StorageGRID verwalten

StorageGRID

NetApp
October 03, 2025

Inhalt

StorageGRID verwalten

Administration StorageGRID: Überblick

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

Informationen zu diesen Anweisungen

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.

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

Bevor Sie beginnen

- 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.

Legen Sie los – mit StorageGRID

Anforderungen an einen Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	Unterstützte Mindestversion
Google Chrome	96
Microsoft Edge	96
Mozilla Firefox	94

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 haben Ihre Anmeldedaten.
- Sie haben die URL für den Grid Manager.
- Sie verwenden ein Unterstützter Webbrowser.
- Cookies sind in Ihrem Webbrowser aktiviert.
- Sie haben spezifische Zugriffsberechtigungen.

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 primäre Schnittstelle der Gruppe ausgewählt werden, sodass Sie beim Zugriff auf den Grid Manager auf den primären Admin-Knoten zugreifen, 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:

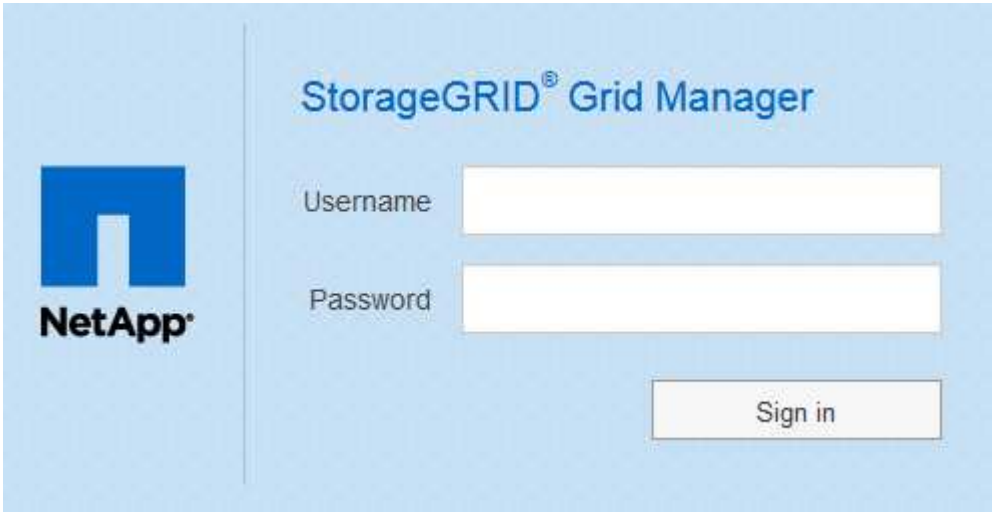
   `https://FQDN_or_Admin_Node_IP:port/`

3. Wenn Sie aufgefordert werden, eine Sicherheitswarnung zu erhalten, installieren Sie das Zertifikat mithilfe des Browser-Installationsassistenten (siehe Informationen zu Sicherheitszertifikaten).
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.

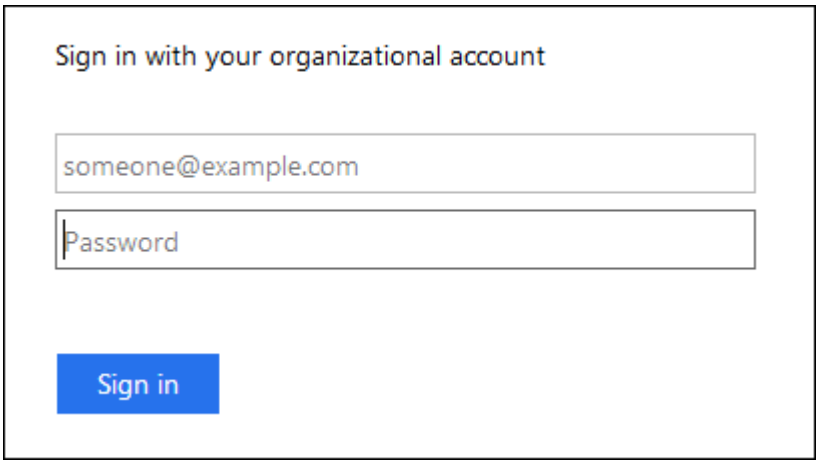
ii. Wählen Sie **Anmelden**.



- Wenn SSO für Ihr StorageGRID-System aktiviert ist und Sie in diesem Browser zum ersten Mal auf die URL zugreifen:

  i. Wählen Sie **Anmelden**. Sie können das Feld Konto-ID leer lassen.

  ii. Geben Sie auf der SSO-Anmeldeseite Ihres Unternehmens Ihre Standard-SSO-Anmeldedaten ein. Beispiel:

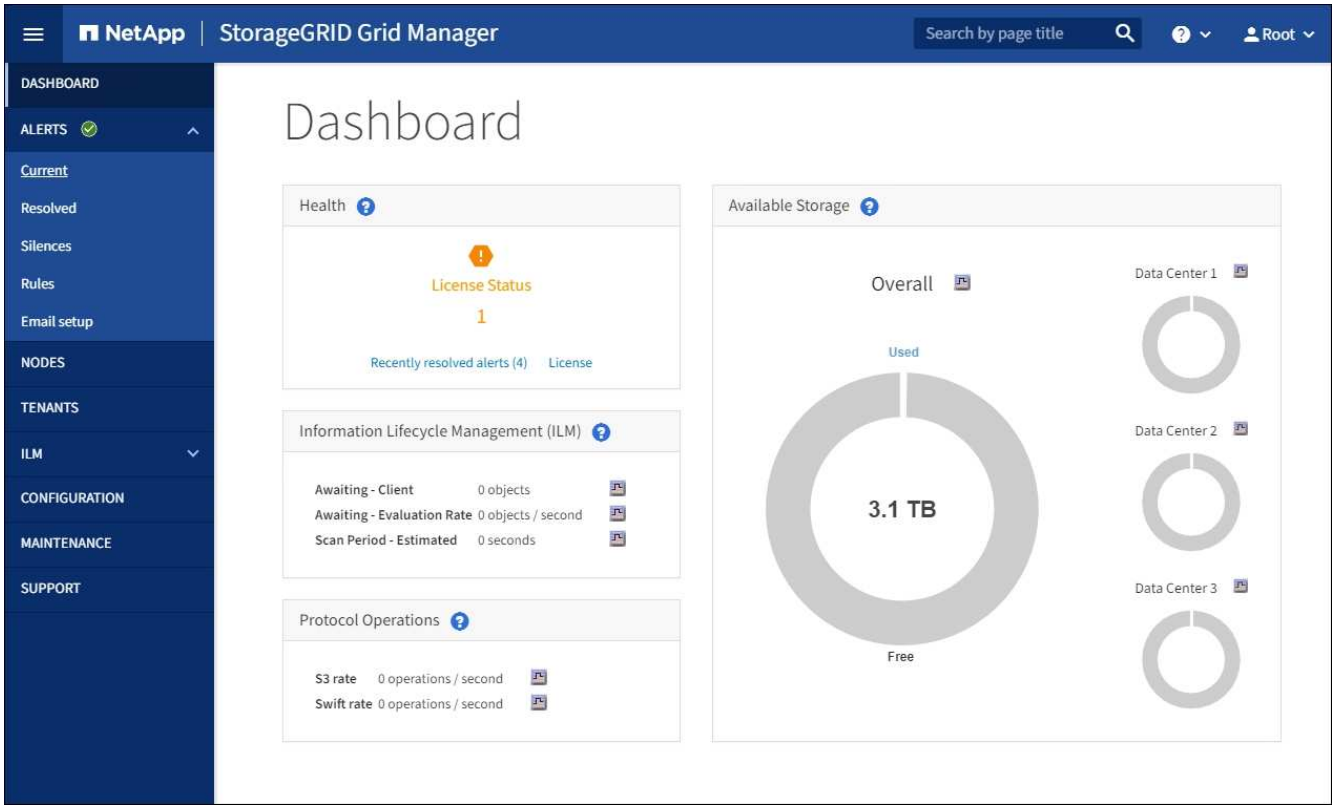


- Wenn SSO für Ihr StorageGRID-System aktiviert ist und Sie zuvor auf den Grid Manager oder ein Mandantenkonto zugegriffen haben:

  i. Führen Sie einen der folgenden Schritte aus:

  - Geben Sie **0** (die Konto-ID für den Grid Manager) ein, und wählen Sie **Anmelden**.
  - Wählen Sie **Grid Manager** aus, wenn er in der Liste der letzten Konten angezeigt wird, und wählen Sie **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 Zeigen Sie das Dashboard an.



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. Wählen Sie **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

- Kontrolle des Zugriffs durch Firewalls

- Konfigurieren Sie Single Sign-On
- Managen von Admin-Gruppen
- Management von Hochverfügbarkeitsgruppen
- Verwenden Sie ein Mandantenkonto
- Monitoring und Fehlerbehebung

Melden Sie sich vom Grid Manager ab

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. Wählen Sie oben rechts Ihren Benutzernamen aus.

2. Wählen Sie **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 Sie Single Sign-On
- Verwenden Sie ein Mandantenkonto

Passwort ändern

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

Was Sie benötigen

Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.

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** aus.
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. Wählen Sie **Speichern**.

Ändern Sie die 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 sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

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 **Abmelden** manuell ausgewählt hat. Der Benutzer muss seine SSO-Anmeldedaten erneut eingeben, um wieder auf StorageGRID zugreifen zu können. Siehe Konfigurieren Sie Single Sign-On.

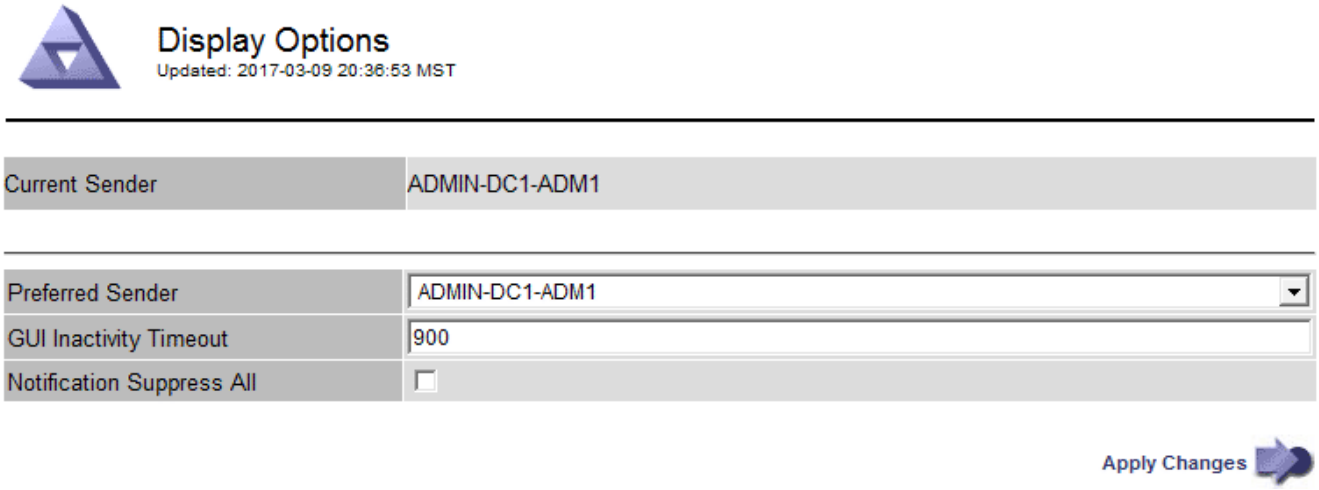
Das Timeout der Benutzersitzung kann auch durch Folgendes gesteuert werden:

- 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 System 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. Wählen Sie **Änderungen Anwenden**.

   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.

Zeigen Sie StorageGRID Lizenzinformationen an

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 sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.

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:

- Wählen Sie im Bedienfeld „Systemzustand“ des Dashboards das Symbol Lizenzstatus oder den Link **Lizenz** aus. 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.

Aktualisieren Sie die StorageGRID-Lizenzinformationen

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 haben eine neue Lizenzdatei für Ihr StorageGRID-System.
- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben die Provisionierungs-Passphrase.

Schritte

1. Wählen Sie **WARTUNG System Lizenz**.

2. Geben Sie die Provisionierungs-Passphrase für Ihr StorageGRID-System im Textfeld **Provisioning-Passphrase** ein.
3. Wählen Sie **Durchsuchen**.
4. Suchen Sie im Dialogfeld Öffnen die neue Lizenzdatei, und wählen Sie sie aus (`.txt`Und wählen Sie **Offen**.

   Die neue Lizenzdatei wird validiert und angezeigt.

5. Wählen Sie **Speichern**.

Verwenden Sie die API

Verwenden Sie die 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.

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. Weitere Informationen finden Sie unter Verwenden Sie ein Mandantenkonto.
- `/private`: Der Zugriff ist auf Grid Manager-Benutzer beschränkt und basiert auf den konfigurierten Gruppenberechtigungen. Die privaten APIs können ohne Vorankündigung geändert werden. Private StorageGRID-Endpunkte ignorieren auch die API-Version der Anforderung.

API-Anforderungen ausgeben

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.

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

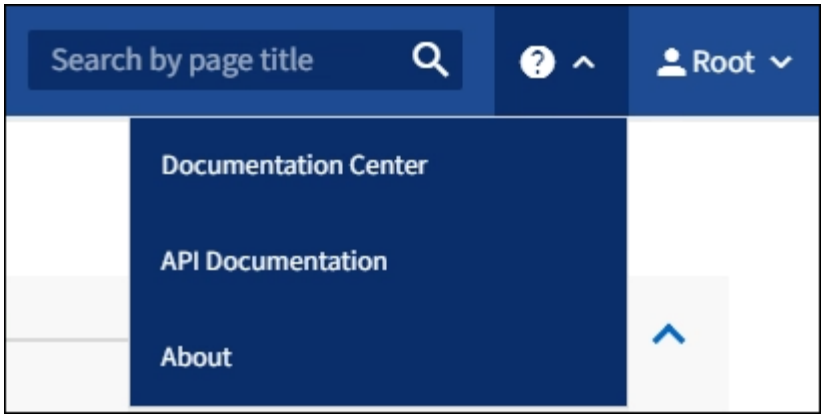
Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

> 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 das Hilfesymbol aus, und wählen Sie **API Documentation** aus.



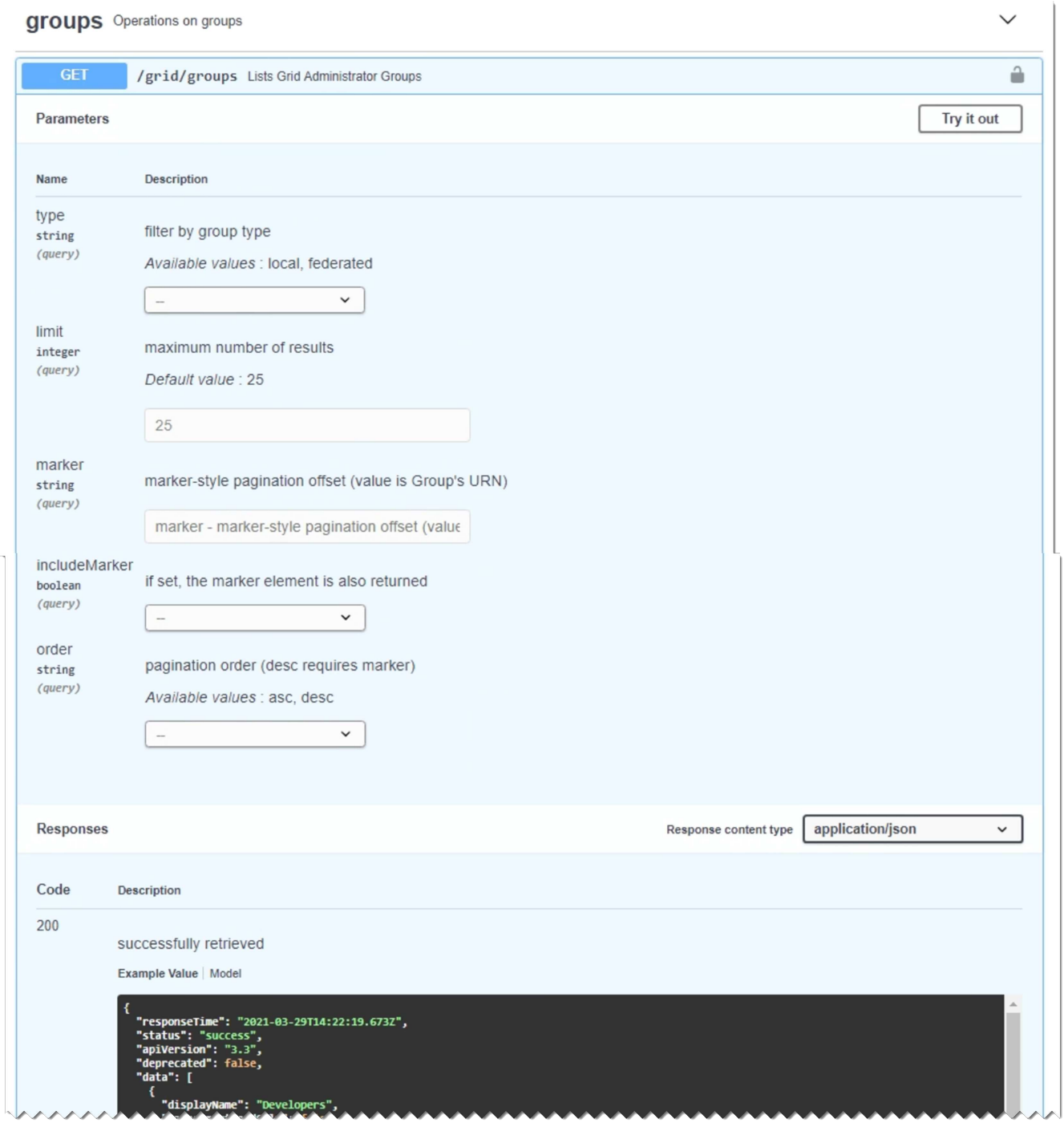
2. Um eine Operation mit der privaten API durchzuführen, wählen Sie auf der StorageGRID Management API-Seite **Gehe zur privaten API-Dokumentation** aus.

   Die privaten APIs können ohne Vorankündigung geändert werden. Private StorageGRID-Endpunkte ignorieren auch die API-Version der Anforderung.

3. 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.

4. 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.



5. 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.
6. Bestimmen Sie, ob Sie den Text für die Beispielanforderung ändern müssen. In diesem Fall können Sie **Modell** wählen, um die Anforderungen für jedes Feld zu erfahren.
7. Wählen Sie **Probieren Sie es aus**.
8. Geben Sie alle erforderlichen Parameter ein, oder ändern Sie den Anforderungskörper nach Bedarf.
9. Wählen Sie **Ausführen**.
10. Überprüfen Sie den Antwortcode, um festzustellen, ob die Anfrage erfolgreich war.

Grid-Management-API-Vorgänge

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

Diese Liste umfasst nur Vorgänge, die in der öffentlichen API verfügbar sind.

- **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-Details** — Betrieb auf Knoten Details.
- **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.

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"
```

Legen Sie fest, 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
  ]
}
```

Geben Sie eine API-Version für eine Anforderung an

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 Sie die API, wenn Single Sign-On aktiviert ist

Verwenden Sie die API, wenn Single Sign-On aktiviert ist (Active Directory).

Wenn Sie haben Konfiguration und Aktivierung von Single Sign On (SSO) Wenn Sie Active Directory als SSO-Provider verwenden, müssen Sie eine Reihe von API-Anforderungen ausstellen, um ein Authentifizierungs-Token zu erhalten, das für die Grid-Management-API oder die Mandantenmanagement-API gültig ist.

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

Diese Anweisungen gelten, wenn Sie Active Directory als SSO-Identitäts-Provider verwenden.

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: `A valid SubjectConfirmation was not found on this Response`.

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

Falls Sie ein Problem mit der URL-Codierung haben, wird möglicherweise der Fehler angezeigt: `Unsupported 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:

   - Die SSO-Methode. Geben Sie ADFS oder adfs ein.
   - Der SSO-Benutzername
   - Die Domäne, in der StorageGRID installiert ist
   - Die Adresse für StorageGRID
   - Die Mandantenkonto-ID, wenn Sie auf die Mandantenmanagement-API zugreifen möchten.

   ```
   python3 storagegrid-ssoauth.py
   sso_method: adfs
   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 weitergeleitet `python -m json.tool` Um die JSON-Kodierung 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=FormsAuthentication" --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.

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

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. Diese Anweisungen gelten, wenn Sie Active Directory als SSO-Identitäts-Provider verwenden

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=fZDNboMwEIRfhZ...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
```

Verwenden der API bei Aktivierung der Single Sign-On (Azure)

Wenn Sie haben Konfiguration und Aktivierung von Single Sign On (SSO) Und Sie verwenden Azure als SSO-Provider. Mit zwei Beispielskripten können Sie ein für die Grid-Management-API oder die Mandanten-Management-API gültiges Authentifizierungs-Token anfordern.

Melden Sie sich bei der API an, wenn die Single-Sign-On-Funktion von Azure aktiviert ist

Diese Anweisungen gelten, wenn Sie Azure als SSO-Identitäts-Provider verwenden

Was Sie benötigen

- Sie kennen die SSO E-Mail-Adresse und das Passwort für einen föderierten Benutzer, der zu einer StorageGRID Benutzergruppe gehört.
- 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 die folgenden Beispielskripte verwenden:

- Der `storagegrid-ssoauth-azure.py` Python-Skript
- Der `storagegrid-ssoauth-azure.js` Node.js-Skript

Beide Skripte befinden sich im Verzeichnis der StorageGRID Installationsdateien (`./rpms` Für Red hat Enterprise Linux oder CentOS, `./debs` Für Ubuntu oder Debian, und `./vsphere` Für VMware).

Informationen zum Schreiben Ihrer eigenen API-Integration in Azure finden Sie im `storagegrid-ssoauth-azure.py` Skript: Das Python-Skript stellt zwei Anfragen direkt an StorageGRID (zuerst um die SAMLRequest zu erhalten, und später um das Autorisierungs-Token zu erhalten) und ruft auch das Node.js-Skript auf, um mit Azure zu interagieren, um die SSO-Operationen durchzuführen.

SSO-Vorgänge können mit einer Reihe von API-Anfragen ausgeführt werden, allerdings ist dies relativ unkompliziert. Das Puppeteer Node.js-Modul wird verwendet, um die Azure SSO-Schnittstelle zu kratzen.

Falls Sie ein Problem mit der URL-Codierung haben, wird möglicherweise der Fehler angezeigt: `Unsupported SAML version.`

Schritte

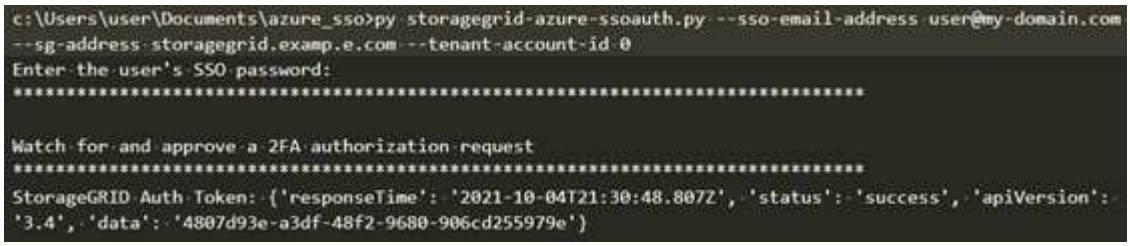
1. Installieren Sie die erforderlichen Abhängigkeiten:
   a. Installieren Sie Node.js (siehe) "https://nodejs.org/en/download/").
   b. Installieren Sie die erforderlichen Node.js-Module (Puppenspieler und jsdom):

      ```
      npm install -g <module>
      ```

2. Übergeben Sie das Python-Skript an den Python-Interpreter, um das Skript auszuführen.

   Das Python-Skript wird dann das entsprechende Node.js-Skript aufrufen, um die Azure SSO-Interaktionen durchzuführen.

3. Geben Sie bei Aufforderung Werte für die folgenden Argumente ein (oder geben Sie diese mit Hilfe von Parametern weiter):
   - Die SSO-E-Mail-Adresse, mit der Sie sich bei Azure anmelden können
   - Die Adresse für StorageGRID
   - Die Mandantenkonto-ID, wenn Sie auf die Mandantenmanagement-API zugreifen möchten
4. Geben Sie bei der entsprechenden Aufforderung das Passwort ein und bereiten Sie sich darauf vor, auf Wunsch Azure eine MFA-Autorisierung zur Verfügung zu stellen.



> Das Skript geht davon aus, dass MFA mithilfe von Microsoft Authenticator ausgeführt wird. Möglicherweise müssen Sie das Skript ändern, um andere Formen von MFA zu unterstützen (z. B. Eingabe eines über eine Textnachricht empfangenen Codes).

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.

Verwenden Sie die API, wenn Single Sign-On aktiviert ist (PingFederate)

Wenn Sie haben Konfiguration und Aktivierung von Single Sign On (SSO) Und Sie verwenden PingFederate als SSO-Provider. Um ein Authentifizierungs-Token zu erhalten, das für die Grid Management API oder die Mandantenmanagement-API gültig ist, müssen Sie eine Reihe von API-Anforderungen ausgeben.

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

Diese Anweisungen gelten, wenn Sie PingFederate als SSO-Identitäts-Provider verwenden

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: `A valid SubjectConfirmation was not found on this Response`.

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

  Falls Sie ein Problem mit der URL-Codierung haben, wird möglicherweise der Fehler angezeigt: `Unsupported 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:

   - Die SSO-Methode. Sie können eine beliebige Variante von „`pingfederate`“ (PINGFEDERATE, pingfederate usw.) eingeben.
   - Der SSO-Benutzername
   - Die Domäne, in der StorageGRID installiert ist. Dieses Feld wird nicht für PingFederate verwendet. Sie können es leer lassen oder einen beliebigen Wert eingeben.
   - Die Adresse für StorageGRID
   - Die Mandantenkonto-ID, wenn Sie auf die Mandantenmanagement-API zugreifen möchten.

```
python3 storagegrid-ssoauth.py
sso_method: pingfederate
saml_user: my-sso-username
saml_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 TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.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://my-pf-baseurl/idp/SSO.saml2?...",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

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

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

   d. Exportieren Sie die Antwort und das Cookie, und wiederholen Sie die Antwort:

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. Exportieren Sie den Wert „pf.adaptterId“, und geben Sie die Antwort ein:

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. Exportieren Sie den 'href'-Wert (entfernen Sie den hinteren Schrägstrich /), und wiederholen Sie die Antwort:

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. Den Wert „Aktion“ exportieren:

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. Senden von Cookies zusammen mit den Zugangsdaten:

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

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.

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

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. Diese Anweisungen gelten, wenn Sie PingFederate als SSO-Identitäts-Provider verwenden

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://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2021-10-12T22:20:30.839Z",
    "status": "success"
}
```

2. Speichern Sie die Abmeldung-URL.

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...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: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

