses Beispiel enthält eine signierte URL, die URL-codiert ist, aber nicht die zusätzliche JSON-Kodierungsschicht enthält.

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Speichern Sie die `SAMLRequest` Aus der Antwort zur Verwendung in nachfolgenden Befehlen.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. Rufen Sie eine vollständige URL ab, die die Client-Anforderungs-ID aus AD FS enthält.

Eine Möglichkeit besteht darin, das Anmeldeformular über die URL der vorherigen Antwort anzufordern.

```
curl
"https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=
$TENANTACCOUNTID" | grep 'form method="post" id="loginForm"'
```

Die Antwort umfasst die Client-Anforderungs-ID:

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Speichern Sie die Client-Anforderungs-ID aus der Antwort.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. Senden Sie Ihre Zugangsdaten an die Formularaktion aus der vorherigen Antwort.

```
curl -X POST
"https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=
$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
  --data
"UserName=$SAMLUSER@$SAMLDOMAIN&Password=$SAMLPASSWORD&AuthMethod=For
msAuthentication" --include
```

AD FS gibt eine Umleitung 302 mit zusätzlichen Informationen in den Kopfzeilen zurück.

> Wenn Multi-Faktor-Authentifizierung (MFA) für Ihr SSO-System aktiviert ist, enthält der Formularpost auch das zweite Passwort oder andere Anmeldedaten.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. Speichern Sie die `MSISAuth` Cookie aus der Antwort.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. Senden Sie eine GET-Anfrage an den angegebenen Ort mit den Cookies aus dem AUTHENTIFIZIERUNGPOST.

```
curl
"https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=
$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
  --cookie "MSISAuth=$MSISAuth" --include
```

Die Antwortheader enthalten AD FS-Sitzungsdaten für die spätere Abmeldung, und der Antwortkörper enthält die SAMLResponse in einem verborgenen Formularfeld.

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. Speichern Sie die `SAMLResponse` Aus dem ausgeblendeten Feld:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Verwenden des gespeicherten `SAMLResponse`, Erstellen Sie eine StorageGRID`/api/saml-response` Anforderung zum Generieren eines StorageGRID-Authentifizierungs-Tokens

Für `RelayState`, Verwenden Sie die Mandanten-Konto-ID oder verwenden Sie 0, wenn Sie sich bei der Grid Management-API anmelden möchten.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

Die Antwort umfasst das Authentifizierungs-Token.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. Speichern Sie das Authentifizierungs-Token in der Antwort als `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Jetzt können Sie verwenden `MYTOKEN` Für andere Anfragen, ähnlich wie Sie die API verwenden würden, wenn SSO nicht verwendet wurde.

Wenn Single Sign-On aktiviert ist, wird die API von der API absigniert

Wenn Single Sign-On (SSO) aktiviert ist, müssen Sie eine Reihe von API-Anforderungen zum Abzeichnen der Grid Management API oder der Mandantenmanagement-API ausstellen.

Über diese Aufgabe

Bei Bedarf können Sie sich einfach von der StorageGRID-API abmelden, indem Sie sich einfach von der Seite Ihres Unternehmens abmelden. Alternativ können Sie einzelne Abmeldungen (SLO) von StorageGRID auslösen, was ein gültiges StorageGRID-Überträger-Token erfordert.

Schritte

1. Um eine signierte Abmeldeanforderung zu erstellen, übergeben `cookie "sso=true"` Zur SLO-API:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Es wird eine Abmeldung-URL zurückgegeben:

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. Speichern Sie die Abmeldung-URL.

```
export
LOGOUT_REQUEST='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEI
RfhZ...HcQ%3D%3D'
```

3. Senden Sie eine Anfrage an die Logout-URL, um SLO auszulösen und zu StorageGRID zurückzukehren.

```
curl --include "$LOGOUT_REQUEST"
```

Die Antwort 302 wird zurückgegeben. Der Umleitungsort gilt nicht für die nur-API-Abmeldung.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. Löschen Sie das StorageGRID-Überträger-Token.

Das Löschen des StorageGRID-Inhabertoken funktioniert auf die gleiche Weise wie ohne SSO. Wenn `cookie "sso=true"` Wird nicht angegeben, wird der Benutzer von StorageGRID abgemeldet, ohne dass der SSO-Status beeinträchtigt wird.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

A `204 No Content` Die Antwort zeigt an, dass der Benutzer jetzt abgemeldet ist.

```
HTTP/1.1 204 No Content
```

StorageGRID-Sicherheitszertifikate werden verwendet

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).

Eine externe Zertifizierungsstelle (CA) kann benutzerdefinierte Zertifikate ausstellen, die vollständig den Informationssicherheitsrichtlinien Ihres Unternehmens entsprechen. StorageGRID umfasst außerdem eine integrierte Zertifizierungsstelle (Certificate Authority, CA), die während der Systeminstallation interne CA-Zertifikate generiert. Diese internen CA-Zertifikate werden standardmäßig zum Schutz des internen StorageGRID-Datenverkehrs verwendet. Obwohl Sie die internen CA-Zertifikate für eine nicht-Produktionsumgebungen verwenden können, empfiehlt es sich, benutzerdefinierte Zertifikate zu verwenden, die von einer externen Zertifizierungsstelle signiert sind. Ungesicherte Verbindungen ohne Zertifikat werden ebenfalls unterstützt, werden jedoch nicht empfohlen.

- Benutzerdefinierte CA-Zertifikate entfernen die internen Zertifikate nicht. Die benutzerdefinierten Zertifikate sollten jedoch die für die Überprüfung der Serververbindungen angegebenen Zertifikate sein.
- Alle benutzerdefinierten Zertifikate müssen den Richtlinien zur Systemhärtung für Serverzertifikate entsprechen.