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
```

Kontrolle des Zugriffs auf StorageGRID

Ändern Sie die 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, Passwörter für die Grid-Node-Konsole und Verschlüsselungsschlüssel für das StorageGRID-System enthalten.

Was Sie benötigen

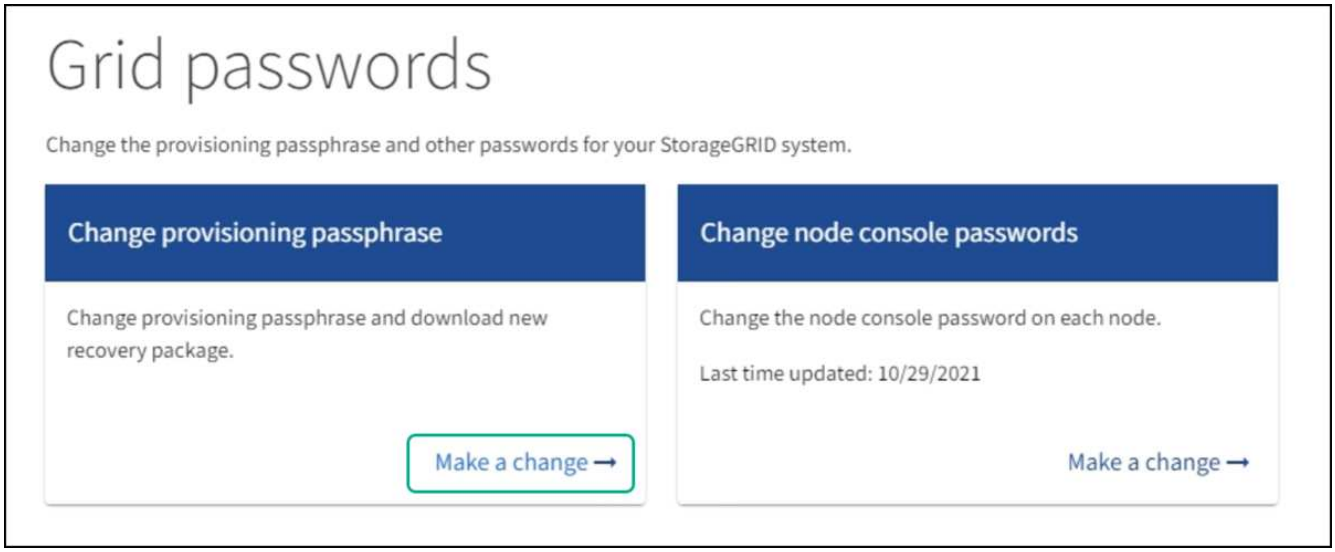
- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie verfügen über Wartungs- oder Root-Zugriffsberechtigungen.
- Sie haben die aktuelle Provisionierungs-Passphrase.

Über diese Aufgabe

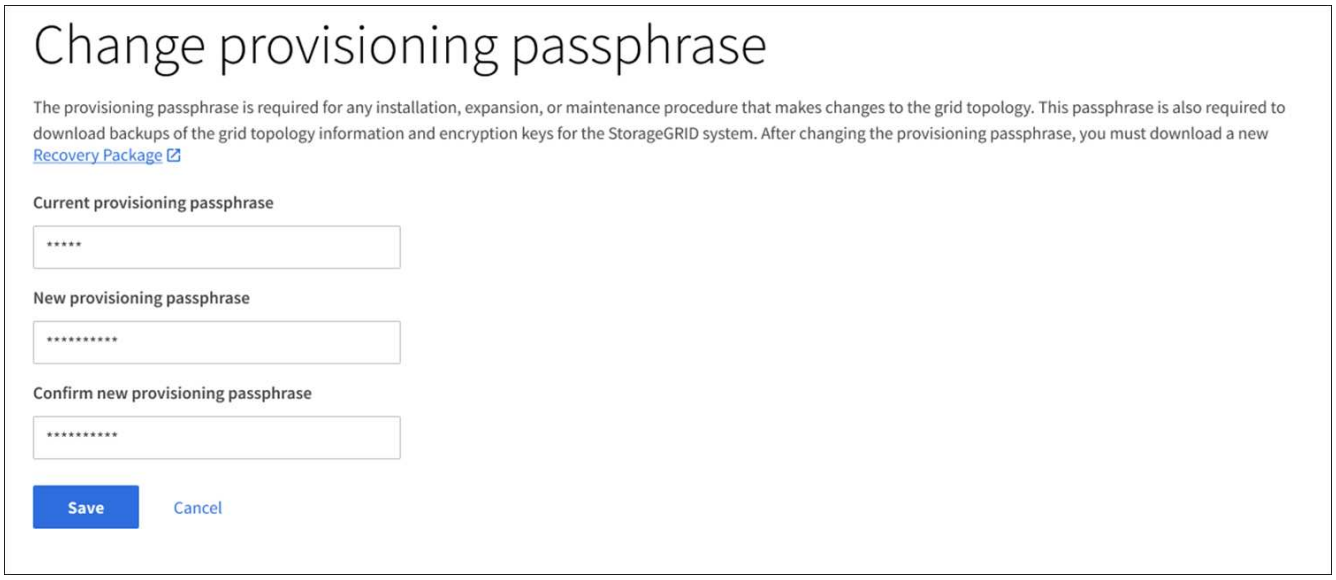
Die Provisionierungs-Passphrase ist für viele Installations- und Wartungsverfahren und für erforderlich Herunterladen des Wiederherstellungspakets. Die Provisionierungs-Passphrase wird im nicht aufgeführt `Passwords.txt` Datei: Achten Sie darauf, die Provisionierungs-Passphrase zu dokumentieren und an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

Schritte

1. Wählen Sie **KONFIGURATION Zugriffskontrolle Grid-Passwörter**.

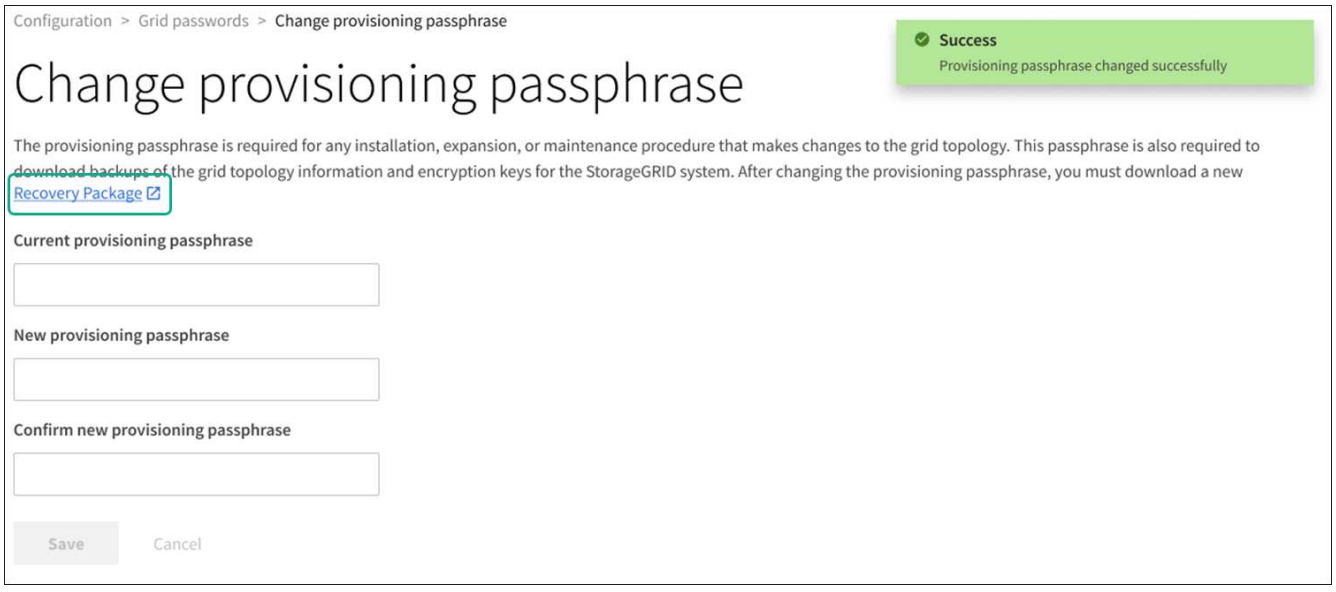


2. Wählen Sie unter **Provisioning-Passphrase ändern** * die Option **Ändern**.



3. Geben Sie Ihre aktuelle Provisionierungs-Passphrase ein.
4. Geben Sie die neue Passphrase ein. Die Passphrase muss mindestens 8 und maximal 32 Zeichen enthalten. Passphrases sind Groß-/Kleinschreibung.
5. Speichern Sie die neue Provisionierungs-Passphrase an einem sicheren Ort. Sie ist für Installations-, Erweiterungs- und Wartungsverfahren erforderlich.
6. Geben Sie die neue Passphrase erneut ein, und wählen Sie **Speichern**.

   Das System zeigt ein grünes Erfolgsbanner an, wenn die Änderung der Provisionierungs-Passphrase abgeschlossen ist.



7. Wählen Sie **Wiederherstellungspaket**.
8. Geben Sie die neue Provisionierungs-Passphrase ein, um das neue Wiederherstellungspaket herunterzuladen.

> 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 Passwörter für die Node-Konsole

Jeder Node in Ihrem Raster verfügt über ein eindeutiges Node-Konsolenpasswort, das Sie sich beim Node einloggen müssen. Verwenden Sie diese Schritte, um jedes eindeutige Node-Konsolenpasswort für jeden Node im Raster zu ändern.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die Berechtigung Wartung oder Stammzugriff.
- Sie haben die aktuelle Provisionierungs-Passphrase.

Über diese Aufgabe

Verwenden Sie das Node-Konsolenpasswort, um sich mit SSH bei einem Knoten als „admin“ oder beim Root-Benutzer einer VM/physischen Konsolenverbindung anzumelden. Mit dem Passwort für die Änderungsknotenkonsole werden für jeden Knoten in der Tabelle neue Passwörter erstellt und die Passwörter in einem aktualisierten System gespeichert `Passwords.txt` Datei im Wiederherstellungspaket. Die Passwörter sind in der Spalte Kennwort im aufgeführt `Passwords.txt` Datei:

> Separate SSH-Zugriffskennwörter für die SSH-Schlüssel, die für die Kommunikation zwischen den Nodes verwendet werden. Die SSH-Zugriffskennwörter werden durch dieses Verfahren nicht geändert.

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **KONFIGURATION Zugriffskontrolle Grid-Passwörter**.
2. Wählen Sie unter **Change Node Console passwords** die Option **make a change** aus.

Geben Sie die Provisionierungs-Passphrase ein

Schritte

1. Geben Sie die Provisionierungs-Passphrase für Ihr Grid ein.
2. Wählen Sie **Weiter**.

Laden Sie das aktuelle Wiederherstellungspaket herunter

Laden Sie das aktuelle Wiederherstellungspaket herunter, bevor Sie die Kennwörter der Node-Konsole ändern. Sie können die Passwörter in dieser Datei verwenden, wenn die Passwortänderung für einen beliebigen Knoten fehlschlägt.

Schritte

1. Wählen Sie **Wiederherstellungspaket herunterladen**.
2. Kopieren Sie die Wiederherstellungspaket-Datei (`.zip`) An zwei sichere und getrennte Stellen.

> Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können.

3. Wählen Sie **Weiter**.

4. Wenn das Bestätigungsdialogfeld angezeigt wird, wählen Sie **Yes** aus, wenn Sie bereit sind, die Kennwörter der Knotenkonsole zu ändern.

   Sie können diesen Vorgang nach dem Start nicht abbrechen.

Ändern der Passwörter für die Node-Konsole

Wenn der Kennwortprozess der Knotenkonsole gestartet wird, wird ein neues Wiederherstellungspaket erstellt, das die neuen Kennwörter enthält. Anschließend werden die Passwörter auf jedem Node aktualisiert.

Schritte

1. Warten Sie, bis das neue Wiederherstellungspaket erstellt wurde. Dies kann einige Minuten dauern.
2. Wählen Sie **Neues Wiederherstellungspaket herunterladen**.
3. Wenn der Download abgeschlossen ist:

   a. Öffnen Sie das `.zip` Datei:

   b. Bestätigen Sie, dass Sie auf den Inhalt zugreifen können, einschließlich `Passwords.txt` Datei, die die neuen Passwörter für die Node-Konsole enthält.

   c. Kopieren Sie die neue Wiederherstellungspaket-Datei (`.zip`) An zwei sichere und getrennte Stellen.

   > Überschreiben Sie das alte Wiederherstellungspaket nicht.

   Die Recovery Package-Datei muss gesichert sein, weil sie Verschlüsselungsschlüssel und Passwörter enthält, die zum Abrufen von Daten vom StorageGRID-System verwendet werden können.

4. Aktivieren Sie das Kontrollkästchen, um anzugeben, dass Sie das neue Wiederherstellungspaket heruntergeladen und den Inhalt überprüft haben.
5. Wählen Sie **Knotenkonsolenpasswörter ändern** und warten Sie, bis alle Knoten mit den neuen Kennwörtern aktualisiert werden. Dies kann einige Minuten dauern.

   Wenn Passwörter für alle Nodes geändert werden, wird ein grünes Erfolgsbanner angezeigt. Fahren Sie mit dem nächsten Schritt fort.

   Wenn während des Aktualisierungsvorgangs ein Fehler auftritt, zeigt eine Bannermeldung die Anzahl der Knoten an, bei denen die Passwörter nicht geändert wurden. Das System wiederholt den Prozess automatisch auf jedem Knoten, bei dem das Kennwort nicht geändert wurde. Wenn der Prozess endet, wenn einige Knoten noch kein geändertes Kennwort haben, wird die Schaltfläche **Wiederholen** angezeigt.

   Wenn die Kennwortaktualisierung für einen oder mehrere Knoten fehlgeschlagen ist:

   a. Überprüfen Sie die in der Tabelle aufgeführten Fehlermeldungen.

   b. Beheben Sie die Probleme.

   c. Wählen Sie **Wiederholen**.

   > Beim erneuten Versuch werden nur die Kennwörter der Knotenkonsole auf den Knoten geändert, die bei früheren Kennwortänderungsversuchen fehlgeschlagen sind.

6. Nachdem die Passwörter für die Node-Konsole für alle Nodes geändert wurden, löschen Sie die Erstes heruntergeladenes Wiederherstellungspaket.

7. Verwenden Sie optional den Link **Recovery Package**, um eine zusätzliche Kopie des neuen Recovery Package herunterzuladen.

Kontrolle des Zugriffs durch Firewalls

Wenn Sie den Zugriff über Firewalls steuern möchten, öffnen oder schließen Sie bestimmte Ports an der externen Firewall.

Kontrolle des Zugriffs über die externe Firewall

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.

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	• 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 Mandanten-Manager oder die Mandanten-Management-API zugreifen. • Anfragen nach internen Inhalten werden abgelehnt.
9443	Eingeschränkter Mandantenmanager-Port an Admin-Nodes	• 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

Verwenden Sie den Identitätsverbund

Durch die Verwendung von Identity Federation lassen sich Gruppen und Benutzer schneller einrichten, und Benutzer können sich mithilfe vertrauter Anmeldedaten bei StorageGRID anmelden.

Konfigurieren Sie die Identitätsföderation für Grid Manager

Sie können eine Identitätsföderation im Grid Manager konfigurieren, wenn Administratorgruppen und Benutzer in einem anderen System, z. B. Active Directory, Azure Active Directory (Azure AD), OpenLDAP oder Oracle Directory Server, gemanagt werden sollen.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.
- Sie verwenden Active Directory, Azure AD, OpenLDAP oder Oracle Directory Server als Identitäts-Provider.

> Wenn Sie einen nicht aufgeführten LDAP v3-Dienst verwenden möchten, wenden Sie sich an den technischen Support.

- Wenn Sie OpenLDAP verwenden möchten, müssen Sie den OpenLDAP-Server konfigurieren. Siehe Richtlinien für die Konfiguration eines OpenLDAP-Servers.
- Wenn Sie Single Sign On (SSO) aktivieren möchten, haben Sie die geprüft Anforderungen für die Nutzung von Single Sign On.
- Wenn Sie Transport Layer Security (TLS) für die Kommunikation mit dem LDAP-Server verwenden möchten, verwendet der Identitäts-Provider TLS 1.2 oder 1.3. Siehe Unterstützte Chiffren für ausgehende TLS-Verbindungen.

Über diese Aufgabe

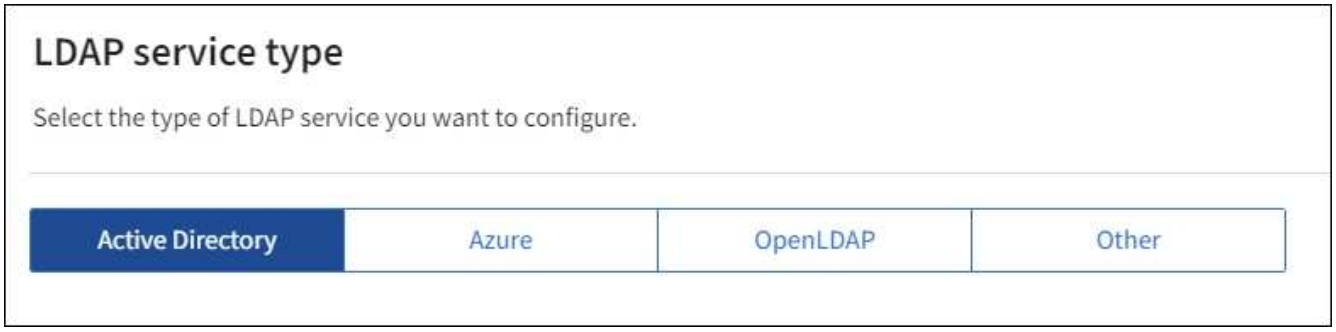
Sie können eine Identitätsquelle für den Grid Manager konfigurieren, wenn Sie Gruppen von einem anderen System wie Active Directory, Azure AD, OpenLDAP oder Oracle Directory Server importieren möchten. Sie können die folgenden Gruppen importieren:

- Admin-Gruppen. Die Benutzer in Admin-Gruppen können sich beim Grid Manager anmelden und anhand der Verwaltungsberechtigungen, die der Gruppe zugewiesen sind, Aufgaben ausführen.
- Mandanten-Benutzergruppen für Mandanten, die ihre eigene Identitätsquelle nicht verwenden Benutzer in Mandantengruppen können sich beim Mandanten-Manager anmelden und Aufgaben ausführen, basierend auf den Berechtigungen, die der Gruppe im Mandanten-Manager zugewiesen sind. Siehe Erstellen eines Mandantenkontos Und Verwenden Sie ein Mandantenkonto Entsprechende Details.

Geben Sie die Konfiguration ein

1. Wählen Sie **KONFIGURATION Zugangskontrolle Identitätsverbund**.
2. Wählen Sie **Identitätsföderation aktivieren**.

3. Wählen Sie im Abschnitt LDAP-Servicetyp den Typ des LDAP-Dienstes aus, den Sie konfigurieren möchten.



   Wählen Sie **Other** aus, um Werte für einen LDAP-Server zu konfigurieren, der Oracle Directory Server verwendet.

4. Wenn Sie **Sonstige** ausgewählt haben, füllen Sie die Felder im Abschnitt LDAP-Attribute aus. Andernfalls fahren Sie mit dem nächsten Schritt fort.
   - **Eindeutiger Benutzername**: Der Name des Attributs, das die eindeutige Kennung eines LDAP-Benutzers enthält. Dieses Attribut ist äquivalent zu `sAMAccountName` Für Active Directory und `uid` Für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `uid`.
   - **Benutzer-UUID**: Der Name des Attributs, das den permanenten eindeutigen Identifier eines LDAP-Benutzers enthält. Dieses Attribut ist äquivalent zu `objectGUID` Für Active Directory und `entryUUID` Für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `nsuniqueid`. Der Wert jedes Benutzers für das angegebene Attribut muss eine 32-stellige Hexadezimalzahl im 16-Byte- oder String-Format sein, wobei Bindestriche ignoriert werden.
   - **Group Unique Name**: Der Name des Attributs, das den eindeutigen Identifier einer LDAP-Gruppe enthält. Dieses Attribut ist äquivalent zu `sAMAccountName` Für Active Directory und `cn` Für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `cn`.
   - **Group UUID**: Der Name des Attributs, das den permanenten eindeutigen Identifier einer LDAP-Gruppe enthält. Dieses Attribut ist äquivalent zu `objectGUID` Für Active Directory und `entryUUID` Für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `nsuniqueid`. Der Wert jeder Gruppe für das angegebene Attribut muss eine 32-stellige Hexadezimalzahl im 16-Byte- oder String-Format sein, wobei Bindestriche ignoriert werden.
5. Geben Sie für alle LDAP-Servicetypen die Informationen zum erforderlichen LDAP-Server und zur Netzwerkverbindung im Abschnitt LDAP-Server konfigurieren ein.
   - **Hostname**: Der vollständig qualifizierte Domainname (FQDN) oder die IP-Adresse des LDAP-Servers.
   - **Port**: Der Port, über den eine Verbindung zum LDAP-Server hergestellt wird.

     Der Standardport für STARTTLS ist 389 und der Standardport für LDAPS ist 636. Sie können jedoch jeden beliebigen Port verwenden, solange Ihre Firewall korrekt konfiguriert ist.

   - **Benutzername**: Der vollständige Pfad des Distinguished Name (DN) für den Benutzer, der eine Verbindung zum LDAP-Server herstellt.

     Für Active Directory können Sie auch den unten angegebenen Anmeldenamen oder den Benutzerprinzipalnamen festlegen.

     Der angegebene Benutzer muss über die Berechtigung zum Auflisten von Gruppen und Benutzern

sowie zum Zugriff auf die folgenden Attribute verfügen:

- `sAMAccountName` Oder `uid`
- `objectGUID`, `entryUUID`, Oder `nsuniqueid`
- `cn`
- `memberOf` Oder `isMemberOf`
- **Active Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, und `userPrincipalName`
- **Azure**: `accountEnabled` Und `userPrincipalName`

◦ **Passwort**: Das mit dem Benutzernamen verknüpfte Passwort.

◦ **Group Base DN**: Der vollständige Pfad des Distinguished Name (DN) für einen LDAP-Unterbaum, nach dem Sie nach Gruppen suchen möchten. Im Active Directory-Beispiel (unten) können alle Gruppen, deren Distinguished Name relativ zum Basis-DN (DC=storagegrid,DC=example,DC=com) ist, als föderierte Gruppen verwendet werden.

> Die **Group Unique Name**-Werte müssen innerhalb des **Group Base DN**, zu dem sie gehören, eindeutig sein.

◦ **User Base DN**: Der vollständige Pfad des Distinguished Name (DN) eines LDAP-Unterbaums, nach dem Sie nach Benutzern suchen möchten.

> Die **Benutzer-eindeutigen Namen**-Werte müssen innerhalb des **User Base DN**, zu dem sie gehören, eindeutig sein.

◦ **Bind username Format** (optional): Das Standard-Username-Muster StorageGRID sollte verwendet werden, wenn das Muster nicht automatisch ermittelt werden kann.

Es wird empfohlen, **Bind username Format** bereitzustellen, da Benutzer sich anmelden können, wenn StorageGRID nicht mit dem Servicekonto verknüpft werden kann.

Geben Sie eines der folgenden Muster ein:

- **UserPrincipalName pattern (Active Directory und Azure)**: `[USERNAME]@*example*.com`
- **Namensmuster für Anmeldung auf der Ebene nach unten (Active Directory und Azure)**: `*example*\[USERNAME]`
- * Distinguished Name pattern*: `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

  Fügen Sie **[USERNAME]** genau wie geschrieben ein.

6. Wählen Sie im Abschnitt Transport Layer Security (TLS) eine Sicherheitseinstellung aus.

◦ **Verwenden Sie STARTTLS**: Verwenden Sie STARTTLS, um die Kommunikation mit dem LDAP-Server zu sichern. Dies ist die empfohlene Option für Active Directory, OpenLDAP oder andere, diese Option wird jedoch für Azure nicht unterstützt.

◦ **LDAPS verwenden**: Die Option LDAPS (LDAP über SSL) verwendet TLS, um eine Verbindung zum LDAP-Server herzustellen. Sie müssen diese Option für Azure auswählen.

◦ **Verwenden Sie keine TLS**: Der Netzwerkverkehr zwischen dem StorageGRID-System und dem LDAP-Server wird nicht gesichert. Diese Option wird für Azure nicht unterstützt.

Die Verwendung der Option **keine TLS** verwenden wird nicht unterstützt, wenn Ihr Active Directory-Server die LDAP-Signatur erzwingt. Sie müssen STARTTLS oder LDAPS verwenden.

7. Wenn Sie STARTTLS oder LDAPS ausgewählt haben, wählen Sie das Zertifikat aus, mit dem die Verbindung gesichert werden soll.
   - **Verwenden Sie das Betriebssystem CA-Zertifikat**: Verwenden Sie das auf dem Betriebssystem installierte Standard-Grid-CA-Zertifikat, um Verbindungen zu sichern.
   - **Benutzerdefiniertes CA-Zertifikat verwenden**: Verwenden Sie ein benutzerdefiniertes Sicherheitszertifikat.

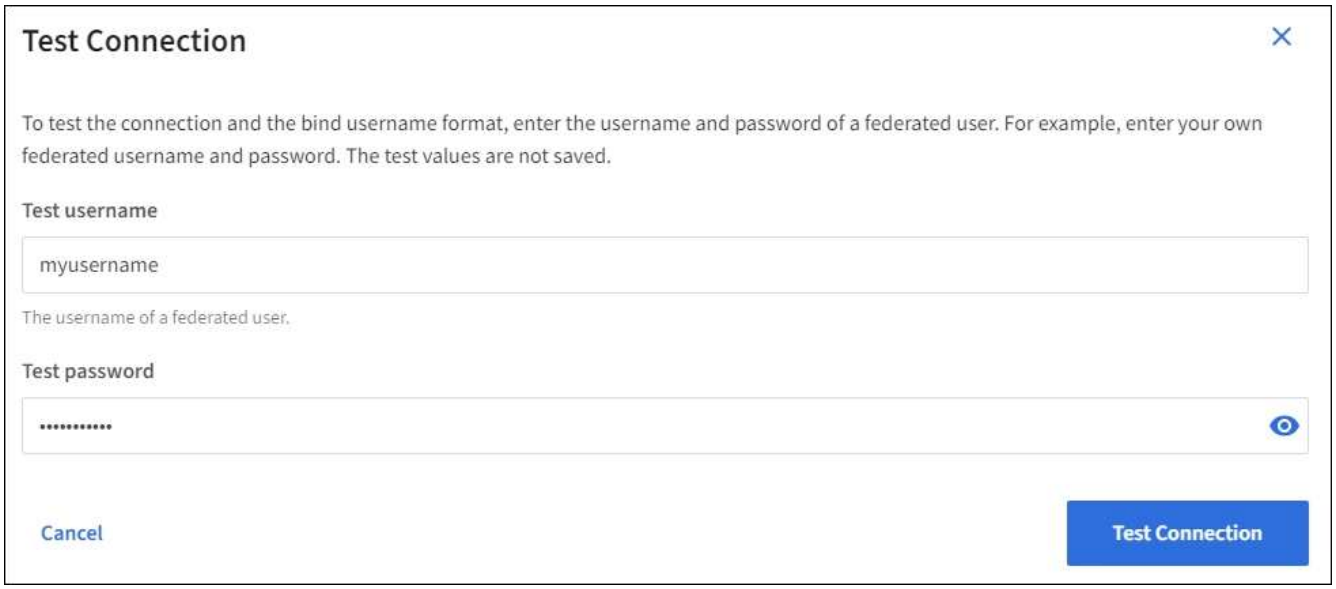
     Wenn Sie diese Einstellung auswählen, kopieren Sie das benutzerdefinierte Sicherheitszertifikat in das Textfeld CA-Zertifikat und fügen Sie es ein.

Testen Sie die Verbindung und speichern Sie die Konfiguration

Nachdem Sie alle Werte eingegeben haben, müssen Sie die Verbindung testen, bevor Sie die Konfiguration speichern können. StorageGRID überprüft die Verbindungseinstellungen für den LDAP-Server und das BIND-Username-Format, wenn Sie es angegeben haben.

1. Wählen Sie **Verbindung testen**.
2. Wenn Sie kein bind username Format angegeben haben:
   - Wenn die Verbindungseinstellungen gültig sind, wird eine Meldung „`Verbindung erfolgreich testen`“ angezeigt. Wählen Sie **Speichern**, um die Konfiguration zu speichern.
   - Wenn die Verbindungseinstellungen ungültig sind, wird eine „`Testverbindung konnte nicht hergestellt werden`“-Meldung angezeigt. Wählen Sie **Schließen**. Beheben Sie anschließend alle Probleme, und testen Sie die Verbindung erneut.
3. Wenn Sie ein bind username Format angegeben haben, geben Sie den Benutzernamen und das Kennwort eines gültigen föderierten Benutzers ein.

   Geben Sie beispielsweise Ihren eigenen Benutzernamen und Ihr Kennwort ein. Geben Sie keine Sonderzeichen in den Benutzernamen ein, z. B. @ oder /.



- Wenn die Verbindungseinstellungen gültig sind, wird eine Meldung „`Verbindung erfolgreich testen`“ angezeigt. Wählen Sie **Speichern**, um die Konfiguration zu speichern.
- Es wird eine Fehlermeldung angezeigt, wenn die Verbindungseinstellungen, das Bind-Username-Format oder der Test-Benutzername und das Kennwort ungültig sind. Beheben Sie alle Probleme, und testen Sie die Verbindung erneut.

Synchronisierung mit der Identitätsquelle erzwingen

Das StorageGRID-System synchronisiert regelmäßig föderierte Gruppen und Benutzer von der Identitätsquelle aus. Sie können die Synchronisierung erzwingen, wenn Sie Benutzerberechtigungen so schnell wie möglich aktivieren oder einschränken möchten.

Schritte

1. Rufen Sie die Seite Identity Federation auf.
2. Wählen Sie oben auf der Seite **Sync Server** aus.

   Der Synchronisierungsprozess kann je nach Umgebung einige Zeit in Anspruch nehmen.

   Die Warnmeldung * Identity Federation Failure* wird ausgelöst, wenn es ein Problem gibt, das die Synchronisierung von föderierten Gruppen und Benutzern aus der Identitätsquelle verursacht.

Deaktivieren Sie den Identitätsverbund

Sie können den Identitätsverbund für Gruppen und Benutzer vorübergehend oder dauerhaft deaktivieren. Wenn die Identitätsföderation deaktiviert ist, besteht keine Kommunikation zwischen StorageGRID und der Identitätsquelle. Allerdings bleiben alle von Ihnen konfigurierten Einstellungen erhalten, sodass Sie die Identitätsföderation zukünftig einfach wieder aktivieren können.

Über diese Aufgabe

Bevor Sie die Identitätsföderation deaktivieren, sollten Sie Folgendes beachten:

- Verbundene Benutzer können sich nicht anmelden.
- Föderierte Benutzer, die sich derzeit anmelden, erhalten bis zu ihrem Ablauf Zugriff auf das StorageGRID-System, können sich jedoch nach Ablauf der Sitzung nicht anmelden.
- Die Synchronisierung zwischen dem StorageGRID-System und der Identitätsquelle erfolgt nicht, und Warnmeldungen oder Alarme werden nicht für Konten ausgelöst, die nicht synchronisiert wurden.
- Das Kontrollkästchen **Identitätsföderation aktivieren** ist deaktiviert, wenn Single Sign-On (SSO) auf **Enabled** oder **Sandbox Mode** gesetzt ist. Der SSO-Status auf der Seite Single Sign-On muss **deaktiviert** sein, bevor Sie die Identitätsföderation deaktivieren können. Siehe Deaktivieren Sie Single Sign-On.

Schritte

1. Rufen Sie die Seite Identity Federation auf.
2. Deaktivieren Sie das Kontrollkästchen * Identitätsföderation aktivieren*.

Richtlinien für die Konfiguration eines OpenLDAP-Servers

Wenn Sie einen OpenLDAP-Server für die Identitätsföderation verwenden möchten, müssen Sie bestimmte Einstellungen auf dem OpenLDAP-Server konfigurieren.

Für Identitätsquellen, die nicht ActiveDirectory oder Azure sind, blockiert StorageGRID den S3-Zugriff nicht automatisch für Benutzer, die extern deaktiviert sind. Um den S3-Zugriff zu blockieren, löschen Sie alle S3-Schlüssel für den Benutzer und entfernen Sie den Benutzer aus allen Gruppen.

Überlagerungen in Memberof und Refint

Die Überlagerungen Memberof und Refint sollten aktiviert sein. Weitere Informationen finden Sie in den Anweisungen zur Wartung der Umkehrgruppenmitgliedschaft imhttp://www.openldap.org/doc/admin24/index.html["OpenLDAP-Dokumentation: Version 2.4 Administratorhandbuch"^].

Indizierung

Sie müssen die folgenden OpenLDAP-Attribute mit den angegebenen Stichwörtern für den Index konfigurieren:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Stellen Sie außerdem sicher, dass die in der Hilfe für den Benutzernamen genannten Felder für eine optimale Leistung indiziert sind.

Weitere Informationen zur Wartung von Gruppenmitgliedschaften finden Sie imhttp://www.openldap.org/doc/admin24/index.html["OpenLDAP-Dokumentation: Version 2.4 Administratorhandbuch"^].

Managen von Admin-Gruppen

Sie können Administratorgruppen erstellen, um die Sicherheitsberechtigungen für einen oder mehrere Admin-Benutzer zu verwalten. Benutzer müssen zu einer Gruppe gehören, die Zugriff auf das StorageGRID-System gewährt.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.
- Wenn Sie eine föderierte Gruppe importieren möchten, haben Sie einen Identitätsverbund konfiguriert, und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.

Erstellen einer Admin-Gruppe

Administratorgruppen ermöglichen es Ihnen, festzulegen, welche Benutzer auf welche Funktionen und Vorgänge im Grid Manager und in der Grid Management API zugreifen können.

Greifen Sie auf den Assistenten zu

1. Wählen Sie **KONFIGURATION Zugriffskontrolle Admin-Gruppen**.

2. Wählen Sie **Gruppe erstellen**.

Wählen Sie einen Gruppentyp aus

Sie können eine lokale Gruppe erstellen oder eine föderierte Gruppe importieren.

- Erstellen Sie eine lokale Gruppe, wenn Sie lokalen Benutzern Berechtigungen zuweisen möchten.
- Erstellen Sie eine föderierte Gruppe, um Benutzer aus der Identitätsquelle zu importieren.

Lokale Gruppe

1. Wählen Sie **Lokale Gruppe**.
2. Geben Sie einen Anzeigenamen für die Gruppe ein, den Sie bei Bedarf später aktualisieren können. Zum Beispiel: „`MWartung Benutzer`“ oder „`ILM-Administratoren`“
3. Geben Sie einen eindeutigen Namen für die Gruppe ein, die Sie später nicht aktualisieren können.
4. Wählen Sie **Weiter**.

Föderierte Gruppe

1. Wählen Sie **Federated Group**.
2. Geben Sie den Namen der Gruppe ein, die importiert werden soll, genau so, wie sie in der konfigurierten Identitätsquelle angezeigt wird.
   - Verwenden Sie für Active Directory und Azure den sAMAccountName.
   - Verwenden Sie für OpenLDAP das CN (Common Name).
   - Verwenden Sie für einen anderen LDAP den entsprechenden eindeutigen Namen für den LDAP-Server.
3. Wählen Sie **Weiter**.

Gruppenberechtigungen verwalten

1. Wählen Sie unter **Zugriffsmodus** aus, ob Benutzer in der Gruppe Einstellungen ändern und Vorgänge im Grid Manager und der Grid Management API ausführen können oder ob sie nur Einstellungen und Funktionen anzeigen können.
   - **Lesen-Schreiben** (Standard): Benutzer können Einstellungen ändern und die Operationen durchführen, die durch ihre Verwaltungsberechtigungen erlaubt sind.
   - **Schreibgeschützt**: Benutzer können nur Einstellungen und Funktionen anzeigen. Sie können keine Änderungen vornehmen oder Vorgänge im Grid Manager oder der Grid Management API ausführen. Lokale schreibgeschützte Benutzer können ihre eigenen Passwörter ändern.

   > ⓘ Wenn ein Benutzer zu mehreren Gruppen gehört und eine beliebige Gruppe auf **schreibgeschützt** gesetzt ist, hat der Benutzer schreibgeschützten Zugriff auf alle ausgewählten Einstellungen und Features.

2. Wählen Sie eine oder mehrere Antworten aus Gruppenberechtigungen.

   Sie müssen jeder Gruppe mindestens eine Berechtigung zuweisen. Andernfalls können sich Benutzer der Gruppe nicht bei StorageGRID anmelden.

3. Wenn Sie eine lokale Gruppe erstellen, wählen Sie **Weiter**. Wenn Sie eine Verbundgruppe erstellen,

wählen Sie **Gruppe erstellen** und **Fertig stellen** aus.

Benutzer hinzufügen (nur lokale Gruppen)

1. Wählen Sie optional einen oder mehrere lokale Benutzer für diese Gruppe aus.

   Wenn Sie noch keine lokalen Benutzer erstellt haben, können Sie die Gruppe speichern, ohne Benutzer hinzuzufügen. Sie können diese Gruppe dem Benutzer auf der Seite Benutzer hinzufügen. SieheBenutzer managen Entsprechende Details.

2. Wählen Sie **Gruppe erstellen** und **Fertig stellen**.

Anzeigen und Bearbeiten von Admin-Gruppen

Sie können Details für vorhandene Gruppen anzeigen, eine Gruppe ändern oder eine Gruppe duplizieren.

- Um grundlegende Informationen für alle Gruppen anzuzeigen, überprüfen Sie die Tabelle auf der Seite Gruppen.
- Um alle Details für eine bestimmte Gruppe anzuzeigen oder eine Gruppe zu bearbeiten, verwenden Sie das Menü **Aktionen** oder die Detailseite.

Aufgabe	Menü „Aktionen“	Detailseite
Zeigen Sie Gruppendetails an	a. Aktivieren Sie das Kontrollkästchen für die Gruppe. b. Wählen Sie **Aktionen Gruppendetails anzeigen**.	Wählen Sie den Gruppennamen in der Tabelle aus.
Anzeigename bearbeiten (nur lokale Gruppen)	a. Aktivieren Sie das Kontrollkästchen für die Gruppe. b. Wählen Sie **Aktionen Gruppenname bearbeiten**. c. Geben Sie den neuen Namen ein. d. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Gruppennamen aus, um die Details anzuzeigen. b. Wählen Sie das Bearbeitungssymbol . c. Geben Sie den neuen Namen ein. d. Wählen Sie **Änderungen speichern**.
Zugriffsmodus oder Berechtigungen bearbeiten	a. Aktivieren Sie das Kontrollkästchen für die Gruppe. b. Wählen Sie **Aktionen Gruppendetails anzeigen**. c. Ändern Sie optional den Zugriffsmodus der Gruppe. d. Wählen Sie optional aus oder heben Sie die Auswahl ab Gruppenberechtigungen. e. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Gruppennamen aus, um die Details anzuzeigen. b. Ändern Sie optional den Zugriffsmodus der Gruppe. c. Wählen Sie optional aus oder heben Sie die Auswahl ab Gruppenberechtigungen. d. Wählen Sie **Änderungen speichern**.

Duplizieren einer Gruppe

1. Aktivieren Sie das Kontrollkästchen für die Gruppe.
2. Wählen Sie **Aktionen Gruppe duplizieren**.
3. Schließen Sie den Assistenten für die doppelte Gruppe ab.

Gruppe löschen

Sie können eine Admin-Gruppe löschen, wenn Sie die Gruppe aus dem System entfernen möchten, und alle mit der Gruppe verknüpften Berechtigungen entfernen. Durch das Löschen einer Admin-Gruppe werden alle Benutzer aus der Gruppe entfernt, die Benutzer jedoch nicht gelöscht.

1. Aktivieren Sie auf der Seite Gruppen das Kontrollkästchen für jede Gruppe, die Sie entfernen möchten.
2. Wählen Sie **Aktionen Gruppe löschen**.
3. Wählen Sie **Gruppen löschen**.

Gruppenberechtigungen

Beim Erstellen von Admin-Benutzergruppen wählen Sie eine oder mehrere Berechtigungen, um den Zugriff auf bestimmte Funktionen des Grid Manager zu steuern. Sie können dann jeden Benutzer einer oder mehreren dieser Admin-Gruppen zuweisen, um zu bestimmen, welche Aufgaben der Benutzer ausführen kann.

Sie müssen jeder Gruppe mindestens eine Berechtigung zuweisen. Andernfalls können sich Benutzer, die dieser Gruppe angehören, nicht beim Grid Manager oder der Grid Management API anmelden.

Standardmäßig kann jeder Benutzer, der zu einer Gruppe mit mindestens einer Berechtigung gehört, die folgenden Aufgaben ausführen:

- Melden Sie sich beim Grid Manager an
- Zeigen Sie das Dashboard an
- Zeigen Sie die Seiten Knoten an
- Monitoring der Grid-Topologie
- Anzeige aktueller und aufgelöster Warnmeldungen
- Aktuelle und historische Alarme anzeigen (Legacy-System)
- Eigenes Kennwort ändern (nur lokale Benutzer)
- Zeigen Sie bestimmte Informationen auf den Seiten Konfiguration und Wartung an

Interaktion zwischen Berechtigungen und Zugriffsmodus

Für alle Berechtigungen bestimmt die Einstellung **Zugriffsmodus** der Gruppe, ob Benutzer Einstellungen ändern und Vorgänge ausführen können oder ob sie nur die zugehörigen Einstellungen und Funktionen anzeigen können. Wenn ein Benutzer zu mehreren Gruppen gehört und eine beliebige Gruppe auf **schreibgeschützt** gesetzt ist, hat der Benutzer schreibgeschützten Zugriff auf alle ausgewählten Einstellungen und Features.

In den folgenden Abschnitten werden die Berechtigungen beschrieben, die Sie beim Erstellen oder Bearbeiten einer Admin-Gruppe zuweisen können. Jede Funktion, die nicht explizit erwähnt wird, erfordert die **Root Access**-Berechtigung.

Root-Zugriff

Mit dieser Berechtigung erhalten Sie Zugriff auf alle Grid-Administrationsfunktionen.

Alarme quittieren (alt)

Diese Berechtigung ermöglicht den Zugriff auf Quittierung und Reaktion auf Alarme (Altsystem). Alle Benutzer, die angemeldet sind, können aktuelle und historische Alarme anzeigen.

Wenn ein Benutzer die Grid-Topologie überwachen und nur Alarme quittieren soll, sollten Sie diese Berechtigung zuweisen.

Root-Passwort des Mandanten ändern

Diese Berechtigung bietet Zugriff auf die Option **Root-Passwort ändern** auf der Seite der Mieter, so dass Sie steuern können, wer das Passwort für den lokalen Root-Benutzer des Mandanten ändern kann. Diese Berechtigung wird auch für die Migration von S3-Schlüsseln verwendet, wenn die S3-Key-Importfunktion aktiviert ist. Benutzer, die diese Berechtigung nicht besitzen, können die Option **Root-Passwort ändern** nicht sehen.

> Um Zugriff auf die Seite Mieter zu gewähren, die die Option **Root Passwort ändern** enthält, weisen Sie auch die Berechtigung **Mandantenkonten** zu.

Konfiguration der Seite der Grid-Topologie

Mit dieser Berechtigung können Sie auf der Seite **SUPPORT Tools Grid Topology** auf die Registerkarten Konfiguration zugreifen.

ILM

Diese Berechtigung bietet Zugriff auf die folgenden **ILM** Menüoptionen:

- Regeln
- Richtlinien
- Erasure Coding
- Regionen
- Storage-Pools

> Benutzer müssen über die Berechtigung **andere Grid-Konfiguration** und **Grid-Topologiekonfiguration** verfügen, um Speicherklassen zu verwalten.

Wartung

Benutzer müssen über die Berechtigung zur Wartung verfügen, um folgende Optionen verwenden zu können:

- **KONFIGURATION Zugangskontrolle**:
  - Grid-Passwörter
- **WARTUNG Aufgaben**:
  - Ausmustern
  - Erweiterung

    - Überprüfung der Objektexistenz
    - Recovery
- **WARTUNG System**:
    - Recovery-Paket
    - Software-Update
- **SUPPORT Tools**:
    - Protokolle

Benutzer, die nicht über die Wartungsberechtigung verfügen, können diese Seiten anzeigen, aber nicht bearbeiten:

- **WARTUNG Netzwerk**:
    - DNS-Server
    - Grid-Netzwerk
    - NTP-Server
- **WARTUNG System**:
    - Lizenz
- **KONFIGURATION Sicherheit**:
    - Zertifikate
    - Domain-Namen
- **KONFIGURATION Überwachung**:
    - Audit- und Syslog-Server

Verwalten von Meldungen

Mit dieser Berechtigung erhalten Sie Zugriff auf Optionen zum Verwalten von Warnmeldungen. Benutzer müssen über diese Berechtigung verfügen, um Stille, Warnmeldungen und Alarmregeln zu verwalten.

Abfrage von Kennzahlen

Mit dieser Berechtigung erhalten Sie Zugriff auf die Seite **SUPPORT Tools Metriken**. Diese Berechtigung bietet auch Zugriff auf benutzerdefinierte Prometheus-metrische Abfragen unter Verwendung des Abschnitts **Metriken** der Grid Management API.

Suche nach Objektmetadaten

Mit dieser Berechtigung erhalten Sie Zugriff auf die Seite **ILM Object Metadaten Lookup**.

Andere Grid-Konfiguration

Diese Berechtigung ermöglicht den Zugriff auf zusätzliche Grid-Konfigurationsoptionen.

> Um diese zusätzlichen Optionen zu sehen, müssen Benutzer auch über die Berechtigung **Grid Topology Page Configuration** verfügen.

- **ILM**:

    - Lagergüten
- **KONFIGURATION Netzwerk**:
    - Verbindungskosten
- **KONFIGURATION System**:
    - Anzeigeoptionen
    - Grid-Optionen
    - Storage-Optionen
- **UNTERSTÜTZUNG Alarme (alt)**:
    - Benutzerdefinierte Events
    - Globale Alarme
    - Einrichtung alter E-Mail-Adressen

Storage Appliance-Administrator

Mit dieser Berechtigung erhalten Sie über den Grid Manager Zugriff auf den SANtricity System Manager der E-Series auf Storage Appliances.

Mandantenkonten

Mit dieser Berechtigung haben Sie Zugriff auf die Seite „Mandanten“, auf der Sie Mandantenkonten erstellen, bearbeiten und entfernen können. Mit dieser Berechtigung können Benutzer auch vorhandene Richtlinien zur Klassifizierung von Verkehrsdaten anzeigen.

Deaktivieren Sie Funktionen mit der API

Mithilfe der Grid Management API können Sie bestimmte Funktionen im StorageGRID-System komplett deaktivieren. Wenn ein Feature deaktiviert ist, kann niemand Berechtigungen zum Ausführen der Aufgaben zugewiesen werden, die mit diesem Feature verbunden sind.

Über diese Aufgabe

Mit dem deaktivierten Features-System können Sie den Zugriff auf bestimmte Funktionen im StorageGRID-System verhindern. Die Deaktivierung einer Funktion ist der einzige Weg, um zu verhindern, dass Root-Benutzer oder Benutzer, die zu Admin-Gruppen mit **Root Access**-Berechtigung gehören, diese Funktion verwenden können.

Um zu verstehen, wie diese Funktionalität nützlich sein kann, gehen Sie folgendermaßen vor:

Unternehmen A ist ein Service Provider, der durch die Erstellung von Mandantenkonten die Storage-Kapazität ihres StorageGRID Systems least. Um die Sicherheit der Objekte ihrer Eigentümer zu schützen, möchte Unternehmen A sicherstellen, dass die eigenen Mitarbeiter nach der Bereitstellung des Kontos niemals auf ein Mandantenkonto zugreifen können.

*Unternehmen A kann dieses Ziel mithilfe des Systems Funktionen deaktivieren in der Grid Management API erreichen. Durch die vollständige Deaktivierung der **Change Tenant Root password**-Funktion im Grid Manager (sowohl die UI als auch die API) kann Unternehmen A sicherstellen, dass kein Admin-Benutzer - einschließlich des Root-Benutzers und der Benutzer, die zu Gruppen mit der **Root Access**-Berechtigung gehören - das Passwort für den Root-Benutzer eines Mandantenkontos ändern kann.*

Schritte

1. Rufen Sie die Swagger-Dokumentation für die Grid Management API auf. Siehe Verwenden Sie die Grid-Management-API.
2. Suchen Sie den Endpunkt zum Deaktivieren von Funktionen.
3. Um eine Funktion, wie z.B. das Root-Passwort des Mandanten ändern, zu deaktivieren, senden Sie einen Text wie folgt an die API:

```
{ "grid": {"changeTenantRootPassword": true} }
```

Nach Abschluss der Anforderung ist die Funktion Root-Passwort ändern deaktiviert. Die Managementberechtigung für das Stammpasswort für den Mandanten * wird in der Benutzeroberfläche nicht mehr angezeigt, und jede API-Anforderung, die versucht, das Root-Passwort für einen Mandanten zu ändern, schlägt mit „`403 Verbotenen`“ fehl.

Deaktivieren Funktionen erneut aktivieren

Standardmäßig können Sie mit der Grid Management API eine deaktivierte Funktion reaktivieren. Wenn Sie jedoch verhindern möchten, dass deaktivierte Funktionen jemals wieder aktiviert werden, können Sie die **activateFeatures**-Funktion selbst deaktivieren.

> Die **activateFeatures**-Funktion kann nicht reaktiviert werden. Wenn Sie sich entscheiden, diese Funktion zu deaktivieren, beachten Sie, dass Sie die Möglichkeit verlieren, alle anderen deaktivierten Funktionen dauerhaft zu reaktivieren. Sie müssen sich an den technischen Support wenden, um verlorene Funktionen wiederherzustellen.

Schritte

1. Rufen Sie die Swagger-Dokumentation für die Grid Management API auf.
2. Suchen Sie den Endpunkt zum Deaktivieren von Funktionen.
3. Um alle Funktionen erneut zu aktivieren, senden Sie einen Text wie folgt an die API:

```
{ "grid": null }
```

Wenn diese Anfrage abgeschlossen ist, werden alle Funktionen, einschließlich der Funktion Root-Passwort ändern, reaktiviert. Die Berechtigung zur Verwaltung von Stammpasswort* des Mandanten wird jetzt in der Benutzeroberfläche angezeigt, und jede API-Anforderung, die versucht, das Root-Passwort für einen Mandanten zu ändern, wird erfolgreich sein, vorausgesetzt der Benutzer hat die Berechtigung * Root Access* oder **Change Tenant Root password** Management.

> Das vorherige Beispiel führt dazu, dass *all* deaktivierte Funktionen reaktiviert werden. Wenn andere Features deaktiviert wurden, die deaktiviert bleiben sollen, müssen Sie diese explizit in der PUT-Anforderung angeben. Um beispielsweise die Funktion Root-Passwort ändern erneut zu aktivieren und die Funktion zur Alarmbestätigung zu deaktivieren, senden Sie diese PUT-Anforderung:
>
> ```
> { "grid": { "alarmAcknowledgment": true } }
> ```

Benutzer managen

Sie können lokale und föderierte Benutzer anzeigen. Sie können auch lokale Benutzer

erstellen und lokalen Administratorgruppen zuordnen, um zu bestimmen, auf welche Grid Manager-Funktionen diese Benutzer zugreifen können.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

Erstellen Sie einen lokalen Benutzer

Sie können einen oder mehrere lokale Benutzer erstellen und jedem Benutzer einer oder mehreren lokalen Gruppen zuweisen. Die Berechtigungen der Gruppe steuern, auf welche Grid Manager- und Grid Management API-Funktionen der Benutzer zugreifen kann.

Sie können nur lokale Benutzer erstellen. Verwenden Sie die externe Identitätsquelle, um verbundene Benutzer und Gruppen zu verwalten.

Der Grid Manager enthält einen vordefinierten lokalen Benutzer mit dem Namen „`root`“. Sie können den Root-Benutzer nicht entfernen.

> Wenn Single Sign-On (SSO) aktiviert ist, können sich lokale Benutzer nicht bei StorageGRID anmelden.

Greifen Sie auf den Assistenten zu

1. Wählen Sie **KONFIGURATION Zugriffskontrolle Admin-Benutzer**.
2. Wählen Sie **Benutzer erstellen**.

Geben Sie die Anmeldedaten des Benutzers ein

1. Geben Sie den vollständigen Namen des Benutzers, einen eindeutigen Benutzernamen und ein Kennwort ein.
2. Wählen Sie optional **Ja** aus, wenn dieser Benutzer keinen Zugriff auf den Grid Manager oder die Grid Management API haben soll.
3. Wählen Sie **Weiter**.

Zu Gruppen zuweisen

1. Weisen Sie den Benutzer optional einer oder mehreren Gruppen zu, um die Berechtigungen des Benutzers zu ermitteln.

   Wenn Sie noch keine Gruppen erstellt haben, können Sie den Benutzer speichern, ohne Gruppen auszuwählen. Sie können diesen Benutzer einer Gruppe auf der Seite Gruppen hinzufügen.

   Wenn ein Benutzer zu mehreren Gruppen gehört, werden die Berechtigungen kumulativ. SieheManagen von Admin-Gruppen Entsprechende Details.

2. Wählen Sie **Benutzer erstellen** und wählen Sie **Fertig**.

Lokale Benutzer anzeigen und bearbeiten

Details zu vorhandenen lokalen und föderierten Benutzern können angezeigt werden. Sie können einen lokalen Benutzer ändern, um den vollständigen Namen, das Kennwort oder die Gruppenmitgliedschaft des

Benutzers zu ändern. Sie können auch vorübergehend verhindern, dass ein Benutzer auf den Grid Manager und die Grid Management API zugreift.

Sie können nur lokale Benutzer bearbeiten. Verwenden Sie die externe Identitätsquelle, um verbundene Benutzer zu verwalten.

- Um grundlegende Informationen für alle lokalen und föderierten Benutzer anzuzeigen, lesen Sie die Tabelle auf der Benutzer-Seite.
- Um alle Details für einen bestimmten Benutzer anzuzeigen, einen lokalen Benutzer zu bearbeiten oder das Passwort eines lokalen Benutzers zu ändern, verwenden Sie das Menü **Aktionen** oder die Detailseite.

  Bei der nächsten Abmeldet sich der Benutzer an und meldet sich dann wieder beim Grid Manager an.

> ⓘ Lokale Benutzer können ihre eigenen Passwörter mit der Option **Passwort ändern** im Banner Grid Manager ändern.

Aufgabe	Menü „Aktionen“	Detailseite
Zeigen Sie Benutzerdetails an	a. Aktivieren Sie das Kontrollkästchen für den Benutzer. b. Wählen Sie **Aktionen Benutzerdetails anzeigen**.	Wählen Sie den Benutzernamen in der Tabelle aus.
Vollständigen Namen bearbeiten (nur lokale Benutzer)	a. Aktivieren Sie das Kontrollkästchen für den Benutzer. b. Wählen Sie **Aktionen vollständigen Namen bearbeiten**. c. Geben Sie den neuen Namen ein. d. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Benutzernamen aus, um die Details anzuzeigen. b. Wählen Sie das Bearbeitungssymbol . c. Geben Sie den neuen Namen ein. d. Wählen Sie **Änderungen speichern**.
StorageGRID-Zugriff verweigern oder zulassen	a. Aktivieren Sie das Kontrollkästchen für den Benutzer. b. Wählen Sie **Aktionen Benutzerdetails anzeigen**. c. Wählen Sie die Registerkarte Zugriff aus. d. Wählen Sie **Ja** aus, um zu verhindern, dass sich der Benutzer beim Grid Manager oder der Grid Management API anmeldet, oder wählen Sie **Nein** aus, damit der Benutzer sich anmelden kann. e. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Benutzernamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte Zugriff aus. c. Wählen Sie **Ja** aus, um zu verhindern, dass sich der Benutzer beim Grid Manager oder der Grid Management API anmeldet, oder wählen Sie **Nein** aus, damit der Benutzer sich anmelden kann. d. Wählen Sie **Änderungen speichern**.

Aufgabe	Menü „Aktionen“	Detailseite
Passwort ändern (nur lokale Benutzer)	a. Aktivieren Sie das Kontrollkästchen für den Benutzer. b. Wählen Sie **Aktionen Benutzerdetails anzeigen**. c. Wählen Sie die Registerkarte Kennwort aus. d. Geben Sie ein neues Passwort ein. e. Wählen Sie **Passwort Ändern**.	a. Wählen Sie den Benutzernamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte Kennwort aus. c. Geben Sie ein neues Passwort ein. d. Wählen Sie **Passwort Ändern**.
Gruppen ändern (nur lokale Benutzer)	a. Aktivieren Sie das Kontrollkästchen für den Benutzer. b. Wählen Sie **Aktionen Benutzerdetails anzeigen**. c. Wählen Sie die Registerkarte Gruppen aus. d. Wählen Sie optional den Link nach einem Gruppennamen aus, um die Details der Gruppe in einer neuen Browserregisterkarte anzuzeigen. e. Wählen Sie **Gruppen bearbeiten**, um verschiedene Gruppen auszuwählen. f. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Benutzernamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte Gruppen aus. c. Wählen Sie optional den Link nach einem Gruppennamen aus, um die Details der Gruppe in einer neuen Browserregisterkarte anzuzeigen. d. Wählen Sie **Gruppen bearbeiten**, um verschiedene Gruppen auszuwählen. e. Wählen Sie **Änderungen speichern**.

Duplizieren eines Benutzers

Sie können einen vorhandenen Benutzer duplizieren, um einen neuen Benutzer mit denselben Berechtigungen zu erstellen.

1. Aktivieren Sie das Kontrollkästchen für den Benutzer.
2. Wählen Sie **Aktionen Benutzer duplizieren**.
3. Schließen Sie den Assistenten für doppelte Benutzer ab.

Löschen Sie einen Benutzer

Sie können einen lokalen Benutzer löschen, um diesen Benutzer dauerhaft aus dem System zu entfernen.

Sie können den Root-Benutzer nicht löschen.

1. Aktivieren Sie auf der Seite Benutzer das Kontrollkästchen für jeden Benutzer, den Sie entfernen möchten.
2. Wählen Sie **Aktionen Benutzer löschen**.
3. Wählen Sie **Benutzer löschen**.

Single Sign On (SSO) verwenden

Konfigurieren Sie Single Sign-On

Wenn Single Sign-On (SSO) aktiviert ist, können Benutzer nur auf den Grid Manager, den Mandanten-Manager, die Grid-Management-API oder die Mandantenmanagement-API zugreifen, wenn ihre Anmeldedaten über den von Ihrem Unternehmen implementierten SSO-Anmeldeprozess autorisiert sind. Lokale Benutzer können sich nicht bei StorageGRID anmelden.

Funktionsweise von Single Sign-On

Das StorageGRID-System unterstützt Single Sign-On (SSO) unter Verwendung des Security Assertion Markup Language 2.0 (SAML 2.0)-Standards.

Prüfen Sie vor der Aktivierung von Single Sign-On (SSO), wie sich die StorageGRID-Anmelde- und -Abmelde -Prozesse bei Aktivierung von SSO auswirken.

Melden Sie sich an, wenn SSO aktiviert ist

Wenn SSO aktiviert ist und Sie sich bei StorageGRID anmelden, werden Sie zur SSO-Seite Ihres Unternehmens weitergeleitet, um Ihre Anmeldedaten zu validieren.

Schritte

1. Geben Sie in einem Webbrowser den vollständig qualifizierten Domänennamen oder die IP-Adresse eines beliebigen StorageGRID-Admin-Knotens ein.

   Die Seite StorageGRID-Anmeldung wird angezeigt.

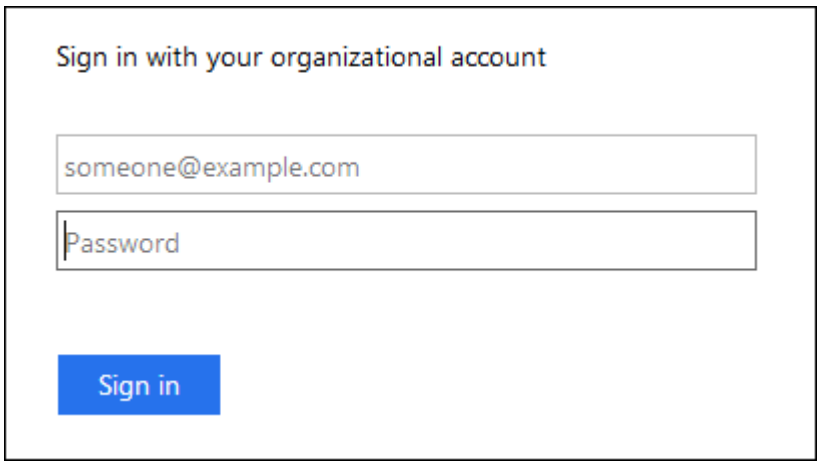
   - Wenn Sie in diesem Browser zum ersten Mal auf die URL zugegriffen haben, werden Sie aufgefordert, eine Konto-ID einzugeben:

   - Wenn Sie zuvor entweder auf den Grid Manager oder den Tenant Manager zugegriffen haben, werden Sie aufgefordert, ein aktuelles Konto auszuwählen oder eine Konto-ID einzugeben:

Die Seite „StorageGRID-Anmeldung“ wird nicht angezeigt, wenn Sie die vollständige URL für ein Mandantenkonto eingeben (d. h. einen vollständig qualifizierten Domain-Namen oder eine IP-Adresse, gefolgt von `/?accountId=20-digit-account-id`). Stattdessen werden Sie sofort auf die SSO-Anmeldeseite Ihres Unternehmens umgeleitet, auf der Sie sich befinden können melden Sie sich mit Ihren SSO-Anmeldedaten an.

2. Geben Sie an, ob Sie auf den Grid Manager oder den Tenant Manager zugreifen möchten:
   - Um auf den Grid Manager zuzugreifen, lassen Sie das Feld **Konto-ID** leer, geben Sie **0** als Konto-ID ein, oder wählen Sie **Grid Manager** aus, wenn es in der Liste der letzten Konten angezeigt wird.
   - Um auf den Mandantenmanager zuzugreifen, geben Sie die 20-stellige Mandantenkonto-ID ein, oder wählen Sie einen Mandanten nach Namen aus, wenn er in der Liste der letzten Konten angezeigt wird.
3. Wählen Sie **Anmelden**

   StorageGRID leitet Sie zur SSO-Anmeldeseite Ihres Unternehmens weiter. Beispiel:



4. Melden Sie sich mit Ihren SSO-Anmeldedaten an.

   Falls Ihre SSO-Anmeldedaten korrekt sind:

   a. Der Identitäts-Provider (IdP) stellt eine Authentifizierungsantwort für StorageGRID bereit.
   b. StorageGRID validiert die Authentifizierungsantwort.
   c. Wenn die Antwort gültig ist und Sie zu einer föderierten Gruppe mit StorageGRID-Zugriffsberechtigungen gehören, werden Sie je nach ausgewähltem Konto beim Grid Manager oder dem Mandanten-Manager angemeldet.

   Wenn das Dienstkonto nicht zugänglich ist, können Sie sich trotzdem anmelden, solange Sie ein vorhandener Benutzer sind, der zu einer föderierten Gruppe mit StorageGRID-Zugriffsberechtigungen gehört.

5. Wenn Sie über ausreichende Berechtigungen verfügen, können Sie optional auf andere Admin-Nodes zugreifen oder auf den Grid Manager oder den Tenant Manager zugreifen.

   Sie müssen Ihre SSO-Anmeldedaten nicht erneut eingeben.

Abmelden, wenn SSO aktiviert ist

Wenn SSO für StorageGRID aktiviert ist, hängt dies davon ab, ab, bei welchem Anmeldefenster Sie sich angemeldet haben und von wo Sie sich abmelden.

Schritte

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

   Die Seite StorageGRID-Anmeldung wird angezeigt. Das Drop-Down **Recent Accounts** wird aktualisiert und enthält **Grid Manager** oder den Namen des Mandanten, sodass Sie in Zukunft schneller auf diese Benutzeroberflächen zugreifen können.

Wenn Sie bei angemeldet sind…	Und Sie melden sich ab von…	Sie sind abgemeldet von…
Grid Manager auf einem oder mehreren Admin-Nodes	Grid Manager auf jedem Admin-Node	Grid Manager auf allen Admin-Nodes **Hinweis:** Wenn Sie Azure für SSO verwenden, kann es einige Minuten dauern, bis Sie von allen Admin-Nodes abgemeldet werden.
Mandantenmanager auf einem oder mehreren Admin-Nodes	Mandanten-Manager auf jedem Admin-Node	Mandantenmanager auf allen Admin-Nodes
Sowohl Grid Manager als auch Tenant Manager	Grid Manager	Nur Grid Manager. Sie müssen sich auch vom Tenant Manager abmelden, um SSO abzumelden.

Die Tabelle fasst zusammen, was passiert, wenn Sie sich abmelden, wenn Sie eine einzelne Browser-Sitzung verwenden. Wenn Sie sich bei StorageGRID über mehrere Browser-Sitzungen hinweg angemeldet haben, müssen Sie sich von allen Browser-Sitzungen separat anmelden.

Anforderungen für die Nutzung von Single Sign On

Bevor Sie Single Sign On (SSO) für ein StorageGRID-System aktivieren, überprüfen Sie die Anforderungen in diesem Abschnitt.

Anforderungen an Identitätsanbieter

StorageGRID unterstützt die folgenden SSO-Identitätsanbieter (IdP):

- Active Directory Federation Service (AD FS)
- Azure Active Directory (Azure AD)
- PingFederate

Sie müssen die Identitätsföderation für Ihr StorageGRID-System konfigurieren, bevor Sie einen SSO-

Identitätsanbieter konfigurieren können. Der Typ des LDAP-Service, den Sie für die Identitätsföderation verwenden, steuert, welcher SSO-Typ Sie implementieren können.

Konfigurierter LDAP-Servicetyp	Optionen für SSO-Identitätsanbieter
Active Directory	• Active Directory • Azure • PingFederate
Azure	Azure

AD-FS-Anforderungen

Sie können eine der folgenden Versionen von AD FS verwenden:

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS

> Windows Server 2016 sollte den verwenden "KB3201845-Update", Oder höher.

- AD FS 3.0, im Lieferumfang von Windows Server 2012 R2 Update oder höher enthalten.

Zusätzlichen Anforderungen

- Transport Layer Security (TLS) 1.2 oder 1.3
- Microsoft .NET Framework, Version 3.5.1 oder höher

Serverzertifikate-Anforderungen

Standardmäßig verwendet StorageGRID auf jedem Admin-Node ein Zertifikat der Managementoberfläche, um den Zugriff auf den Grid Manager, den Mandanten-Manager, die Grid-Management-API und die Mandanten-Management-API zu sichern. Wenn Sie Trusts (AD FS), Enterprise-Anwendungen (Azure) oder Service Provider Connections (PingFederate) für StorageGRID konfigurieren, verwenden Sie das Serverzertifikat als Signaturzertifikat für StorageGRID-Anfragen.

Falls nicht bereits erfolgt Ein benutzerdefiniertes Zertifikat für die Managementoberfläche konfiguriert, Sie sollten das jetzt tun. Wenn Sie ein benutzerdefiniertes Serverzertifikat installieren, wird es für alle Administratorknoten verwendet, und Sie können es in allen StorageGRID-Vertrauensstellungen, Unternehmensanwendungen oder SP-Verbindungen verwenden.

> Es wird nicht empfohlen, das Standardserverzertifikat eines Admin Node in einer Vertrauensstelle, einer Unternehmensanwendungen oder einer SP-Verbindung zu verwenden. Wenn der Knoten ausfällt und Sie ihn wiederherstellen, wird ein neues Standard-Serverzertifikat generiert. Bevor Sie sich beim wiederhergestellten Knoten anmelden können, müssen Sie das Vertrauensverhältnis der zu bestellenden Partei, die Enterprise-Anwendung oder die SP-Verbindung mit dem neuen Zertifikat aktualisieren.

Sie können auf das Serverzertifikat eines Admin-Knotens zugreifen, indem Sie sich bei der Befehlshülle des Knotens anmelden und auf die zugreifen `/var/local/mgmt-api` Verzeichnis. Ein benutzerdefiniertes

Serverzertifikat ist benannt `custom-server.crt`. Das Standardserverzertifikat des Node wird mit benannt `server.crt`.

Port-Anforderungen

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. Siehe Kontrolle des Zugriffs durch Firewalls.

Bestätigen Sie, dass verbundene Benutzer sich anmelden können

Bevor Sie Single Sign-On (SSO) aktivieren, müssen Sie bestätigen, dass sich mindestens ein verbundener Benutzer beim Grid Manager und beim Tenant Manager für alle bestehenden Mandantenkonten anmelden kann.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben bereits einen Identitätsverbund konfiguriert.

Schritte

1. Falls bereits vorhandene Mandantenkonten vorhanden sind, bestätigen Sie, dass kein Mandant seine eigene Identitätsquelle verwendet.

   > Wenn Sie SSO aktivieren, wird eine im Mandantenmanager konfigurierte Identitätsquelle von der im Grid Manager konfigurierten Identitätsquelle außer Kraft gesetzt. Benutzer, die zur Identitätsquelle des Mandanten gehören, können sich nicht mehr anmelden, es sei denn, sie verfügen über ein Konto bei der Identitätsquelle des Grid Manager.

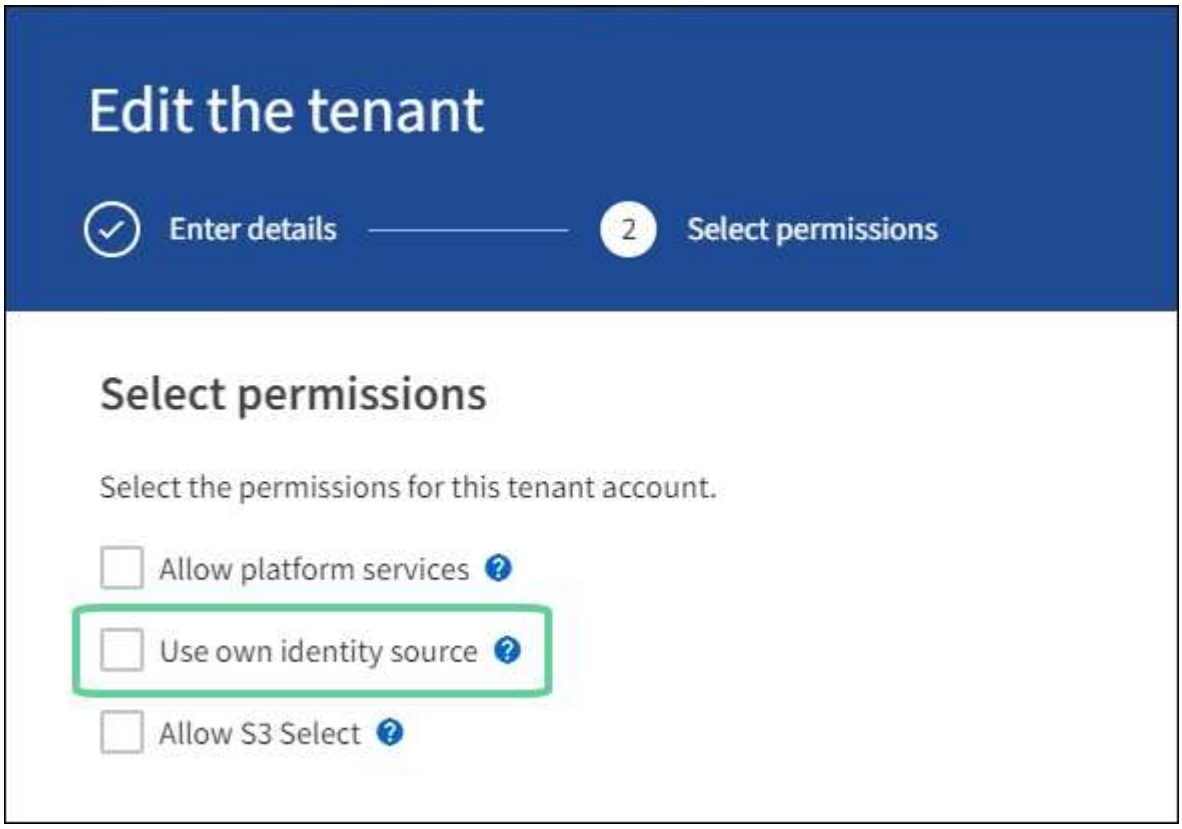
   a. Melden Sie sich für jedes Mandantenkonto bei Tenant Manager an.
   b. Wählen Sie **ZUGRIFFSMANAGEMENT Identitätsverbund** aus.
   c. Bestätigen Sie, dass das Kontrollkästchen **Identitätsföderation aktivieren** nicht aktiviert ist.
   d. Wenn dies der Fall ist, bestätigen Sie, dass alle föderierten Gruppen, die für dieses Mandantenkonto verwendet werden, nicht mehr erforderlich sind. Deaktivieren Sie das Kontrollkästchen, und wählen Sie **Speichern**.

2. Bestätigen Sie, dass ein verbundener Benutzer auf den Grid Manager zugreifen kann:
   a. Wählen Sie im Grid Manager **KONFIGURATION Zugriffskontrolle Admin-Gruppen**.
   b. Stellen Sie sicher, dass mindestens eine föderierte Gruppe aus der Active Directory-Identitätsquelle importiert wurde und dass ihr die Root-Zugriffsberechtigung zugewiesen wurde.
   c. Abmelden.
   d. Bestätigen Sie, dass Sie sich wieder bei Grid Manager als Benutzer in der föderierten Gruppe anmelden können.

3. Wenn es bereits bestehende Mandantenkonten gibt, bestätigen Sie, dass sich ein föderaler Benutzer mit Root-Zugriffsberechtigung anmelden kann:
   a. Wählen Sie im Grid Manager die Option **MITERS** aus.
   b. Wählen Sie das Mandantenkonto aus und wählen Sie **Aktionen Bearbeiten**.

c. Wählen Sie auf der Registerkarte Details eingeben die Option **Weiter**.

d. Wenn das Kontrollkästchen **eigene Identitätsquelle verwenden** aktiviert ist, deaktivieren Sie das Kontrollkästchen und wählen Sie **Speichern**.



Die Seite Mandant wird angezeigt.

a. Wählen Sie das Mandantenkonto aus, wählen Sie **Anmelden** und melden Sie sich als lokaler Root-Benutzer beim Mandantenkonto an.

b. Wählen Sie im Mandantenmanager die Option **ZUGRIFFSVERWALTUNG Gruppen** aus.

c. Stellen Sie sicher, dass mindestens eine föderierte Gruppe aus dem Grid Manager die Root-Zugriffsberechtigung für diesen Mandanten zugewiesen wurde.

d. Abmelden.

e. Bestätigen Sie, dass Sie sich wieder bei dem Mandanten als Benutzer in der föderierten Gruppe anmelden können.

Verwandte Informationen

- Anforderungen für die Nutzung von Single Sign On
- Managen von Admin-Gruppen
- Verwenden Sie ein Mandantenkonto

Verwenden Sie den Sandbox-Modus

Sie können den Sandbox-Modus verwenden, um Single Sign-On (SSO) zu konfigurieren und zu testen, bevor Sie es für alle StorageGRID-Benutzer aktivieren. Nachdem SSO aktiviert wurde, können Sie jederzeit wieder in den Sandbox-Modus wechseln, wenn Sie

die Konfiguration ändern oder erneut testen müssen.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben die Root-Zugriffsberechtigung.
- Sie haben eine Identitätsföderation für Ihr StorageGRID System konfiguriert.
- Für die Identitätsföderation **LDAP-Diensttyp** haben Sie entweder Active Directory oder Azure ausgewählt, basierend auf dem SSO-Identitäts-Provider, den Sie verwenden möchten.

Konfigurierter LDAP-Servicetyp	Optionen für SSO-Identitätsanbieter
Active Directory	• Active Directory • Azure • PingFederate
Azure	Azure

Über diese Aufgabe

Wenn SSO aktiviert ist und ein Benutzer versucht, sich bei einem Admin-Node anzumelden, sendet StorageGRID eine Authentifizierungsanforderung an den SSO-Identitäts-Provider. Der SSO-Identitäts-Provider sendet wiederum eine Authentifizierungsantwort zurück an StorageGRID, die angibt, ob die Authentifizierungsanforderung erfolgreich war. Für erfolgreiche Anfragen:

- Die Antwort von Active Directory oder PingFederate enthält eine Universally Unique Identifier (UUID) für den Benutzer.
- Die Antwort von Azure umfasst einen User Principal Name (UPN).

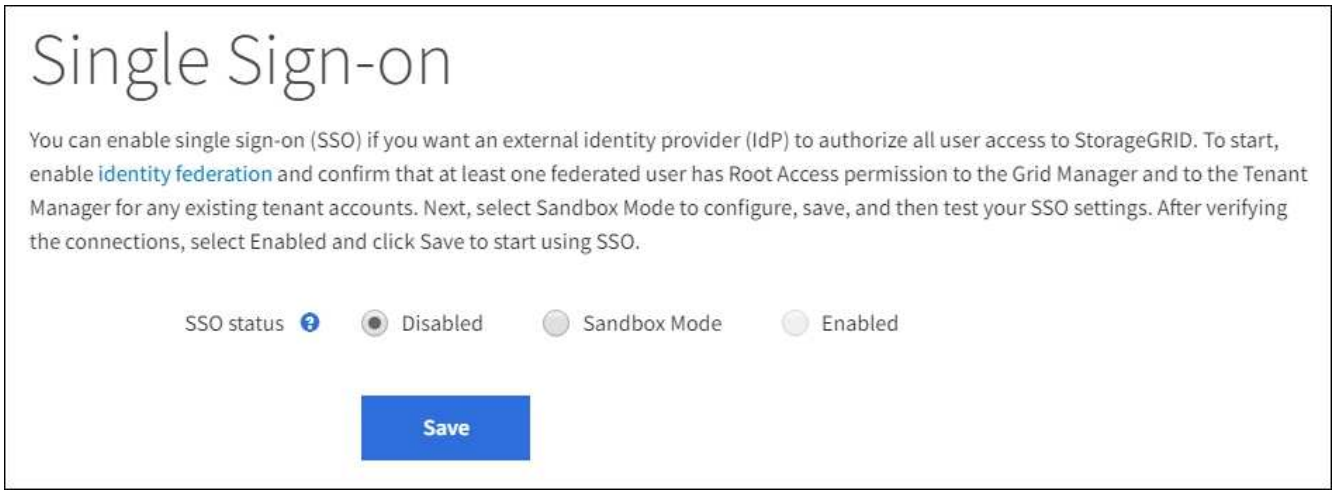
Damit StorageGRID (der Service-Provider) und der SSO-Identitäts-Provider sicher über Benutzerauthentifizierungsanforderungen kommunizieren können, müssen Sie bestimmte Einstellungen in StorageGRID konfigurieren. Als Nächstes müssen Sie die Software des SSO-Identitätsanbieters verwenden, um für jeden Admin-Node ein Vertrauensverhältnis (AD FS), eine Enterprise-Applikation (Azure) oder einen Serviceprovider (PingFederate) zu erstellen. Abschließend müssen Sie zu StorageGRID zurückkehren, um SSO zu aktivieren.

Im Sandbox-Modus ist es einfach, diese Rückkehrkonfiguration durchzuführen und alle Einstellungen zu testen, bevor Sie SSO aktivieren. Wenn Sie den Sandbox-Modus verwenden, können sich Benutzer nicht mit SSO anmelden.

Zugriff auf den Sandbox-Modus

1. Wählen Sie **KONFIGURATION Zugangskontrolle Single Sign-On**.

   Die Seite Single Sign-On wird angezeigt, wobei die Option **deaktiviertes** ausgewählt ist.



Wenn die Optionen für den SSO-Status nicht angezeigt werden, bestätigen Sie, dass Sie den Identitätsanbieter als föderierte Identitätsquelle konfiguriert haben. Siehe Anforderungen für die Nutzung von Single Sign On.

2. Wählen Sie **Sandbox-Modus**.

   Der Abschnitt „Identitätsanbieter“ wird angezeigt.

Geben Sie die Daten des Identitätsanbieters ein

1. Wählen Sie aus der Dropdown-Liste den **SSO-Typ** aus.
2. Füllen Sie die Felder im Abschnitt Identitäts-Provider basierend auf dem von Ihnen ausgewählten SSO-Typ aus.

Active Directory

1. Geben Sie den **Federationsdienstnamen** für den Identitätsanbieter ein, genau wie er im Active Directory Federation Service (AD FS) angezeigt wird.

   > Um den Namen des Föderationsdienstes zu finden, gehen Sie zu Windows Server Manager. Wählen Sie **Tools AD FS Management** aus. Wählen Sie im Menü Aktion die Option **Eigenschaften des Föderationsdienstes bearbeiten** aus. Der Name des Föderationsdienstes wird im zweiten Feld angezeigt.

2. Geben Sie an, welches TLS-Zertifikat zur Sicherung der Verbindung verwendet wird, wenn der Identitäts-Provider SSO-Konfigurationsinformationen als Antwort auf StorageGRID-Anforderungen sendet.
   - **Verwenden Sie das Betriebssystem CA-Zertifikat**: Verwenden Sie das auf dem Betriebssystem installierte Standard-CA-Zertifikat, um die Verbindung zu sichern.
   - **Benutzerdefiniertes CA-Zertifikat verwenden**: Verwenden Sie ein benutzerdefiniertes CA-Zertifikat, um die Verbindung zu sichern.

     Wenn Sie diese Einstellung auswählen, kopieren Sie den Text des benutzerdefinierten Zertifikats und fügen Sie ihn in das Textfeld **CA-Zertifikat** ein.

   - **Verwenden Sie keine TLS**: Verwenden Sie kein TLS-Zertifikat, um die Verbindung zu sichern.
3. Geben Sie im Abschnitt „Einvertrauende Partei“ die **bezeichner der bevertrauenden Partei** für StorageGRID an. Dieser Wert steuert den Namen, den Sie für jedes Vertrauen der betreffenden Partei in AD FS verwenden.
   - Wenn Ihr Grid beispielsweise nur einen Admin-Node hat und Sie nicht erwarten, dass künftig weitere Admin-Nodes hinzugefügt werden, geben Sie ein `SG` Oder `StorageGRID`.
   - Wenn Ihr Grid mehr als einen Admin-Node enthält, fügen Sie die Zeichenfolge ein `[HOSTNAME]` In der Kennung. Beispiel: `SG-[HOSTNAME]`. Dadurch wird eine Tabelle erstellt, die die ID der betreffenden Partei für jeden Admin-Knoten in Ihrem System anhand des Hostnamen des Knotens anzeigt.

   > Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID-System ein Vertrauensverhältnis aufbauen. Mit einer Vertrauensbasis für jeden Admin-Knoten wird sichergestellt, dass Benutzer sich sicher bei und aus jedem Admin-Knoten anmelden können.

4. Wählen Sie **Speichern**.

   Ein grünes Häkchen wird für einige Sekunden auf der Schaltfläche **Speichern** angezeigt.

Azure

1. Geben Sie an, welches TLS-Zertifikat zur Sicherung der Verbindung verwendet wird, wenn der Identitäts-Provider SSO-Konfigurationsinformationen als Antwort auf StorageGRID-Anforderungen sendet.

- **Verwenden Sie das Betriebssystem CA-Zertifikat**: Verwenden Sie das auf dem Betriebssystem installierte Standard-CA-Zertifikat, um die Verbindung zu sichern.
- **Benutzerdefiniertes CA-Zertifikat verwenden**: Verwenden Sie ein benutzerdefiniertes CA-Zertifikat, um die Verbindung zu sichern.

  Wenn Sie diese Einstellung auswählen, kopieren Sie den Text des benutzerdefinierten Zertifikats und fügen Sie ihn in das Textfeld **CA-Zertifikat** ein.

- **Verwenden Sie keine TLS**: Verwenden Sie kein TLS-Zertifikat, um die Verbindung zu sichern.

2. Geben Sie im Abschnitt Enterprise-Anwendung den **Enterprise-Anwendungsnamen** für StorageGRID an. Dieser Wert steuert den Namen, den Sie für die einzelnen Enterprise-Applikationen in Azure AD verwenden.

   - Wenn Ihr Grid beispielsweise nur einen Admin-Node hat und Sie nicht erwarten, dass künftig weitere Admin-Nodes hinzugefügt werden, geben Sie ein `SG` Oder `StorageGRID`.
   - Wenn Ihr Grid mehr als einen Admin-Node enthält, fügen Sie die Zeichenfolge ein `[HOSTNAME]` In der Kennung. Beispiel: `SG-[HOSTNAME]`. Dadurch wird eine Tabelle mit dem Namen einer Enterprise-Anwendung für jeden Admin-Knoten in Ihrem System generiert, basierend auf dem Hostnamen des Knotens.

   > Sie müssen eine Enterprise-Anwendung für jeden Admin-Knoten in Ihrem StorageGRID-System erstellen. Mit einer Enterprise-Anwendung für jeden Admin-Node wird sichergestellt, dass Benutzer sich sicher bei und aus jedem Admin-Node anmelden können.

3. Befolgen Sie die Schritte unter Erstellen von Enterprise-Applikationen in Azure AD So erstellen Sie für jeden in der Tabelle aufgeführten Admin-Knoten eine Enterprise-Anwendung.
4. Kopieren Sie in Azure AD die Federungs-Metadaten-URL für jede Enterprise-Applikation. Fügen Sie dann diese URL in das entsprechende Feld **Federation Metadaten URL** in StorageGRID ein.
5. Nachdem Sie eine URL für die Federation Metadaten für alle Administratorknoten kopiert und eingefügt haben, wählen Sie **Speichern**.

   Ein grünes Häkchen wird für einige Sekunden auf der Schaltfläche **Speichern** angezeigt.

PingFederate

1. Geben Sie an, welches TLS-Zertifikat zur Sicherung der Verbindung verwendet wird, wenn der Identitäts-Provider SSO-Konfigurationsinformationen als Antwort auf StorageGRID-Anforderungen sendet.
   - **Verwenden Sie das Betriebssystem CA-Zertifikat**: Verwenden Sie das auf dem Betriebssystem installierte Standard-CA-Zertifikat, um die Verbindung zu sichern.
   - **Benutzerdefiniertes CA-Zertifikat verwenden**: Verwenden Sie ein benutzerdefiniertes CA-Zertifikat, um die Verbindung zu sichern.

     Wenn Sie diese Einstellung auswählen, kopieren Sie den Text des benutzerdefinierten Zertifikats und fügen Sie ihn in das Textfeld **CA-Zertifikat** ein.

- **Verwenden Sie keine TLS**: Verwenden Sie kein TLS-Zertifikat, um die Verbindung zu sichern.

2. Geben Sie im Abschnitt Dienstanbieter (SP) die **SP-Verbindungs-ID** für StorageGRID an. Dieser Wert steuert den Namen, den Sie für jede SP-Verbindung in PingFederate verwenden.

   - Wenn Ihr Grid beispielsweise nur einen Admin-Node hat und Sie nicht erwarten, dass künftig weitere Admin-Nodes hinzugefügt werden, geben Sie ein `SG` Oder `StorageGRID`.
   - Wenn Ihr Grid mehr als einen Admin-Node enthält, fügen Sie die Zeichenfolge ein `[HOSTNAME]` In der Kennung. Beispiel: `SG-[HOSTNAME]`. Dadurch wird basierend auf dem Hostnamen des Node eine Tabelle mit der SP-Verbindungs-ID für jeden Admin-Node im System generiert.

   > Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID-System eine SP-Verbindung erstellen. Durch eine SP-Verbindung für jeden Admin-Node wird sichergestellt, dass Benutzer sich sicher bei und aus jedem Admin-Node anmelden können.

3. Geben Sie im Feld **Federation Metadaten-URL** die URL der Federation Metadaten für jeden Admin-Node an.

   Verwenden Sie das folgende Format:

   ```
   https://<Federation Service Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP Connection ID>
   ```

4. Wählen Sie **Speichern**.

   Ein grünes Häkchen wird für einige Sekunden auf der Schaltfläche **Speichern** angezeigt.

Konfigurieren Sie Vertrauensstellungen von Drittanbietern, Unternehmensanwendungen oder SP-Verbindungen

Wenn die Konfiguration gespeichert ist, wird die Bestätigungsmeldung des Sandbox-Modus angezeigt. Dieser Hinweis bestätigt, dass der Sandbox-Modus jetzt aktiviert ist und eine Übersicht enthält.

StorageGRID kann so lange wie erforderlich im Sandbox-Modus verbleiben. Wenn jedoch **Sandbox-Modus** auf der Single Sign-On-Seite ausgewählt ist, ist SSO für alle StorageGRID-Benutzer deaktiviert. Nur lokale Benutzer können sich anmelden.

Führen Sie diese Schritte aus, um Trusts (Active Directory) von Vertrauensstellen (Vertrauensstellen), vollständige Enterprise-Applikationen (Azure) zu konfigurieren oder SP-Verbindungen (PingFederate) zu konfigurieren.

Active Directory

1. Wechseln Sie zu Active Directory Federation Services (AD FS).
2. Erstellen Sie eine oder mehrere Treuhänder für StorageGRID, die sich auf der StorageGRID Single Sign-On-Seite in der Tabelle befinden.

   Sie müssen für jeden in der Tabelle aufgeführten Admin-Node ein Vertrauen erstellen.

   Weitere Anweisungen finden Sie unter Erstellen Sie Vertrauensstellungen von vertrauenswürdigen Parteien in AD FS.

Azure

1. Wählen Sie auf der Seite Single Sign-On für den Admin-Node, bei dem Sie sich aktuell angemeldet haben, die Schaltfläche zum Herunterladen und Speichern der SAML-Metadaten aus.
2. Wiederholen Sie dann für alle anderen Admin-Knoten in Ihrem Raster die folgenden Schritte:
   a. Melden Sie sich beim Knoten an.
   b. Wählen Sie **KONFIGURATION Zugangskontrolle Single Sign-On**.
   c. Laden Sie die SAML-Metadaten für diesen Node herunter, und speichern Sie sie.
3. Wechseln Sie zum Azure-Portal.
4. Befolgen Sie die Schritte unter Erstellen von Enterprise-Applikationen in Azure AD So laden Sie die SAML-Metadatendatei für jeden Admin-Node in die entsprechende Azure-Enterprise-Applikation hoch.

PingFederate

1. Wählen Sie auf der Seite Single Sign-On für den Admin-Node, bei dem Sie sich aktuell angemeldet haben, die Schaltfläche zum Herunterladen und Speichern der SAML-Metadaten aus.
2. Wiederholen Sie dann für alle anderen Admin-Knoten in Ihrem Raster die folgenden Schritte:
   a. Melden Sie sich beim Knoten an.
   b. Wählen Sie **KONFIGURATION Zugangskontrolle Single Sign-On**.
   c. Laden Sie die SAML-Metadaten für diesen Node herunter, und speichern Sie sie.
3. Fahren Sie zur PingFederate.
4. Erstellen Sie eine oder mehrere SP-Verbindungen (Service-Provider) für StorageGRID. Verwenden Sie die SP-Verbindungs-ID für jeden Admin-Node (siehe Tabelle auf der Seite StorageGRID Single Sign-On) und die SAML-Metadaten, die Sie für diesen Admin-Node heruntergeladen haben.

   Für jeden in der Tabelle aufgeführten Admin-Node müssen Sie eine SP-Verbindung erstellen.

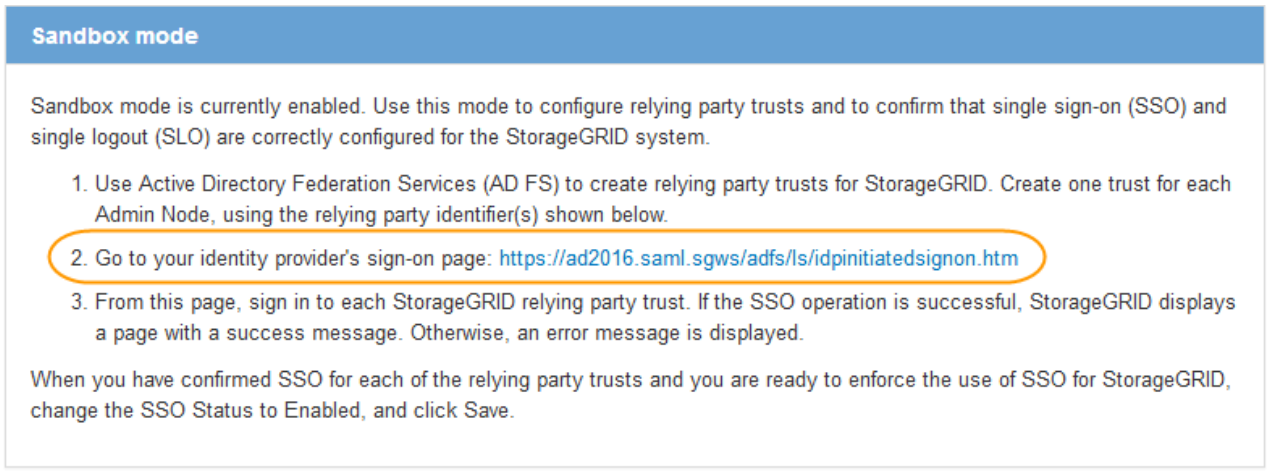
Testen Sie SSO-Verbindungen

Bevor Sie die Verwendung von Single Sign-On für Ihr gesamtes StorageGRID-System erzwingen, sollten Sie bestätigen, dass Single Sign-On und Single Logout für jeden Admin-Knoten korrekt konfiguriert sind.

Active Directory

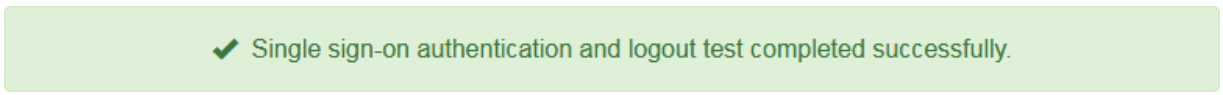
1. Suchen Sie auf der StorageGRID Single Sign-On-Seite den Link in der Meldung Sandbox-Modus.

   Die URL wird aus dem Wert abgeleitet, den Sie im Feld **Federation Service Name** eingegeben haben.



2. Wählen Sie den Link aus, oder kopieren Sie die URL in einen Browser, um auf die Anmeldeseite Ihres Identitätsanbieters zuzugreifen.
3. Um zu bestätigen, dass Sie SSO zur Anmeldung bei StorageGRID verwenden können, wählen Sie **Anmelden bei einer der folgenden Sites**, wählen Sie die bevertrauenden Partei-ID für Ihren primären Admin-Knoten und wählen Sie **Anmelden**.