  "Systemhärtung"

- 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.

Zertifikat	Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Administrator-Client-Zertifikat	Client	Wird auf jedem Client installiert, sodass StorageGRID den externen Client-Zugriff authentifizieren kann. • Ermöglicht autorisierten externen Clients den Zugriff auf die StorageGRID Prometheus-Datenbank. • Ermöglicht die sichere Überwachung von StorageGRID mit externen Tools.	**Konfiguration** > **Zugangskontrolle** > **Client-Zertifikate**	"Administrator-Client-Zertifikate werden konfiguriert"

Zertifikat	Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Zertifikat für Identitätsföderation	Server	Authentifiziert die Verbindung zwischen StorageGRID und einem externen Active Directory-, OpenLDAP- oder Oracle Directory-Server.wird für die Identitätsföderation verwendet, sodass Administratorgruppen und Benutzer von einem externen System gemanagt werden können.	**Konfiguration** > **Zugangskontrolle** > **Identitätsföderation**	"Identitätsföderation verwenden"
SSO-Zertifikat (Single Sign On)	Server	Authentifiziert die Verbindung zwischen Active Directory Federation Services (AD FS) und StorageGRID, die für SSO-Anfragen (Single Sign On) verwendet werden.	**Konfiguration** > **Zugangskontrolle** > **Single Sign-On**	"Konfigurieren der Single Sign-On-Konfiguration"
KMS-Zertifikat (Key Management Server)	Server und Client	Authentifiziert die Verbindung zwischen StorageGRID und einem externen Verschlüsselungsmanagement-Server (KMS), der Verschlüsselungsschlüssel für die StorageGRID Appliance-Nodes bereitstellt.	**Konfiguration** > **Systemeinstellungen** > **Schlüsselverwaltungsserver**	"Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)"

Zertifikat	Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Zertifikat für eine E-Mail-Benachrichtigung	Server und Client	Authentifiziert die Verbindung zwischen einem SMTP-E-Mail-Server und StorageGRID, die für Benachrichtigungen verwendet werden. • Wenn die Kommunikation mit dem SMTP-Server TLS (Transport Layer Security) erfordert, müssen Sie das CA-Zertifikat für den E-Mail-Server angeben. • Geben Sie ein Clientzertifikat nur an, wenn für den SMTP-E-Mail-Server Clientzertifikate zur Authentifizierung erforderlich sind.	**Alarme** > **E-Mail-Einrichtung**	"Monitor Fehlerbehebung"

Zertifikat	Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Endpunkt-Zertifikat für Load Balancer	Server	Authentifiziert die Verbindung zwischen S3- oder Swift-Clients und dem StorageGRID Load Balancer-Service auf Gateway-Nodes oder Admin-Nodes. Sie laden ein Load Balancer-Zertifikat hoch oder generieren ein Load Balancer-Zertifikat, wenn Sie einen Load Balancer-Endpunkt konfigurieren.Client-Anwendungen verwenden das Load Balancer-Zertifikat bei der Verbindung zu StorageGRID zum Speichern und Abrufen von Objektdaten. **Hinweis:** das Load Balancer-Zertifikat ist das am häufigsten verwendete Zertifikat während des normalen StorageGRID-Betriebs.	**Konfiguration** > **Netzwerkeinstellungen** > **Load Balancer Endpoints**	• "Konfigurieren von Load Balancer-Endpunkten" • Erstellen eines Endpunkts für den Load Balancer für FabricPool "Konfigurieren Sie StorageGRID für FabricPool"

Zertifikat	Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Zertifikat Für Den Management Interface Server	Server	Authentifiziert die Verbindung zwischen Client-Webbrowsern und der StorageGRID-Managementoberfläche, sodass Benutzer ohne Sicherheitswarnungen auf Grid-Manager und Mandantenmanager zugreifen können. Dieses Zertifikat authentifiziert auch Grid Management-API- und Mandantenmanagement-API-Verbindungen. Sie können das interne CA-Zertifikat verwenden oder ein benutzerdefiniertes Zertifikat hochladen.	**Konfiguration** > **Netzwerkeinstellungen** > **Serverzertifikate**	• "Serverzertifikate werden konfiguriert" • "Konfigurieren eines benutzerdefinierten Serverzertifikats für den Grid Manager und den Tenant Manager"
Endpunkt-Zertifikat für Cloud Storage Pool	Server	Authentifiziert die Verbindung vom StorageGRID Cloud Storage Pool an einem externen Storage-Standort (z. B. S3 Glacier oder Microsoft Azure Blob Storage). Für jeden Cloud-Provider-Typ ist ein anderes Zertifikat erforderlich.	**ILM** > **Speicherpools**	"Objektmanagement mit ILM"
Endpoint-Zertifikat für Plattform-Services	Server	Authentifiziert die Verbindung vom StorageGRID Plattform-Service zu einer S3-Storage-Ressource.	**Tenant Manager** > **STORAGE (S3)** > **Plattform-Services-Endpunkte**	"Verwenden Sie ein Mandantenkonto"

Zertifikat	Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Endpoint Server-Zertifikat für den Objekt-Storage-API-Service	Server	Authentifiziert sichere S3- oder Swift-Client-Verbindungen mit dem LDR-Service (Local Distribution Router) auf einem Storage-Node oder zum veralteten Connection Load Balancer (CLB)-Service auf einem Gateway-Node.	**Konfiguration** > **Netzwerkeinstellungen** > **Load Balancer Endpoints**	"Konfigurieren eines benutzerdefinierten Serverzertifikats für Verbindungen mit dem Speicherknoten oder dem CLB-Dienst"

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.