4. Geben Sie Ihren föderierten Benutzernamen und Ihr Kennwort ein.
   - Wenn die SSO-Anmelde- und -Abmeldevorgänge erfolgreich sind, wird eine Erfolgsmeldung angezeigt.



   - Wenn der SSO-Vorgang nicht erfolgreich ist, wird eine Fehlermeldung angezeigt. Beheben Sie das Problem, löschen Sie die Cookies des Browsers, und versuchen Sie es erneut.
5. Wiederholen Sie diese Schritte, um die SSO-Verbindung für jeden Admin-Node in Ihrem Raster zu überprüfen.

Azure

1. Wechseln Sie im Azure-Portal zur Seite Single Sign On.
2. Wählen Sie **Diese Anwendung testen**.
3. Geben Sie die Anmeldeinformationen eines föderierten Benutzers ein.
   - Wenn die SSO-Anmelde- und -Abmeldevorgänge erfolgreich sind, wird eine Erfolgsmeldung angezeigt.

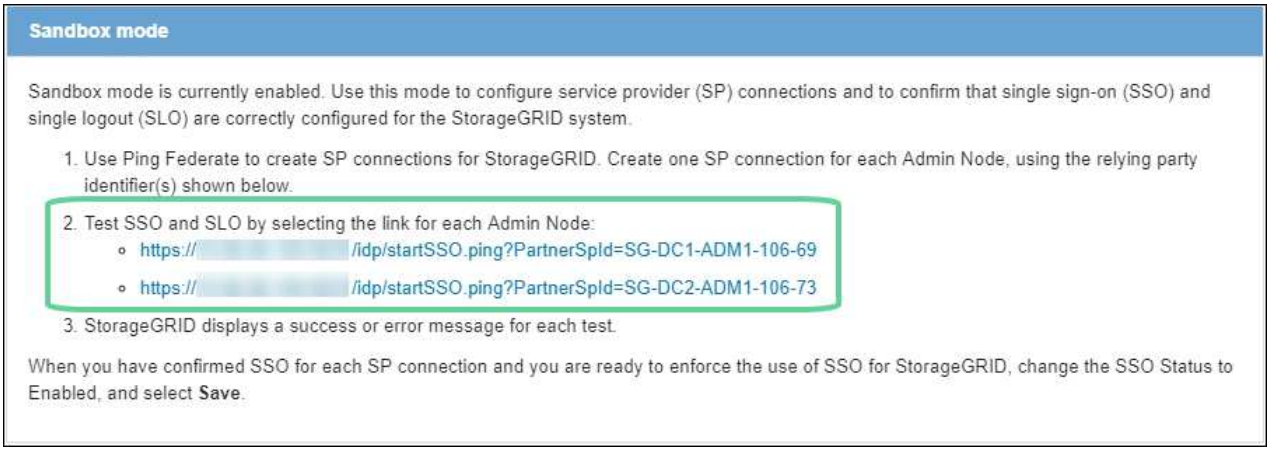
     ✔ Single sign-on authentication and logout test completed successfully.

   - Wenn der SSO-Vorgang nicht erfolgreich ist, wird eine Fehlermeldung angezeigt. Beheben Sie das Problem, löschen Sie die Cookies des Browsers, und versuchen Sie es erneut.
4. Wiederholen Sie diese Schritte, um die SSO-Verbindung für jeden Admin-Node in Ihrem Raster zu überprüfen.

PingFederate

1. Wählen Sie auf der StorageGRID-Seite Single Sign-On den ersten Link in der Meldung Sandbox-Modus aus.

   Wählen Sie jeweils einen Link aus, und testen Sie ihn.

2. Geben Sie die Anmeldeinformationen eines föderierten Benutzers ein.
   - Wenn die SSO-Anmelde- und -Abmeldevorgänge erfolgreich sind, wird eine Erfolgsmeldung angezeigt.

     ✔ Single sign-on authentication and logout test completed successfully.

   - Wenn der SSO-Vorgang nicht erfolgreich ist, wird eine Fehlermeldung angezeigt. Beheben Sie das Problem, löschen Sie die Cookies des Browsers, und versuchen Sie es erneut.
3. Wählen Sie den nächsten Link aus, um die SSO-Verbindung für jeden Admin-Node in Ihrem Raster zu überprüfen.

   Wenn eine Nachricht mit abgelaufener Seite angezeigt wird, wählen Sie in Ihrem Browser die Schaltfläche **Zurück** aus, und senden Sie Ihre Anmeldedaten erneut.

Aktivieren Sie Single Sign On

Wenn Sie bestätigt haben, dass Sie sich mit SSO bei jedem Admin-Node anmelden können, können Sie SSO für Ihr gesamtes StorageGRID System aktivieren.

> Wenn SSO aktiviert ist, müssen alle Benutzer SSO verwenden, um auf den Grid Manager, den Mandanten-Manager, die Grid-Management-API und die Mandanten-Management-API zuzugreifen. Lokale Benutzer können nicht mehr auf StorageGRID zugreifen.

1. Wählen Sie **KONFIGURATION Zugangskontrolle Single Sign-On**.
2. Ändern Sie den SSO-Status in **aktiviert**.
3. Wählen Sie **Speichern**.
4. Überprüfen Sie die Warnmeldung, und wählen Sie **OK**.

   Single Sign-On ist jetzt aktiviert.

> Wenn Sie das Azure-Portal verwenden und über denselben Computer auf StorageGRID zugreifen, mit dem Sie auf Azure zugreifen, stellen Sie sicher, dass der Azure-Portal-Benutzer auch ein autorisierter StorageGRID-Benutzer ist (ein Benutzer in einer föderierten Gruppe, die in StorageGRID importiert wurde). Oder melden Sie sich vom Azure-Portal ab, bevor Sie sich bei StorageGRID anmelden.

Erstellen Sie Vertrauensstellungen von vertrauenswürdigen Parteien in AD FS

Sie müssen Active Directory Federation Services (AD FS) verwenden, um ein Vertrauensverhältnis für jeden Admin-Knoten in Ihrem System zu erstellen. Sie können vertraut mit PowerShell-Befehlen erstellen, SAML-Metadaten von StorageGRID importieren oder die Daten manuell eingeben.

Was Sie benötigen

- Sie haben Single Sign-On für StorageGRID konfiguriert und als SSO-Typ **AD FS** ausgewählt.
- **Der Sandbox-Modus** ist auf der Single Sign-On-Seite im Grid Manager ausgewählt. Siehe Verwenden Sie den Sandbox-Modus.
- Sie kennen den vollständig qualifizierten Domänennamen (oder die IP-Adresse) und die bevertrauenden Partei-ID für jeden Admin-Knoten in Ihrem System. Diese Werte finden Sie in der Detailtabelle Admin Nodes auf der StorageGRID Single Sign-On-Seite.

  > Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID-System ein Vertrauensverhältnis aufbauen. Mit einer Vertrauensbasis für jeden Admin-Knoten wird sichergestellt, dass Benutzer sich sicher bei und aus jedem Admin-Knoten anmelden können.

- Sie haben Erfahrung beim Erstellen von Vertrauensstellungen von Vertrauensstellen in AD FS, oder Sie haben Zugriff auf die Microsoft AD FS-Dokumentation.
- Sie verwenden das Snap-in AD FS Management und gehören der Gruppe Administratoren an.
- Wenn Sie das Vertrauen der Vertrauensstelle manuell erstellen, haben Sie das benutzerdefinierte Zertifikat, das für die StorageGRID-Managementoberfläche hochgeladen wurde, oder Sie wissen, wie Sie sich von der Eingabeaufforderung-Shell bei einem Admin-Knoten anmelden.

Über diese Aufgabe

Diese Anweisungen gelten für Windows Server 2016 AD FS. Wenn Sie eine andere Version von AD FS verwenden, werden Sie kleine Unterschiede im Verfahren bemerken. Wenn Sie Fragen haben, lesen Sie bitte die Microsoft AD FS-Dokumentation.

Erstellen Sie mit Windows PowerShell ein Vertrauensverhältnis, das sich auf die Kunden stützt

Mit Windows PowerShell können Sie schnell ein oder mehrere Vertrauensstellen von vertrauenswürdigen Parteien erstellen.

Schritte

1. Wählen Sie im Windows-Startmenü mit der rechten Maustaste das PowerShell-Symbol aus und wählen Sie **als Administrator ausführen** aus.
2. Geben Sie an der PowerShell-Eingabeaufforderung den folgenden Befehl ein:

   ```
   Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
   "https://Admin_Node_FQDN/api/saml-metadata"
   ```

   - Für *Admin_Node_Identifier*, Geben Sie die ID für den Admin-Knoten auf, die sich auf der Seite Single Sign-On befindet, genau so ein, wie sie auf der Seite „Single Sign-On“ angezeigt wird. Beispiel: `SG-DC1-ADM1`.
   - Für *Admin_Node_FQDN*, Geben Sie den vollständig qualifizierten Domänennamen für denselben Admin-Knoten ein. (Bei Bedarf können Sie stattdessen die IP-Adresse des Node verwenden. Wenn Sie hier jedoch eine IP-Adresse eingeben, beachten Sie, dass Sie dieses Vertrauen der Vertrauensbasis aktualisieren oder neu erstellen müssen, wenn sich diese IP-Adresse immer ändert.)
3. Wählen Sie im Windows Server Manager **Tools AD FS Management** aus.

   Das AD FS Management Tool wird angezeigt.
4. Wählen Sie **AD FS Treuhand-Party-Trusts**.

   Die Liste der Vertrauensstellen wird angezeigt.
5. Fügen Sie eine Zugriffskontrollrichtlinie zum neu erstellten Vertrauen der Vertrauensstellenden Partei hinzu:
   a. Suchen Sie das Vertrauen der Vertrauensgesellschaft, das Sie gerade erstellt haben.
   b. Klicken Sie mit der rechten Maustaste auf das Vertrauen und wählen Sie **Zugriffskontrollrichtlinie bearbeiten**.
   c. Wählen Sie eine Zugriffskontrollrichtlinie aus.
   d. Wählen Sie **Anwenden**, und wählen Sie **OK**
6. Fügen Sie dem neu erstellten Treuhandgesellschaft eine Richtlinie zur Ausstellung von Forderungen hinzu:
   a. Suchen Sie das Vertrauen der Vertrauensgesellschaft, das Sie gerade erstellt haben.
   b. Klicken Sie mit der rechten Maustaste auf das Vertrauen und wählen Sie **Richtlinie zur Bearbeitung von Forderungen** aus.
   c. Wählen Sie **Regel hinzufügen**.
   d. Wählen Sie auf der Seite Regelvorlage auswählen in der Liste **LDAP-Attribute als Ansprüche senden** aus, und wählen Sie **Weiter**.
   e. Geben Sie auf der Seite Regel konfigurieren einen Anzeigenamen für diese Regel ein.

Beispiel: **ObjectGUID an Name ID**.

f. Wählen Sie im Attributspeicher die Option **Active Directory** aus.

g. Geben Sie in der Spalte LDAP-Attribut der Mapping-Tabelle **objectGUID** ein.

h. Wählen Sie in der Spalte Abgehender Antragstyp der Zuordnungstabelle in der Dropdown-Liste **Name ID** aus.

i. Wählen Sie **Fertig**, und wählen Sie **OK**.

7. Bestätigen Sie, dass die Metadaten erfolgreich importiert wurden.

   a. Klicken Sie mit der rechten Maustaste auf das Vertrauen der Vertrauenssteller, um seine Eigenschaften zu öffnen.

   b. Vergewissern Sie sich, dass die Felder auf den Registerkarten **Endpunkte**, **Identifier** und **Signatur** ausgefüllt sind.

      Wenn die Metadaten fehlen, bestätigen Sie, dass die Federation-Metadatenadresse korrekt ist, oder geben Sie einfach die Werte manuell ein.

8. Wiederholen Sie diese Schritte, um ein Vertrauensverhältnis für alle Administratorknoten in Ihrem StorageGRID-System zu konfigurieren.

9. Wenn Sie fertig sind, kehren Sie zu StorageGRID zurück und testen Sie alle Treuhänder der Vertrauensstellen, um zu bestätigen, dass sie richtig konfiguriert sind. Siehe Verwenden Sie den Sandbox-Modus Weitere Anweisungen.

Erstellen Sie durch den Import von Federationmetadaten ein Vertrauen von Kunden

Sie können die Werte für jedes Vertrauen der betreffenden Anbieter importieren, indem Sie für jeden Admin-Node auf die SAML-Metadaten zugreifen.

Schritte

1. Wählen Sie im Windows Server Manager **Tools** aus, und wählen Sie dann **AD FS Management** aus.
2. Wählen Sie unter Aktionen **Vertrauensstellung hinzufügen** aus.
3. Wählen Sie auf der Begrüßungsseite * Claims Aware* aus, und wählen Sie **Start**.
4. Wählen Sie **Daten über die online veröffentlichte oder auf einem lokalen Netzwerk** importieren.
5. Geben Sie unter **Federation Metadatenadresse (Hostname oder URL)** den Speicherort der SAML-Metadaten für diesen Admin-Node ein:

   `https://Admin_Node_FQDN/api/saml-metadata`

   Für *`Admin_Node_FQDN`*, Geben Sie den vollständig qualifizierten Domänennamen für denselben Admin-Knoten ein. (Bei Bedarf können Sie stattdessen die IP-Adresse des Node verwenden. Wenn Sie hier jedoch eine IP-Adresse eingeben, beachten Sie, dass Sie dieses Vertrauen der Vertrauensbasis aktualisieren oder neu erstellen müssen, wenn sich diese IP-Adresse immer ändert.)

6. Schließen Sie den Assistenten „Vertrauen in die Vertrauensstellung“, speichern Sie das Vertrauen der zu vertrauenden Partei und schließen Sie den Assistenten.

> Verwenden Sie bei der Eingabe des Anzeigennamens die bevertrauende Partei-ID für den Admin-Node genau so, wie sie auf der Seite Single Sign-On im Grid Manager angezeigt wird. Beispiel: `SG-DC1-ADM1`.

7. Fügen Sie eine Antragsregel hinzu:
   a. Klicken Sie mit der rechten Maustaste auf das Vertrauen und wählen Sie **Richtlinie zur Bearbeitung von Forderungen** aus.
   b. Wählen Sie **Regel hinzufügen**:
   c. Wählen Sie auf der Seite Regelvorlage auswählen in der Liste **LDAP-Attribute als Ansprüche senden** aus, und wählen Sie **Weiter**.
   d. Geben Sie auf der Seite Regel konfigurieren einen Anzeigenamen für diese Regel ein.

      Beispiel: **ObjectGUID an Name ID**.

   e. Wählen Sie im Attributspeicher die Option **Active Directory** aus.
   f. Geben Sie in der Spalte LDAP-Attribut der Mapping-Tabelle **objectGUID** ein.
   g. Wählen Sie in der Spalte Abgehender Antragstyp der Zuordnungstabelle in der Dropdown-Liste **Name ID** aus.
   h. Wählen Sie **Fertig**, und wählen Sie **OK**.
8. Bestätigen Sie, dass die Metadaten erfolgreich importiert wurden.
   a. Klicken Sie mit der rechten Maustaste auf das Vertrauen der Vertrauenssteller, um seine Eigenschaften zu öffnen.
   b. Vergewissern Sie sich, dass die Felder auf den Registerkarten **Endpunkte**, **Identifier** und **Signatur** ausgefüllt sind.

      Wenn die Metadaten fehlen, bestätigen Sie, dass die Federation-Metadatenadresse korrekt ist, oder geben Sie einfach die Werte manuell ein.

9. Wiederholen Sie diese Schritte, um ein Vertrauensverhältnis für alle Administratorknoten in Ihrem StorageGRID-System zu konfigurieren.
10. Wenn Sie fertig sind, kehren Sie zu StorageGRID zurück und testen Sie alle Treuhänder der Vertrauensstellen, um zu bestätigen, dass sie richtig konfiguriert sind. Siehe Verwenden Sie den Sandbox-Modus Weitere Anweisungen.

Erstellen Sie manuell ein Vertrauen der Vertrauensbasis

Wenn Sie sich entscheiden, die Daten für die Treuhanddienste des Treuhandteils nicht zu importieren, können Sie die Werte manuell eingeben.

Schritte

1. Wählen Sie im Windows Server Manager **Tools** aus, und wählen Sie dann **AD FS Management** aus.
2. Wählen Sie unter Aktionen **Vertrauensstellung hinzufügen** aus.
3. Wählen Sie auf der Begrüßungsseite * Claims Aware* aus, und wählen Sie **Start**.
4. Wählen Sie **Geben Sie Daten über den Besteller manuell** ein, und wählen Sie **Weiter**.
5. Schließen Sie den Assistenten für Vertrauen in die vertrauende Partei ab:
   a. Geben Sie einen Anzeigenamen für diesen Admin-Node ein.

      Verwenden Sie für Konsistenz den Admin-Node mit der bewirtenden Partei-Kennung, genau wie er auf der Seite Single Sign-On im Grid Manager angezeigt wird. Beispiel: `SG-DC1-ADM1`.

b. Überspringen Sie den Schritt, um ein optionales Token-Verschlüsselungszertifikat zu konfigurieren.

c. Aktivieren Sie auf der Seite „URL konfigurieren“ das Kontrollkästchen **Unterstützung für das SAML 2.0 WebSSO-Protokoll** aktivieren.

d. Geben Sie die Endpunkt-URL des SAML-Service für den Admin-Node ein:

`https://Admin_Node_FQDN/api/saml-response`

Für `*Admin_Node_FQDN*`Geben Sie den vollständig qualifizierten Domänennamen für den Admin-Knoten ein. (Bei Bedarf können Sie stattdessen die IP-Adresse des Node verwenden. Wenn Sie hier jedoch eine IP-Adresse eingeben, beachten Sie, dass Sie dieses Vertrauen der Vertrauensbasis aktualisieren oder neu erstellen müssen, wenn sich diese IP-Adresse immer ändert.)

e. Geben Sie auf der Seite Configure Identifiers die befolgende Partei-ID für denselben Admin-Node an:

Admin_Node_Identifier

Für *Admin_Node_Identifier*, Geben Sie die ID für den Admin-Knoten auf, die sich auf der Seite Single Sign-On befindet, genau so ein, wie sie auf der Seite „Single Sign-On“ angezeigt wird. Beispiel: `SG-DC1-ADM1`.

f. Überprüfen Sie die Einstellungen, speichern Sie das Vertrauen der Vertrauensstellungsgesellschaft, und schließen Sie den Assistenten.

Das Dialogfeld „Forderungsrichtlinie bearbeiten“ wird angezeigt.

Wenn das Dialogfeld nicht angezeigt wird, klicken Sie mit der rechten Maustaste auf das Vertrauen und wählen Sie **Richtlinie zur Bearbeitung von Forderungen** aus.

6. Um den Assistenten für die Antragsregel zu starten, wählen Sie **Regel hinzufügen**:

a. Wählen Sie auf der Seite Regelvorlage auswählen in der Liste **LDAP-Attribute als Ansprüche senden** aus, und wählen Sie **Weiter**.

b. Geben Sie auf der Seite Regel konfigurieren einen Anzeigenamen für diese Regel ein.

Beispiel: **ObjectGUID an Name ID**.

c. Wählen Sie im Attributspeicher die Option **Active Directory** aus.

d. Geben Sie in der Spalte LDAP-Attribut der Mapping-Tabelle **objectGUID** ein.

e. Wählen Sie in der Spalte Abgehender Antragstyp der Zuordnungstabelle in der Dropdown-Liste **Name ID** aus.

f. Wählen Sie **Fertig**, und wählen Sie **OK**.

7. Klicken Sie mit der rechten Maustaste auf das Vertrauen der Vertrauenssteller, um seine Eigenschaften zu öffnen.

8. Konfigurieren Sie auf der Registerkarte **Endpunkte** den Endpunkt für einzelne Abmeldung (SLO):

a. Wählen Sie **SAML hinzufügen**.

b. Wählen Sie **Endpunkttyp SAML Logout**.

c. Wählen Sie **Bindung Umleiten**.

d. Geben Sie im Feld **Trusted URL** die URL ein, die für Single Logout (SLO) von diesem Admin-Node verwendet wird:

`https://Admin_Node_FQDN/api/saml-logout`

Für `Admin_Node_FQDN`, Geben Sie den vollständig qualifizierten Domänennamen des Admin-Knotens ein. (Bei Bedarf können Sie stattdessen die IP-Adresse des Node verwenden. Wenn Sie hier jedoch eine IP-Adresse eingeben, beachten Sie, dass Sie dieses Vertrauen der Vertrauensbasis aktualisieren oder neu erstellen müssen, wenn sich diese IP-Adresse immer ändert.)

a. Wählen Sie **OK**.

9. Geben Sie auf der Registerkarte **Signatur** das Signaturzertifikat für dieses Vertrauen der bevertrauenden Partei an:

   a. Fügen Sie das benutzerdefinierte Zertifikat hinzu:

      - Wenn Sie über das benutzerdefinierte Managementzertifikat verfügen, das Sie in StorageGRID hochgeladen haben, wählen Sie dieses Zertifikat aus.
      - Wenn Sie nicht über das benutzerdefinierte Zertifikat verfügen, melden Sie sich beim Admin-Knoten an, gehen Sie zu `/var/local/mgmt-api` Verzeichnis des Admin-Knotens, und fügen Sie das hinzu `custom-server.crt` Zertifikatdatei.

        Hinweis: das Standardzertifikat des Admin-Knotens verwenden (`server.crt`) Wird nicht empfohlen. Wenn der Admin-Knoten ausfällt, wird das Standardzertifikat neu generiert, wenn Sie den Knoten wiederherstellen, und Sie müssen das Vertrauen der Vertrauensstelle aktualisieren.

   b. Wählen Sie **Anwenden**, und wählen Sie **OK**.

      Die Eigenschaften der zu vertrauenden Partei werden gespeichert und geschlossen.

10. Wiederholen Sie diese Schritte, um ein Vertrauensverhältnis für alle Administratorknoten in Ihrem StorageGRID-System zu konfigurieren.
11. Wenn Sie fertig sind, kehren Sie zu StorageGRID zurück und testen Sie alle Treuhänder der Vertrauensstellen, um zu bestätigen, dass sie richtig konfiguriert sind. Siehe Verwenden Sie den Sandbox-Modus Weitere Anweisungen.

Erstellen von Enterprise-Applikationen in Azure AD

Mit Azure AD erstellen Sie für jeden Admin-Node in Ihrem System eine Enterprise-Applikation.

Was Sie benötigen

- Sie haben mit der Konfiguration der Single Sign-On-Funktion für StorageGRID begonnen und als SSO-Typ **Azure** ausgewählt.
- **Der Sandbox-Modus** ist auf der Single Sign-On-Seite im Grid Manager ausgewählt. Siehe Verwenden Sie den Sandbox-Modus.
- Sie haben den **Enterprise-Anwendungsnamen** für jeden Admin-Knoten in Ihrem System. Sie können diese Werte aus der Detailtabelle „Admin-Knoten“ auf der Seite „StorageGRID Single Sign-On“ kopieren.

> Sie müssen eine Enterprise-Anwendung für jeden Admin-Knoten in Ihrem StorageGRID-System erstellen. Mit einer Enterprise-Anwendung für jeden Admin-Node wird sichergestellt, dass Benutzer sich sicher bei und aus jedem Admin-Node anmelden können.

- Sie haben Erfahrung beim Erstellen von Enterprise-Applikationen in Azure Active Directory.

- Sie verfügen über ein Azure Konto mit einem aktiven Abonnement.
- Im Azure-Konto verfügen Sie über eine der folgenden Rollen: Global Administrator, Cloud Application Administrator, Application Administrator oder Eigentümer des Service-Principal.

Zugriff auf Azure AD

1. Melden Sie sich beim an "Azure-Portal".
2. Navigieren Sie zu "Azure Active Directory".
3. Wählen Sie "Enterprise-Applikationen".

Erstellen von Enterprise-Applikationen und Speichern von StorageGRID SSO-Konfiguration

Um die SSO-Konfiguration für Azure in StorageGRID zu speichern, müssen Sie mit Azure eine Enterprise-Applikation für jeden Admin-Node erstellen. Sie kopieren die Federation Metadaten-URLs aus Azure und fügen sie in die entsprechenden Felder **Federation Metadaten-URL** auf der StorageGRID Single Sign-on-Seite ein.

1. Wiederholen Sie die folgenden Schritte für jeden Admin-Node.
   a. Wählen Sie im Fensterbereich Azure Enterprise-Anwendungen **Neue Anwendung** aus.
   b. Wählen Sie **Erstellen Sie Ihre eigene Anwendung**.
   c. Geben Sie für den Namen den **Enterprise-Anwendungsnamen** ein, den Sie aus der Tabelle Admin-Knoten Details auf der StorageGRID-Seite Single Sign-On kopiert haben.
   d. Lassen Sie das * eine andere Anwendung integrieren, die Sie nicht in der Galerie finden (nicht-Galerie)* Optionsfeld ausgewählt.
   e. Wählen Sie **Erstellen**.
   f. Wählen Sie im **2 den Link *Get Started** aus. Aktivieren Sie das Feld Single Sign On*, oder wählen Sie den Link **Single Sign-On** im linken Rand.
   g. Wählen Sie das Feld **SAML** aus.
   h. Kopieren Sie die **App Federation Metadaten-URL**, die Sie unter **Step 3 SAML-Signierungszertifikat** finden können.
   i. Gehen Sie auf die Seite StorageGRID Single Sign-On und fügen Sie die URL in das Feld **Federation Metadaten-URL** ein, das dem von Ihnen verwendeten **Enterprise-Anwendungsnamen** entspricht.
2. Nachdem Sie für jeden Admin-Knoten eine Metadaten-URL für den Verbund eingefügt haben und alle weiteren erforderlichen Änderungen an der SSO-Konfiguration vorgenommen haben, wählen Sie auf der Seite StorageGRID Single Sign-On die Option **Speichern** aus.

Laden Sie für jeden Admin-Node SAML-Metadaten herunter

Nachdem die SSO-Konfiguration gespeichert ist, können Sie für jeden Admin-Node in Ihrem StorageGRID-System eine SAML-Metadatendatei herunterladen.

Wiederholen Sie diese Schritte für jeden Admin-Knoten:

1. Melden Sie sich über den Admin-Node bei StorageGRID an.
2. Wählen Sie **KONFIGURATION Zugangskontrolle Single Sign-On**.
3. Wählen Sie die Schaltfläche, um die SAML-Metadaten für diesen Admin-Node herunterzuladen.
4. Speichern Sie die Datei, die Sie in Azure AD hochladen möchten.

Hochladen von SAML-Metadaten in jede Enterprise-Applikation

Nach dem Herunterladen einer SAML-Metadatendatei für jeden StorageGRID-Admin-Node führen Sie die folgenden Schritte in Azure AD aus:

1. Zurück zum Azure-Portal.
2. Wiederholen Sie diese Schritte für jede Enterprise-Applikation:

   > Möglicherweise müssen Sie die Seite Enterprise-Applikationen aktualisieren, um Anwendungen anzuzeigen, die Sie zuvor in der Liste hinzugefügt haben.

   a. Gehen Sie zur Seite Eigenschaften für die Enterprise-Anwendung.
   b. Legen Sie **Zuweisung erforderlich** auf **Nein** fest (es sei denn, Sie möchten Aufgaben separat konfigurieren).
   c. Rufen Sie die Seite Single Sign-On auf.
   d. Schließen Sie die SAML-Konfiguration ab.
   e. Wählen Sie die Schaltfläche **Metadatendatei hochladen** aus, und wählen Sie die SAML-Metadatendatei aus, die Sie für den entsprechenden Admin-Node heruntergeladen haben.
   f. Nachdem die Datei geladen wurde, wählen Sie **Speichern** und dann **X** aus, um das Fenster zu schließen. Sie gelangen zurück zur Seite Single Sign-On mit SAML einrichten.
3. Befolgen Sie die Schritte unter Verwenden Sie den Sandbox-Modus Um jede Applikation zu testen.

Erstellen von SP-Verbindungen (Service Provider) in PingFederate

Sie verwenden PingFederate, um für jeden Admin-Node in Ihrem System eine SP-Verbindung (Service Provider) zu erstellen. Um den Prozess zu beschleunigen, importieren Sie die SAML-Metadaten aus StorageGRID.

Was Sie benötigen

- Sie haben Single Sign-On für StorageGRID konfiguriert und als SSO-Typ * Ping föderate* ausgewählt.
- **Der Sandbox-Modus** ist auf der Single Sign-On-Seite im Grid Manager ausgewählt. Siehe Verwenden Sie den Sandbox-Modus.
- Sie haben die **SP-Verbindungs-ID** für jeden Admin-Knoten in Ihrem System. Diese Werte finden Sie in der Detailtabelle Admin Nodes auf der StorageGRID Single Sign-On-Seite.
- Sie haben die **SAML-Metadaten** für jeden Admin-Knoten in Ihrem System heruntergeladen.
- Sie haben Erfahrung beim Erstellen von SP-Verbindungen in PingFederate Server.
- Sie haben diehttps://docs.pingidentity.com/bundle/pingfederate-103/page/kfj1564002962494.html["Administrator’s Reference Guide"^] Für PingFederate Server. Die PingFederate-Dokumentation bietet detaillierte Schritt-für-Schritt-Anleitungen und Erklärungen.
- Sie haben die Administratorberechtigung für PingFederate Server.

Über diese Aufgabe

Mit diesen Anweisungen wird zusammengefasst, wie PingFederate Server Version 10.3 als SSO-Anbieter für StorageGRID konfiguriert wird. Wenn Sie eine andere Version von PingFederate verwenden, müssen Sie diese Anweisungen möglicherweise anpassen. Detaillierte Anweisungen für Ihre Version finden Sie in der Dokumentation zu PingFederate Server.

Alle Voraussetzungen in PingFederate

Bevor Sie die SP-Verbindungen erstellen können, die Sie für StorageGRID verwenden, müssen Sie die erforderlichen Aufgaben in PingFederate ausführen. Beim Konfigurieren der SP-Verbindungen verwenden Sie Informationen aus diesen Voraussetzungen.

Datenspeicher erstellen

Falls noch nicht, erstellen Sie einen Datenspeicher, um PingFederate mit dem AD FS LDAP-Server zu verbinden. Verwenden Sie die Werte, die Sie verwendet haben, wenn Identitätsföderation wird konfiguriert Im StorageGRID.

- **Typ**: Verzeichnis (LDAP)
- **LDAP-Typ**: Active Directory
- **Binärattribut Name**: Geben Sie **objectGUID** auf der Registerkarte LDAP Binärattribute genau wie dargestellt ein.

Passwortvalididator[[Password-Validator] erstellen

Wenn Sie noch nicht vorhanden sind, erstellen Sie einen Validierer für Kennwortausweise.

- **Typ**: LDAP Benutzername Passwort Zugangsdaten Validierer
- **Datenspeicher**: Wählen Sie den von Ihnen erstellten Datenspeicher aus.
- **Search base**: Geben Sie Informationen aus LDAP ein (z. B. DC=saml,DC=sgws).
- **Suchfilter**: SAMAccountName=€{username}
- **Umfang**: Unterbaum

IdP-Adapterinstanz erstellen

Wenn Sie noch nicht, erstellen Sie eine IdP-Adapterinstanz.

1. Gehen Sie zu **Authentifizierung Integration IdP-Adapter**.
2. Wählen Sie **Neue Instanz Erstellen**.
3. Wählen Sie auf der Registerkarte Typ die Option **HTML-Formular-IdP-Adapter** aus.
4. Wählen Sie auf der Registerkarte IdP-Adapter **Neue Zeile zu 'Credential Validators'** hinzufügen.
5. Wählen Sie die aus Gültigkeitsprüfung für Kennwortausweise Sie haben erstellt.
6. Wählen Sie auf der Registerkarte Adapterattribute das Attribut **Benutzername** für **Pseudonym** aus.
7. Wählen Sie **Speichern**.

Signaturzertifikat erstellen oder importieren

Wenn Sie noch nicht, erstellen oder importieren Sie das Signierungszertifikat.

1. Gehen Sie zu **Sicherheit Signieren von Entschlüsselungszertifikaten**.
2. Erstellen oder importieren Sie das Signieren-Zertifikat.

Erstellen Sie eine SP-Verbindung in PingFederate

Wenn Sie eine SP-Verbindung in PingFederate erstellen, importieren Sie die SAML-Metadaten, die Sie für den

Admin-Node von StorageGRID heruntergeladen haben. Die Metadatendatei enthält viele der spezifischen Werte, die Sie benötigen.

> Sie müssen für jeden Admin-Node in Ihrem StorageGRID-System eine SP-Verbindung erstellen, damit sich Benutzer sicher bei und aus einem beliebigen Node anmelden können. Erstellen Sie anhand dieser Anweisungen die erste SP-Verbindung. Fahren Sie dann mit fort Erstellen Sie zusätzliche SP-Verbindungen Um zusätzliche Verbindungen zu erstellen, die Sie benötigen.

Wählen Sie den SP-Verbindungstyp

1. Gehen Sie zu **Anwendungen Integration SP-Verbindungen**.
2. Wählen Sie **Verbindung Erstellen**.
3. Wählen Sie **Verwenden Sie keine Vorlage für diese Verbindung**.
4. Wählen Sie als Protokoll **Browser SSO Profile** und **SAML 2.0** aus.

Importieren der SP-Metadaten

1. Wählen Sie auf der Registerkarte Metadaten importieren die Option **Datei**.
2. Wählen Sie die SAML-Metadatendatei, die Sie für den Admin-Node von der StorageGRID-Seite für Single Sign-On heruntergeladen haben.
3. Überprüfen Sie die Metadaten-Zusammenfassung und die Informationen auf der Registerkarte Allgemeine Informationen.

   Die Entity-ID des Partners und der Verbindungsname werden auf die Verbindungs-ID des StorageGRID-SP festgelegt. (Z. B. 10.96.105.200-DC1-ADM1-105-200). Die Basis-URL ist die IP des StorageGRID-Admin-Knotens.

4. Wählen Sie **Weiter**.

Konfigurieren Sie SSO für den IdP-Browser

1. Wählen Sie auf der Registerkarte Browser-SSO * die Option * Browser-SSO konfigurieren* aus.
2. Wählen Sie auf der Registerkarte SAML-Profile die Optionen **SP-initiated SSO**, **SP-initial SLO**, **IdP-initiated SSO** und **IdP-initiated SLO** aus.
3. Wählen Sie **Weiter**.
4. Nehmen Sie auf der Registerkarte Assertion Lifetime keine Änderungen vor.
5. Wählen Sie auf der Registerkarte Assertion Creation die Option **Assertion Creation konfigurieren** aus.
   a. Wählen Sie auf der Registerkarte Identitätszuordnung die Option **Standard**.
   b. Verwenden Sie auf der Registerkarte „Attributvertrag“ die Registerkarte **SAML_SUBJECT** als Attributvertrag und das undefinierte Namensformat, das importiert wurde.
6. Wenn Sie den Vertrag verlängern möchten, wählen Sie **Löschen** aus, um den zu entfernen `urn:oid`, Die nicht verwendet wird.

Adapterinstanz zuordnen

1. Wählen Sie auf der Registerkarte Authentication Source Mapping die Option **Map New Adapter Instance**.
2. Wählen Sie auf der Registerkarte Adapterinstanz das aus Adapterinstanz Sie haben erstellt.

3. Wählen Sie auf der Registerkarte Zuordnungsmethode die Option **Weitere Attribute aus einem Datenspeicher abrufen** aus.
4. Wählen Sie auf der Registerkarte Attributquelle User Lookup die Option **Attributquelle hinzufügen** aus.
5. Geben Sie auf der Registerkarte Data Store eine Beschreibung ein, und wählen Sie die aus Datastore Sie haben hinzugefügt.
6. Auf der Registerkarte LDAP-Verzeichnissuche:
   - Geben Sie den **Basis-DN** ein, der exakt mit dem Wert übereinstimmt, den Sie in StorageGRID für den LDAP-Server eingegeben haben.
   - Wählen Sie für den Suchumfang die Option **Subtree** aus.
   - Suchen Sie für die Root Object Class nach dem Attribut **objectGUID** und fügen Sie es hinzu.
7. Wählen Sie auf der Registerkarte LDAP Binary Attribute Encoding Types **Base64** für das Attribut **objectGUID** aus.
8. Geben Sie auf der Registerkarte LDAP-Filter **sAMAccountName=€{username}** ein.
9. Wählen Sie auf der Registerkarte „Attributvertragserfüllung“ im Dropdown-Menü „Quelle“ die Option **LDAP (Attribut)** aus und wählen Sie in der Dropdown-Liste Wert die Option **objectGUID** aus.
10. Überprüfen und speichern Sie dann die Attributquelle.
11. Wählen Sie auf der Registerkarte Attributquelle failsave die Option **SSO-Transaktion abbrechen** aus.
12. Überprüfen Sie die Zusammenfassung und wählen Sie **Fertig**.
13. Wählen Sie * Fertig*.

Konfigurieren von Protokolleinstellungen

1. Wählen Sie auf der Registerkarte **SP-Verbindung Browser SSO Protokolleinstellungen** die Option **Protokolleinstellungen konfigurieren** aus.
2. Akzeptieren Sie auf der Registerkarte Assertion Consumer Service URL die Standardwerte, die aus den StorageGRID SAML Metadaten importiert wurden (**POST** für binding und `/api/saml-response` Für Endpunkt-URL).
3. Akzeptieren Sie auf der Registerkarte SLO-Dienst-URLs die Standardwerte, die aus den StorageGRID-SAML-Metadaten importiert wurden (**REDIRECT** für Binding und `/api/saml-logout` Für Endpunkt-URL.
4. Heben Sie auf der Registerkarte zulässige SAML-Bindungen die Auswahl von **ARTEFAKT** und **SOAP** auf. Es sind nur **POST** und **REDIRECT** erforderlich.
5. Lassen Sie auf der Registerkarte Signature Policy die Kontrollkästchen **AUTHN Requests to be sign** und **always Sign Assertion** aktivieren.
6. Wählen Sie auf der Registerkarte Verschlüsselungsrichtlinie die Option **Keine** aus.
7. Überprüfen Sie die Zusammenfassung und wählen Sie **Fertig**, um die Protokolleinstellungen zu speichern.
8. Überprüfen Sie die Zusammenfassung und wählen Sie **Fertig**, um die SSO-Einstellungen des Browsers zu speichern.

Anmeldedaten konfigurieren

1. Wählen Sie auf der Registerkarte SP-Verbindung die Option **Anmeldeinformationen** aus.
2. Wählen Sie auf der Registerkarte Anmeldeinformationen die Option **Anmeldeinformationen konfigurieren**.
3. Wählen Sie die aus Signieren des Zertifikats Sie haben erstellt oder importiert.

4. Wählen Sie **Weiter** aus, um zu **Einstellungen zur Signature-Verifizierung verwalten** zu gelangen.
   a. Wählen Sie auf der Registerkarte Vertrauensmodell die Option **nicht verankert** aus.
   b. Überprüfen Sie auf der Registerkarte Signaturverifizierungszertifikat die Signature Certificate-Informationen, die aus den StorageGRID SAML-Metadaten importiert wurden.
5. Prüfen Sie die Übersichtsbildschirme und wählen Sie **Speichern**, um die SP-Verbindung zu speichern.

Erstellen Sie zusätzliche SP-Verbindungen

Sie können die erste SP-Verbindung kopieren, um die für jeden Admin-Node in Ihrem Raster erforderlichen SP-Verbindungen zu erstellen. Sie laden für jede Kopie neue Metadaten hoch.

> Die SP-Verbindungen für verschiedene Admin-Nodes verwenden identische Einstellungen, mit Ausnahme der Entity-ID des Partners, der Basis-URL, der Verbindungs-ID, des Verbindungsnamens, der Signaturverifizierung, Und SLO Response-URL.

1. Wählen Sie **Aktion Kopieren** aus, um für jeden zusätzlichen Admin-Node eine Kopie der anfänglichen SP-Verbindung zu erstellen.
2. Geben Sie die Verbindungs-ID und den Verbindungsnamen für die Kopie ein, und wählen Sie **Speichern**.
3. Wählen Sie die dem Admin-Node entsprechende Metadatendatei:
   a. Wählen Sie **Aktion Aktualisieren mit Metadaten**.
   b. Wählen Sie **Datei auswählen** und laden Sie die Metadaten hoch.
   c. Wählen Sie **Weiter**.
   d. Wählen Sie **Speichern**.
4. Beheben Sie den Fehler aufgrund des nicht verwendeten Attributs:
   a. Wählen Sie die neue Verbindung aus.
   b. Wählen Sie **Browser SSO konfigurieren Assertion Creation Attributvertrag konfigurieren**.
   c. Löschen Sie den Eintrag für **Urne:oid**.
   d. Wählen Sie **Speichern**.

Deaktivieren Sie Single Sign-On

Sie können Single Sign-On (SSO) deaktivieren, wenn Sie diese Funktion nicht mehr verwenden möchten. Sie müssen Single Sign-On deaktivieren, bevor Sie die Identitätsföderation deaktivieren können.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

Schritte

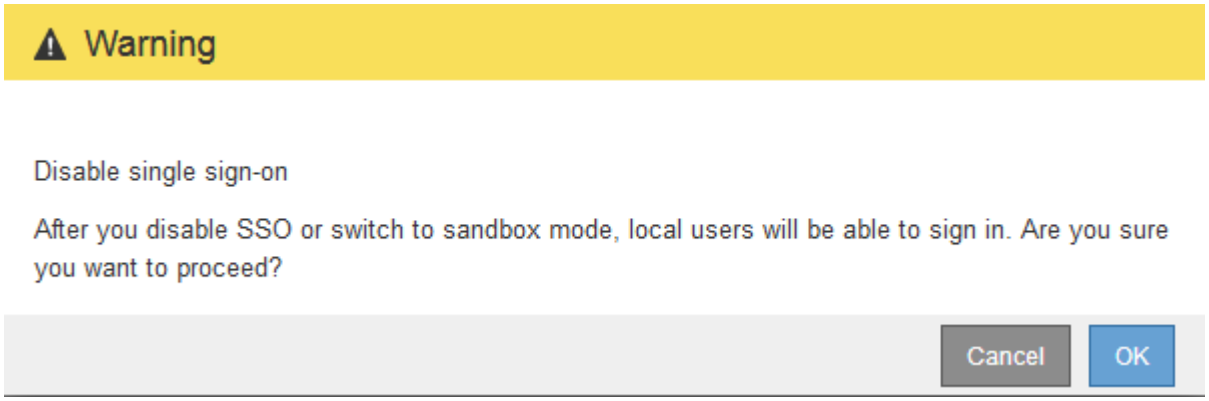
1. Wählen Sie **KONFIGURATION Zugangskontrolle Single Sign-On**.

   Die Seite Single Sign-On wird angezeigt.

2. Wählen Sie die Option **deaktiviert** aus.

3. Wählen Sie **Speichern**.

   Es wird eine Warnmeldung angezeigt, die darauf hinweist, dass lokale Benutzer sich jetzt anmelden können.



4. Wählen Sie **OK**.

   Wenn Sie sich das nächste Mal bei StorageGRID anmelden, wird die Seite StorageGRID-Anmeldung angezeigt. Sie müssen den Benutzernamen und das Kennwort für einen lokalen oder föderierten StorageGRID-Benutzer eingeben.

Deaktivieren Sie die einmalige Anmeldung für einen Admin-Knoten vorübergehend und aktivieren Sie sie erneut

Sie können sich möglicherweise nicht beim Grid-Manager anmelden, wenn das SSO-System (Single Sign-On) ausfällt. In diesem Fall können Sie SSO für einen Admin-Node vorübergehend deaktivieren und erneut aktivieren. Um SSO zu deaktivieren und dann erneut zu aktivieren, müssen Sie auf die Befehlshaber des Node zugreifen.

Was Sie benötigen

- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben die `Passwords.txt` Datei:
- Sie kennen das Passwort für den lokalen Root-Benutzer.

Über diese Aufgabe

Nachdem Sie SSO für einen Admin-Node deaktiviert haben, können Sie sich beim Grid-Manager als lokaler Root-Benutzer anmelden. Zum Sichern Ihres StorageGRID-Systems müssen Sie die Befehlshaber des Node verwenden, um SSO auf dem Admin-Node erneut zu aktivieren, sobald Sie sich abmelden.

> Das Deaktivieren von SSO für einen Admin-Node wirkt sich nicht auf die SSO-Einstellungen für andere Admin-Nodes im Raster aus. Das Kontrollkästchen **SSO aktivieren** auf der Seite Single Sign-On im Grid Manager bleibt aktiviert, und alle vorhandenen SSO-Einstellungen bleiben erhalten, wenn Sie sie nicht aktualisieren.

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:`disable-saml`

Eine Meldung gibt an, dass der Befehl nur für diesen Admin-Knoten gilt.

3. Bestätigen Sie, dass Sie SSO deaktivieren möchten.

Eine Meldung gibt an, dass Single Sign-On auf dem Knoten deaktiviert ist.

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

Die Anmeldeseite für den Grid Manager wird jetzt angezeigt, weil SSO deaktiviert wurde.

5. Melden Sie sich mit dem Benutzernamen root und dem Passwort des lokalen Root-Benutzers an.
6. Wenn Sie SSO vorübergehend deaktiviert haben, da Sie die SSO-Konfiguration korrigieren mussten:
   a. Wählen Sie **KONFIGURATION Zugangskontrolle Single Sign-On**.
   b. Ändern Sie die falschen oder veralteten SSO-Einstellungen.
   c. Wählen Sie **Speichern**.

   Wenn Sie auf der Seite Single Sign-On **Save** wählen, wird SSO für das gesamte Raster automatisch wieder aktiviert.

7. Wenn Sie SSO vorübergehend deaktiviert haben, weil Sie aus einem anderen Grund auf den Grid Manager zugreifen mussten:
   a. Führen Sie alle Aufgaben oder Aufgaben aus, die Sie ausführen müssen.
   b. Wählen Sie **Abmelden**, und schließen Sie den Grid Manager.
   c. SSO auf dem Admin-Node erneut aktivieren. Sie können einen der folgenden Schritte ausführen:

      - Führen Sie den folgenden Befehl aus: `enable-saml`

        Eine Meldung gibt an, dass der Befehl nur für diesen Admin-Knoten gilt.

      Bestätigen Sie, dass Sie SSO aktivieren möchten.

   Eine Meldung gibt an, dass Single Sign-On auf dem Knoten aktiviert ist.

      ◦ Booten Sie den Grid-Node neu: `reboot`

8. Greifen Sie über einen Webbrowser über denselben Admin-Node auf den Grid-Manager zu.
9. Vergewissern Sie sich, dass die Seite StorageGRID-Anmeldung angezeigt wird und Sie Ihre SSO-Anmeldedaten für den Zugriff auf den Grid-Manager eingeben müssen.

Sicherheitseinstellungen verwalten

Verwalten von Zertifikaten

Informationen zu Sicherheitszertifikaten

Sicherheitszertifikate sind kleine Datendateien, die zur Erstellung sicherer, vertrauenswürdiger Verbindungen zwischen StorageGRID-Komponenten und zwischen StorageGRID-Komponenten und externen Systemen verwendet werden.

StorageGRID verwendet zwei Arten von Sicherheitszertifikaten:

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

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

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

Standard Grid CA-Zertifikat

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

- Benutzerdefinierte CA-Zertifikate entfernen die internen Zertifikate nicht. Die benutzerdefinierten Zertifikate sollten jedoch die für die Überprüfung der Serververbindungen angegebenen Zertifikate sein.
- Alle benutzerdefinierten Zertifikate müssen den erfüllen Richtlinien zur Systemhärtung Für Serverzertifikate.
- StorageGRID unterstützt das Bündeln von Zertifikaten aus einer Zertifizierungsstelle in einer einzelnen Datei (Bundle als CA-Zertifikat).

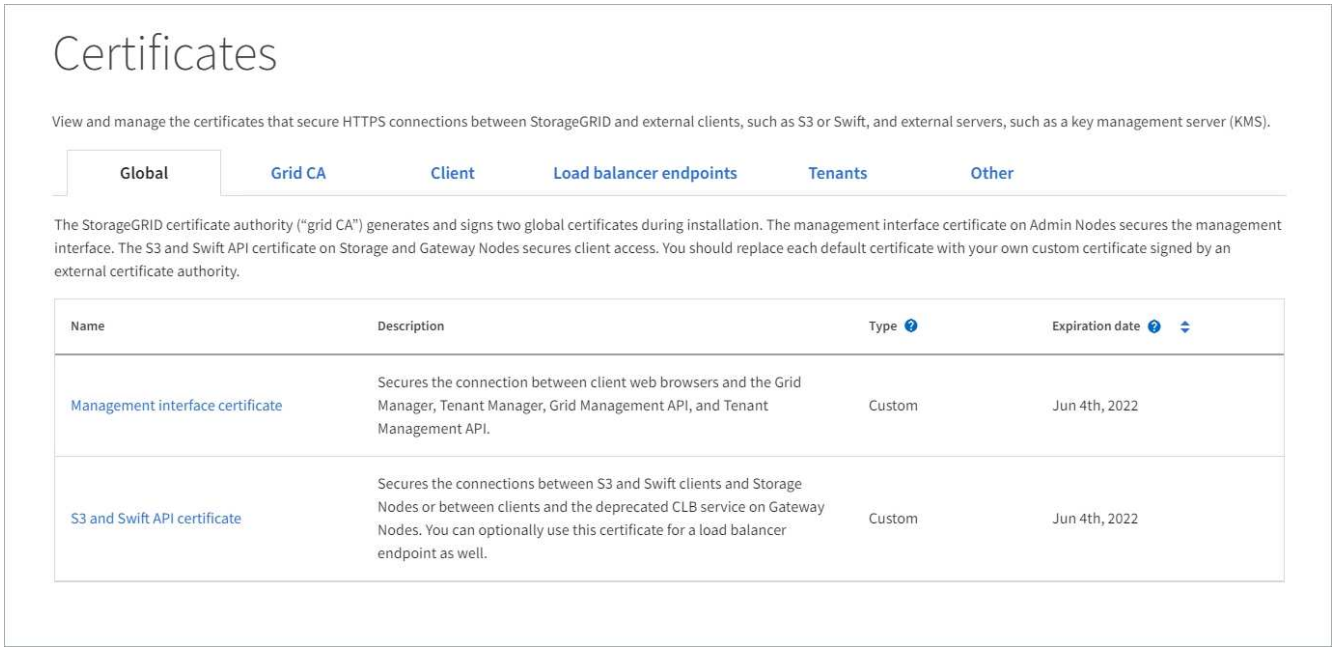
> ⓘ StorageGRID enthält auch CA-Zertifikate für das Betriebssystem, die in allen Grids identisch sind. Stellen Sie in Produktionsumgebungen sicher, dass Sie ein benutzerdefiniertes Zertifikat angeben, das von einer externen Zertifizierungsstelle anstelle des CA-Zertifikats des Betriebssystems signiert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

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

Greifen Sie auf Sicherheitszertifikate zu

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

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



2. Wählen Sie auf der Seite Zertifikate eine Registerkarte aus, um Informationen zu den einzelnen Zertifikatkategorien zu erhalten und auf die Zertifikatseinstellungen zuzugreifen. Sie können nur auf eine Registerkarte zugreifen, wenn Sie über die entsprechende Berechtigung verfügen.

   - **Global**: Sichert den StorageGRID-Zugriff von Webbrowsern und externen API-Clients.
   - **Raster CA**: Sichert internen StorageGRID-Datenverkehr.
   - **Kunde**: Sichert Verbindungen zwischen externen Clients und der StorageGRID Prometheus Datenbank.
   - **Load Balancer-Endpunkte**: Sichert Verbindungen zwischen S3- und Swift-Clients und dem StorageGRID Load Balancer.
   - **Mandanten**: Sichert Verbindungen zu Identitäts-Federation-Servern oder von Plattform-Service-Endpunkten zu S3-Storage-Ressourcen.
   - **Sonstiges**: Sichert StorageGRID-Verbindungen, die bestimmte Zertifikate erfordern.

   Jede Registerkarte wird unten mit Links zu weiteren Zertifikatdetails beschrieben.

Weltweit

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

- Zertifikat für die Managementoberfläche: Sichert Client-Web-Browser-Verbindungen zu StorageGRID-Management-Schnittstellen.
- S3- und Swift-API-Zertifikat: Sichert Client-API-Verbindungen zu Storage-Nodes, Admin-Nodes und Gateway-Nodes, über die S3- und Swift-Client-Applikationen Objektdaten hochladen und herunterladen.

Informationen zu den installierten globalen Zertifikaten umfassen:

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

Ihre Vorteile:

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

Grid CA

Der Grid-CA-Zertifikat, Von der StorageGRID-Zertifizierungsstelle während der StorageGRID-Installation erzeugt, sichert den gesamten internen StorageGRID-Verkehr.

Zertifikatsinformationen umfassen das Ablaufdatum des Zertifikats und den Zertifikatinhalt.

Das können Sie Kopieren Sie das Grid-CA-Zertifikat, oder laden Sie es herunter, Aber Sie können es nicht ändern.

Client

Client-Zertifikate, Generiert von einer externen Zertifizierungsstelle, sichern Sie die Verbindungen zwischen externen Monitoring-Tools und der StorageGRID Prometheus Datenbank.

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

verwendet werden kann.

Ihre Vorteile:

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

Load Balancer-Endpunkte

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

Die Endpunkttabelle für Load Balancer verfügt über eine Reihe für jeden konfigurierten Load Balancer-Endpunkt und gibt an, ob das globale S3- und Swift-API-Zertifikat oder ein benutzerdefiniertes Load Balancer-Endpoint-Zertifikat für den Endpunkt verwendet wird. Es wird auch das Ablaufdatum für jedes Zertifikat angezeigt.

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

Ihre Vorteile:

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

Mandanten

Die Mandanten nutzen können Identity Federation Server-Zertifikate Oder Endpoint-Zertifikate für Plattformservice Um ihre Verbindungen mit StorageGRID zu sichern.

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

Ihre Vorteile:

- Wählen Sie einen Mandantennamen aus, um sich beim Mandanten-Manager anzumelden
- Wählen Sie einen Mandantennamen aus, um Details zur Identitätsföderation des Mandanten anzuzeigen
- Wählen Sie einen Mandantennamen aus, um Details zu den Services der Mandantenplattform anzuzeigen

- Festlegen eines Endpunktzertifikats für den Plattformservice während der Endpunkterstellung

Andere

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

- Zertifikate für Identitätsföderation
- Cloud Storage Pool-Zertifikate
- KMS-Zertifikate (Key Management Server)
- Einzelanmelde-Zertifikate
- Benachrichtigungszertifikate per E-Mail senden
- Externe Syslog-Server-Zertifikate

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

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

Ihre Vorteile:

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

Details zum Sicherheitszertifikat

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

Zertifikat für die Managementoberfläche

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

S3- und Swift-API-Zertifikat

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

Grid-CA-Zertifikat

Siehe Beschreibung des Standard Grid CA-Zertifikats.

Administrator-Client-Zertifikat

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

Endpunkt-Zertifikat für Load Balancer

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

Zertifikat für Identitätsföderation

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

Endpoint-Zertifikat für Plattform-Services

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

Endpunkt-Zertifikat für Cloud Storage Pool

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

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)

SSO-Zertifikat (Single Sign On)

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

Zertifikat für eine E-Mail-Benachrichtigung

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

Externes Syslog-Serverzertifikat

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	Authentifiziert die TLS- oder RELP/TLS-Verbindung zwischen einem externen Syslog-Server, der Ereignisse in StorageGRID protokolliert. **Hinweis:** für TCP-, RELP/TCP- und UDP-Verbindungen zu einem externen Syslog-Server ist kein externes Syslog-Serverzertifikat erforderlich.	**KONFIGURATION Überwachung Audit- und Syslog-Server** und dann **externen Syslog-Server konfigurieren**	Konfigurieren Sie einen externen Syslog-Server

Beispiele für Zertifikate

Beispiel 1: Load Balancer Service

In diesem Beispiel fungiert StorageGRID als Server.

1. Sie konfigurieren einen Load Balancer-Endpunkt und laden ein Serverzertifikat in StorageGRID hoch oder erstellen.
2. Sie konfigurieren eine S3- oder Swift-Client-Verbindung zum Endpunkt des Load Balancer und laden dasselbe Zertifikat auf den Client hoch.
3. Wenn der Client Daten speichern oder abrufen möchte, stellt er über HTTPS eine Verbindung zum Load Balancer-Endpunkt her.
4. StorageGRID antwortet mit dem Serverzertifikat, das einen öffentlichen Schlüssel enthält, und mit einer Signatur auf Grundlage des privaten Schlüssels.
5. Der Client überprüft dieses Zertifikat, indem er die Serversignatur mit der Signatur seiner Kopie des Zertifikats vergleicht. Wenn die Signaturen übereinstimmen, startet der Client eine Sitzung mit demselben öffentlichen Schlüssel.
6. Der Client sendet Objektdaten an StorageGRID.

Beispiel 2: Externer KMS (Key Management Server)

In diesem Beispiel fungiert StorageGRID als Client.

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

Konfigurieren Sie Serverzertifikate

Unterstützte Serverzertifikatstypen

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

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

Konfigurieren Sie Zertifikate für die Managementoberfläche

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

Über diese Aufgabe

Standardmäßig wird jeder Admin-Node ein von der Grid-CA signiertes Zertifikat ausgestellt. Diese CA-signierten Zertifikate können durch ein einziges allgemeines Zertifikat für benutzerdefinierte Verwaltungsschnittstellen und einen entsprechenden privaten Schlüssel ersetzt werden.

Da für alle Admin-Nodes ein einzelnes Zertifikat für eine benutzerdefinierte Managementoberfläche verwendet wird, müssen Sie das Zertifikat als Platzhalter- oder Multi-Domain-Zertifikat angeben, wenn Clients den Hostnamen bei der Verbindung mit Grid Manager und Tenant Manager überprüfen müssen. Definieren Sie das benutzerdefinierte Zertifikat so, dass es mit allen Admin-Nodes im Raster übereinstimmt.

Sie müssen die Konfiguration auf dem Server abschließen. Je nach der von Ihnen verwendeten Root Certificate Authority (CA) müssen Benutzer möglicherweise auch das Grid CA-Zertifikat in den Webbrowser installieren, mit dem sie auf den Grid Manager und den Tenant Manager zugreifen können.

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

> Wenn Sie mit einem Domänennamen anstelle einer IP-Adresse auf den Grid Manager oder den Tenant Manager zugreifen, zeigt der Browser einen Zertifikatfehler 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 Zertifikatinhalt zum Einfügen an eine andere Stelle zu kopieren.

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

Zertifikat wird generiert

Erstellen Sie die Serverzertifikatdateien.

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

a. Wählen Sie **Zertifikat erstellen**.

b. Geben Sie die Zertifikatsinformationen an:

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

c. Wählen Sie **Erzeugen**.

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

- Wählen Sie **Zertifikat herunterladen**, um die 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.

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

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

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

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

Stellen Sie das Standardzertifikat für die Managementoberfläche wieder her

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

Schritte

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

   Wenn Sie das Standardzertifikat für die 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.

Was Sie benötigen

- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben die `Passwords.txt` Datei:

Über diese Aufgabe

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

Schritte

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

   > Die Gültigkeitsdauer eines Zertifikats beginnt, wenn `make-certificate` Wird ausgeführt. Sie müssen sicherstellen, dass der Management-Client mit der gleichen Datenquelle wie StorageGRID synchronisiert wird. Andernfalls kann der Client das Zertifikat ablehnen.

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

   Die resultierende Ausgabe enthält das öffentliche Zertifikat, das vom Management-API-Client benötigt wird.
4. Wählen Sie das Zertifikat aus, und kopieren Sie es.

   Geben Sie DIE START- und DAS ENDE-Tags in Ihre Auswahl ein.
5. Melden Sie sich von der Eingabeaufforderung-Shell ab. `$ exit`
6. Bestätigen Sie, dass das Zertifikat konfiguriert wurde:
   a. Greifen Sie auf den Grid Manager zu.

b. Wählen Sie **KONFIGURATION Sicherheit Zertifikate**

c. Wählen Sie auf der Registerkarte **Global** die Option **Management Interface Certificate** aus.

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

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

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

Schritte

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

Laden Sie die Zertifikatdatei oder das CA-Paket herunter

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

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

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

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

Beispiel: `storagegrid_certificate.pem`

Zertifikat oder CA-Bundle-PEM kopieren

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

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

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

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

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

Beispiel: `storagegrid_certificate.pem`

Konfigurieren von S3- und Swift-API-Zertifikaten

Sie können das Serverzertifikat, das für S3- oder Swift-Client-Verbindungen zu Storage-Nodes verwendet wird, ersetzen oder wiederherstellen, den veralteten Connection Load

Balancer (CLB)-Service auf Gateway-Nodes oder zum Laden von Balancer-Endpunkten. Das benutzerdefinierte Ersatzserverzertifikat ist speziell für Ihr Unternehmen bestimmt.

Über diese Aufgabe

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

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

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

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

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

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

Schritte

1. Wählen Sie **KONFIGURATION Sicherheit Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global S3 und Swift API Zertifikat**.
3. Wählen Sie **Benutzerdefiniertes Zertifikat verwenden**.
4. Hochladen oder Generieren des Zertifikats

Zertifikat hochladen

Laden Sie die erforderlichen Serverzertifikatdateien hoch.

a. Wählen Sie **Zertifikat hochladen**.

b. Laden Sie die erforderlichen Serverzertifikatdateien hoch:

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

> Private EC-Schlüssel müssen 224 Bit oder größer sein. RSA Private Keys müssen mindestens 2048 Bit groß sein.

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

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

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

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

  Beispiel: `storagegrid_certificate.pem`

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

d. Wählen Sie **Speichern**.

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

Zertifikat wird generiert

Erstellen Sie die Serverzertifikatdateien.

a. Wählen Sie **Zertifikat erstellen**.

b. Geben Sie die Zertifikatsinformationen an:

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

c. Wählen Sie **Erzeugen**.

d. Wählen Sie **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 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.

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 einen Tag lang alle damit verbundenen Warnmeldungen zum Ablauf des Zertifikats löschen.

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

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

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

Schritte

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

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

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

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

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

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

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

Schritte

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

Laden Sie die Zertifikatdatei oder das CA-Paket herunter

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

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

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

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

   Beispiel: `storagegrid_certificate.pem`

Zertifikat oder CA-Bundle-PEM kopieren

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

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

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

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

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

   Beispiel: `storagegrid_certificate.pem`

Verwandte Informationen

- S3 verwenden
- Verwenden Sie Swift
- Konfigurieren von S3-API-Endpunkt-Domain-Namen

Kopieren Sie das Grid-CA-Zertifikat

StorageGRID verwendet eine interne Zertifizierungsstelle (Certificate Authority, CA) zum

Schutz des internen Datenverkehrs. Dieses Zertifikat ändert sich nicht, wenn Sie Ihre eigenen Zertifikate hochladen.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Wenn ein benutzerdefiniertes Serverzertifikat konfiguriert wurde, sollten Client-Anwendungen den Server anhand des benutzerdefinierten Serverzertifikats überprüfen. Sie sollten das CA-Zertifikat nicht aus dem StorageGRID-System kopieren.

Schritte

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

Laden Sie die Zertifikatdatei herunter

Laden Sie das Zertifikat herunter `.pem` Datei:

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

   Beispiel: `storagegrid_certificate.pem`

Zertifikat PEM kopieren

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

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

   Beispiel: `storagegrid_certificate.pem`

Konfigurieren Sie StorageGRID-Zertifikate für FabricPool

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

Was Sie benötigen

- Sie haben spezifische Zugriffsberechtigungen.
- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.

Über diese Aufgabe

Wenn Sie einen Load Balancer-Endpunkt erstellen, können Sie ein selbstsigniertes Serverzertifikat generieren oder ein Zertifikat hochladen, das von einer bekannten Zertifizierungsstelle signiert ist. In Produktionsumgebungen sollten Sie ein Zertifikat verwenden, das von einer bekannten Zertifizierungsstelle signiert ist. Von einer Zertifizierungsstelle signierte Zertifikate können unterbrechungsfrei gedreht werden. Sie sind außerdem sicherer, weil sie einen besseren Schutz vor man-in-the-Middle-Angriffen bieten.

In den folgenden Schritten finden Sie allgemeine Richtlinien für S3-Clients, die FabricPool verwenden. Weitere Informationen und Verfahren finden Sie unter Konfigurieren Sie StorageGRID für FabricPool.

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

Schritte

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

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

3. Fügen Sie StorageGRID als Cloud-Tier in ONTAP bei.

   Geben Sie den Endpunkt-Port des Load Balancer und den vollständig qualifizierten Domänennamen an, der im hochgeladenen CA-Zertifikat verwendet wird. Geben Sie dann das CA-Zertifikat ein.

> Wenn eine Zwischenzertifizierungsstelle das StorageGRID-Zertifikat ausgestellt hat, müssen Sie das Zertifikat der Zwischenzertifizierungsstelle vorlegen. Wenn das StorageGRID-Zertifikat direkt von der Root-CA ausgestellt wurde, müssen Sie das Root-CA-Zertifikat bereitstellen.

Konfigurieren Sie Client-Zertifikate

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

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

Weitere Informationen finden Sie unter Allgemeine Verwendung des Sicherheitszertifikats Und Konfigurieren von benutzerdefinierten Serverzertifikaten.

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

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

Was Sie benötigen

- Sie haben Root-Zugriffsberechtigung.
- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- So konfigurieren Sie ein Clientzertifikat:
  - Sie haben die IP-Adresse oder den Domänennamen des Admin-Knotens.
  - Wenn Sie das Zertifikat für die StorageGRID-Managementoberfläche konfiguriert haben, verfügen Sie über die CA, das Client-Zertifikat und den privaten Schlüssel, mit dem Sie das Zertifikat für die Managementoberfläche konfigurieren können.
  - Um Ihr eigenes Zertifikat hochzuladen, steht der private Schlüssel für das Zertifikat auf Ihrem lokalen Computer zur Verfügung.
  - Der private Schlüssel muss zum Zeitpunkt der Erstellung gespeichert oder aufgezeichnet worden sein. Wenn Sie nicht über den ursprünglichen privaten Schlüssel verfügen, müssen Sie einen neuen Schlüssel erstellen.
- So bearbeiten Sie ein Clientzertifikat:
  - Sie haben die IP-Adresse oder den Domänennamen des Admin-Knotens.
  - Um Ihr eigenes Zertifikat oder ein neues Zertifikat hochzuladen, sind der private Schlüssel, das Clientzertifikat und die CA (sofern verwendet) auf Ihrem lokalen Computer verfügbar.

Fügen Sie Client-Zertifikate hinzu

Befolgen Sie die Vorgehensweise für Ihr Szenario, um ein Clientzertifikat hinzuzufügen:

- Das Zertifikat der Managementoberfläche ist bereits konfiguriert
- KANN Client-Zertifikat AUSGESTELLT haben
- Zertifikat vom Grid Manager generiert

Das Zertifikat der Managementoberfläche ist bereits konfiguriert

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

Schritte

1. Wählen Sie im Grid Manager die Option **KONFIGURATION Sicherheit Zertifikate** und wählen Sie dann die Registerkarte **Client** aus.
2. Wählen Sie **Hinzufügen**.
3. Geben Sie einen Zertifikatnamen ein, der mindestens 1 und nicht mehr als 32 Zeichen enthält.
4. Um mit Ihrem externen Monitoring-Tool auf die Prometheus-Kennzahlen zuzugreifen, wählen Sie **Prometheus erlauben**.
5. Laden Sie im Abschnitt **Zertifikatstyp** das Zertifikat der Verwaltungsschnittstelle hoch `.pem` Datei:
   a. Wählen Sie **Zertifikat hochladen** und dann **Weiter**.

b. Laden Sie die Zertifikatdatei der Managementoberfläche hoch (`.pem`).

   - Wählen Sie **Client Certificate Details** aus, um die Zertifikatmetadaten und das Zertifikat PEM anzuzeigen.
   - Wählen Sie **Zertifikat kopieren PEM** aus, um den Zertifikatinhalt zum Einfügen an eine andere Stelle zu kopieren.

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

   Das neue Zertifikat wird auf der Registerkarte Client angezeigt.

6. Konfigurieren Sie die folgenden Einstellungen für Ihr externes Monitoring-Tool, z. B. Grafana.

   a. **Name**: Geben Sie einen Namen für die Verbindung ein.

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

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

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

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

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

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

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

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

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

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

Weitere Informationen zu den Metriken finden Sie im Anweisungen zur Überwachung von StorageGRID.

KANN Client-Zertifikat AUSGESTELLT haben

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

Schritte

1. Führen Sie die Schritte zu aus Konfigurieren Sie ein Zertifikat für die Managementoberfläche.
2. Wählen Sie im Grid Manager die Option **KONFIGURATION Sicherheit Zertifikate** und wählen Sie dann die Registerkarte **Client** aus.

3. Wählen Sie **Hinzufügen**.
4. Geben Sie einen Zertifikatnamen ein, der mindestens 1 und nicht mehr als 32 Zeichen enthält.
5. Um mit Ihrem externen Monitoring-Tool auf die Prometheus-Kennzahlen zuzugreifen, wählen Sie **Prometheus erlauben**.
6. Laden Sie im Abschnitt **Zertifikatstyp** das Clientzertifikat, den privaten Schlüssel und das CA-Paket hoch `.pem` Dateien:
   a. Wählen Sie **Zertifikat hochladen** und dann **Weiter**.
   b. Laden Sie Client-Zertifikat, privaten Schlüssel und CA-Bundle-Dateien hoch (`.pem`).
      - Wählen Sie **Client Certificate Details** aus, um die Zertifikatmetadaten und das Zertifikat PEM anzuzeigen.
      - Wählen Sie **Zertifikat kopieren PEM** aus, um den Zertifikatinhalt zum Einfügen an eine andere Stelle zu kopieren.
   c. Wählen Sie **Erstellen**, um das Zertifikat im Grid Manager zu speichern.

      Die neuen Zertifikate werden auf der Registerkarte Client angezeigt.
7. Konfigurieren Sie die folgenden Einstellungen für Ihr externes Monitoring-Tool, z. B. Grafana.
   a. **Name**: Geben Sie einen Namen für die Verbindung ein.

      StorageGRID benötigt diese Informationen nicht, Sie müssen jedoch einen Namen angeben, um die Verbindung zu testen.
   b. **URL**: Geben Sie den Domain-Namen oder die IP-Adresse für den Admin-Node ein. Geben Sie HTTPS und Port 9091 an.

      Beispiel: `https://admin-node.example.com:9091`
   c. Aktivieren Sie **TLS Client Auth** und **mit CA Cert**.
   d. Kopieren Sie unter TLS/SSL Auth Details und fügen Sie: + ein
      - Das Management-Interface-CA-Zertifikat nach **CA-Zertifikat**
      - Das Client-Zertifikat an **Client-Zertifikat**
      - Der private Schlüssel zu **Client Key**
   e. **ServerName**: Geben Sie den Domainnamen des Admin-Knotens ein.

      Servername muss mit dem Domänennamen übereinstimmen, wie er im Zertifikat der Verwaltungsschnittstelle angezeigt wird.
   f. Speichern und testen Sie das Zertifikat und den privaten Schlüssel, das Sie aus StorageGRID oder einer lokalen Datei kopiert haben.

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

Weitere Informationen zu den Metriken finden Sie im Anweisungen zur Überwachung von StorageGRID.

Zertifikat vom Grid Manager generiert

Verwenden Sie dieses Verfahren, um ein Administrator-Client-Zertifikat hinzuzufügen, wenn ein Zertifikat der Verwaltungsschnittstelle nicht konfiguriert wurde und Sie planen, ein Clientzertifikat für Prometheus hinzuzufügen, das die Funktion Zertifikat generieren in Grid Manager verwendet.

Schritte

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

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

   - Wählen Sie **Zertifikat kopieren PEM** aus, um den 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.
9. Wählen Sie **Erstellen**, um das Zertifikat im Grid Manager zu speichern.

   Das neue Zertifikat wird auf der Registerkarte Client angezeigt.
10. Wählen Sie im Grid Manager die Option **KONFIGURATION Sicherheit Zertifikate** und wählen Sie dann die Registerkarte **Global** aus.

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

       Das neue Zertifikat wird auf der Registerkarte Client angezeigt.
14. Konfigurieren Sie die folgenden Einstellungen für Ihr externes Monitoring-Tool, z. B. Grafana.
    a. **Name**: Geben Sie einen Namen für die Verbindung ein.

       StorageGRID benötigt diese Informationen nicht, Sie müssen jedoch einen Namen angeben, um die Verbindung zu testen.
    b. **URL**: Geben Sie den Domain-Namen oder die IP-Adresse für den Admin-Node ein. Geben Sie HTTPS und Port 9091 an.

       Beispiel: `https://admin-node.example.com:9091`
    c. Aktivieren Sie **TLS Client Auth** und **mit CA Cert**.
    d. Kopieren Sie unter TLS/SSL Auth Details und fügen Sie: + ein
       - Das Management-Interface-Client-Zertifikat für beide ***CA Cert** und **Client-Zertifikat**
       - Der private Schlüssel zu **Client Key**
    e. **ServerName**: Geben Sie den Domainnamen des Admin-Knotens ein.

       Servername muss mit dem Domänennamen übereinstimmen, wie er im Zertifikat der Verwaltungsschnittstelle angezeigt wird.
    f. Speichern und testen Sie das Zertifikat und den privaten Schlüssel, das Sie aus StorageGRID oder einer lokalen Datei kopiert haben.

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

Weitere Informationen zu den Metriken finden Sie im Anweisungen zur Überwachung von StorageGRID.

Client-Zertifikate bearbeiten

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

Schritte

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

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

und eine Warnmeldung wird ausgelöst.

2. Wählen Sie das Zertifikat aus, das Sie bearbeiten möchten.
3. Wählen Sie **Bearbeiten** und dann **Name und Berechtigung bearbeiten** aus
4. Geben Sie einen Zertifikatnamen ein, der mindestens 1 und nicht mehr als 32 Zeichen enthält.
5. Um mit Ihrem externen Monitoring-Tool auf die Prometheus-Kennzahlen zuzugreifen, wählen Sie **Prometheus erlauben**.
6. Wählen Sie **Weiter**, um das Zertifikat im Grid Manager zu speichern.

   Das aktualisierte Zertifikat wird auf der Registerkarte Client angezeigt.

Verbinden Sie das neue Clientzertifikat

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

Schritte

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

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

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

Zertifikat hochladen

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

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

b. Laden Sie den Namen des Clientzertifikats hoch (`.pem`).

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

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

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

   Beispiel: `storagegrid_certificate.pem`

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

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

   Das aktualisierte Zertifikat wird auf der Registerkarte Client angezeigt.

Zertifikat wird generiert

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

a. Wählen Sie **Zertifikat erstellen**.

b. Geben Sie die Zertifikatsinformationen an:

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

c. Wählen Sie **Erzeugen**.

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

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

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

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

   Beispiel: `storagegrid_certificate.pem`

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

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

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

Das neue Zertifikat wird auf der Registerkarte Client angezeigt.

Herunterladen oder Kopieren von Clientzertifikaten

Sie können ein Clientzertifikat zur Verwendung an anderer Stelle herunterladen oder kopieren.

Schritte

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

Laden Sie die Zertifikatdatei herunter

Laden Sie das Zertifikat herunter `.pem` Datei:

a. Wählen Sie **Zertifikat herunterladen**.

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

   Beispiel: `storagegrid_certificate.pem`

Zertifikat kopieren

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

a. Wählen Sie **Zertifikat kopieren PEM**.

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

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

   Beispiel: `storagegrid_certificate.pem`

Entfernen Sie Client-Zertifikate

Wenn Sie kein Administrator-Clientzertifikat mehr benötigen, können Sie es entfernen.

Schritte

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

2. Wählen Sie das Zertifikat aus, das Sie entfernen möchten.
3. Wählen Sie **Löschen** und bestätigen Sie dann.

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

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

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 sind, können Sie erst auf sämtliche 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.

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 Verschlüsselungsmethoden.

Verschlüsselungsoption	So funktioniert es	Gilt für
Verschlüsselungsmanagement-Server (KMS) in Grid Manager	Sie konfigurieren einen Schlüsselverwaltungsserver für den StorageGRID-Standort (**CONFIGURATION Security Key Management Server**) und aktivieren die Knotenverschlüsselung 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.	Appliance-Knoten, deren **Node Encryption** während der Installation aktiviert ist. Alle Daten auf der Appliance sind gegen physischen Verlust oder aus dem Datacenter geschützt. Das Management von Verschlüsselungen mit einem KMS wird nur für Storage Nodes und Service-Appliances unterstützt.
Laufwerkssicherheit in SANtricity System Manager	Wenn die Laufwerkssicherheitsfunktion für eine Speicher-Appliance aktiviert ist, können Sie den Sicherheitsschlüssel mit SANtricity System Manager erstellen und verwalten. Der Schlüssel ist erforderlich, um auf die Daten auf den gesicherten Laufwerken zuzugreifen.	Storage-Applikationen mit Full Disk Encryption-Laufwerken (FDE) oder FIPS-Laufwerken (Federal Information Processing Standard) Alle Daten auf den gesicherten Laufwerken sind vor physischem Verlust oder Entfernung aus dem Datacenter geschützt. Nicht bei einigen Storage-Appliances oder Service-Appliances verwendet werden können. • SG6000 Storage-Appliances • SG5700 Storage-Appliances • SG5600 Storage Appliances
Grid-Option „gespeicherte Objektverschlüsselung“	Die Option **Stored Object Encryption** kann im Grid Manager (**CONFIGURATION System Grid options**) aktiviert werden. Bei Aktivierung werden alle neuen Objekte, die nicht auf Bucket-Ebene oder auf Objektebene verschlüsselt sind, während der Aufnahme verschlüsselt.	Neu aufgenommene S3- und Swift-Objektdaten Vorhandene gespeicherte Objekte werden nicht verschlüsselt. Objekt-Metadaten und andere sensible Daten sind nicht verschlüsselt. • Gespeicherte Objektverschlüsselung konfigurieren

Verschlüsselungsoption	So funktioniert es	Gilt für
S3-Bucket-Verschlüsselung	Sie stellen eine PUT-Bucket-Verschlüsselungsanforderung bereit, um die Verschlüsselung für den Bucket zu aktivieren. Neue Objekte, die nicht auf Objektebene verschlüsselt sind, werden bei der Aufnahme verschlüsselt.	Nur neu aufgenommene S3-Objektdaten Für den Bucket muss eine Verschlüsselung angegeben werden. Vorhandene Bucket-Objekte sind nicht verschlüsselt. Objekt-Metadaten und andere sensible Daten sind nicht verschlüsselt. • S3 verwenden
S3-Objektserverseitige Verschlüsselung (SSE)	Sie geben eine S3-Anforderung zum Speichern eines Objekts aus und schließen das ein `x-amz-server-side-encryption` Kopfzeile der Anfrage.	Nur neu aufgenommene S3-Objektdaten Für das Objekt muss eine Verschlüsselung angegeben werden. Objekt-Metadaten und andere sensible Daten sind nicht verschlüsselt. StorageGRID verwaltet die Schlüssel. • S3 verwenden
S3 Objektserverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln (SSE-C)	Sie geben eine S3-Anforderung zum Speichern eines Objekts aus und enthalten drei Anfrageheader. • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	Nur neu aufgenommene S3-Objektdaten Für das Objekt muss eine Verschlüsselung angegeben werden. Objekt-Metadaten und andere sensible Daten sind nicht verschlüsselt. Schlüssel werden außerhalb von StorageGRID gemanagt. • S3 verwenden

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.	Alle Objektdaten, Metadaten und Systemkonfigurationsdaten, wobei jedes Volume oder jeder Datastore verschlüsselt ist Eine externe Verschlüsselungsmethode bietet eine engere Kontrolle über Verschlüsselungsalgorithmen und -Schlüssel. Kann mit den anderen aufgeführten Methoden kombiniert werden.
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.	Nur Objektdaten und Metadaten (Systemkonfigurationsdaten sind nicht verschlüsselt). Eine externe Verschlüsselungsmethode bietet eine engere Kontrolle über Verschlüsselungsalgorithmen und -Schlüssel. Kann mit den anderen aufgeführten Methoden kombiniert werden. • "Amazon Simple Storage Service – Developer Guide: Schutz von Daten mit Client-seitiger Verschlüsselung"

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 Laufwerksicherheitsfunktion in SANtricity System Manager die Daten „`double verschlüsselte`“ auf den Self-Encrypting Drives in denselben Appliances verschlüsselt werden.
- Mit einem KMS lassen sich Daten auf Appliance-Nodes sichern. Zudem kann die Grid-Option „Speichered Object Encryption“ verwendet werden, um alle Objekte bei der Aufnahme zu verschlüsseln.

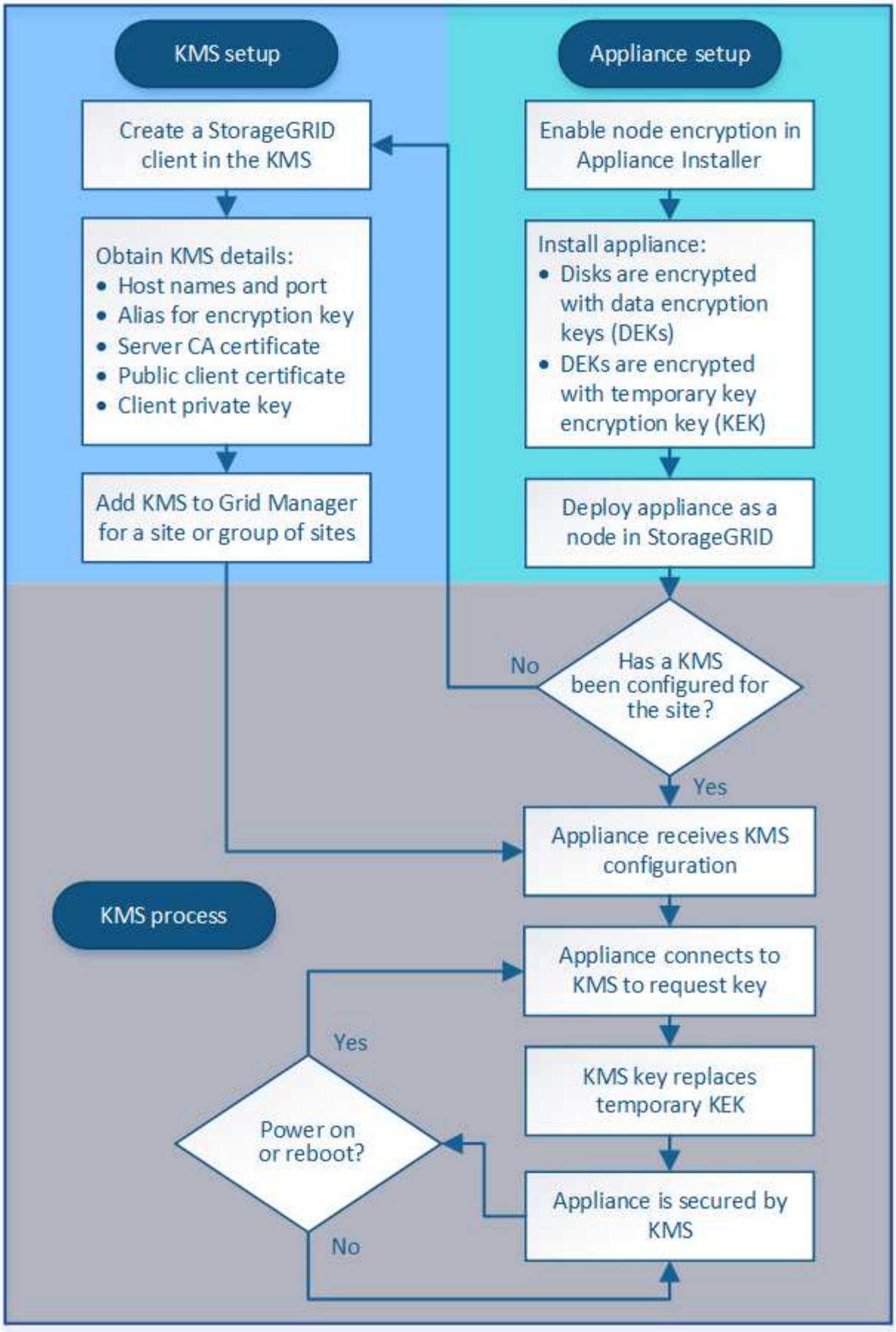
Wenn nur ein kleiner Teil Ihrer Objekte eine Verschlüsselung erfordern, sollten Sie stattdessen die Verschlüsselung auf Bucket- oder Objektebene kontrollieren. Durch die Aktivierung diverser Verschlüsselungsstufen entstehen zusätzliche Performance-Kosten.

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 ein Gerät zum Grid hinzugefügt wurde, und Sie können keine externe Schlüsselverwaltung für Geräte verwenden, bei denen die Node-Verschlüsselung nicht 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 GerätebOS 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.

Weitere Informationen finden Sie unter:

- SG100- und SG1000-Services-Appliances
- SG6000 Storage-Appliances
- SG5700 Storage-Appliances

- SG5600 Storage Appliances

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 wird, kann keinen Stromausfall oder Neustart überstehen.

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 können Sie die Node-Verschlüsselung nicht aktivieren. Appliances, bei denen die Node-Verschlüsselung nicht aktiviert ist, können externes Verschlüsselungsmanagement nicht verwenden.

Der konfigurierte KMS kann für die folgenden StorageGRID Appliances und Appliance-Nodes verwendet werden:

Appliance	Node-Typ
SG1000 Services-Appliance	Admin-Node oder Gateway-Node
SG100 Services-Appliance	Admin-Node oder Gateway-Node
SG6000 Storage Appliance	Storage-Node
SG5700 Storage-Appliance	Storage-Node
SG5600 Storage-Appliance	Storage-Node

Der konfigurierte KMS kann nicht für softwarebasierte (nicht-Appliance-) Nodes verwendet werden, einschließlich folgender Elemente:

- 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?

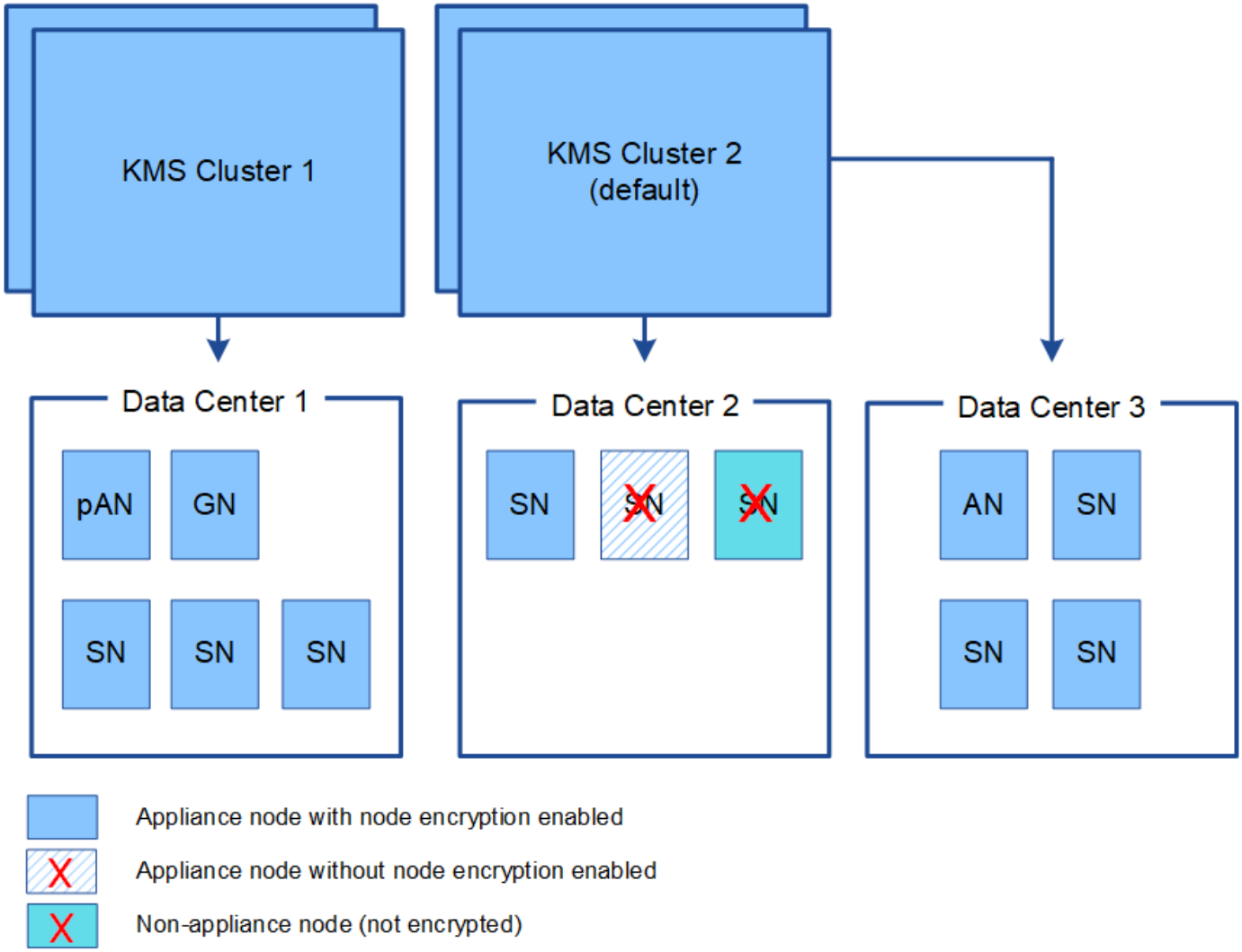
Sie können einen oder mehrere externe Verschlüsselungsmanagementserver konfigurieren, um die Appliance-Nodes in Ihrem StorageGRID-System Verschlüsselungen bereitzustellen. Jeder KMS stellt den StorageGRID Appliance-Nodes an einem einzelnen Standort oder einer Gruppe von Standorten einen einzelnen Verschlüsselungsschlüssel 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 keinen KMS für nicht-Appliance-Knoten oder für Appliance-Knoten verwenden können, bei denen die **Node Encryption**-Einstellung 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 auf einen ganz anderen Schlüssel.

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 nicht zur Verschlüsselung von Appliance-Volumes aus irgendeinem Grund verwendet werden kann, wird für den Appliance-Node die Warnung **KMS-Verschlüsselungsschlüsseldrehung fehlgeschlagen** 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 die KMS-Konfiguration mit dem Installationsprogramm der StorageGRID-Appliance löschen. 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.

Verwandte Informationen

- SG100- und SG1000-Services-Appliances
- SG6000 Storage-Appliances
- SG5700 Storage-Appliances
- SG5600 Storage Appliances

Überlegungen für das Ändern des KMS für einen Standort

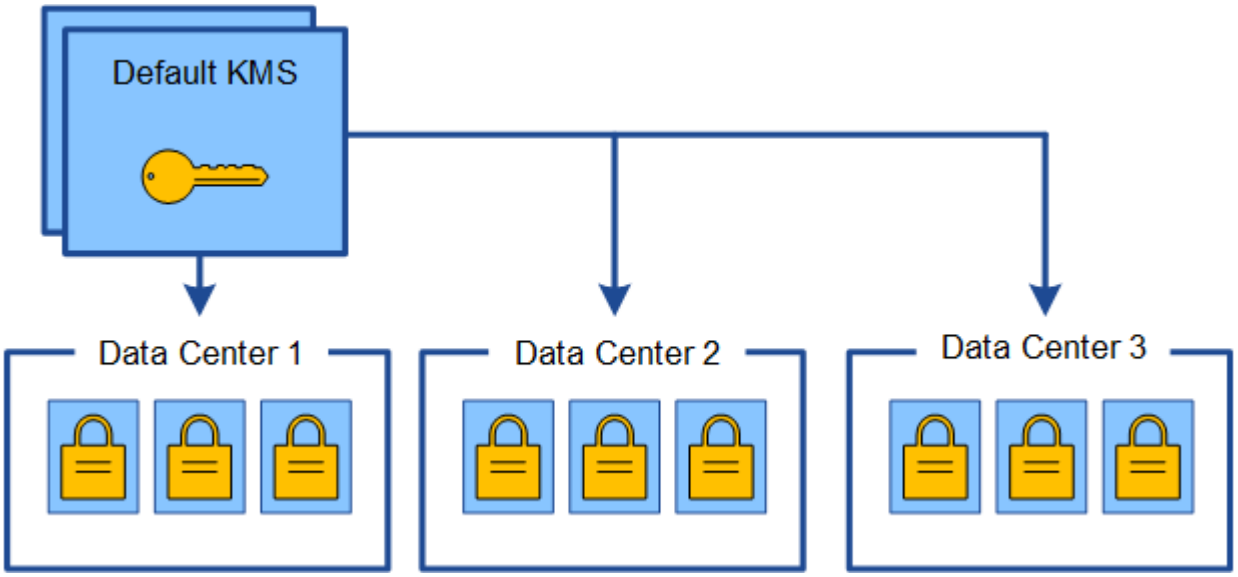
Jeder Verschlüsselungsmanagement-Server (KMS) oder KMS-Cluster gewährt allen Appliance-Nodes an einem einzelnen Standort oder einer Gruppe von Standorten einen Verschlüsselungsschlüssel. Wenn Sie ändern müssen, welcher KMS für einen Standort verwendet wird, müssen Sie den Verschlüsselungsschlüssel möglicherweise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

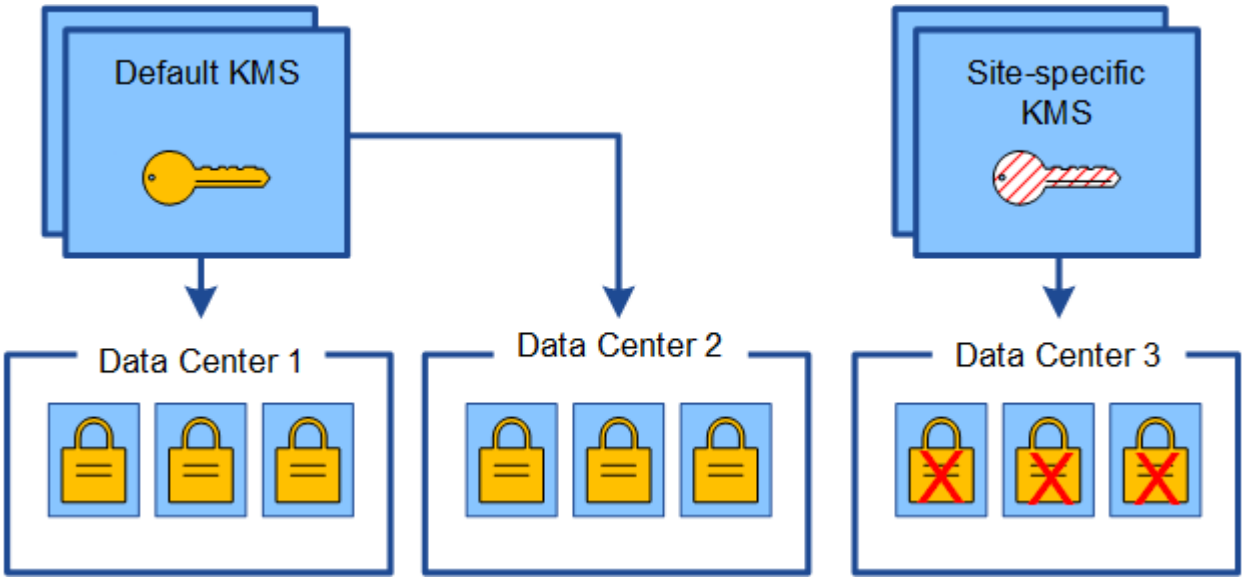
entschlüsseln.

Beispiel:

1. Sie konfigurieren zunächst einen Standard-KMS, der für alle Standorte gilt, die keinen dedizierten KMS besitzen.
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.

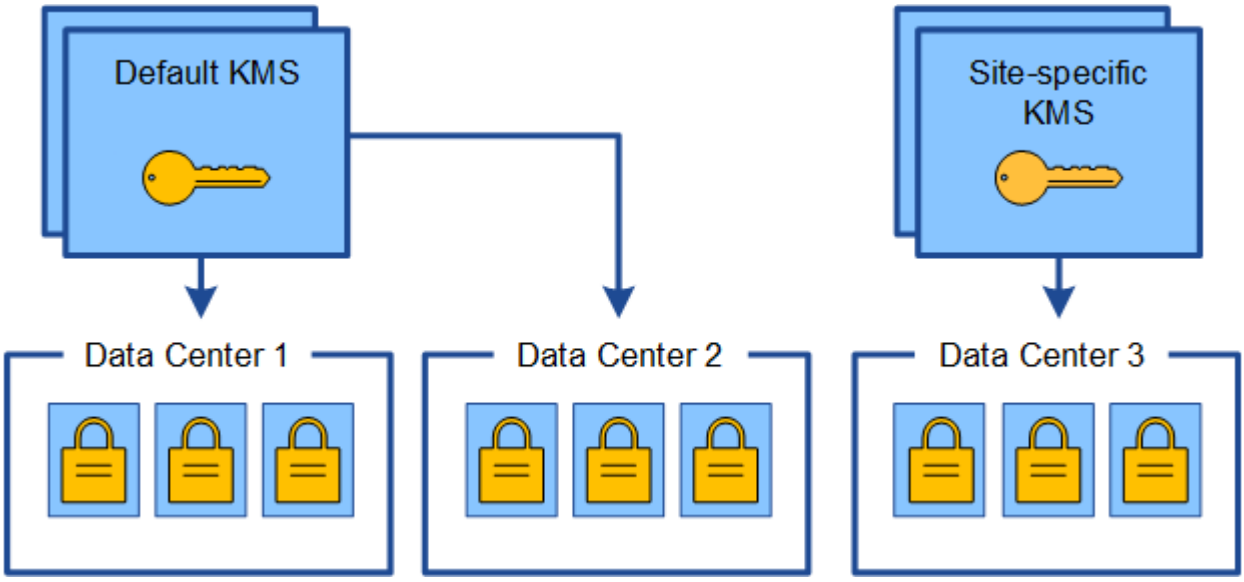


3. Sie entscheiden, einen standortspezifischen KMS für einen Standort hinzuzufügen (Datacenter 3 in der Abbildung). Da die Appliance-Nodes jedoch bereits verschlüsselt sind, tritt ein Validierungsfehler auf, wenn Sie versuchen, die Konfiguration für den standortspezifischen KMS zu speichern. Der Fehler 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.	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. Er gilt für alle Websites, die keinen dedizierten KMS haben. Bearbeiten eines Verschlüsselungsmanagement-Servers (KMS)
Sie haben einen Standard-KMS, und Sie fügen eine neue Site in einer Erweiterung hinzu. Sie möchten den Standard-KMS für die neue Site nicht verwenden.	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. Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)

Anwendungsfall zum Ändern des KMS einer Site	Erforderliche Schritte
Sie möchten, dass der KMS für eine Site einen anderen Server verwendet.	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. Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)

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 k170v, Versionen 2.0, 2.1 und 2.2. Wenn Sie Fragen zur Verwendung eines anderen Verschlüsselungsmanagementservers mit StorageGRID haben, wenden Sie sich an den technischen Support.

"Thales CipherTrust Manager"

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.

   Die Verschlüsselung muss 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 Domänennamen (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.

Was Sie benötigen

- 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.

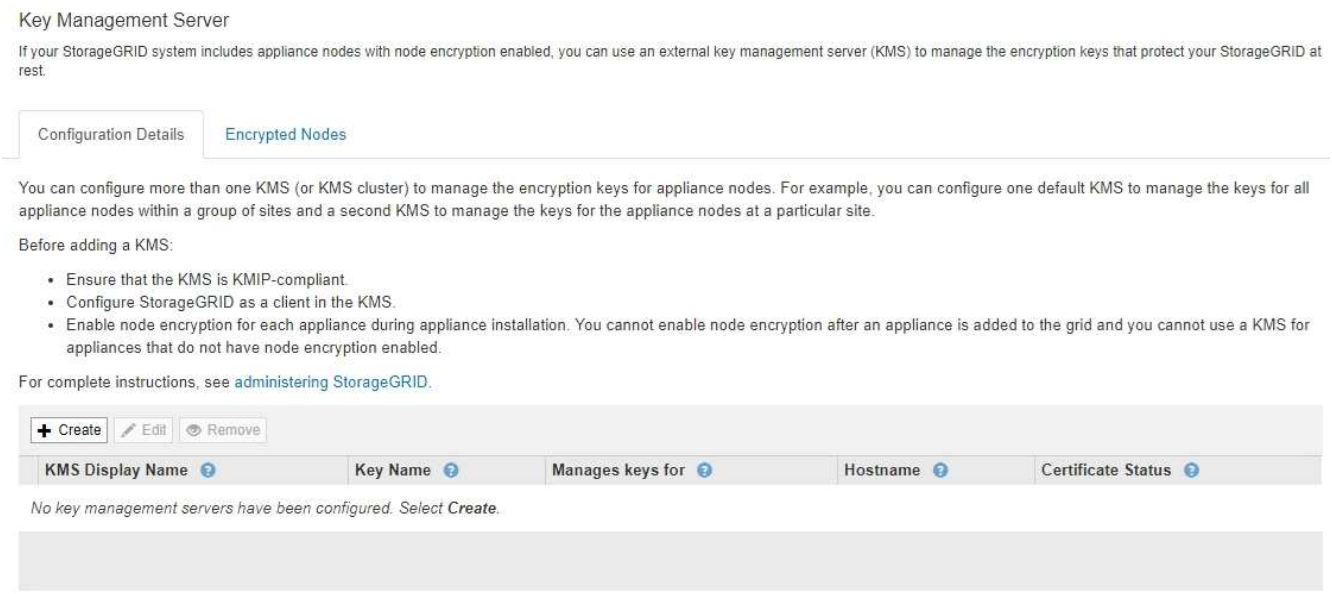
Schritt 1: Geben Sie KMS-Details ein

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

Schritte

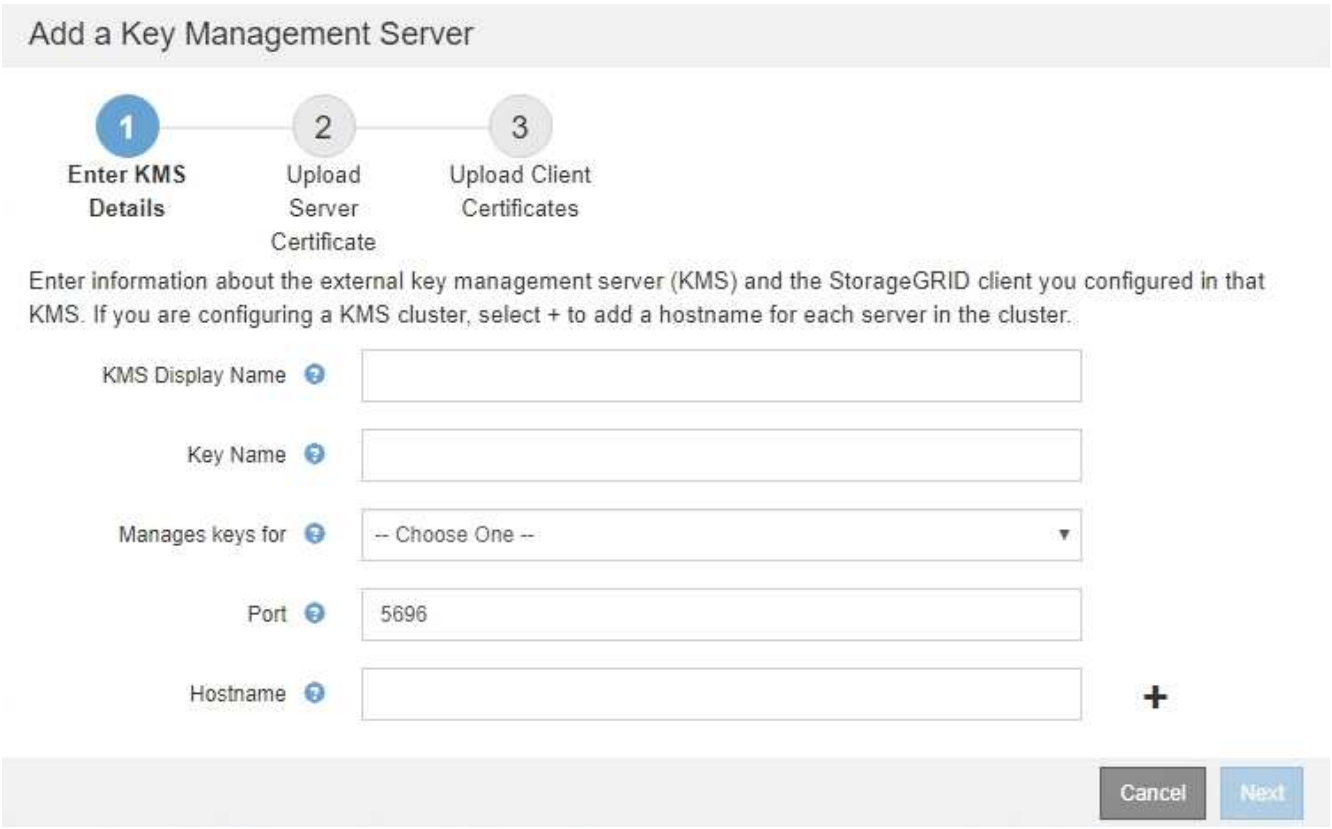
1. Wählen Sie **KONFIGURATION Sicherheit Schlüsselverwaltungsserver**.

Die Seite Key Management Server wird angezeigt, wobei die Registerkarte Konfigurationsdetails ausgewählt ist.



2. Wählen Sie **Erstellen**.

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



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

Feld	Beschreibung
KMS-Anzeigename	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.
Verwaltet Schlüssel für	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. • Wählen Sie einen Standort aus, wenn dieser KMS Verschlüsselungen für die Appliance-Nodes an einem bestimmten Standort managt. • Wählen Sie **Sites, die nicht von einem anderen KMS (Standard KMS)** verwaltet werden, um einen Standard-KMS zu konfigurieren, der für alle Sites gilt, die keinen dedizierten KMS haben, und für alle Sites, die Sie in nachfolgenden Erweiterungen hinzufügen. **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.
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	Der vollständig qualifizierte Domänenname oder die IP-Adresse für den KMS. **Hinweis:** das SAN-Feld 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.

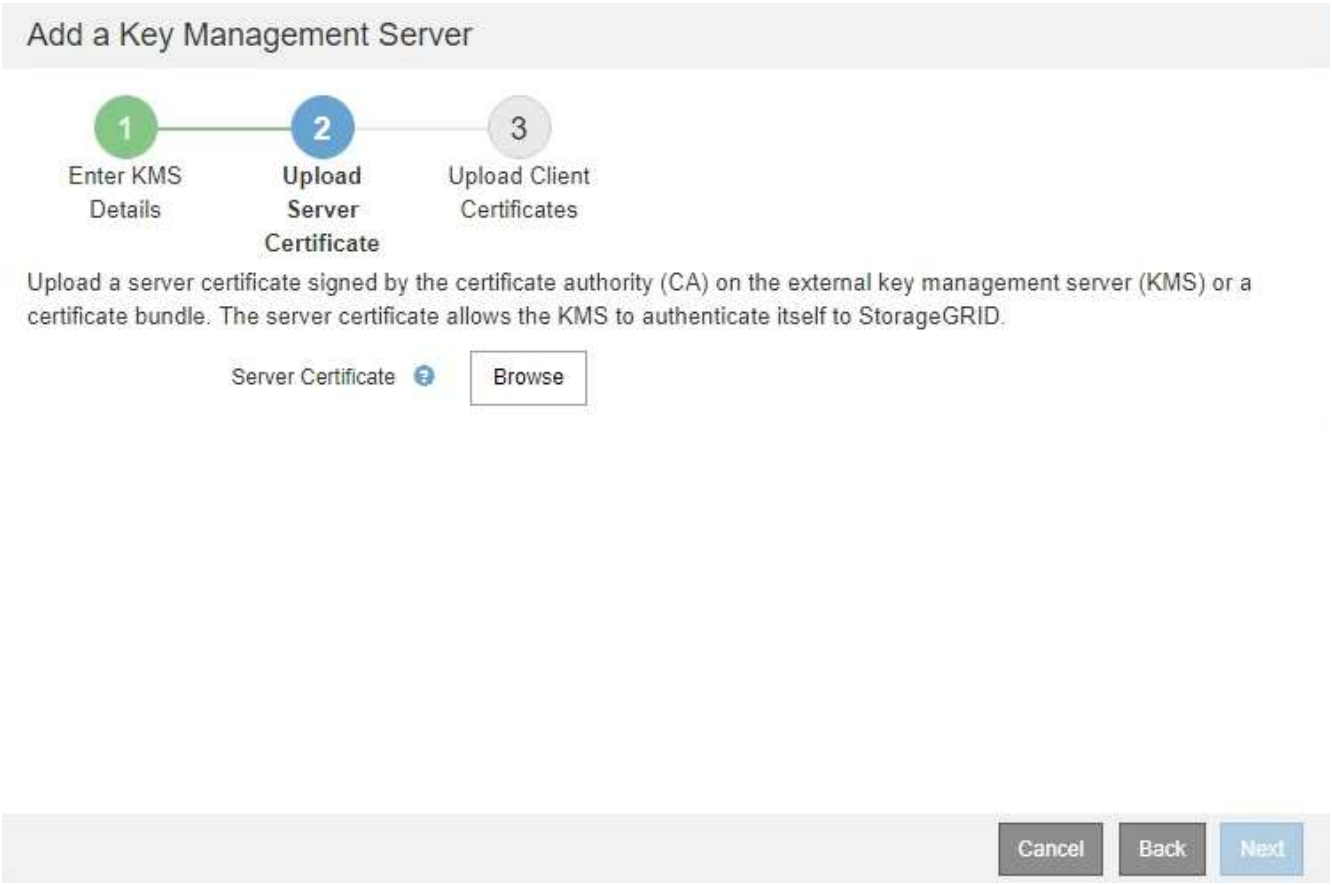
4. Wenn Sie einen KMS-Cluster verwenden, wählen Sie das Pluszeichen aus ➕ Um einen Hostnamen für jeden Server im Cluster hinzuzufügen.
5. Wählen Sie **Weiter**.

Schritt: Serverzertifikat Hochladen

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

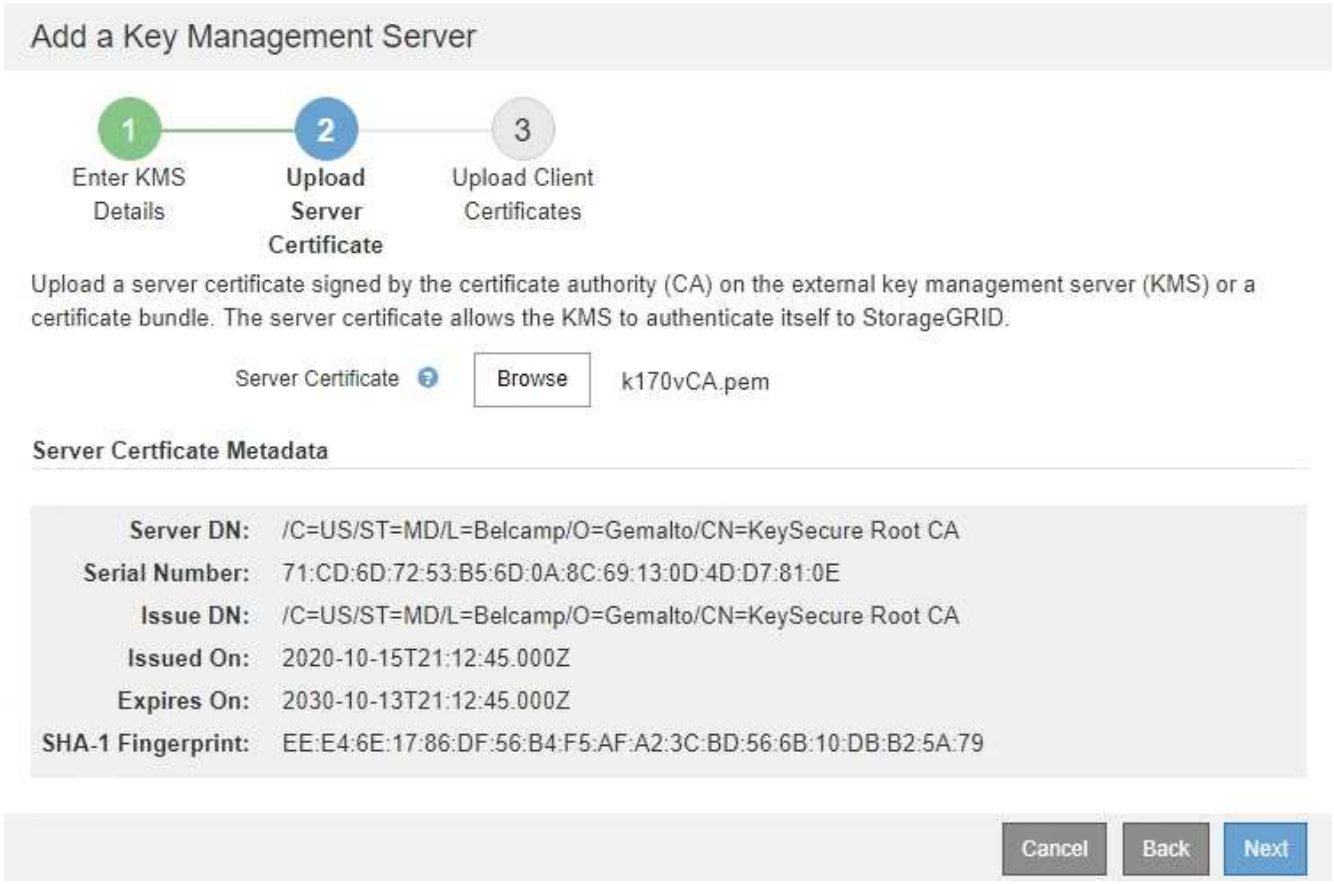
Schritte

1. Navigieren Sie ab **Schritt 2 (Serverzertifikat hochladen)** zum Speicherort des gespeicherten Serverzertifikats oder Zertifikatpakets.



2. Laden Sie die Zertifikatdatei hoch.

   Die Metadaten des Serverzertifikats werden angezeigt.



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

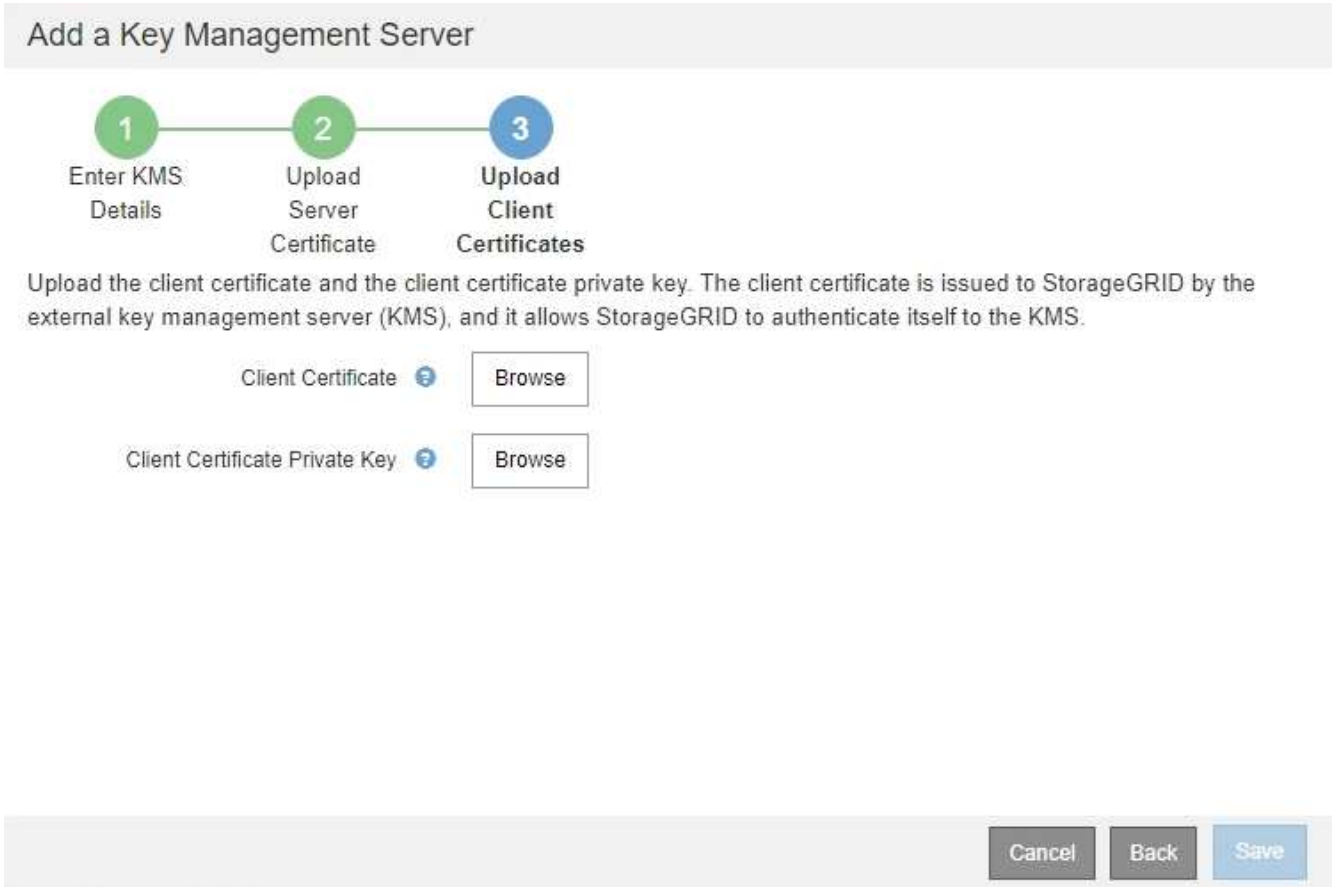
3. Wählen Sie **Weiter**.

Schritt 3: Laden Sie Client-Zertifikate Hoch

In Schritt 3 (Upload Client Certificates) des Assistenten Add a Key Management Server laden Sie das Clientzertifikat und den privaten Schlüssel des Clientzertifikats hoch. Das Client-Zertifikat ermöglicht StorageGRID, sich am KMS zu authentifizieren.

Schritte

1. Ab **Schritt 3 (Upload Client Certificates)** navigieren Sie zum Speicherort des Clientzertifikats.

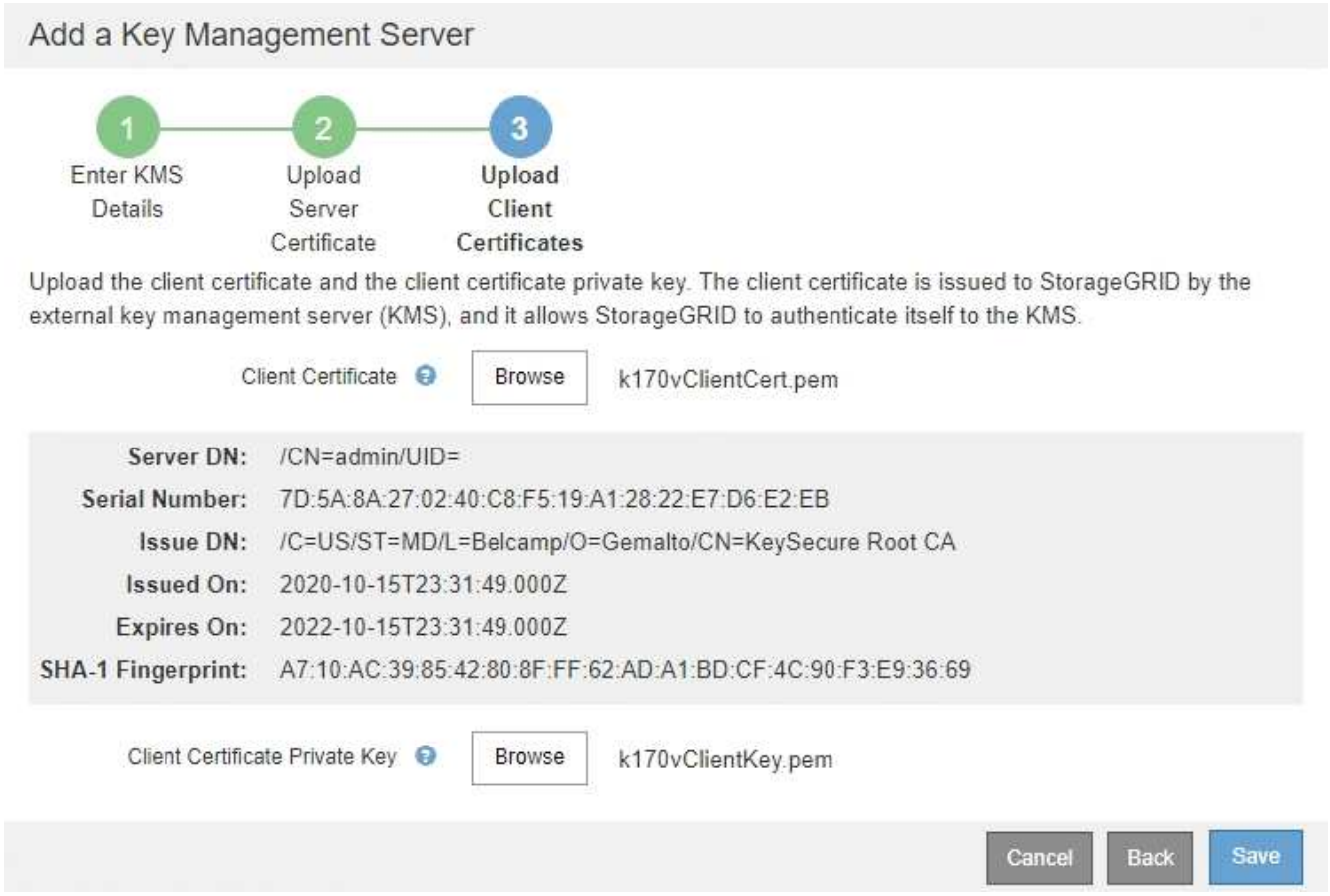


2. Laden Sie die Clientzertifikatdatei hoch.

   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.

   Die Metadaten für das Clientzertifikat und der private Schlüssel für das Clientzertifikat werden angezeigt.



5. Wählen Sie **Speichern**.

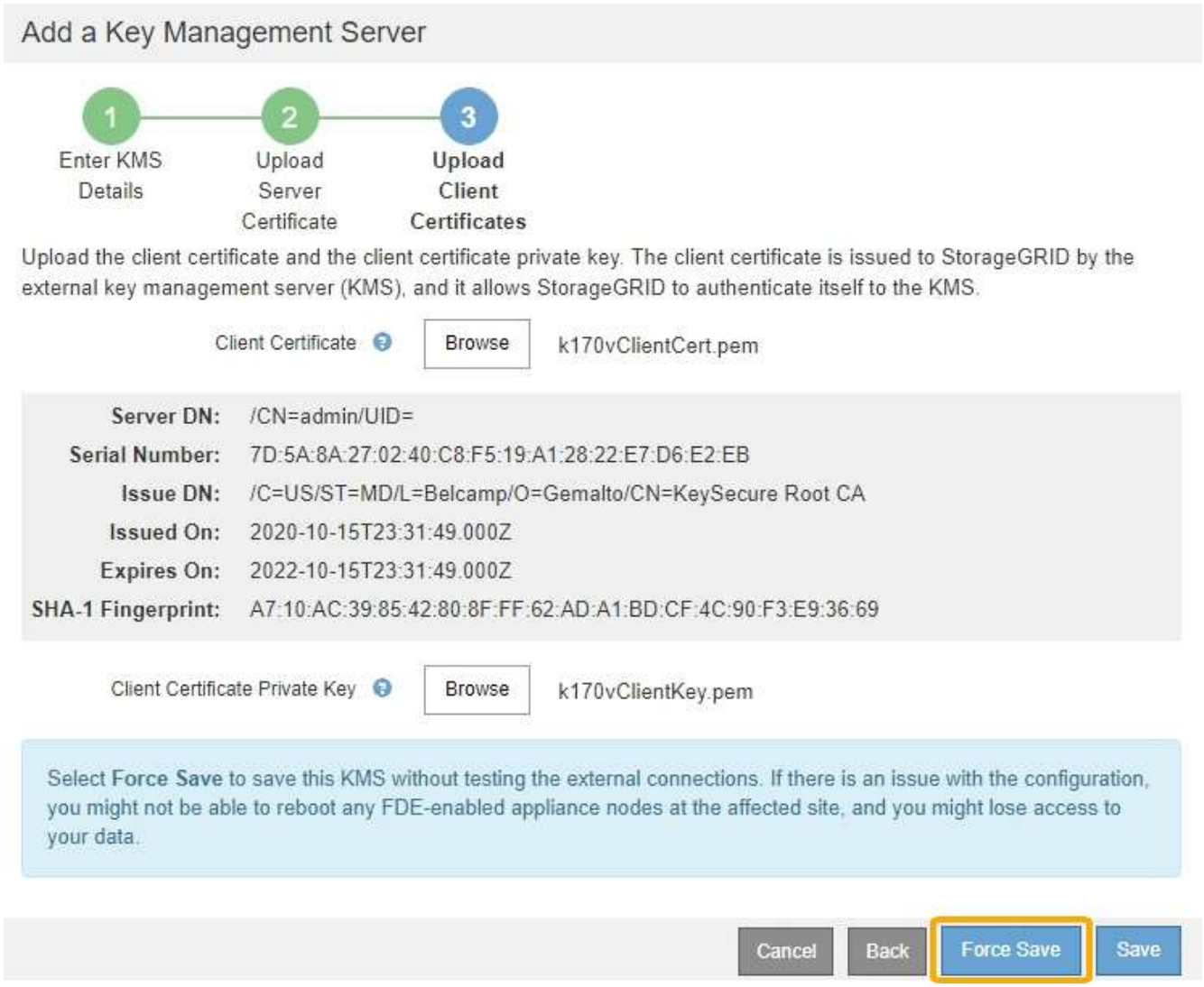
   Die Verbindungen zwischen dem Verschlüsselungsmanagement-Server und den Appliance-Nodes werden getestet. Wenn alle Verbindungen gültig sind und der korrekte Schlüssel auf dem KMS gefunden wird, wird der neue Schlüsselverwaltungsserver der Tabelle auf der Seite des Key Management Servers hinzugefügt.

   > 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 beim Auswählen von **Speichern** eine Fehlermeldung angezeigt wird, überprüfen Sie die Nachrichtendetails und wählen Sie dann **OK** aus.

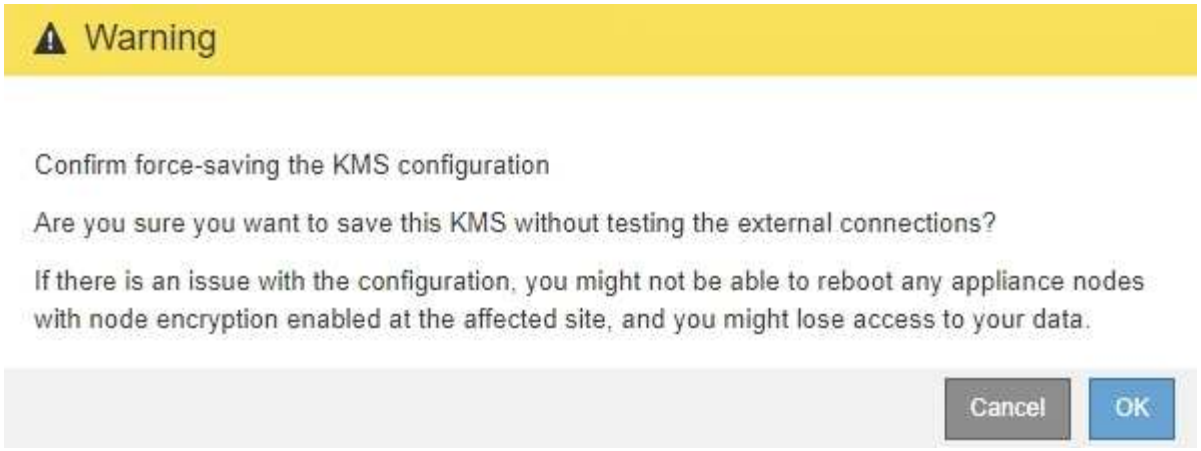
   Beispiel: Wenn ein Verbindungstest fehlgeschlagen ist, können Sie einen Fehler bei unbearbeitbarer Einheit mit 422: Nicht verarbeitbarer Einheit erhalten.

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



Durch die Auswahl von **Erzwingen speichern** wird die KMS-Konfiguration gespeichert, die externe Verbindung von jedem Gerät zu diesem KMS wird jedoch 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.

8. 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.

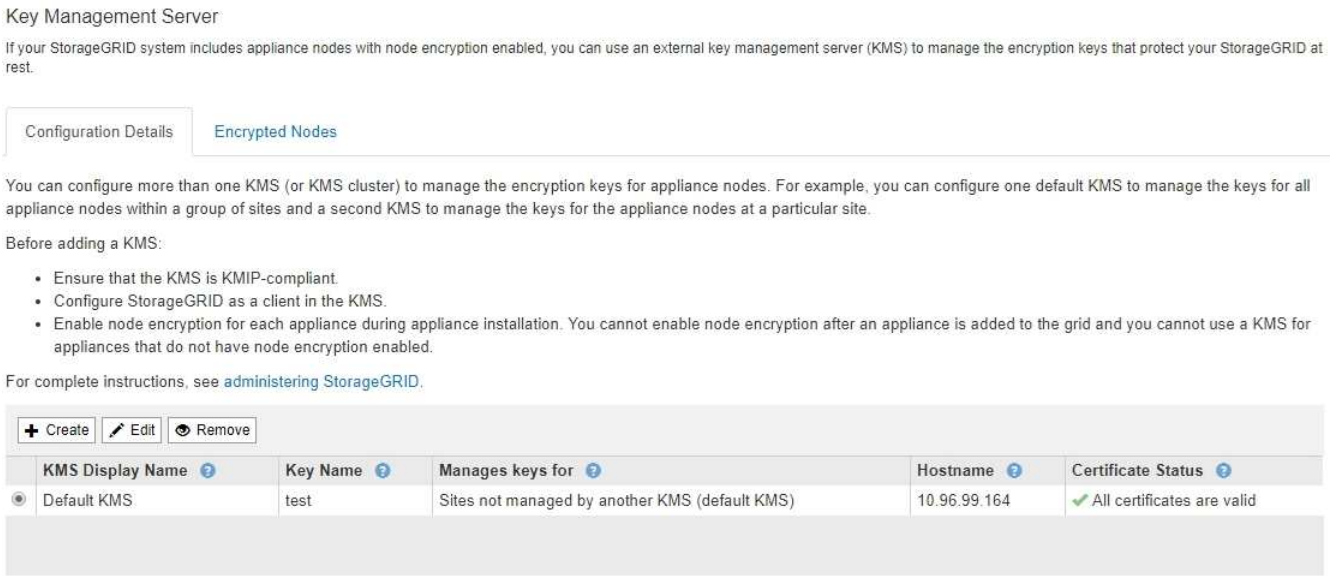
KMS-Details anzeigen

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

Schritte

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

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



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

Feld	Beschreibung
KMS-Anzeigename	Der beschreibende Name des KMS.

Feld	Beschreibung
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).**
Hostname	Der vollständig qualifizierte Domänenname oder die IP-Adresse des KMS. 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. Beispiel: `10.10.10.10 and 10.10.10.11` Oder `10.10.10.10 and 2 others`. Um alle Hostnamen in einem Cluster anzuzeigen, wählen Sie einen KMS aus, und wählen Sie dann **Bearbeiten** aus.
Zertifikatsstatus	Aktueller Status des Serverzertifikats, des optionalen CA-Zertifikats und des Client-Zertifikats: Gültig, abgelaufen, bald abgelaufen oder unbekannt. **Hinweis:** möglicherweise dauert StorageGRID bis zu 30 Minuten, um Updates zum Zertifikatsstatus zu erhalten. Sie müssen Ihren Webbrowser aktualisieren, um die aktuellen Werte anzuzeigen.

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

> 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.

4. Wenn in der Spalte „Zertifikatsstatus“ angegeben ist, dass ein Zertifikat abgelaufen ist oder sich dem

Ablauf nähert, beheben Sie das Problem so schnell wie möglich.

Lesen Sie die empfohlenen Aktionen für die Warnmeldungen **KMS CA CA CA-Zertifikatexpiration**, **KMS-Clientzertifikat-Ablauf** und **KMS-Serverzertifikat-Ablauf** in den Anweisungen für StorageGRID zur Überwachung und Fehlerbehebung.

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

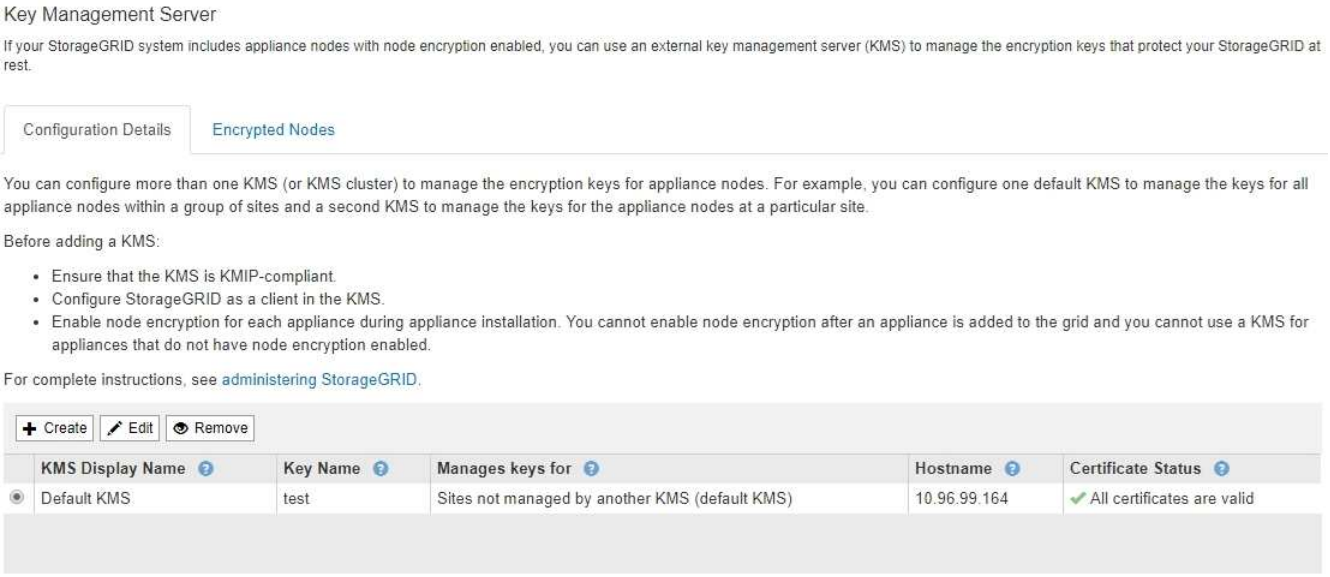
Verschlüsselte Nodes anzeigen

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

Schritte

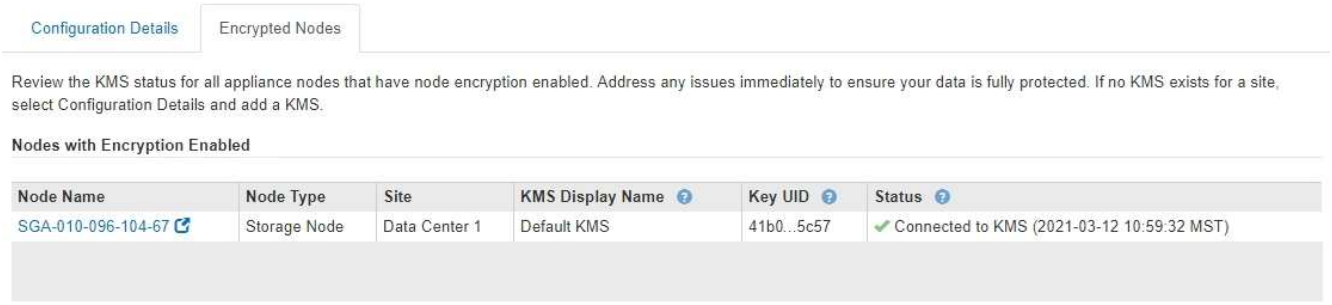
1. Wählen Sie **KONFIGURATION Sicherheit Schlüsselverwaltungsserver**.

   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, bei denen 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-Anzeigename	Der beschreibende Name des für den Knoten verwendeten KMS. Wenn kein KMS aufgeführt ist, wählen Sie die Registerkarte Konfigurationsdetails aus, um einen KMS hinzuzufügen. Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)
Schlüssel-UID	Die eindeutige ID des Verschlüsselungsschlüssels, der zur Verschlüsselung und Entschlüsselung von Daten auf dem Appliance-Node verwendet wird. Wenn Sie eine vollständige Schlüssel-UID anzeigen möchten, bewegen Sie den Mauszeiger über die Zelle. Ein Bindestrich (-) gibt an, dass die Schlüssel-UID unbekannt ist, möglicherweise wegen eines Verbindungsproblem zwischen dem Appliance-Node und dem KMS.
Status	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. **Hinweis:** Sie müssen Ihren Webbrowser aktualisieren, um die neuen Werte zu sehen.

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

Die empfohlenen Aktionen für diese Warnmeldungen finden Sie in den Anweisungen für StorageGRID zur Überwachung und Fehlerbehebung.

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.

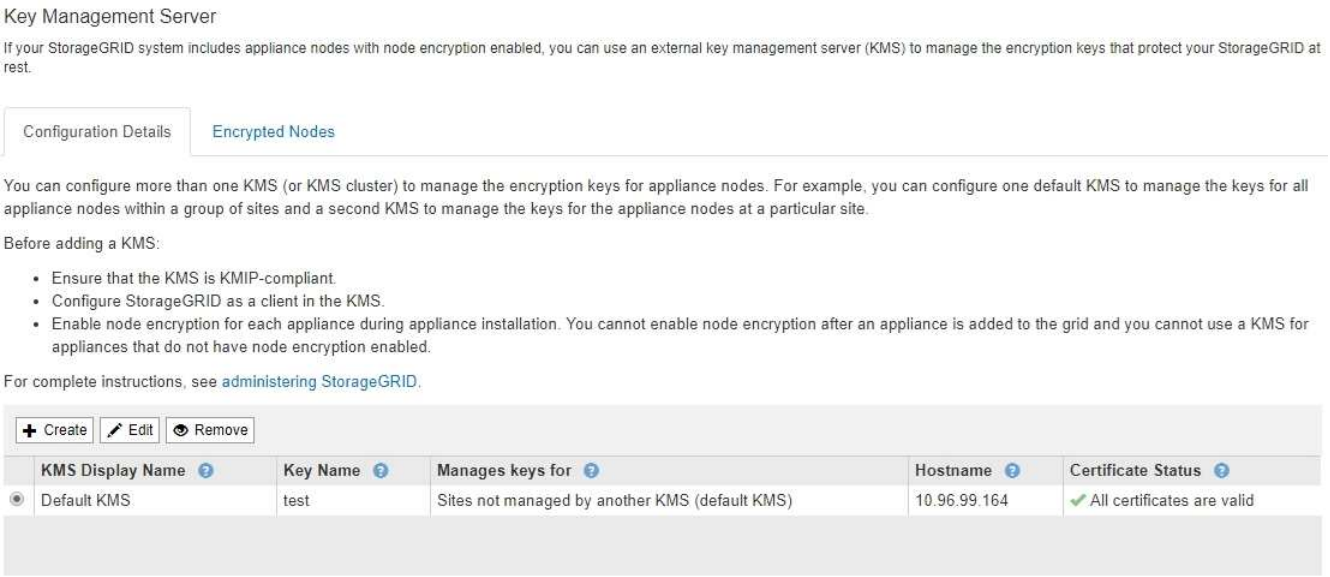
Was Sie benötigen

- 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**.

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



2. Wählen Sie den KMS aus, den Sie bearbeiten möchten, und wählen Sie **Bearbeiten**.
3. Aktualisieren Sie optional die Details in **Schritt 1 (KMS-Details eingeben)** des Assistenten zum Bearbeiten eines Schlüsselverwaltungsservers.

Feld	Beschreibung
KMS-Anzeigename	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. 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. 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. Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers
Verwaltet Schlüssel für	Wenn Sie einen Site-spezifischen KMS bearbeiten und noch keinen Standard-KMS haben, wählen Sie optional **Sites, die nicht von einem anderen KMS (Standard KMS)** verwaltet werden. Diese Auswahl konvertiert einen standortspezifischen KMS in den Standard-KMS, der für alle Sites gilt, die keinen dedizierten KMS haben, und für alle Sites, die in einer Erweiterung hinzugefügt wurden. **Hinweis:** Wenn Sie einen Site-spezifischen KMS bearbeiten, können Sie keine andere Site auswählen. Wenn Sie den Standard-KMS bearbeiten, können Sie keine bestimmte Site auswählen.
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	Der vollständig qualifizierte Domänenname oder die IP-Adresse für den KMS. **Hinweis:** das SAN-Feld 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.

4. Wenn Sie einen KMS-Cluster konfigurieren, wählen Sie das Pluszeichen aus ➕ Um einen Hostnamen für jeden Server im Cluster hinzuzufügen.
5. Wählen Sie **Weiter**.

   Schritt 2 (Serverzertifikat hochladen) des Assistenten „Schlüssel-Management-Server bearbeiten“ 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 (Upload Client Certificates) des Assistenten Edit a Key Management Server 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 **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**.

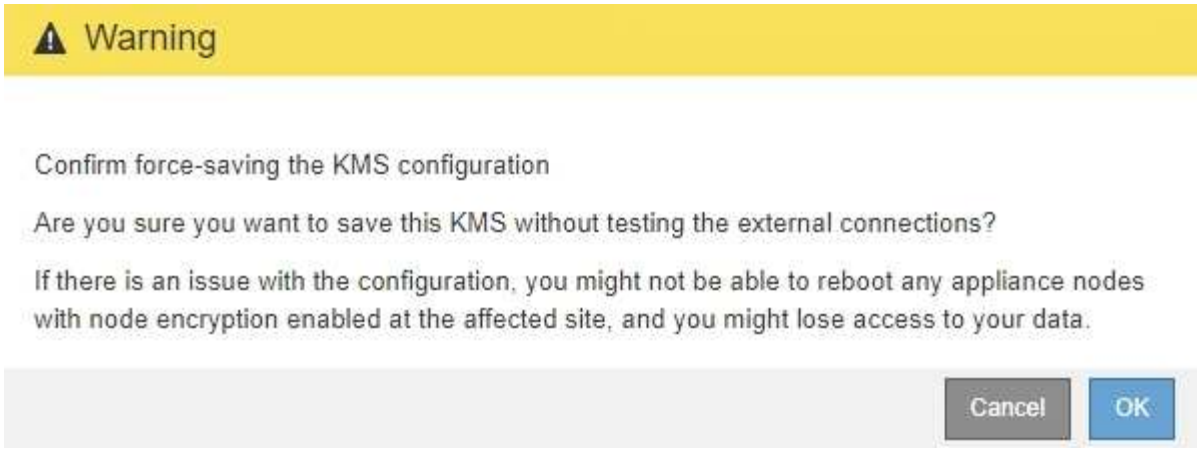
    Sie können beispielsweise einen Fehler bei der nicht verarbeitbaren Einheit von 422 erhalten, wenn die für diesen KMS ausgewählte Site bereits von einem anderen KMS verwaltet wird oder wenn ein Verbindungstest fehlgeschlagen ist.

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

    > ⓘ Durch die Auswahl von **Erzwingen speichern** wird die KMS-Konfiguration gespeichert, die externe Verbindung von jedem Gerät zu diesem KMS wird jedoch 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.

Was Sie benötigen

- 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

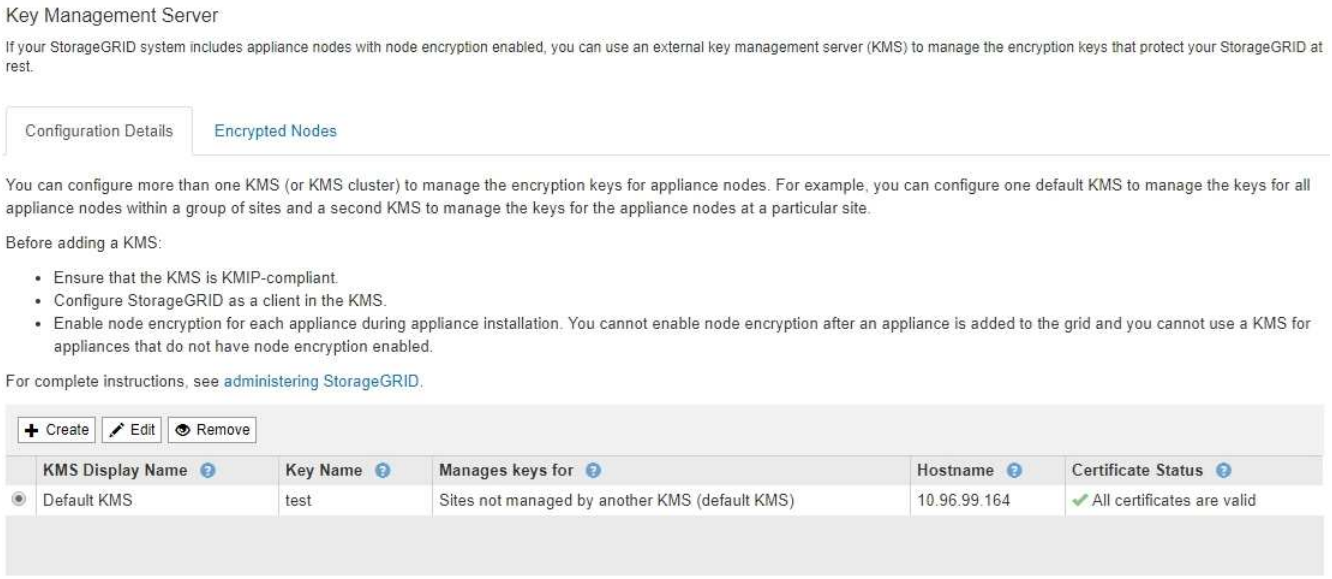
In diesen Fällen können Sie einen KMS entfernen:

- 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.

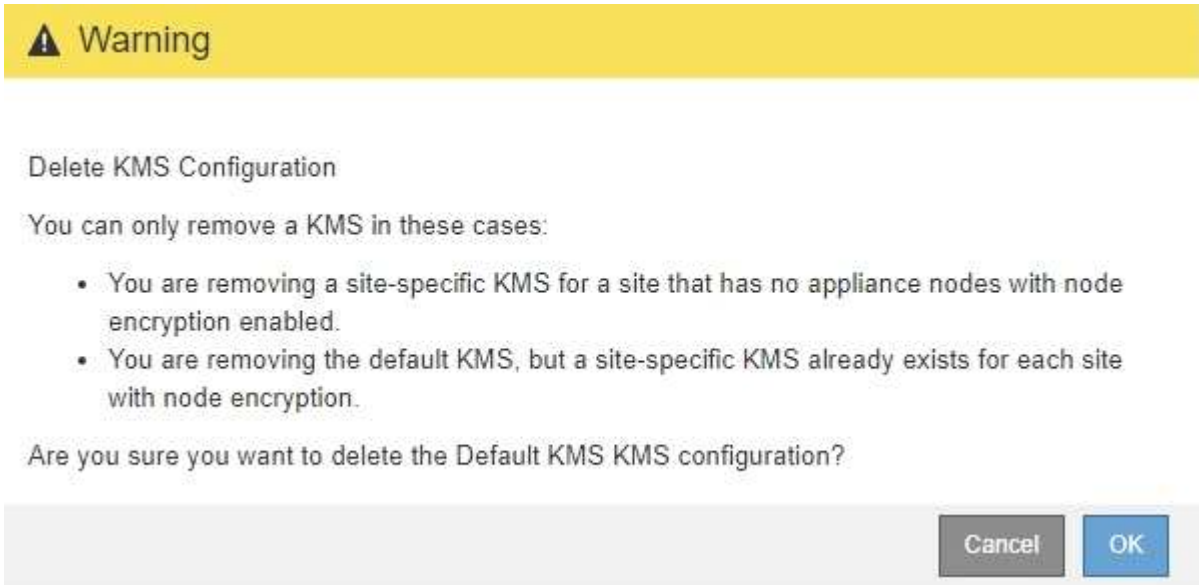
Schritte

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

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



2. Wählen Sie das Optionsfeld für den KMS, den Sie entfernen möchten, und wählen Sie **Entfernen**.
3. Prüfen Sie die Überlegungen im Warndialogfeld.



4. Wählen Sie **OK**.

   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.

Was Sie benötigen

- Sie haben spezifische Zugriffsberechtigungen.
- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.

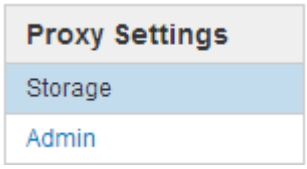
Über diese Aufgabe

Sie können die Einstellungen für einen einzelnen Speicherproxy konfigurieren.

Schritte

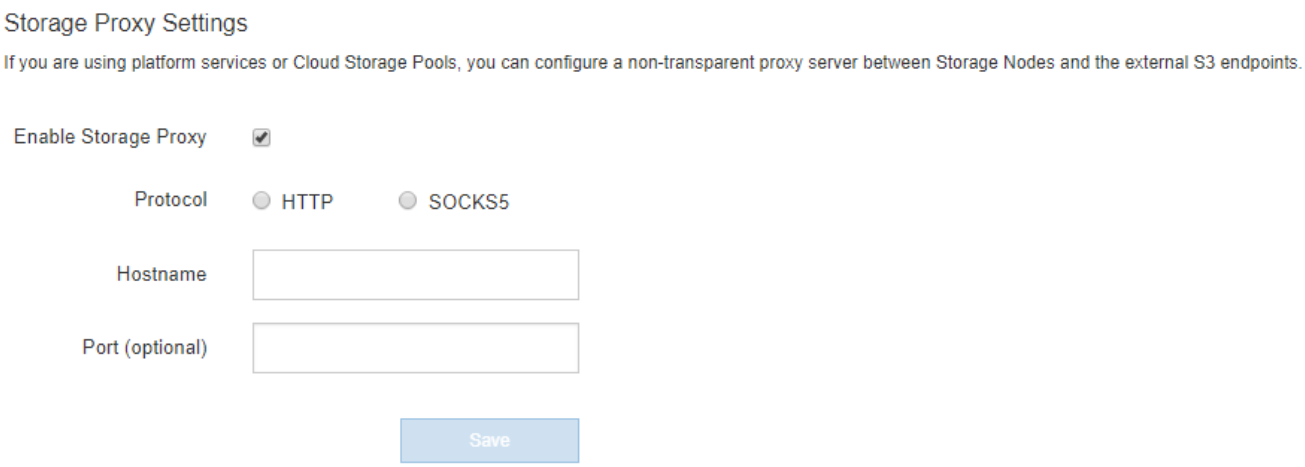
1. Wählen Sie **KONFIGURATION Sicherheit Proxy-Einstellungen**.

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



2. Aktivieren Sie das Kontrollkästchen * Storage Proxy aktivieren*.

   Die Felder zum Konfigurieren eines Speicher-Proxys werden angezeigt.



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 möchten, deaktivieren Sie das Kontrollkästchen **Storage Proxy aktivieren** und wählen Sie **Speichern**.

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.

Was Sie benötigen

- Sie haben spezifische Zugriffsberechtigungen.
- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.

Über diese Aufgabe

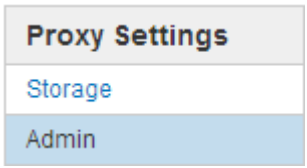
Sie können die Einstellungen für einen einzigen Admin-Proxy konfigurieren.

Schritte

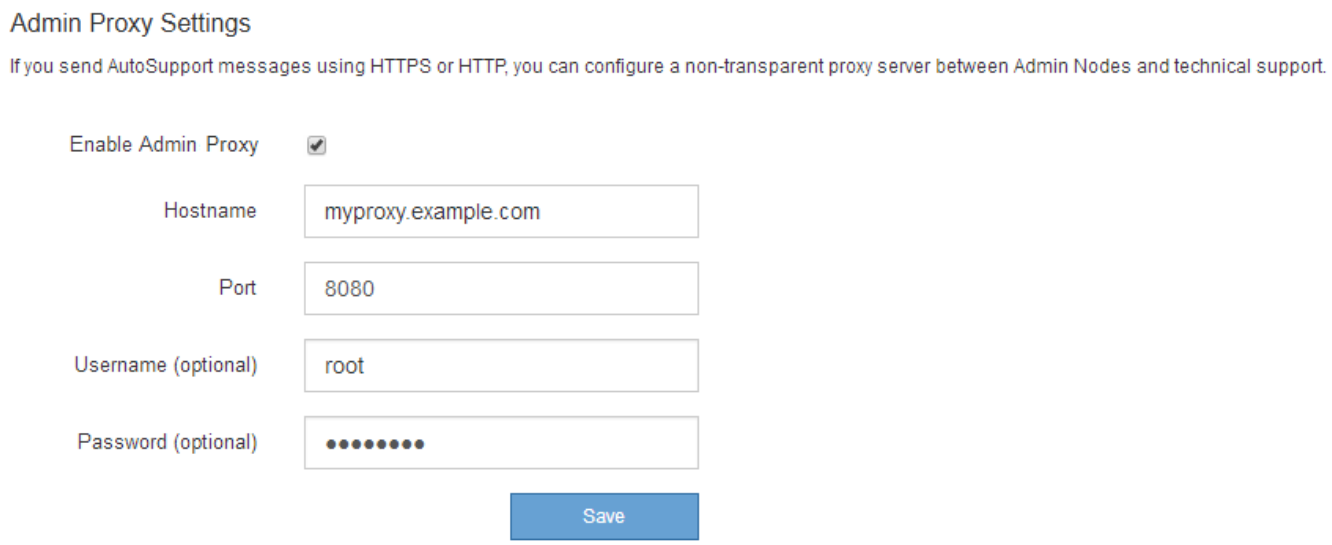
1. Wählen Sie **KONFIGURATION Sicherheit Proxy-Einstellungen**.

   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*.



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 **Speichern**.

Verwalten von nicht vertrauenswürdigen Clientnetzwerken

Verwaltung von nicht vertrauenswürdigen Client-Netzwerken: Übersicht

Wenn Sie ein Client-Netzwerk verwenden, können Sie StorageGRID vor feindlichen Angriffen schützen, indem Sie eingehenden Client-Datenverkehr nur auf explizit konfigurierten Endpunkten akzeptieren.

Standardmäßig ist das Client-Netzwerk auf jedem Grid-Knoten *Trusted*. Das heißt, StorageGRID vertraut standardmäßig eingehende Verbindungen zu jedem Grid-Knoten auf allen verfügbaren externen Ports (siehe Informationen über externe Kommunikation in Netzwerkrichtlinien).

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 Node nicht vertrauenswürdig ist, akzeptiert der Knoten nur eingehende Verbindungen an Ports, die

explizit als Load Balancer-Endpunkte konfiguriert sind. Siehe Konfigurieren von Load Balancer-Endpunkten.

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. Konfigurieren Sie auf der Seite Load Balancer Endpoints einen Endpunkt für den Load Balancer für S3 über HTTPS am Port 443.
2. Geben Sie auf der Seite nicht vertrauenswürdige Clientnetzwerke an, dass das Client-Netzwerk auf dem Gateway-Node 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 Datenverkehr des Outbound-S3-Plattformdienstes von einem Speicherknoten aktivieren, jedoch eingehende Verbindungen zu diesem Storage-Node im Client-Netzwerk verhindern. Sie würden diesen allgemeinen Schritt durchführen:

- Geben Sie auf der Seite nicht vertrauenswürdige Clientnetzwerke an, dass das Client-Netzwerk auf dem Speicherknoten nicht vertrauenswürdig ist.

Nachdem Sie Ihre Konfiguration gespeichert haben, akzeptiert der Speicherknoten keinen eingehenden Datenverkehr im Client-Netzwerk mehr, aber er erlaubt weiterhin ausgehende Anfragen an Amazon Web Services.

Das Client-Netzwerk des Node angeben ist nicht vertrauenswürdig

Wenn Sie ein Client-Netzwerk verwenden, können Sie angeben, ob das Client-Netzwerk jedes Node vertrauenswürdig oder nicht vertrauenswürdig ist. Sie können auch die Standardeinstellung für neue Knoten festlegen, die in einer Erweiterung hinzugefügt werden.

Was Sie benötigen

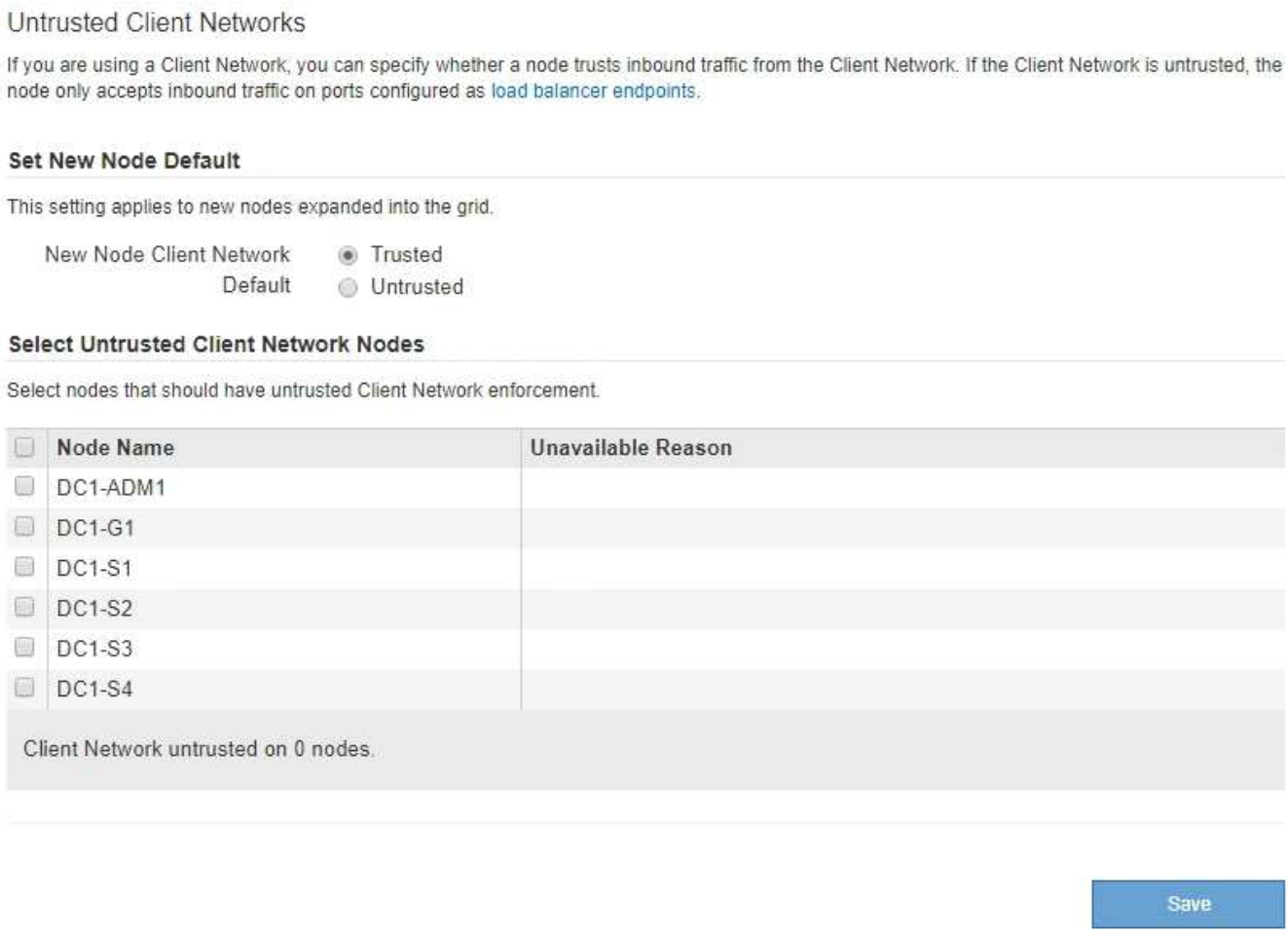
- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben die Root-Zugriffsberechtigung.
- Wenn ein Admin-Node oder Gateway-Node nur eingehenden Datenverkehr auf explizit konfigurierten Endpunkten annehmen soll, haben Sie die Load Balancer-Endpunkte definiert.

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

Schritte

1. Wählen Sie **KONFIGURATION Sicherheit nicht vertrauenswürdige Client-Netzwerke**.

   Auf der Seite nicht vertrauenswürdige Clientnetzwerke werden alle Knoten Ihres StorageGRID-Systems aufgelistet. Die Spalte „nicht verfügbar“ enthält einen Eintrag, wenn das Client-Netzwerk auf dem Knoten vertrauenswürdig sein muss.



2. Geben Sie im Abschnitt **Neue Knoten Standard** festlegen an, was die Standardeinstellung sein soll, wenn neue Knoten in einem Erweiterungsvorgang zum Raster hinzugefügt werden.

   - **Trusted**: Wenn ein Knoten in einer Erweiterung hinzugefügt wird, wird seinem Client-Netzwerk vertraut.
   - **UnTrusted**: Wenn ein Knoten in einer Erweiterung hinzugefügt wird, ist sein Client-Netzwerk nicht vertrauenswürdig. Sie können bei Bedarf zu dieser Seite zurückkehren, um die Einstellung für einen bestimmten neuen Knoten zu ändern.

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

3. Wählen Sie im Abschnitt **nicht vertrauenswürdige Client-Netzwerkknoten auswählen** die Knoten aus, die Clientverbindungen nur auf explizit konfigurierten Load-Balancer-Endpunkten zulassen sollen.

   Sie können das Kontrollkästchen im Titel auswählen oder deaktivieren, um alle Knoten auszuwählen oder zu deaktivieren.

4. Wählen Sie **Speichern**.

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

Verwalten von Mandanten

Verwalten von Mandanten

Als Grid-Administrator erstellen und managen Sie die Mandantenkonten, die S3 und Swift-Clients verwenden, um Objekte zu speichern und abzurufen, die Storage-Nutzung zu überwachen und die Aktionen zu managen, die Clients mit Ihrem StorageGRID System durchführen können.

Was sind Mandantenkonten?

Mandantenkonten ermöglichen Client-Applikationen, die die Simple Storage Service (S3) REST-API oder die Swift REST API verwenden, um Objekte auf StorageGRID zu speichern und abzurufen.

Jedes Mandantenkonto unterstützt die Verwendung eines einzelnen Protokolls, das Sie beim Erstellen des Kontos angeben. Zum Speichern und Abrufen von Objekten in einem StorageGRID System mit beiden Protokollen müssen Sie zwei Mandantenkonten erstellen: Eine für S3 Buckets und Objekte, eine für Swift Container und Objekte. Jedes Mandantenkonto hat seine eigene Account-ID, autorisierte Gruppen und Benutzer, Buckets oder Container und Objekte.

Optional können Sie zusätzliche Mandantenkonten erstellen, wenn Sie die auf Ihrem System gespeicherten Objekte durch verschiedene Einheiten trennen möchten. Beispielsweise können Sie in einem der folgenden Anwendungsfälle mehrere Mandantenkonten einrichten:

- **Anwendungsbeispiel für Unternehmen:** Wenn Sie ein StorageGRID-System in einer Enterprise-Anwendung verwalten, sollten Sie den Objekt-Storage des Grid möglicherweise von den verschiedenen Abteilungen Ihres Unternehmens trennen. In diesem Fall können Sie Mandantenkonten für die Marketingabteilung, die Kundenbetreuung, die Personalabteilung usw. erstellen.

  > Wenn Sie das S3-Client-Protokoll verwenden, können Sie mithilfe von S3-Buckets und Bucket-Richtlinien Objekte zwischen den Abteilungen eines Unternehmens trennen. Sie müssen keine Mandantenkonten verwenden. Weitere Informationen finden Sie in den Anweisungen zur Implementierung von S3-Client-Applikationen.

- **Anwendungsbeispiel Service Provider:** Wenn Sie ein StorageGRID-System als Service-Provider verwalten, können Sie den Objekt-Storage des Grid durch die verschiedenen Entitäten verteilen, die den Storage auf Ihrem Grid leasen. In diesem Fall würden Sie Mandantenkonten für Unternehmen A, Unternehmen B, Unternehmen C usw. erstellen.

Mandantenkonten erstellen und konfigurieren

Wenn Sie ein Mandantenkonto erstellen, geben Sie die folgenden Informationen an:

- Zeigt den Namen des Mandantenkontos an.
- Welches Client-Protokoll wird vom Mandantenkonto verwendet (S3 oder Swift).
- Bei S3-Mandantenkonten: Unabhängig davon, ob das Mandantenkonto die Berechtigung hat, Plattform-Services mit S3 Buckets zu verwenden. Wenn Sie Mandantenkonten für die Nutzung von Plattformdiensten zulassen, müssen Sie sicherstellen, dass das Grid für seine Nutzung konfiguriert ist. Siehe „`MAnaging Platform Services`“.
- Optional: Ein Storage-Kontingent für das Mandantenkonto – die maximale Anzahl der Gigabyte, Terabyte oder Petabyte, die für die Mandantenobjekte verfügbar sind. Wenn das Kontingent überschritten wird, kann

der Mandant keine neuen Objekte erstellen.

> Das Storage-Kontingent eines Mandanten stellt eine logische Menge (Objektgröße) und keine physische Menge (Größe auf der Festplatte) dar.

- Wenn die Identitätsföderation für das StorageGRID-System aktiviert ist, hat die föderierte Gruppe Root-Zugriffsberechtigungen, um das Mandantenkonto zu konfigurieren.
- Wenn Single Sign-On (SSO) nicht für das StorageGRID-System verwendet wird, gibt das Mandantenkonto seine eigene Identitätsquelle an oder teilt die Identitätsquelle des Grid mit, und zwar mit dem anfänglichen Passwort für den lokalen Root-Benutzer des Mandanten.

Nachdem ein Mandantenkonto erstellt wurde, können Sie die folgenden Aufgaben durchführen:

- **Plattformdienste für das Grid verwalten**: Wenn Sie Plattformdienste für Mandantenkonten aktivieren, sollten Sie wissen, wie Plattform-Services-Nachrichten bereitgestellt werden und welche Netzwerkanforderungen die Verwendung von Plattformservices für Ihre StorageGRID-Bereitstellung stellen.
- **Überwachen der Storage-Nutzung eines Mandantenkontos**: Nachdem Mandanten ihre Konten verwenden, können Sie mithilfe von Grid Manager überwachen, wie viel Storage die einzelnen Mandanten verbrauchen.

  > Die Werte für die Storage-Nutzung eines Mandanten sind möglicherweise nicht mehr aktuell, wenn Nodes von anderen Nodes im Grid isoliert werden. Die Gesamtwerte werden aktualisiert, wenn die Netzwerkverbindung wiederhergestellt ist.

  Wenn Sie Quoten für Mieter festgelegt haben, können Sie die Warnung **Tenant Quotenverbrauch hoch** aktivieren, um festzustellen, ob Mieter ihre Quoten verbrauchen. Wenn diese Meldung aktiviert ist, wird diese Meldung ausgelöst, wenn ein Mandant 90 % seines Kontingents verwendet hat. Weitere Informationen finden Sie unter Alerts Referenz in den Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID.

- **Client-Vorgänge konfigurieren**: Sie können konfigurieren, wenn einige Arten von Client-Operationen verboten sind.

S3-Mandanten konfigurieren

Nachdem ein S3-Mandantenkonto erstellt wurde, können Mandantenbenutzer auf den Mandanten-Manager zugreifen, um Aufgaben wie die folgenden auszuführen:

- Einrichten von Identitätsföderation (es sei denn, die Identitätsquelle wird gemeinsam mit dem Grid verwendet) und Erstellen lokaler Gruppen und Benutzer
- Verwalten von S3-Zugriffsschlüsseln
- Erstellen und Managen von S3 Buckets
- Monitoring der Storage-Auslastung
- Verwenden von Plattform-Services (falls aktiviert)

> Mandantenbenutzer von S3 können mit Mandanten-Manager S3-Zugriffsschlüssel und -Buckets erstellen und managen. Sie müssen jedoch eine S3-Client-Applikation verwenden, um Objekte aufzunehmen und zu managen.

Konfigurieren Sie Swift Mandanten

Nach der Erstellung eines Swift-Mandantenkontos kann der Root-Benutzer des Mandanten auf den Mandanten Manager zugreifen, um Aufgaben wie die folgenden auszuführen:

- Einrichten von Identitätsföderation (es sei denn, die Identitätsquelle wird gemeinsam mit dem Grid verwendet) und Erstellen lokaler Gruppen und Benutzer
- Monitoring der Storage-Auslastung

> Swift-Benutzer müssen über die Root-Zugriffsberechtigung für den Zugriff auf den Mandanten-Manager verfügen. Die Berechtigung Root-Zugriff erlaubt Benutzern jedoch nicht, sich in der Swift REST-API zu authentifizieren, um Container zu erstellen und Objekte aufzunehmen. Benutzer müssen über die Swift-Administratorberechtigung verfügen, um sich bei der Swift-REST-API zu authentifizieren.

Verwandte Informationen

Verwenden Sie ein Mandantenkonto

Erstellen eines Mandantenkontos

Sie müssen mindestens ein Mandantenkonto erstellen, um den Zugriff auf den Storage in Ihrem StorageGRID-System zu kontrollieren.

Wenn Sie ein Mandantenkonto erstellen, geben Sie einen Namen, ein Client-Protokoll und optional ein Storage-Kontingent an. Wenn Single Sign-On (SSO) für StorageGRID aktiviert ist, geben Sie außerdem an, welche föderierte Gruppe Root-Zugriffsberechtigungen hat, um das Mandantenkonto zu konfigurieren. Wenn StorageGRID keine Single-Sign-On verwendet, müssen Sie außerdem angeben, ob das Mandantenkonto seine eigene Identitätsquelle verwendet und das erste Passwort für den lokalen Root-Benutzer des Mandanten konfiguriert.

Der Grid Manager enthält einen Assistenten, der Sie durch die Schritte zum Erstellen eines Mandantenkontos führt. Je nachdem, ob die Schritte variieren Identitätsföderation Und Single Sign On Sind konfiguriert und ob das Grid Manager-Konto, das Sie zum Erstellen des Mandantenkontos verwenden, einer Admin-Gruppe mit Root-Zugriffsberechtigung angehört.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.
- Wenn das Mandantenkonto die für den Grid Manager konfigurierte Identitätsquelle verwendet und Sie einer föderierten Gruppe Root-Zugriffsberechtigungen für das Mandantenkonto gewähren möchten, haben Sie diese föderierte Gruppe in den Grid Manager importiert. Sie müssen dieser Admin-Gruppe keine Grid Manager-Berechtigungen zuweisen. Siehe Anweisungen zum Verwalten von Admin-Gruppen.

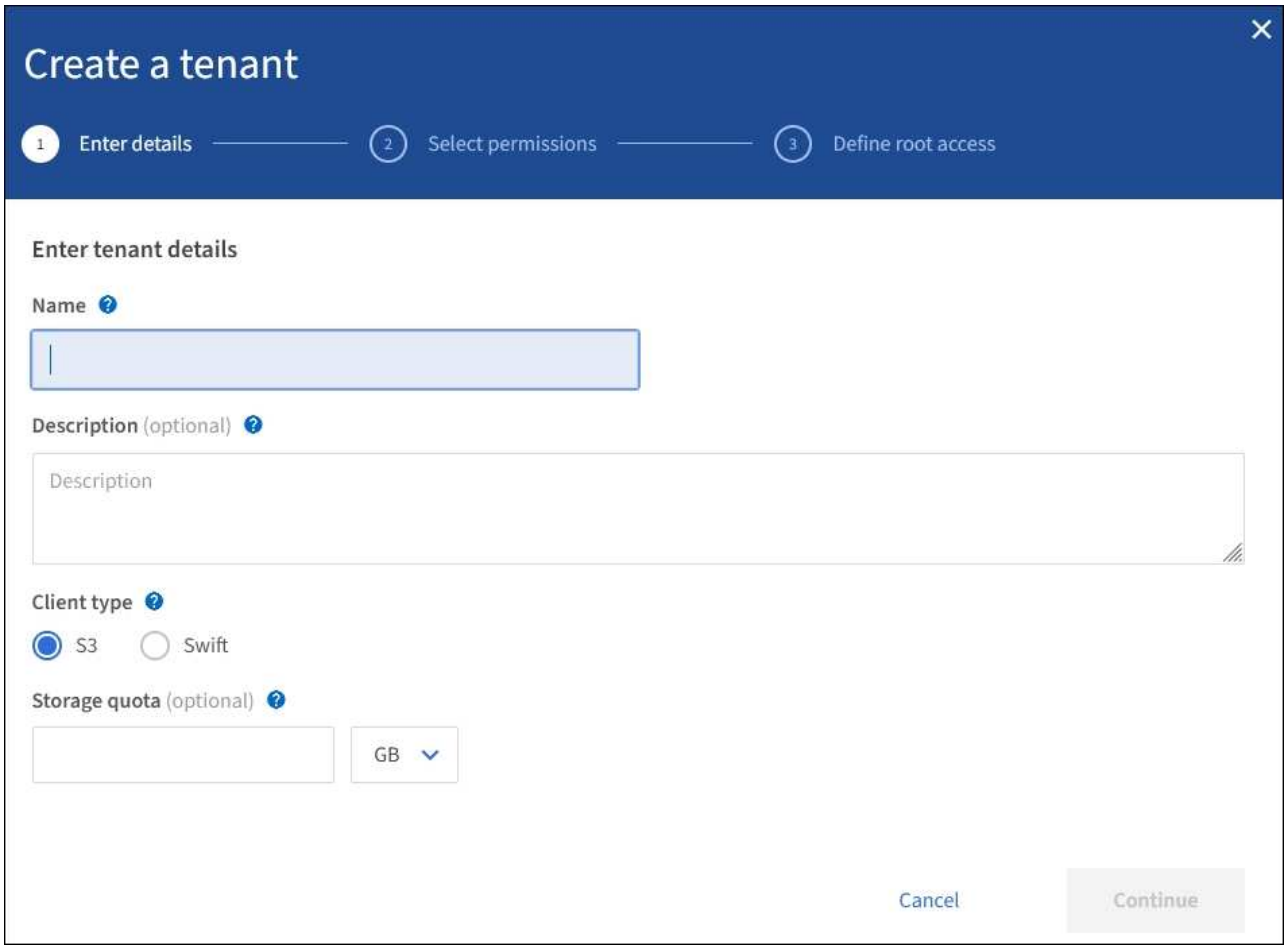
Schritte

1. Wählen Sie **MIETER**.
2. Wählen Sie **Erstellen** und geben Sie folgende Informationen für den Mieter ein:
   a. **Name**: Geben Sie einen Namen für das Mandantenkonto ein. Mandantennamen müssen nicht eindeutig sein. Wenn das Mandantenkonto erstellt wird, erhält es eine eindeutige, numerische Konto-ID.
   b. **Beschreibung** (optional): Geben Sie eine Beschreibung ein, mit der Sie den Mieter identifizieren

können.

c. **Client-Typ**: Wählen Sie den Client-Typ von **S3** oder **Swift** aus.

d. **Speicherkontingent** (optional): Wenn dieser Mieter ein Speicherkontingent haben soll, geben Sie einen numerischen Wert für das Kontingent ein und wählen Sie die richtigen Einheiten (GB, TB oder PB) aus.



3. Wählen Sie **Weiter** und konfigurieren Sie den S3- oder Swift-Mandanten.

S3-Mandant

Wählen Sie die entsprechenden Berechtigungen für den Mandanten aus. Einige dieser Berechtigungen haben zusätzliche Anforderungen. Weitere Informationen finden Sie in der Online-Hilfe zu jeder Berechtigung.

- Unterstützung von Plattform-Services
- Eigene Identitätsquelle verwenden (nur bei Nichtverwendung von SSO wählbar)
- S3-Auswahl zulassen (siehe Management von S3 Select für Mandantenkonten)

Swift-Mandant

Wenn der Mieter seine eigene Identitätsquelle verwendet, wählen Sie **eigene Identitätsquelle verwenden** (nur wählbar, wenn SSO nicht verwendet wird).

1. Wählen Sie **Weiter** und definieren Sie den Root-Zugriff für das Mandantenkonto.

Identitätsföderation nicht konfiguriert

1. Geben Sie ein Passwort für den lokalen Root-Benutzer ein.
2. Wählen Sie **Create Tenant**.

SSO aktiviert

Wenn SSO für StorageGRID aktiviert ist, muss der Mandant die für den Grid Manager konfigurierte Identitätsquelle verwenden. Keine lokalen Benutzer können sich anmelden. Sie geben an, welche föderierte Gruppe Root-Zugriffsberechtigungen hat, um das Mandantenkonto zu konfigurieren.

1. Wählen Sie eine vorhandene föderierte Gruppe aus dem Grid Manager aus, um die ursprüngliche Root-Zugriffsberechtigung für den Mandanten zu erhalten.

   Wenn Sie über ausreichende Berechtigungen verfügen, werden die vorhandenen föderierten Gruppen aus dem Grid Manager aufgelistet, wenn Sie das Feld auswählen. Geben Sie andernfalls den eindeutigen Namen der Gruppe ein.

2. Wählen Sie **Create Tenant**.

SSO ist nicht aktiviert

1. Führen Sie die in der Tabelle beschriebenen Schritte aus, je nachdem, ob der Mandant seine eigenen Gruppen und Benutzer verwaltet oder die für den Grid Manager konfigurierte Identitätsquelle verwendet.

Falls der Mandant…	Tun Sie das…
Verwaltung ihrer eigenen Gruppen und Benutzer	a. Wählen Sie **eigene Identitätsquelle verwenden**. **Hinweis**: Wenn dieses Kontrollkästchen aktiviert ist und Sie Identity Federation für Mandantengruppen und Benutzer verwenden möchten, muss der Mandant seine eigene Identitätsquelle konfigurieren. Siehe Anweisungen zur Verwendung von Mandantenkonten. b. Geben Sie ein Passwort für den lokalen Root-Benutzer des Mandanten an, und wählen Sie dann **Create Tenant**. c. Wählen Sie **Anmelden als root**, um den Mandanten zu konfigurieren, oder wählen Sie **Fertig**, um den Mandanten später zu konfigurieren.

Falls der Mandant…	Tun Sie das…
Verwenden Sie die für den Grid Manager konfigurierten Gruppen und Benutzer	a. Führen Sie einen oder beide der folgenden Schritte aus: ◦ Wählen Sie eine vorhandene föderierte Gruppe aus dem Grid Manager aus, die über die ursprüngliche Root-Zugriffsberechtigung für den Mandanten verfügen sollte. **Hinweis**: Wenn Sie über ausreichende Berechtigungen verfügen, werden die vorhandenen föderierten Gruppen aus dem Grid Manager aufgelistet, wenn Sie das Feld auswählen. Geben Sie andernfalls den eindeutigen Namen der Gruppe ein. ◦ Geben Sie ein Passwort für den lokalen Root-Benutzer des Mandanten an. b. Wählen Sie **Create Tenant**.

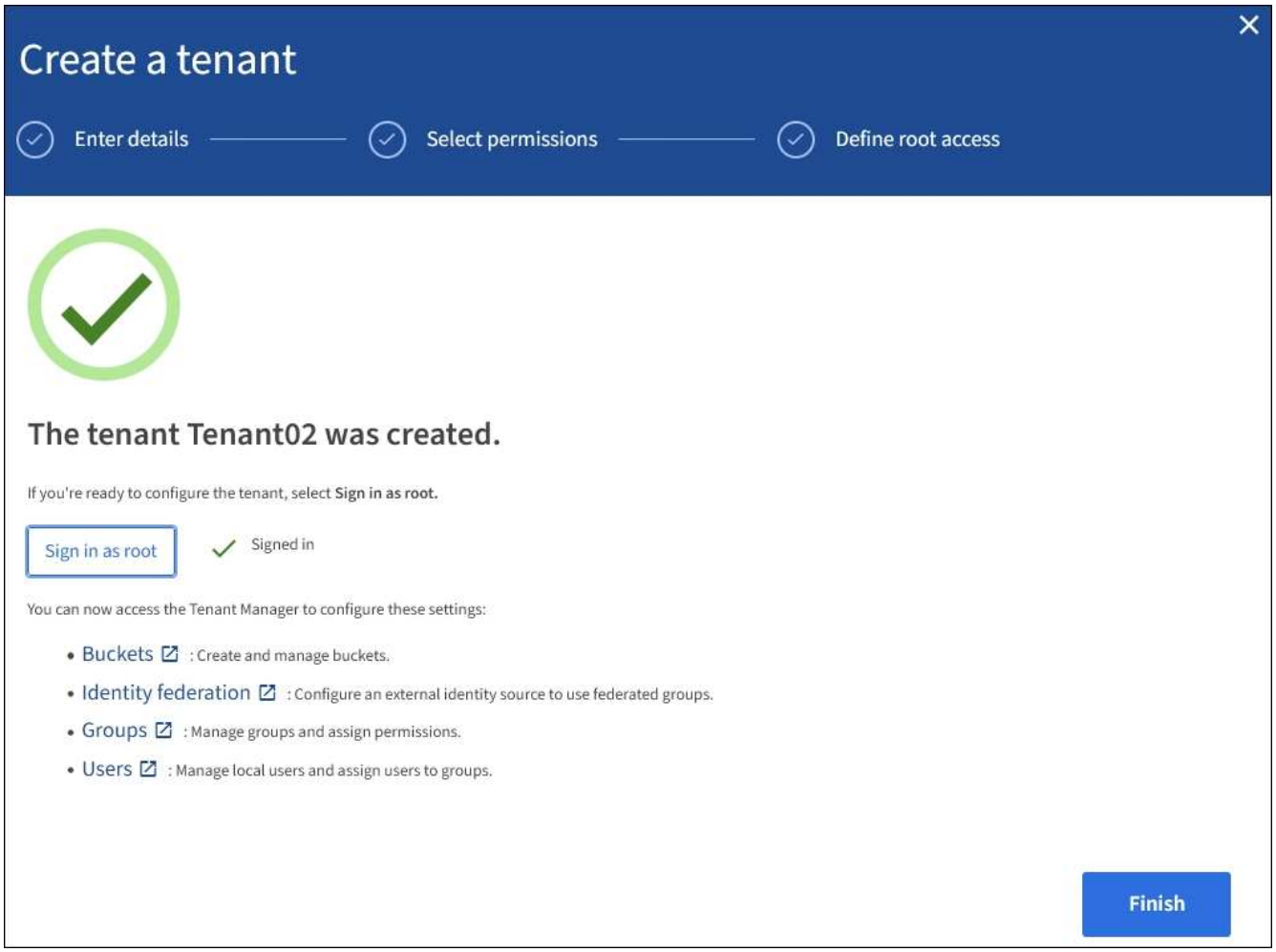
1. So melden Sie sich jetzt beim Mieter an:
   - Wenn Sie über einen eingeschränkten Port auf den Grid Manager zugreifen, wählen Sie in der Mandantentabelle **eingeschränkt** aus, um mehr über den Zugriff auf dieses Mandantenkonto zu erfahren.

     Die URL für den Tenant Manager weist folgendes Format auf:

     `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/`

     - *`FQDN_or_Admin_Node_IP`* Ist ein vollständig qualifizierter Domain-Name oder die IP-Adresse eines Admin-Knotens
     - *`port`* Ist der reine Mandantenport
     - *`20-digit-account-id`* Die eindeutige Account-ID des Mandanten
   - Wenn Sie am Port 443 auf den Grid Manager zugreifen, aber kein Passwort für den lokalen Root-Benutzer festgelegt haben, wählen Sie in der Tabelle Mandanten des Grid Manager die Option **Anmelden** aus, und geben Sie die Anmeldeinformationen für einen Benutzer in die föderierte Gruppe Root Access ein.
   - Wenn Sie auf den Grid Manager auf Port 443 zugreifen und ein Passwort für den lokalen Root-Benutzer festlegen:
     i. Wählen Sie **Anmelden als root**, um den Mandanten jetzt zu konfigurieren.

     Wenn Sie sich anmelden, werden Links zum Konfigurieren von Buckets oder Containern, Identitätsföderation, Gruppen und Benutzern angezeigt.



i. Wählen Sie die Links aus, um das Mandantenkonto zu konfigurieren.

   Jeder Link öffnet die entsprechende Seite im Tenant Manager. Informationen zum Ausfüllen der Seite finden Sie im Anweisungen zur Verwendung von Mandantenkonten.

ii. Andernfalls wählen Sie **Fertig**, um später auf den Mieter zuzugreifen.

2. So greifen Sie später auf den Mandanten zu:

Sie verwenden…	Führen Sie eine dieser…
Port 443	• Wählen Sie im Grid Manager **MIETERS** aus und wählen Sie **Anmelden** rechts neben dem Mieternamen aus. • Geben Sie die URL des Mandanten in einen Webbrowser ein: `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* Ist ein vollständig qualifizierter Domain-Name oder die IP-Adresse eines Admin-Knotens ◦ *20-digit-account-id* Die eindeutige Account-ID des Mandanten

Sie verwenden…	Führen Sie eine dieser…
Ein eingeschränkter Port	• Wählen Sie im Grid Manager die Option **MITERS** aus, und wählen Sie **eingeschränkt**. • Geben Sie die URL des Mandanten in einen Webbrowser ein: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ *FQDN_or_Admin_Node_IP* Ist ein vollständig qualifizierter Domain-Name oder die IP-Adresse eines Admin-Knotens ◦ *port* Ist der ausschließlich auf Mandanten beschränkte Port ◦ *20-digit-account-id* Die eindeutige Account-ID des Mandanten

Verwandte Informationen

- Kontrolle des Zugriffs durch Firewalls
- Management von Plattform-Services für S3-Mandantenkonten

Ändern Sie das Passwort für den lokalen Root-Benutzer des Mandanten

Möglicherweise müssen Sie das Passwort für den lokalen Root-Benutzer eines Mandanten ändern, wenn der Root-Benutzer aus dem Konto gesperrt ist.

Was Sie benötigen

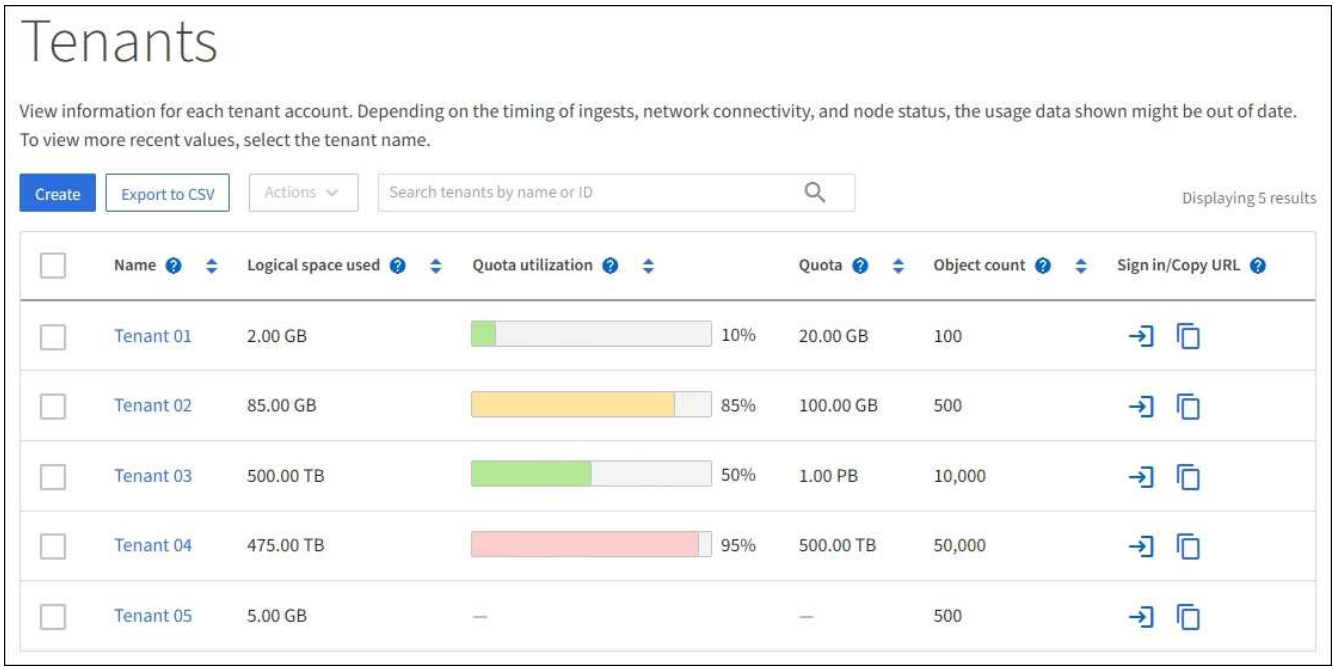
- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Wenn Single Sign On (SSO) für Ihr StorageGRID-System aktiviert ist, kann sich der lokale Root-Benutzer nicht beim Mandantenkonto anmelden. Um Root-Benutzeraufgaben auszuführen, müssen Benutzer einer föderierten Gruppe angehören, die über die Root-Zugriffsberechtigung für den Mandanten verfügt.

Schritte

1. Wählen Sie **MIETER**.



2. Wählen Sie das Mandantenkonto aus, das Sie bearbeiten möchten.

   Die Schaltfläche Aktionen wird aktiviert.

3. Wählen Sie im Dropdown-Menü **Aktionen** die Option **Root-Passwort ändern** aus.
4. Geben Sie das neue Kennwort für das Mandantenkonto ein.
5. Wählen Sie **Speichern**.

Mandantenkonto bearbeiten

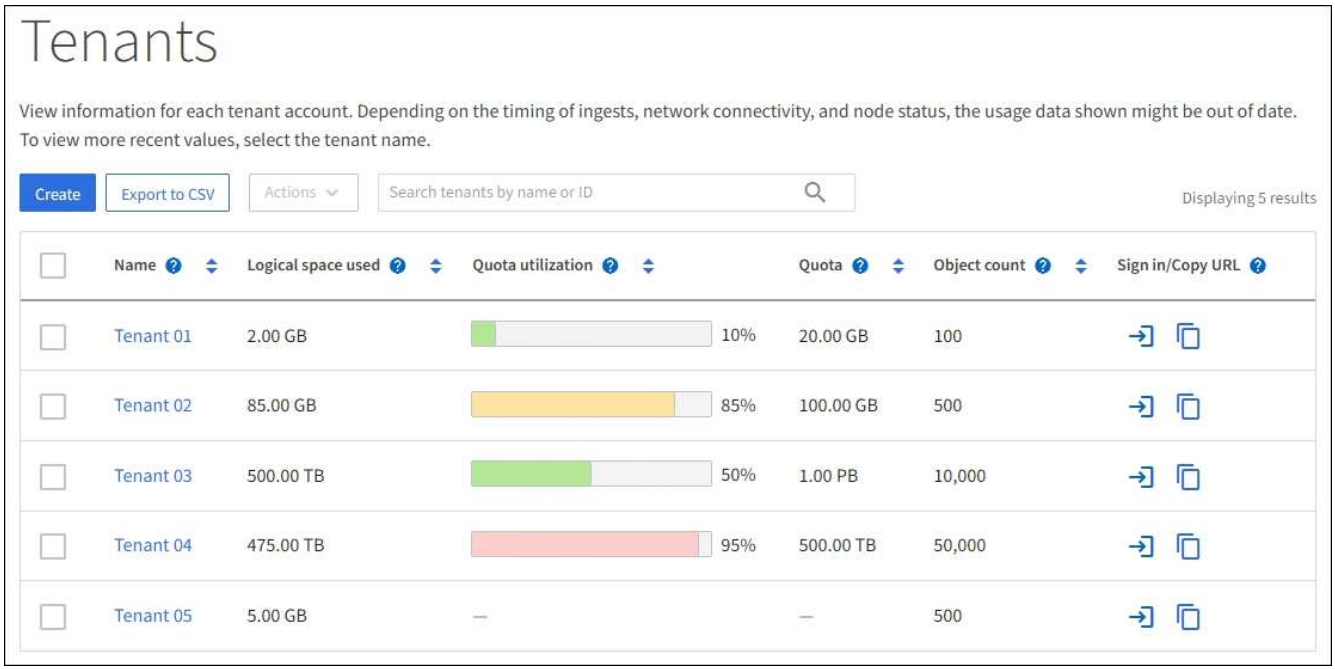
Sie können ein Mandantenkonto bearbeiten, um den Anzeigenamen zu ändern, die Einstellung für die Identitätsquelle zu ändern, Plattformservices zu ermöglichen oder zu verlassen oder ein Speicherkontingent einzugeben.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

Schritte

1. Wählen Sie **MIETER**.

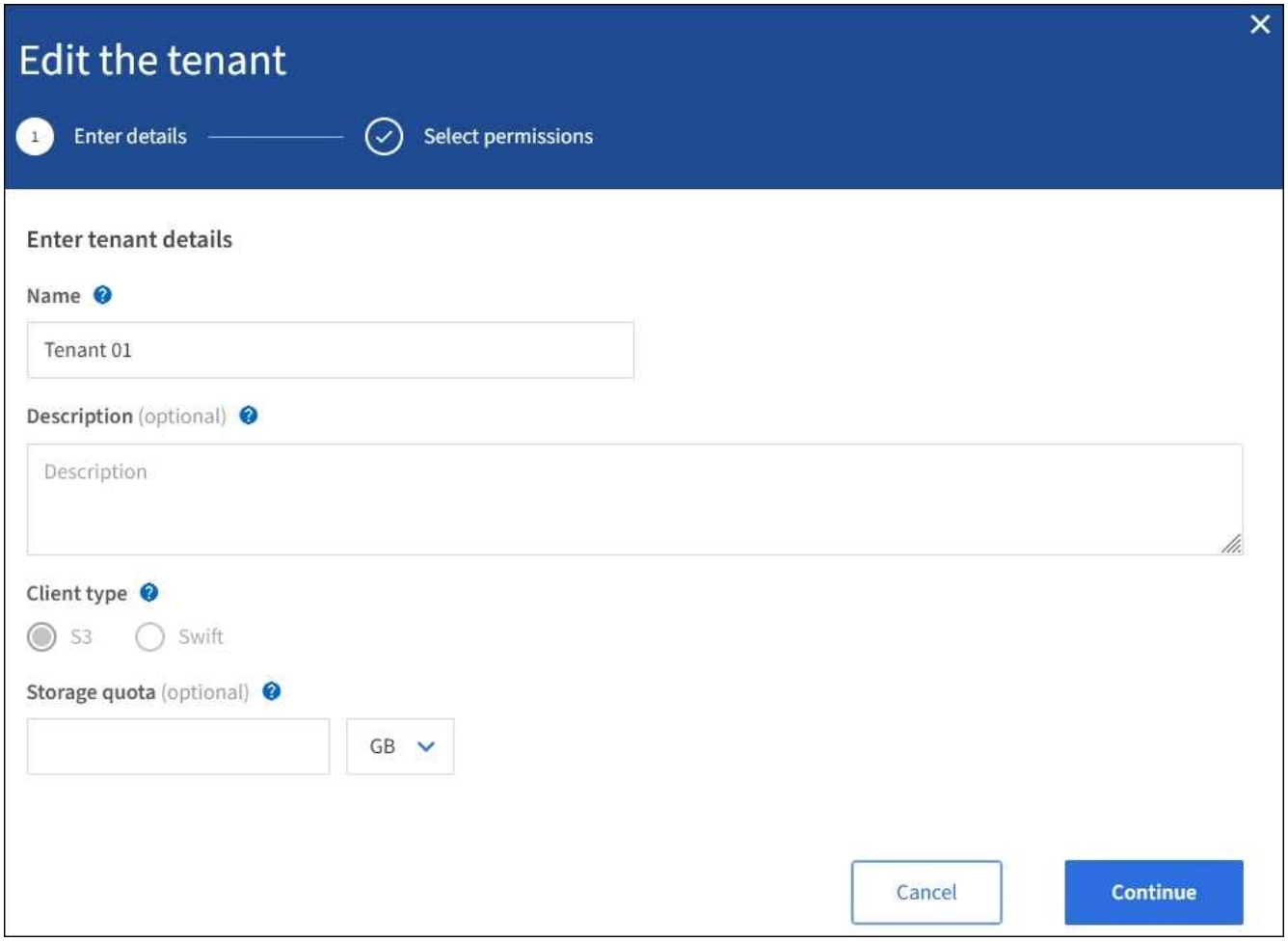


2. Wählen Sie das Mandantenkonto aus, das Sie bearbeiten möchten.

   Verwenden Sie das Suchfeld, um nach einem Mandantenkonto nach Name oder Mandanten-ID zu suchen.

3. Wählen Sie aus der Dropdown-Liste Aktionen die Option **Bearbeiten** aus.

   Dieses Beispiel gilt für ein Raster, in dem keine SSO (Single Sign On) verwendet wird. Dieses Mandantenkonto hat keine eigene Identitätsquelle konfiguriert.



4. Ändern Sie die Werte für diese Felder nach Bedarf:
   - **Name**
   - **Beschreibung**
   - **Client-Typ**
   - **Speicherquote**
5. Wählen Sie **Weiter**.
6. Wählen Sie die Berechtigungen für das Mandantenkonto aus, oder heben Sie die Auswahl auf.
   - Wenn Sie **Platform Services** für einen Mandanten deaktivieren, der diese bereits nutzt, werden die Dienste, die er für seine S3-Buckets konfiguriert hat, nicht mehr funktionieren. Es wird keine Fehlermeldung an den Mandanten gesendet. Wenn der Mandant beispielsweise die Replizierung von CloudMirror für einen S3-Bucket konfiguriert hat, können sie Objekte weiterhin im Bucket speichern, doch werden Kopien dieser Objekte nicht mehr im externen S3-Bucket erstellt, den sie als Endpunkt konfiguriert haben.
   - Ändern Sie das Kontrollkästchen **nutzt eigene Identitätsquelle**, um zu bestimmen, ob das Mandantenkonto eine eigene Identitätsquelle oder die für den Grid Manager konfigurierte Identitätsquelle verwendet.

     Wenn das Kontrollkästchen * eigene Identitätsquelle verwendet*:

     - Deaktiviert und überprüft, hat der Mandant bereits seine eigene Identitätsquelle aktiviert. Ein Mandant muss seine Identitätsquelle deaktivieren, bevor er die für den Grid Manager konfigurierte Identitätsquelle verwenden kann.

        - Deaktiviert und deaktiviert ist, ist SSO für das StorageGRID System aktiviert. Der Mandant muss die Identitätsquelle verwenden, die für den Grid Manager konfiguriert wurde.
    - Aktiviert oder deaktiviert **S3 Select** nach Bedarf. Siehe Management von S3 Select für Mandantenkonten.
7. Wählen Sie **Speichern**.

Verwandte Informationen

- Management von Plattform-Services für S3-Mandantenkonten
- Verwenden Sie ein Mandantenkonto

Mandantenkonto löschen

Sie können ein Mandantenkonto löschen, wenn Sie den Zugriff des Mandanten auf das System dauerhaft entfernen möchten.

Was Sie benötigen

- Sie müssen mit einem beim Grid Manager angemeldet sein Unterstützter Webbrowser.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen alle Buckets (S3), Container (Swift) und Objekte, die mit dem Mandantenkonto verknüpft sind, entfernt haben.

Schritte

1. Wählen Sie **MIETER**.
2. Wählen Sie das Mandantenkonto aus, das gelöscht werden soll.

   Verwenden Sie das Suchfeld, um nach einem Mandantenkonto nach Name oder Mandanten-ID zu suchen.
3. Wählen Sie im Dropdown-Menü **Aktionen** die Option **Löschen** aus.
4. Wählen Sie **OK**.

Management von Plattform-Services

Management von Plattform-Services für S3-Mandantenkonten

Wenn Sie Plattformservices für S3-Mandantenkonten aktivieren, müssen Sie Ihr Grid so konfigurieren, dass Mandanten auf die externen Ressourcen zugreifen können, die für die Nutzung dieser Services erforderlich sind.

Was sind Plattform-Services?

Zu den Plattform-Services zählen die CloudMirror-Replizierung, Ereignisbenachrichtigungen und der Such-Integrationsservice.

Dank dieser Services können Mandanten die folgenden Funktionen mit ihren S3 Buckets nutzen:

- **CloudMirror Replikation**: Der StorageGRID CloudMirror Replikationsservice wird verwendet, um bestimmte Objekte von einem StorageGRID-Bucket auf ein bestimmtes externes Ziel zu spiegeln.

  So können Sie beispielsweise CloudMirror Replizierung verwenden, um spezifische Kundendaten in

Amazon S3 zu spiegeln und anschließend AWS Services für Analysen Ihrer Daten nutzen.

> Die CloudMirror-Replizierung wird nicht unterstützt, wenn im Quell-Bucket S3-Objektsperre aktiviert ist.

- **Benachrichtigungen**: Per Bucket-Ereignisbenachrichtigungen werden verwendet, um Benachrichtigungen über bestimmte Aktionen, die an Objekten ausgeführt werden, an einen bestimmten externen Amazon Simple Notification Service™ (SNS) zu senden.

  Beispielsweise können Sie Warnmeldungen so konfigurieren, dass sie an Administratoren über jedes Objekt, das einem Bucket hinzugefügt wurde, gesendet werden, wo die Objekte Protokolldateien darstellen, die mit einem kritischen Systemereignis verbunden sind.

  > Obwohl die Ereignisbenachrichtigung für einen Bucket konfiguriert werden kann, bei dem S3 Object Lock aktiviert ist, werden die S3 Object Lock Metadaten (einschließlich „Aufbewahrung bis Datum“ und „Legal Hold“-Status) der Objekte in den Benachrichtigungsmeldungen nicht enthalten.

- **Suchintegrationsdienst**: Der Suchintegrationsdienst dient dazu, S3-Objektmetadaten an einen bestimmten Elasticsearch-Index zu senden, in dem die Metadaten mit dem externen Dienst durchsucht oder analysiert werden können.

  Sie könnten beispielsweise die Buckets konfigurieren, um S3 Objekt-Metadaten an einen Remote-Elasticsearch-Service zu senden. Anschließend kann Elasticsearch verwendet werden, um nach Buckets zu suchen und um anspruchsvolle Analysen der Muster in den Objektmetadaten durchzuführen.

  > Die Elasticsearch-Integration kann auf einem Bucket konfiguriert werden, bei dem die S3-Objektsperre aktiviert ist, aber die S3-Objektsperrmetadaten (einschließlich Aufbewahrung bis Datum und Status der Aufbewahrung) der Objekte werden nicht in die Benachrichtigungen einbezogen.

Dank Plattform-Services können Mandanten externe Storage-Ressourcen, Benachrichtigungsservices und Such- oder Analyseservices für ihre Daten nutzen. Da sich der Zielstandort für Plattformservices in der Regel außerhalb Ihrer StorageGRID-Implementierung befindet, müssen Sie entscheiden, ob die Nutzung dieser Services durch Mandanten gestattet werden soll. Wenn Sie dies tun, müssen Sie die Verwendung von Plattform-Services aktivieren, wenn Sie Mandantenkonten erstellen oder bearbeiten. Sie müssen auch Ihr Netzwerk so konfigurieren, dass die von Mandanten generierten Plattformservices Meldungen ihre Ziele erreichen können.

Empfehlungen für die Nutzung von Plattform-Services

Vor der Verwendung von Plattform-Services sollten Sie sich der folgenden Empfehlungen bewusst sein:

- Wenn in einem S3-Bucket im StorageGRID System sowohl die Versionierung als auch die CloudMirror-Replizierung aktiviert sind, sollten Sie für den Zielendpunkt auch die S3-Bucket-Versionierung aktivieren. So kann die CloudMirror-Replizierung ähnliche Objektversionen auf dem Endpunkt generieren.
- Sie sollten nicht mehr als 100 aktive Mandanten mit S3-Anfragen verwenden, die CloudMirror-Replizierung, Benachrichtigungen und Suchintegration erfordern. Mehr als 100 aktive Mandanten können zu einer langsameren S3-Client-Performance führen.
- Anfragen, die nicht abgeschlossen werden können, werden auf maximal 500,000 Anforderungen in die Warteschlange gestellt. Dieses Limit wird gleich von aktiven Mandanten gemeinsam genutzt. Neue Mieter dürfen diese Grenze von 500,000 vorübergehend überschreiten, so dass neu erstellte Mieter nicht

ungerecht bestraft werden.

Verwandte Informationen

- Verwenden Sie ein Mandantenkonto
- Konfigurieren Sie Speicher-Proxy-Einstellungen
- Monitoring und Fehlerbehebung

Netzwerk und Ports für Plattformservices

Wenn ein S3-Mandant Plattformservices verwendet, müssen Sie das Netzwerk für das Grid konfigurieren, um sicherzustellen, dass Plattformservices-Meldungen an seine Ziele gesendet werden können.

Sie können Plattformservices für ein S3-Mandantenkonto aktivieren, wenn Sie das Mandantenkonto erstellen oder aktualisieren. Wenn Plattformservices aktiviert sind, kann der Mandant Endpunkte erstellen, die als Ziel für die CloudMirror-Replizierung, Ereignisbenachrichtigungen oder Integrationsmeldungen aus seinen S3-Buckets dienen. Diese Plattform-Services-Meldungen werden von Storage-Nodes gesendet, die den ADC-Service an die Ziel-Endpunkte ausführen.

Beispielsweise können Mandanten die folgenden Typen von Ziel-Endpunkten konfigurieren:

- Ein lokal gehostetes Elasticsearch-Cluster ausführen
- Eine lokale Anwendung, die den Empfang von SNS-Meldungen (Simple Notification Service) unterstützt
- Ein lokal gehosteter S3-Bucket auf derselben oder einer anderen Instanz von StorageGRID
- Einem externen Endpunkt wie einem Endpunkt auf Amazon Web Services

Um sicherzustellen, dass Meldungen von Plattformservices bereitgestellt werden können, müssen Sie das Netzwerk oder die Netzwerke mit den ADC-Speicherknoten konfigurieren. Sie müssen sicherstellen, dass die folgenden Ports zum Senden von Plattformservices-Meldungen an die Ziel-Endpunkte verwendet werden können.

Standardmäßig werden Plattform-Services-Meldungen an die folgenden Ports gesendet:

- **80**: Für Endpunkt-URIs, die mit http beginnen
- **443**: Für Endpunkt-URIs, die mit https beginnen

Mandanten können bei der Erstellung oder Bearbeitung eines Endpunkts einen anderen Port angeben.

> Wenn eine StorageGRID-Bereitstellung als Ziel für die CloudMirror-Replikation verwendet wird, können Replikationsmeldungen auf einem anderen Port als 80 oder 443 empfangen werden. Vergewissern Sie sich, dass der von der Ziel-StorageGRID-Implementierung für S3 verwendete Port im Endpunkt angegeben ist.

Wenn Sie einen nicht-transparenten Proxy-Server verwenden, müssen Sie auch Konfigurieren Sie Speicher-Proxy-Einstellungen Damit Nachrichten an externe Endpunkte gesendet werden können, z. B. an einem Endpunkt im Internet.

Verwandte Informationen

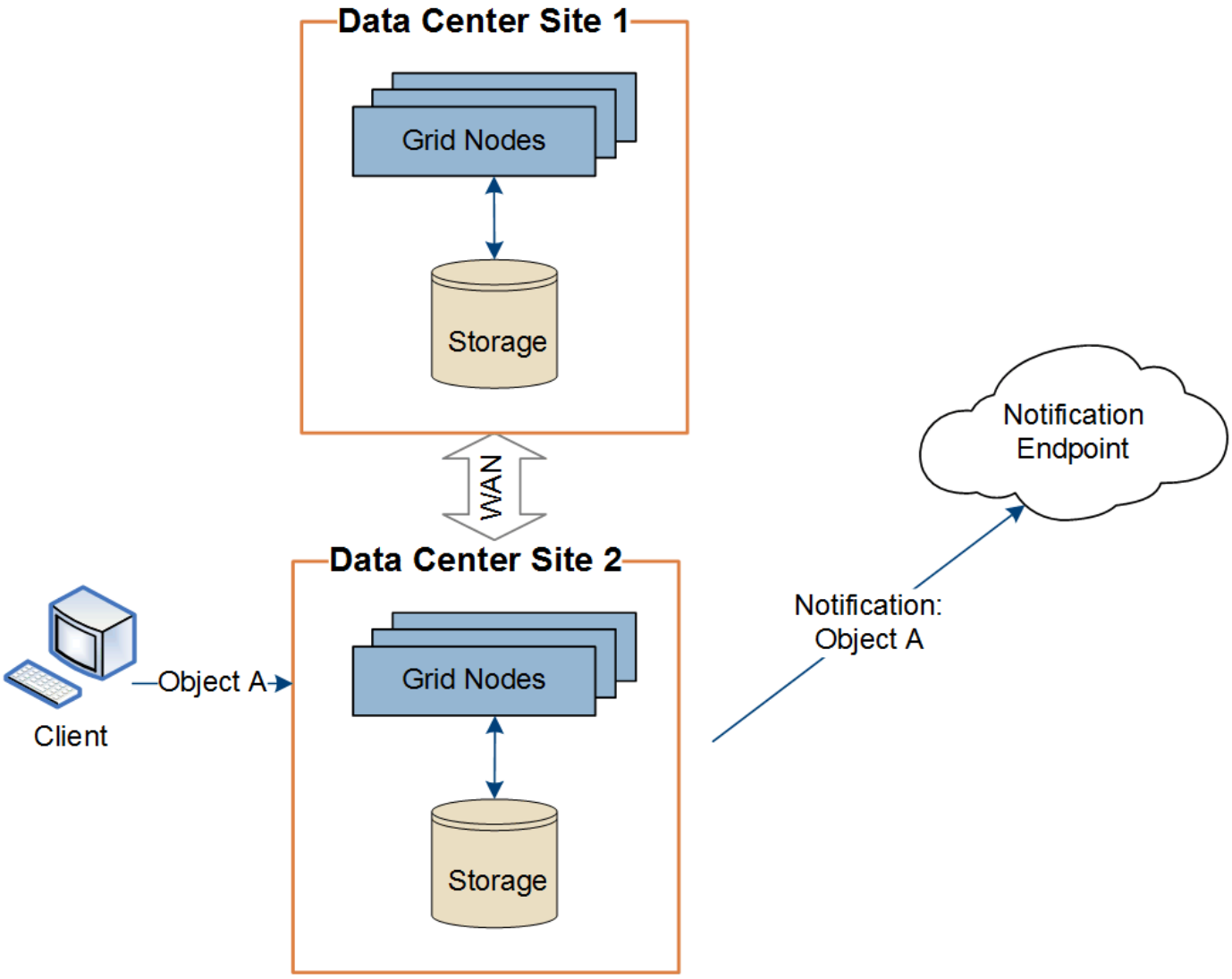
- Verwenden Sie ein Mandantenkonto

Bereitstellung von Plattform-Services am Standort

Alle Vorgänge von Plattform-Services werden am Standort durchgeführt.

Wenn ein Mandant einen Client verwendet, um einen S3 API Create-Vorgang für ein Objekt durch eine Verbindung zu einem Gateway-Node an Datacenter Standort 1 durchzuführen, wird die Benachrichtigung über diese Aktion von Datacenter Standort 1 ausgelöst und gesendet.

Wenn der Client anschließend einen S3-API-Löschvorgang auf demselben Objekt von Data Center Site 2 aus durchführt, wird die Benachrichtigung über die Löschaktion ausgelöst und von Data Center Site 2 gesendet.



Stellen Sie sicher, dass das Netzwerk an jedem Standort so konfiguriert ist, dass Plattformdienste-Meldungen an ihre Ziele gesendet werden können.

Fehlerbehebung bei Plattform-Services

Die in Plattform-Services verwendeten Endpunkte werden von Mandantenbenutzern im Mandanten-Manager erstellt und gewartet. Falls jedoch Probleme bei der Konfiguration oder Verwendung von Plattformservices bei einem Mandanten auftreten, können Sie das Problem mithilfe des Grid Manager beheben.

Probleme mit neuen Endpunkten

Bevor ein Mandant Plattform-Services nutzen kann, muss er mithilfe des Mandanten-Manager einen oder mehrere Endpunkte erstellen. Jeder Endpunkt stellt ein externes Ziel für einen Plattform-Service dar, wie einen StorageGRID S3 Bucket, einen Amazon Web Services Bucket, ein Thema „Simple Notification Service“ oder ein Elasticsearch-Cluster, der lokal oder in AWS gehostet wird. Jeder Endpunkt umfasst sowohl den Standort der externen Ressource als auch die für den Zugriff auf diese Ressource erforderlichen Zugangsdaten.

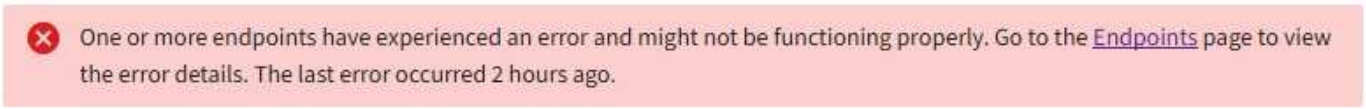
Wenn ein Mandant einen Endpunkt erstellt, überprüft das StorageGRID System, ob der Endpunkt vorhanden ist und ob er mit den angegebenen Zugangsdaten erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Node an jedem Standort validiert.

Wenn die Endpoint-Validierung fehlschlägt, erklärt eine Fehlermeldung, warum die Endpoint-Validierung fehlgeschlagen ist. Der Mandantenbenutzer sollte das Problem lösen, und versuchen Sie dann erneut, den Endpunkt zu erstellen.

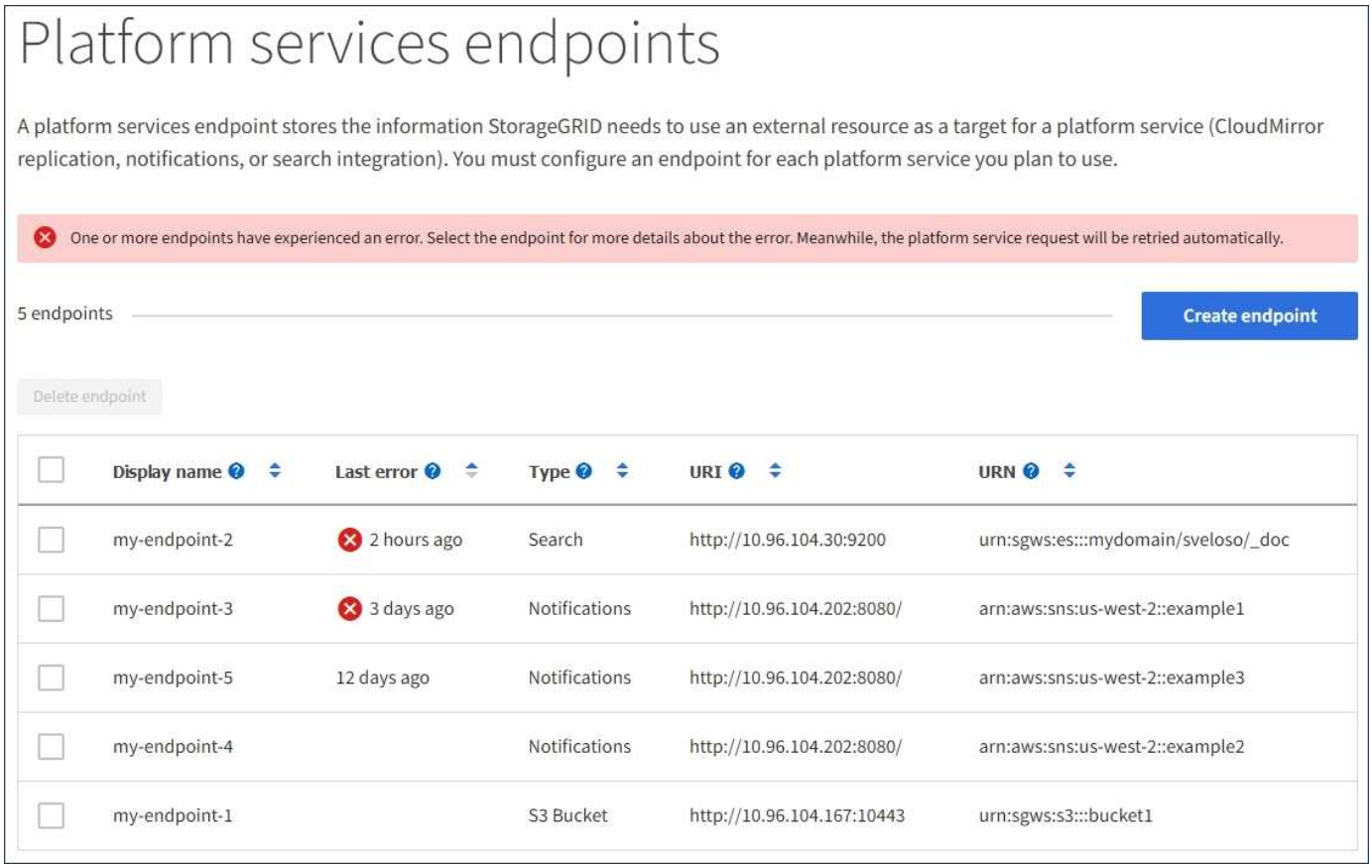
> ⓘ Die Erstellung von Endgeräten schlägt fehl, wenn Plattformdienste für das Mandantenkonto nicht aktiviert sind.

Probleme mit vorhandenen Endpunkten

Wenn StorageGRID versucht, einen vorhandenen Endpunkt zu erreichen, tritt ein Fehler auf, wird im Mandantenmanager auf dem Dashboard eine Meldung angezeigt.



Mandantenbenutzer können auf der Seite Endpunkte die aktuellste Fehlermeldung für jeden Endpunkt lesen und herausfinden, wie lange der Fehler bereits aufgetreten ist. Die Spalte **Letzter Fehler** zeigt die aktuellste Fehlermeldung für jeden Endpunkt an und gibt an, wie lange der Fehler aufgetreten ist. Fehler, die das enthalten  Das Symbol trat innerhalb der letzten 7 Tage auf.



Einige Fehlermeldungen in der Spalte **Letzter Fehler** können eine LOGID in Klammern enthalten. Ein Grid-Administrator oder technischer Support kann diese ID verwenden, um ausführlichere Informationen über den Fehler im bycast.log zu finden.

Probleme im Zusammenhang mit Proxy-Servern

Wenn Sie einen Speicher-Proxy zwischen Speicherknoten und Plattform-Service-Endpunkten konfiguriert haben, treten möglicherweise Fehler auf, wenn Ihr Proxydienst keine Meldungen von StorageGRID zulässt. Um diese Probleme zu beheben, überprüfen Sie die Einstellungen Ihres Proxy-Servers, um sicherzustellen, dass die Nachrichten für den Plattformdienst nicht blockiert sind.

Ermitteln Sie, ob ein Fehler aufgetreten ist

Wenn innerhalb der letzten 7 Tage Endpoint-Fehler aufgetreten sind, wird im Dashboard im Tenant Manager eine Warnmeldung angezeigt. Sie können die Seite Endpoints aufrufen, um weitere Details über den Fehler zu sehen.

Client-Betrieb schlägt fehl

Einige Probleme bei Plattform-Services können zum Ausfall von Client-Operationen auf dem S3-Bucket führen. Beispielsweise schlägt der S3-Client-Betrieb fehl, wenn der interne RSM-Service (Replicated State Machine) ausfällt oder es zu viele Plattformservices-Nachrichten in Warteschlange für die Lieferung gibt.

So überprüfen Sie den Status der Dienste:

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***site Storage Node* SSM Services** aus.

Behebbare und nicht wiederherstellbare Endpunktfehler

Nach der Erstellung von Endpunkten können Fehler bei Plattformservice-Anfragen aus verschiedenen Gründen auftreten. Einige Fehler lassen sich durch Benutzereingriffe wiederherstellen. Beispielsweise können behebbare Fehler aus den folgenden Gründen auftreten:

- Die Anmeldedaten des Benutzers wurden gelöscht oder abgelaufen.
- Der Ziel-Bucket ist nicht vorhanden.
- Die Benachrichtigung kann nicht zugestellt werden.

Wenn bei StorageGRID ein wiederherstellbarer Fehler auftritt, wird die Serviceanfrage für die Plattform erneut versucht, bis sie erfolgreich ist.

Andere Fehler können nicht behoben werden. Beispielsweise tritt ein nicht behebbarer Fehler auf, wenn der Endpunkt gelöscht wird.

Wenn bei StorageGRID ein nicht behebbarer Endpunktfehler auftritt, wird im Grid Manager der alte Alarm „Total Events“ (SMTT) ausgelöst. So zeigen Sie den alten Alarm „Ereignisse insgesamt“ an:

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***site Node* SSM Events** aus.
3. Letztes Ereignis oben in der Tabelle anzeigen.

   Ereignismeldungen sind auch in aufgeführt `/var/local/log/bycast-err.log`.

4. Befolgen Sie die Anweisungen im SMTT-Alarminhalt, um das Problem zu beheben.
5. Wählen Sie die Registerkarte **Konfiguration**, um die Ereignisanzahl zurückzusetzen.
6. Benachrichtigen Sie den Mieter über die Objekte, deren Plattform-Services-Nachrichten nicht geliefert wurden.
7. Weisen Sie den Mandanten an, die fehlgeschlagene Replikation oder Benachrichtigung durch Aktualisieren der Metadaten oder Tags des Objekts erneut auszulösen.

   Der Mieter kann die vorhandenen Werte erneut einreichen, um unerwünschte Änderungen zu vermeiden.

Plattform-Services-Meldungen können nicht bereitgestellt werden

Wenn im Ziel ein Problem auftritt, das verhindert, dass Plattformdienste-Meldungen akzeptiert werden, wird der Client-Vorgang auf dem Bucket erfolgreich ausgeführt, die Plattform-Services-Meldung wird jedoch nicht geliefert. Dieser Fehler kann z. B. auftreten, wenn die Anmeldeinformationen auf dem Ziel aktualisiert werden, sodass sich StorageGRID nicht mehr beim Ziel-Service authentifizieren kann.

Wenn Meldungen von Plattform-Services aufgrund eines nicht behebbaren Fehlers nicht zugestellt werden können, wird der alte Alarm „Total Events“ (SMTT) im Grid Manager ausgelöst.

Langsamere Performance für Plattform-Service-Anfragen

StorageGRID kann eingehende S3-Anfragen für einen Bucket drosseln, wenn die Rate, mit der die Anforderungen gesendet werden, die Rate übersteigt, mit der der Zielendpunkt die Anforderungen empfangen kann. Eine Drosselung tritt nur auf, wenn ein Rückstand von Anfragen besteht, die auf den Zielendpunkt warten.

Der einzige sichtbare Effekt besteht darin, dass die eingehenden S3-Anforderungen länger in Anspruch

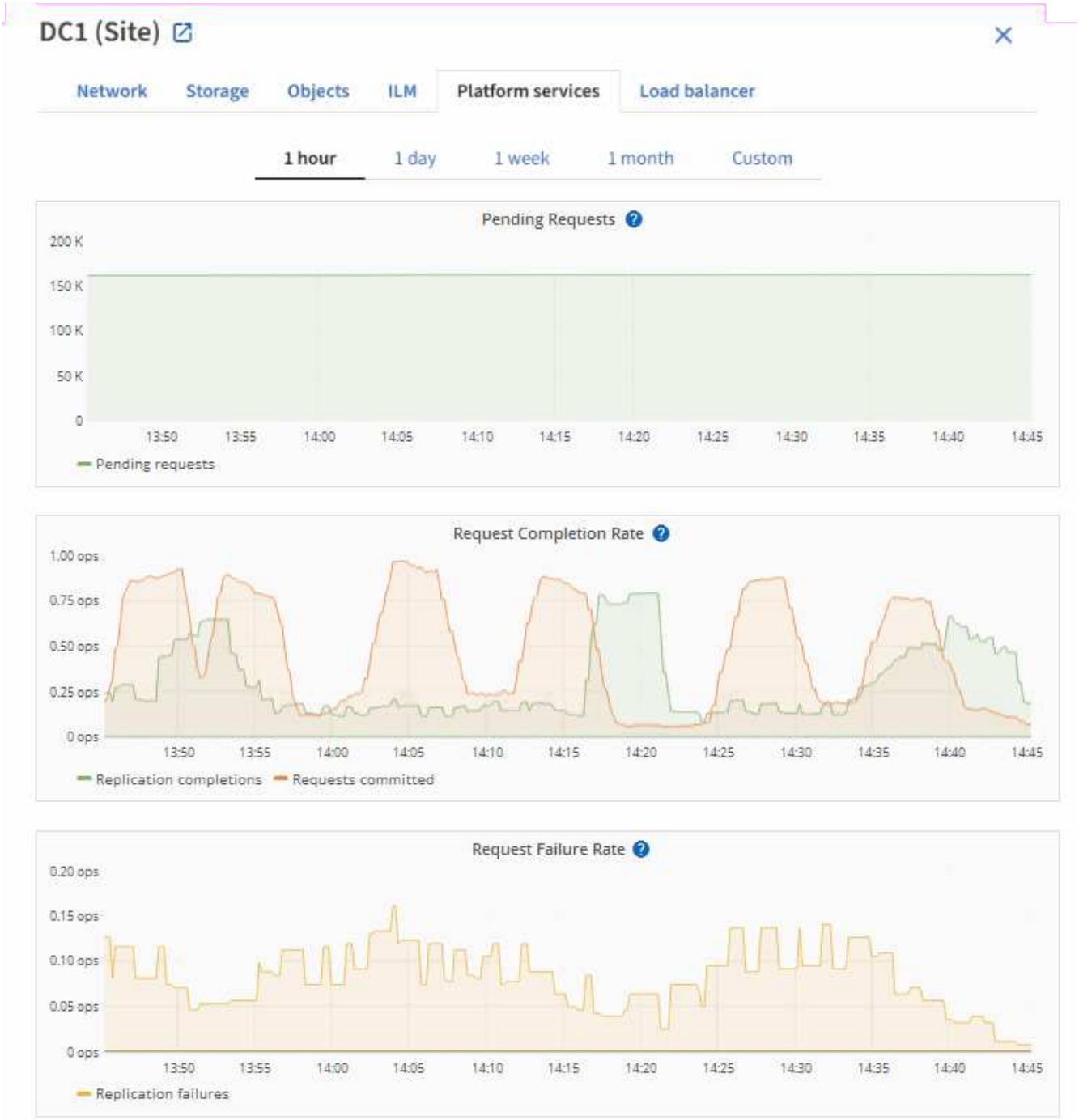
nehmen. Wenn Sie die Performance deutlich schlechter erkennen, sollten Sie die Aufnahmerate reduzieren oder einen Endpunkt mit höherer Kapazität verwenden. Falls der Rückstand von Anforderungen weiterhin wächst, scheitern Client-S3-Vorgänge (wie Z. B. PUT-Anforderungen) letztendlich.

CloudMirror-Anforderungen sind wahrscheinlicher von der Performance des Zielendpunkts betroffen, da diese Anfragen in der Regel mehr Datentransfer beinhalten als Anfragen zur Suchintegration oder Ereignisbenachrichtigung.

Plattformdienstanfragen schlagen fehl

So zeigen Sie die Ausfallrate der Anfrage für Plattformdienste an:

1. Wählen Sie **KNOTEN**.
2. Wählen Sie ***site* Platform Services**.
3. Zeigen Sie das Diagramm Fehlerrate anfordern an.



Plattformdienste – Warnung nicht verfügbar

Die Warnmeldung **Platform Services nicht verfügbar** zeigt an, dass an einem Standort keine Plattformservicevorgänge ausgeführt werden können, da zu wenige Speicherknoten mit dem RSM-Dienst ausgeführt oder verfügbar sind.

Der RSM-Dienst stellt sicher, dass Plattformserviceanforderungen an die jeweiligen Endpunkte gesendet werden.

Um diese Warnmeldung zu beheben, legen Sie fest, welche Speicherknoten am Standort den RSM-Service enthalten. (Der RSM-Service ist auf Speicherknoten vorhanden, die auch den ADC-Service enthalten.) Stellen Sie anschließend sicher, dass ein einfacher Großteil dieser Speicherknoten ausgeführt und verfügbar ist.

Wenn mehr als ein Speicherknoten, der den RSM-Dienst enthält, an einem Standort ausfällt, verlieren Sie alle ausstehenden Plattformserviceanforderungen für diesen Standort.

Zusätzliche Anleitung zur Fehlerbehebung für Endpunkte von Plattformservices

Weitere Informationen über die Problembehandlung von Endpunkten für Plattformdienste finden Sie in den Anweisungen für Verwenden eines Mandantenkontos.

Verwandte Informationen

- Monitoring und Fehlerbehebung
- Konfigurieren Sie Speicher-Proxy-Einstellungen

Management von S3 Select für Mandantenkonten

Bestimmte S3-Mandanten können S3 Select verwenden, um SelectObjectContent-Anfragen für einzelne Objekte auszulösen.

S3 Select bietet eine effiziente Möglichkeit, große Datenmengen zu durchsuchen, ohne eine Datenbank und zugehörige Ressourcen bereitstellen zu müssen, um die Suche zu ermöglichen. Es senkt auch die Kosten und die Latenz beim Abrufen der Daten.

Was ist S3 Select?

Mit S3 Select können S3-Clients SelectObjectContent-Anfragen verwenden, um nur die von einem Objekt benötigten Daten zu filtern und abzurufen. Die StorageGRID Implementierung von S3 Select enthält eine Untergruppe von S3 Select-Befehlen und -Funktionen.

Überlegungen und Anforderungen bei der Verwendung von S3 Select

StorageGRID erfordert für S3 Select-Abfragen Folgendes:

- Das Objekt, das Sie abfragen möchten, ist im CSV-Format oder eine komprimierte Datei mit GZIP oder BZIP2, die eine Datei im CSV-Format enthält.
- Mandanten müssen vom Grid-Administrator die S3-Select-Fähigkeit erhalten. Wählen Sie **S3-Auswahl zulassen** aus, wann Erstellen eines Mandanten Oder Bearbeiten eines Mandanten.
- Die SelectObjectContent-Anforderung muss an ein gesendet werden Endpunkt des StorageGRID-Load-Balancer. Die vom Endpunkt verwendeten Admin- und Gateway-Nodes müssen SG100- oder SG1000-Appliance-Nodes oder VMware-basierte Software-Nodes sein.

Beachten Sie die folgenden Einschränkungen:

- Bare-Metal-Load-Balancer-Nodes werden nicht unterstützt.
- Abfragen können nicht direkt an Speicherknoten gesendet werden.
- Abfragen, die über den veralteten CLB-Dienst gesendet wurden, werden nicht unterstützt.

SelectObjectContent-Anforderungen können die Load Balancer-Performance für alle S3-Clients und alle Mandanten reduzieren. Aktivieren Sie diese Funktion nur bei Bedarf und nur für vertrauenswürdige Mandanten.

Siehe Anweisungen zur Verwendung von S3 Select.

Um sie anzuzeigen Grafana-Diagramme Für S3 Wählen Sie im Grid Manager Operationen im Zeitdauer aus, wählen Sie im Grid Manager * SUPPORT* **Tools Metrics** aus.

Konfiguration von S3- und Swift-Client-Verbindungen

Informationen zu S3- und Swift-Client-Verbindungen

Als Grid-Administrator managen Sie die Konfigurationsoptionen, die steuern, wie S3- und Swift-Mandanten Client-Applikationen mit Ihrem StorageGRID-System verbinden können, um Daten zu speichern und abzurufen. Es stehen verschiedene Optionen zur Verfügung, um verschiedene Anforderungen von Kunden und Mandanten zu erfüllen.

Client-Applikationen können Objekte speichern oder abrufen, indem sie eine Verbindung mit folgenden Komponenten herstellen:

- Der Lastverteilungsservice an Admin-Nodes oder Gateway-Nodes oder optional die virtuelle IP-Adresse einer HA-Gruppe (High Availability, Hochverfügbarkeit) von Admin-Nodes oder Gateway-Nodes
- Der CLB-Dienst auf Gateway-Knoten oder optional die virtuelle IP-Adresse einer Hochverfügbarkeitsgruppe von Gateway-Knoten

> Der CLB-Service ist veraltet. Clients, die vor der Version StorageGRID 11.3 konfiguriert wurden, können den CLB-Service auf Gateway-Knoten weiterhin verwenden. Alle anderen Client-Applikationen, die zum Lastausgleich vom StorageGRID abhängig sind, sollten über den Load Balancer Service eine Verbindung herstellen.

- Storage-Nodes mit oder ohne externen Load Balancer

Auf dem StorageGRID-System können Sie optional die folgenden Funktionen konfigurieren:

- **VLAN-Schnittstellen**: Sie können virtuelle LAN-Schnittstellen (VLAN) auf Admin-Knoten und Gateway-Knoten erstellen, um Client- und Mandantenverkehr zu isolieren und zu partitionieren, um Sicherheit, Flexibilität und Leistung zu erzielen. Nach dem Erstellen einer VLAN-Schnittstelle fügen Sie sie einer HA-Gruppe (High Availability, Hochverfügbarkeit) hinzu.
- **Hochverfügbarkeitsgruppen**: Sie können eine HA-Gruppe der Schnittstellen für Gateway-Nodes oder Admin-Nodes erstellen, um eine aktiv/aktiv-Backup-Konfiguration zu erstellen, oder Round-Robin-DNS oder einen Load Balancer eines Drittanbieters und mehrere HA-Gruppen verwenden, um eine aktiv/aktiv-Konfiguration zu erreichen. Client-Verbindungen werden mithilfe der virtuellen IP-Adressen der HA-Gruppen hergestellt.
- **Load Balancer Service**: Sie können Clients den Load Balancer Service durch die Erstellung von Load Balancer Endpunkten für Client-Verbindungen verwenden. Beim Erstellen eines Load Balancer-Endpunkts geben Sie eine Portnummer an, ob der Endpunkt HTTP- oder HTTPS-Verbindungen akzeptiert, der Client-Typ (S3 oder Swift), der den Endpunkt verwendet, und das Zertifikat, das für HTTPS-Verbindungen verwendet werden soll (falls zutreffend).
- **UnTrusted Client Network**: Sie können das Client-Netzwerk sicherer machen, indem Sie es als unvertrauenswürdig konfigurieren. Wenn das Client-Netzwerk nicht vertrauenswürdig ist, können Clients nur über Load Balancer-Endpunkte eine Verbindung herstellen.

Sie können auch die Verwendung von HTTP für Clients aktivieren, die eine Verbindung zu StorageGRID entweder direkt zu Storage-Nodes oder über den CLB-Dienst (veraltet) herstellen, und Sie können S3-API-Endpunktdomänennamen für S3-Clients konfigurieren.

Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen

Client-Applikationen können sich mithilfe der IP-Adresse eines Grid-Node und der Port-Nummer eines Service auf diesem Node mit StorageGRID verbinden. Bei Konfiguration von Hochverfügbarkeitsgruppen (High Availability, HA) können Client-Applikationen eine Verbindung über die virtuelle IP-Adresse der HA-Gruppe herstellen.

Über diese Aufgabe

In dieser Tabelle sind die verschiedenen Verbindungsmethoden aufgeführt, mit denen Clients eine Verbindung zu StorageGRID herstellen können, sowie die für den jeweiligen Verbindungstyp verwendeten IP-Adressen und Ports. Die Anleitung beschreibt das Auffinden dieser Informationen im Grid Manager, wenn die Endpunkte des Load Balancer und Gruppen für Hochverfügbarkeit (HA) bereits konfiguriert sind.

Wo eine Verbindung hergestellt wird	Dienst, mit dem der Client verbunden ist	IP-Adresse	Port
HA-Gruppe	Lastausgleich	Virtuelle IP-Adresse einer HA-Gruppe	• Endpunkt-Port des Load Balancer
HA-Gruppe	CLB **Hinweis:** der CLB-Service ist veraltet.	Virtuelle IP-Adresse einer HA-Gruppe	S3-Standard-Ports: • HTTPS: 8082 • HTTP: 8084 Swift-Standardports: • HTTPS:8083 • HTTP:8085
Admin-Node	Lastausgleich	IP-Adresse des Admin-Knotens	• Endpunkt-Port des Load Balancer
Gateway-Node	Lastausgleich	IP-Adresse des Gateway-Node	• Endpunkt-Port des Load Balancer
Gateway-Node	CLB **Hinweis:** der CLB-Service ist veraltet.	IP-Adresse des Gateway-Node **Hinweis:** standardmäßig sind HTTP-Ports für CLB und LDR nicht aktiviert.	S3-Standard-Ports: • HTTPS: 8082 • HTTP: 8084 Swift-Standardports: • HTTPS:8083 • HTTP:8085

Wo eine Verbindung hergestellt wird	Dienst, mit dem der Client verbunden ist	IP-Adresse	Port
Storage-Node	LDR	IP-Adresse des Speicherknoten	S3-Standard-Ports: • HTTPS: 18082 • HTTP: 18084 Swift-Standardports: • HTTPS: 18083 • HTTP:18085

Beispiele

Verwenden Sie eine strukturierte URL, wie unten gezeigt, um einen S3-Client mit dem Load Balancer-Endpunkt einer HA-Gruppe von Gateway-Nodes zu verbinden:

- `https://VIP-of-HA-group:LB-endpoint-port`

Wenn beispielsweise die virtuelle IP-Adresse der HA-Gruppe 192.0.2.5 lautet und die Portnummer eines S3 Load Balancer Endpunkts 10443 ist, kann ein S3-Client die folgende URL zur Verbindung mit StorageGRID verwenden:

- `https://192.0.2.5:10443`

Verwenden Sie eine strukturierte URL, wie unten gezeigt, um einen Swift-Client mit dem Load Balancer-Endpunkt einer HA-Gruppe von Gateway-Nodes zu verbinden:

- `https://VIP-of-HA-group:LB-endpoint-port`

Wenn beispielsweise die virtuelle IP-Adresse der HA-Gruppe 192.0.2.6 lautet und die Portnummer eines Swift Load Balancer Endpunkts 10444 ist, kann ein Swift-Client die folgende URL zur Verbindung mit StorageGRID verwenden:

- `https://192.0.2.6:10444`

Ein DNS-Name kann für die IP-Adresse konfiguriert werden, die Clients zum Herstellen der Verbindung mit StorageGRID verwenden. Wenden Sie sich an Ihren Netzwerkadministrator vor Ort.

Schritte

1. Melden Sie sich mit einem bei Grid Manager an Unterstützter Webbrowser.
2. So suchen Sie die IP-Adresse eines Grid-Knotens:
   a. Wählen Sie **KNOTEN**.
   b. Wählen Sie den Admin-Node, Gateway-Node oder Storage-Node aus, mit dem Sie eine Verbindung herstellen möchten.
   c. Wählen Sie die Registerkarte **Übersicht**.
   d. Notieren Sie im Abschnitt Node-Informationen die IP-Adressen für den Node.
   e. Wählen Sie **Mehr anzeigen**, um IPv6-Adressen und Schnittstellen-Zuordnungen anzuzeigen.

      Sie können Verbindungen von Client-Anwendungen zu einer beliebigen IP-Adresse in der Liste

herstellen:

- **Eth0:** Grid Network
- **Eth1:** Admin-Netzwerk (optional)
- **Eth2:** Client-Netzwerk (optional)

> Wenn ein Admin-Node oder ein Gateway-Node angezeigt wird und dieser in einer Hochverfügbarkeitsgruppe der aktive Node ist, wird auf eth2 die virtuelle IP-Adresse der HA-Gruppe angezeigt.

3. So finden Sie die virtuelle IP-Adresse einer Hochverfügbarkeitsgruppe:
   a. Wählen Sie **KONFIGURATION Netzwerk Hochverfügbarkeitsgruppen**.
   b. Notieren Sie in der Tabelle die virtuelle IP-Adresse der HA-Gruppe.
4. So finden Sie die Portnummer eines Load Balancer-Endpunkts:
   a. Wählen Sie **KONFIGURATION Netzwerk Load Balancer-Endpunkte** aus.

      Die Seite Load Balancer Endpoints wird angezeigt und zeigt die Liste der bereits konfigurierten Endpunkte an.

   b. Wählen Sie einen Endpunkt aus, und wählen Sie **Endpunkt bearbeiten**.

      Das Fenster Endpunkt bearbeiten wird geöffnet und zeigt weitere Details zum Endpunkt an.

   c. Bestätigen Sie, dass der ausgewählte Endpunkt für die Verwendung mit dem korrekten Protokoll konfiguriert ist (S3 oder Swift), und wählen Sie dann **Abbrechen**.
   d. Notieren Sie sich die Portnummer für den Endpunkt, den Sie für eine Clientverbindung verwenden möchten.

> Wenn die Portnummer 80 oder 443 ist, wird der Endpunkt nur auf Gateway-Knoten konfiguriert, da diese Ports auf Admin-Nodes reserviert sind. Alle anderen Ports werden sowohl an Gateway-Knoten als auch an Admin-Nodes konfiguriert.

Konfigurieren Sie die VLAN-Schnittstellen

Sie können virtuelle LAN-Schnittstellen (VLAN) auf Admin-Nodes und Gateway-Nodes erstellen und diese in HA-Gruppen und Load Balancer-Endpunkten verwenden, um den Datenverkehr für Sicherheit, Flexibilität und Performance zu isolieren und zu partitionieren.

Überlegungen zu VLAN-Schnittstellen

- Sie erstellen eine VLAN-Schnittstelle, indem Sie eine VLAN-ID eingeben und eine übergeordnete Schnittstelle auf einem oder mehreren Nodes auswählen.
- Eine übergeordnete Schnittstelle muss als Trunk-Schnittstelle am Switch konfiguriert sein.
- Eine übergeordnete Schnittstelle kann das Grid-Netzwerk (eth0), das Client-Netzwerk (eth2) oder eine zusätzliche Trunk-Schnittstelle für die VM oder Bare-Metal-Host (z. B. ens256) sein.
- Sie können für jede VLAN-Schnittstelle nur eine übergeordnete Schnittstelle für einen bestimmten Node auswählen. Sie können beispielsweise nicht sowohl die Grid-Netzwerkschnittstelle als auch die Client-

Netzwerkschnittstelle auf demselben Gateway-Node wie die übergeordnete Schnittstelle für dasselbe VLAN verwenden.

- Wenn die VLAN-Schnittstelle für den Admin-Node-Datenverkehr dient, der Datenverkehr zum Grid-Manager und dem Mandanten-Manager enthält, wählen Sie nur Schnittstellen auf Admin-Nodes aus.
- Wenn die VLAN-Schnittstelle für S3- oder Swift-Client-Datenverkehr dient, wählen Sie Schnittstellen entweder auf Admin-Nodes oder Gateway-Nodes aus.
- Wenn Sie Leitungsbündelschnittstellen hinzufügen müssen, lesen Sie die folgenden Informationen:
  - **VMware (nach der Installation des Knotens)**: VMware: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node
  - **RHEL oder CentOS (vor dem Installieren des Knotens)**: Erstellen von Node-Konfigurationsdateien
  - **Ubuntu oder Debian (vor der Installation des Knotens)**: Erstellen von Node-Konfigurationsdateien
  - **RHEL, CentOS, Ubuntu oder Debian (nach der Installation des Knotens)**: Linux: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node

Erstellen einer VLAN-Schnittstelle

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben die Root-Zugriffsberechtigung.
- Im Netzwerk wurde eine Trunk-Schnittstelle konfiguriert und mit dem VM- oder Linux-Node verbunden. Sie kennen den Namen der Trunk-Schnittstelle.
- Sie kennen die ID des zu konfigurierende VLANs.

Über diese Aufgabe

Ihr Netzwerkadministrator hat möglicherweise eine oder mehrere Trunk-Schnittstellen und ein oder mehrere VLANs konfiguriert, um den Client- oder Admin-Datenverkehr verschiedener Applikationen oder Mandanten zu trennen. Jedes VLAN wird durch eine numerische ID oder ein Tag identifiziert. Beispielsweise könnte Ihr Netzwerk VLAN 100 für FabricPool-Datenverkehr und VLAN 200 für eine Archivierungsanwendung verwenden.

Sie können den Grid-Manager verwenden, um VLAN-Schnittstellen zu erstellen, die Clients den Zugriff auf StorageGRID in einem bestimmten VLAN ermöglichen. Wenn Sie VLAN-Schnittstellen erstellen, geben Sie die VLAN-ID an und wählen Sie übergeordnete Schnittstellen (Trunk) auf einem oder mehreren Nodes aus.

Greifen Sie auf den Assistenten zu

1. Wählen Sie **KONFIGURATION Netzwerk VLAN-Schnittstellen**.
2. Wählen Sie **Erstellen**.

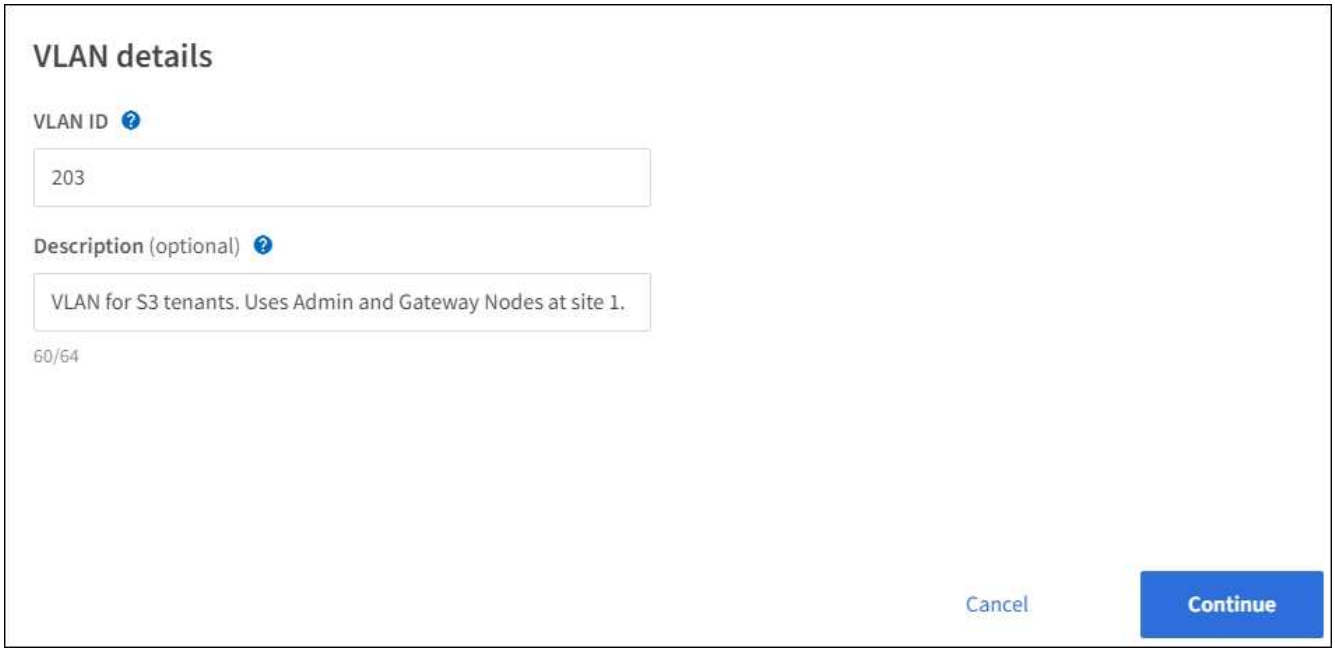
Geben Sie Details zu den VLAN-Schnittstellen ein

1. Geben Sie die ID des VLANs in Ihrem Netzwerk an. Sie können einen beliebigen Wert zwischen 1 und 4094 eingeben.

   VLAN-IDs müssen nicht eindeutig sein. Beispielsweise können Sie die VLAN-ID 200 für den Admin-Datenverkehr an einem Standort und dieselbe VLAN-ID für den Client-Datenverkehr an einem anderen Standort verwenden. Sie können separate VLAN-Schnittstellen mit verschiedenen Gruppen von übergeordneten Schnittstellen an jedem Standort erstellen. Jedoch können zwei VLAN-Schnittstellen mit derselben ID nicht dieselbe Schnittstelle auf einem Node teilen.

Wenn Sie eine ID angeben, die bereits verwendet wurde, wird eine Meldung angezeigt. Sie können mit der Erstellung einer anderen VLAN-Schnittstelle für dieselbe VLAN-ID fortfahren, oder Sie können **Abbrechen** auswählen und dann die vorhandene ID bearbeiten.

2. Geben Sie optional eine kurze Beschreibung für die VLAN-Schnittstelle ein.



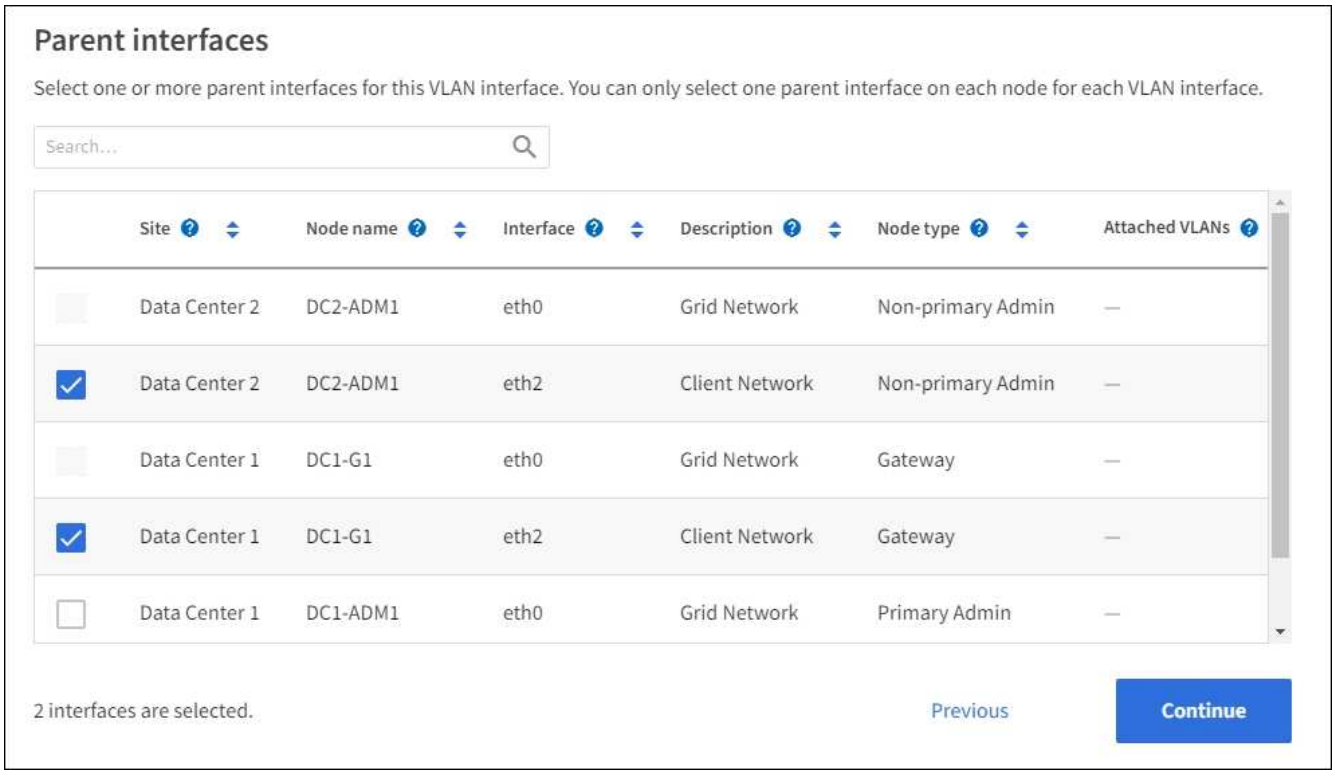
3. Wählen Sie **Weiter**.

Wählen Sie übergeordnete Schnittstellen

In der Tabelle sind die verfügbaren Schnittstellen für alle Admin-Nodes und Gateway-Nodes an jedem Standort im Raster aufgeführt. Admin-Netzwerk-Schnittstellen (eth1) können nicht als übergeordnete Schnittstellen verwendet werden und werden nicht angezeigt.

1. Wählen Sie eine oder mehrere übergeordnete Schnittstellen aus, an die dieses VLAN angeschlossen werden soll.

   Sie möchten beispielsweise ein VLAN an die Schnittstelle „Client Network“ (eth2) für einen Gateway-Node und einen Admin-Node anschließen.



2. Wählen Sie **Weiter**.

Bestätigen Sie die Einstellungen

1. Überprüfen Sie die Konfiguration und nehmen Sie alle Änderungen vor.
   - Wenn Sie die VLAN-ID oder Beschreibung ändern möchten, wählen Sie oben auf der Seite **VLAN-Details eingeben** aus.
   - Wenn Sie eine übergeordnete Schnittstelle ändern möchten, wählen Sie oben auf der Seite die Option **übergeordnete Schnittstellen auswählen** aus, oder wählen Sie **Zurück**.
   - Wenn Sie eine übergeordnete Schnittstelle entfernen müssen, wählen Sie den Papierkorb aus .
2. Wählen Sie **Speichern**.
3. Warten Sie bis zu 5 Minuten, bis die neue Schnittstelle als Auswahl auf der Seite Hochverfügbarkeitsgruppen angezeigt wird und in der Tabelle **Netzwerkschnittstellen** für den Knoten (**NODES *Parent Interface Node* Network**) aufgelistet wird.

Bearbeiten Sie eine VLAN-Schnittstelle

Wenn Sie eine VLAN-Schnittstelle bearbeiten, können Sie die folgenden Arten von Änderungen vornehmen:

- Ändern Sie die VLAN-ID oder -Beschreibung.
- Übergeordnete Schnittstellen hinzufügen oder entfernen.

Sie möchten beispielsweise eine übergeordnete Schnittstelle von einer VLAN-Schnittstelle entfernen, wenn Sie den zugeordneten Node außer Betrieb setzen möchten.

Beachten Sie Folgendes:

- Sie können keine VLAN-ID ändern, wenn die VLAN-Schnittstelle in einer HA-Gruppe verwendet wird.

- Sie können eine übergeordnete Schnittstelle nicht entfernen, wenn diese übergeordnete Schnittstelle in einer HA-Gruppe verwendet wird.

  Nehmen Sie beispielsweise an, dass VLAN 200 an den übergeordneten Schnittstellen auf den Nodes A und B. angeschlossen ist Wenn eine HA-Gruppe die VLAN 200-Schnittstelle für Node A und die eth2-Schnittstelle für Node B verwendet, können Sie die nicht verwendete übergeordnete Schnittstelle für Node B entfernen, Sie können jedoch die verwendete übergeordnete Schnittstelle für Node A nicht entfernen

Schritte

1. Wählen Sie **KONFIGURATION Netzwerk VLAN-Schnittstellen**.
2. Aktivieren Sie das Kontrollkästchen für die VLAN-Schnittstelle, die Sie bearbeiten möchten. Wählen Sie dann **Aktionen Bearbeiten** aus.
3. Optional können Sie die VLAN-ID oder die Beschreibung aktualisieren. Wählen Sie anschließend **Weiter**.

   Sie können keine VLAN-ID aktualisieren, wenn das VLAN in einer HA-Gruppe verwendet wird.

4. Aktivieren Sie optional die Kontrollkästchen, um übergeordnete Schnittstellen hinzuzufügen oder nicht verwendete Schnittstellen zu entfernen. Wählen Sie anschließend **Weiter**.
5. Überprüfen Sie die Konfiguration und nehmen Sie alle Änderungen vor.
6. Wählen Sie **Speichern**.

Entfernen Sie eine VLAN-Schnittstelle

Sie können eine oder mehrere VLAN-Schnittstellen entfernen.

Sie können eine VLAN-Schnittstelle nicht entfernen, wenn sie derzeit in einer HA-Gruppe verwendet wird. Sie müssen die VLAN-Schnittstelle aus der HA-Gruppe entfernen, bevor Sie sie entfernen können.

Um Unterbrechungen des Client-Traffic zu vermeiden, sollten Sie einen der folgenden Schritte in Betracht ziehen:

- Fügen Sie einer neuen VLAN-Schnittstelle zur HA-Gruppe hinzu, bevor Sie diese VLAN-Schnittstelle entfernen.
- Erstellen Sie eine neue HA-Gruppe, die diese VLAN-Schnittstelle nicht verwendet.
- Wenn die VLAN-Schnittstelle, die Sie entfernen möchten, derzeit die aktive Schnittstelle ist, bearbeiten Sie die HA-Gruppe. Verschieben Sie die VLAN-Schnittstelle, die Sie entfernen möchten, auf die Unterseite der Prioritätenliste. Warten Sie, bis die Kommunikation auf der neuen primären Schnittstelle eingerichtet ist, und entfernen Sie dann die alte Schnittstelle aus der HA-Gruppe. Schließlich, löschen Sie die VLAN-Schnittstelle auf diesem Knoten.

Schritte

1. Wählen Sie **KONFIGURATION Netzwerk VLAN-Schnittstellen**.
2. Aktivieren Sie das Kontrollkästchen für jede VLAN-Schnittstelle, die Sie entfernen möchten. Wählen Sie dann **Aktionen Löschen** aus.
3. Wählen Sie **Ja**, um Ihre Auswahl zu bestätigen.

   Alle ausgewählten VLAN-Schnittstellen werden entfernt. Auf der Seite VLAN-Schnittstellen wird ein grünes Erfolgsbanner angezeigt.

Management von Hochverfügbarkeitsgruppen

Verwaltung von Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen): Übersicht

Die Netzwerkschnittstellen mehrerer Admin- und Gateway-Nodes können in einer HA-Gruppe (High Availability, Hochverfügbarkeit) gruppieren. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle den Workload verwalten.

Was ist eine HA-Gruppe?

Darüber hinaus können HA-Gruppen (High Availability, Hochverfügbarkeit) für hochverfügbare Datenverbindungen für S3 und Swift Clients verwendet oder hochverfügbare Verbindungen mit dem Grid Manager und dem Mandanten Manager hergestellt werden.

Jede HA-Gruppe bietet Zugriff auf die Shared Services auf den ausgewählten Nodes.

- HA-Gruppen, die Gateway-Nodes, Admin-Nodes oder beide umfassen, bieten hochverfügbare Datenverbindungen für S3- und Swift-Clients.
- HA-Gruppen, die nur Admin-Nodes enthalten, bieten hochverfügbare Verbindungen zum Grid Manager und dem Mandanten-Manager.
- Eine HA-Gruppe, die nur SG100- oder SG1000-Appliances und VMware-basierte Software-Nodes enthält, kann für hochverfügbare Verbindungen bereitstellen S3-Mandanten, die S3 Select nutzen. HA-Gruppen werden empfohlen, wenn S3 Select verwendet wird, jedoch nicht erforderlich.

Wie erstellen Sie eine HA-Gruppe?

1. Sie wählen eine Netzwerkschnittstelle für einen oder mehrere Admin-Nodes oder Gateway-Knoten aus. Sie können eine Grid Network (eth0)-Schnittstelle, eine eth2-Schnittstelle (Client Network), eine VLAN-Schnittstelle oder eine Access-Interface verwenden, die Sie dem Node hinzugefügt haben.

   > Sie können einer HA-Gruppe keine Schnittstelle hinzufügen, wenn ihr eine DHCP-zugewiesene IP-Adresse zugewiesen ist.

2. Sie geben an, dass die primäre Schnittstelle sein soll. Die primäre Schnittstelle ist die aktive Schnittstelle, sofern kein Fehler auftritt.
3. Sie bestimmen die Prioritätsreihenfolge für alle Backup-Schnittstellen.
4. Sie weisen der Gruppe eine bis 10 virtuelle IP-Adressen (VIP) zu. Client-Anwendungen können eine dieser VIP-Adressen verwenden, um eine Verbindung zu StorageGRID herzustellen.

Anweisungen hierzu finden Sie unter Konfigurieren Sie Hochverfügbarkeitsgruppen.

Was ist die aktive Schnittstelle?

Im normalen Betrieb werden alle VIP-Adressen für die HA-Gruppe der primären Schnittstelle hinzugefügt, die die erste Schnittstelle in der Prioritätsreihenfolge ist. Solange die primäre Schnittstelle verfügbar bleibt, wird sie verwendet, wenn sich Clients mit einer beliebigen VIP-Adresse für die Gruppe verbinden. Das heißt, während des normalen Betriebs ist die primäre Schnittstelle die Schnittstelle „`Active`“ für die Gruppe.

Ebenso fungieren alle Schnittstellen mit niedriger Priorität für die HA-Gruppe im normalen Betrieb als „`Backup`“-Schnittstellen. Diese Backup-Schnittstellen werden nur verwendet, wenn die primäre (derzeit aktive) Schnittstelle nicht mehr verfügbar ist.

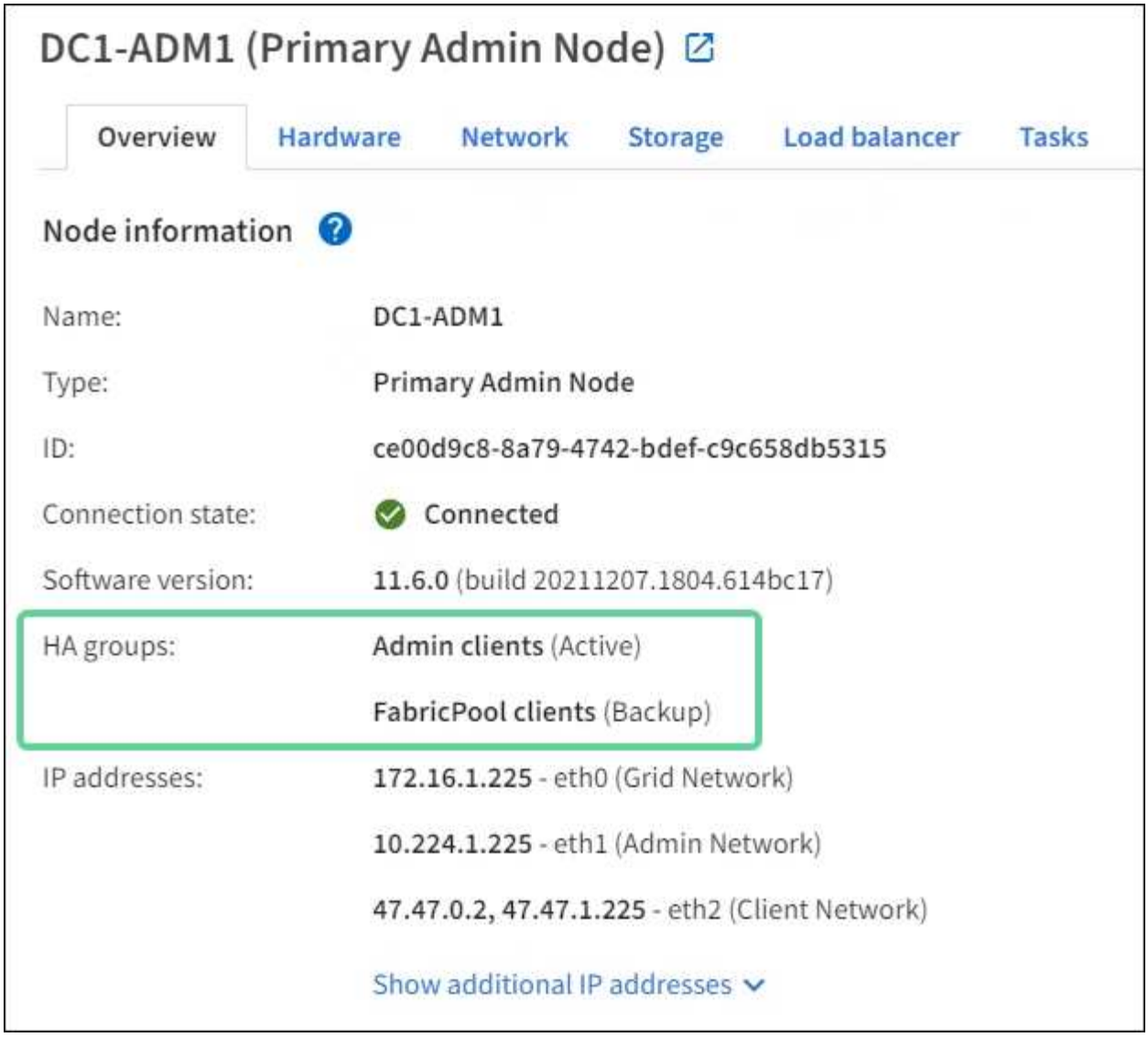
Anzeigen des aktuellen HA-Gruppen-Status eines Node

Um zu ermitteln, ob ein Node einer HA-Gruppe zugewiesen ist und seinen aktuellen Status ermittelt, wählen Sie **NODES** ***Node*** aus.

Wenn die Registerkarte **Übersicht** einen Eintrag für **HA-Gruppen** enthält, wird der Knoten den aufgeführten HA-Gruppen zugewiesen. Der Wert nach dem Gruppennamen ist der aktuelle Status des Node in der HA-Gruppe:

- **Aktiv**: Die HA-Gruppe wird derzeit auf diesem Knoten gehostet.
- **Backup**: Die HA-Gruppe benutzt derzeit nicht diesen Knoten; dies ist ein Backup Interface.
- **Angehalten**: Die HA-Gruppe kann nicht auf diesem Knoten gehostet werden, da der Service für hohe Verfügbarkeit (keepalived) manuell beendet wurde.
- **Fehler**: Die HA-Gruppe kann auf diesem Node nicht gehostet werden, weil einer oder mehrere der folgenden Gründe:
  - Der Lastverteilungsservice (nginx-gw) wird auf dem Knoten nicht ausgeführt.
  - Die eth0- oder VIP-Schnittstelle des Node ist nicht aktiv.
  - Der Node ist ausgefallen.

In diesem Beispiel wurde der primäre Admin-Node zwei HA-Gruppen hinzugefügt. Dieser Knoten ist derzeit die aktive Schnittstelle für die Gruppe Admin-Clients und eine Sicherungsschnittstelle für die Gruppe FabricPool-Clients.



Was geschieht, wenn die aktive Schnittstelle ausfällt?

Die Schnittstelle, die derzeit die VIP-Adressen hostet, ist die aktive Schnittstelle. Wenn die HA-Gruppe mehrere Schnittstellen umfasst und die aktive Schnittstelle ausfällt, verschieben sich die VIP-Adressen auf die erste verfügbare Backup-Schnittstelle in der Prioritätsreihenfolge. Wenn diese Schnittstelle ausfällt, wechseln die VIP-Adressen zur nächsten verfügbaren Backup-Schnittstelle usw.

Ein Failover kann aus einem der folgenden Gründe ausgelöst werden:

- Der Node, auf dem die Schnittstelle konfiguriert ist, schaltet sich aus.
- Der Node, auf dem die Schnittstelle konfiguriert ist, verliert mindestens 2 Minuten lang die Verbindung zu allen anderen Nodes.
- Die aktive Schnittstelle ausfällt.
- Der Lastverteiler-Dienst wird angehalten.
- Der High Availability Service stoppt.

Der Failover wird möglicherweise nicht durch Netzwerkausfälle außerhalb des Node ausgelöst, der die aktive Schnittstelle hostet. Ebenso wird der Failover nicht durch den Ausfall des CLB-Dienstes (veraltet) oder der Dienste für den Grid-Manager oder den Mandanten-Manager ausgelöst.

Der Failover-Prozess dauert in der Regel nur wenige Sekunden und ist schnell genug, dass Client-Applikationen nur geringe Auswirkungen haben und sich auf normale Wiederholungsmuster verlassen können, um den Betrieb fortzusetzen.

Wenn ein Fehler behoben ist und eine Schnittstelle mit höherer Priorität wieder verfügbar wird, werden die VIP-Adressen automatisch auf die verfügbare Schnittstelle mit der höchsten Priorität verschoben.

Wie werden HA-Gruppen verwendet?

Es können HA-Gruppen (High Availability, Hochverfügbarkeit) verwendet werden, um hochverfügbare Verbindungen zu StorageGRID für Objektdaten und zur Verwendung durch den Administrator zur Verfügung zu stellen.

- Eine HA-Gruppe kann hochverfügbare administrative Verbindungen mit dem Grid Manager oder dem Mandanten Manager bereitstellen.
- Eine HA-Gruppe kann hochverfügbare Datenverbindungen für S3 und Swift Clients bieten.
- Eine HA-Gruppe, die nur eine Schnittstelle enthält, ermöglicht es Ihnen, viele VIP-Adressen bereitzustellen und explizit IPv6-Adressen festzulegen.

Eine HA-Gruppe kann nur Hochverfügbarkeit bieten, wenn alle Nodes in der Gruppe dieselben Services bereitstellen. Wenn Sie eine HA-Gruppe erstellen, fügen Sie Schnittstellen von den Typen von Nodes hinzu, die die erforderlichen Services bereitstellen.

- **Admin Nodes**: Schließen Sie den Load Balancer Service ein und ermöglichen Sie den Zugriff auf den Grid Manager oder den Tenant Manager.
- **Gateway-Knoten**: Schließen Sie den Load Balancer Service und den CLB-Dienst (veraltet) ein.

Zweck der HA-Gruppe	Fügen Sie diesem Typ Nodes der HA-Gruppe hinzu
Zugriff auf Grid Manager	• Primärer Admin-Node (**Primär**) • Nicht primäre Admin-Nodes **Hinweis:** der primäre Admin-Knoten muss die primäre Schnittstelle sein. Einige Wartungsvorgänge können nur vom primären Admin-Node ausgeführt werden.
Zugriff nur auf Tenant Manager	• Primäre oder nicht primäre Admin-Nodes
S3- oder Swift-Client-Zugriff – Load Balancer Service	• Admin-Nodes • Gateway-Nodes

Zweck der HA-Gruppe	Fügen Sie diesem Typ Nodes der HA-Gruppe hinzu
S3-Client-Zugriff für S3 Select	• SG100- oder SG1000-Appliances • VMware-basierte Software-Nodes **Hinweis**: HA-Gruppen werden bei der Verwendung von S3 Select empfohlen, aber nicht erforderlich.
S3- oder Swift-Client-Zugriff — CLB-Service **Hinweis:** der CLB-Service ist veraltet.	• Gateway-Nodes

Einschränkungen bei der Verwendung von HA-Gruppen mit Grid Manager oder Tenant Manager

Wenn ein Grid Manager oder der Tenant Manager-Dienst ausfällt, wird das Failover von HA-Gruppen nicht ausgelöst.

Wenn Sie sich bei einem Failover beim Grid Manager oder beim Tenant Manager angemeldet haben, werden Sie abgemeldet und müssen sich erneut anmelden, um Ihre Aufgabe fortzusetzen.

Einige Wartungsvorgänge können nicht ausgeführt werden, wenn der primäre Admin-Node nicht verfügbar ist. Während des Failovers können Sie Ihr StorageGRID-System mit dem Grid-Manager überwachen.

Einschränkungen bei der Verwendung von HA-Gruppen mit dem CLB-Service

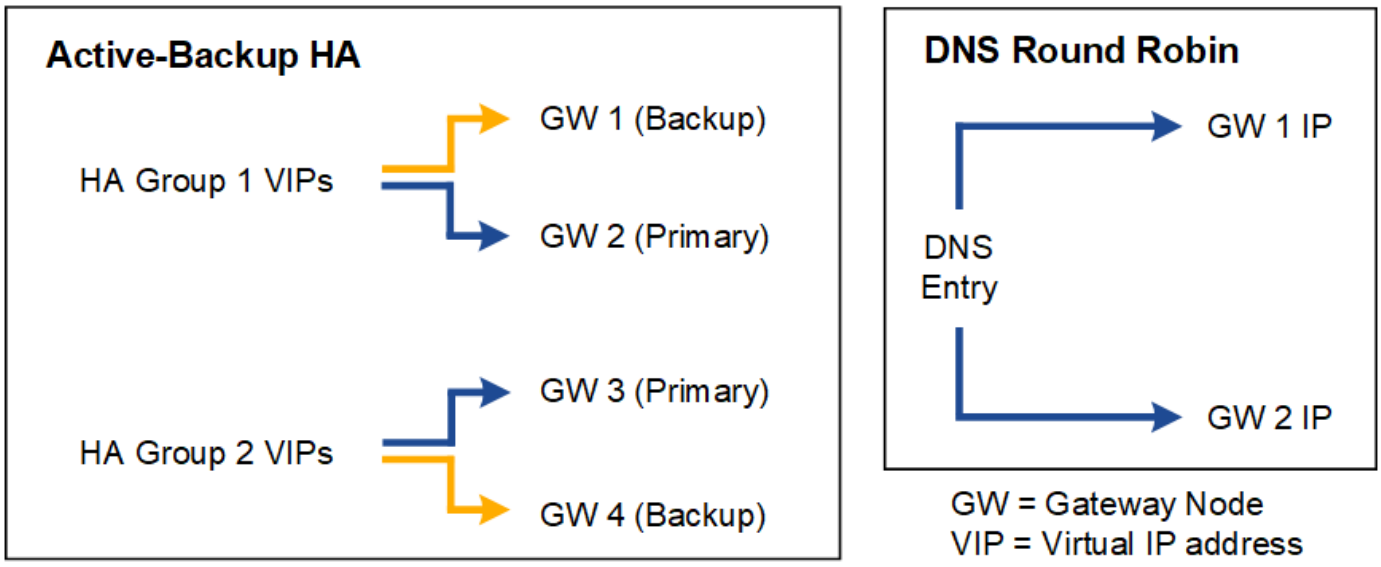
Der Ausfall des CLB-Dienstes löst nicht ein Failover innerhalb der HA-Gruppe aus.

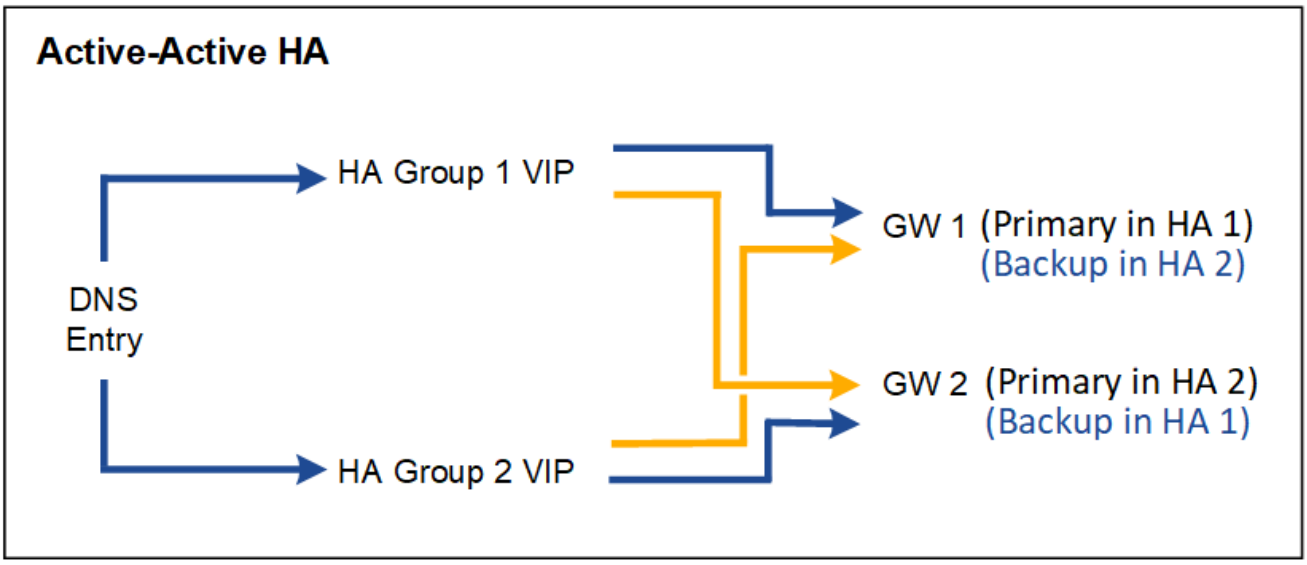
Der CLB-Service ist veraltet.

Konfigurationsoptionen für HA-Gruppen

Die folgenden Diagramme bieten Beispiele für verschiedene Möglichkeiten zum Konfigurieren von HA-Gruppen. Jede Option hat vor- und Nachteile.

In den Diagrammen zeigt blau die primäre Schnittstelle in der HA-Gruppe an und gelb gibt die Backup-Schnittstelle in der HA-Gruppe an.





Die Tabelle enthält eine Zusammenfassung der Vorteile der einzelnen HA-Konfigurationen, die in der Abbildung dargestellt sind.

Konfiguration	Vorteile	Nachteile
Aktiv/Backup HA	• Management über StorageGRID ohne externe Abhängigkeiten • Schnelles Failover.	• In einer HA-Gruppe ist nur ein Node aktiv. Mindestens ein Node pro HA-Gruppe bleibt im Ruhezustand.
DNS Round Robin	• Erhöhter Aggregatdurchsatz: • Keine leerlaufenden Hosts	• Langsamer Failover, der vom Client-Verhalten abhängen kann. • Konfiguration von Hardware außerhalb von StorageGRID erforderlich • Benötigt eine vom Kunden implementierte Zustandsprüfung.

Konfiguration	Vorteile	Nachteile
Aktiv/aktiv-HA	• Der Datenverkehr wird über mehrere HA-Gruppen verteilt. • Hoher Aggregatdurchsatz, der mit der Anzahl der HA-Gruppen skaliert werden kann • Schnelles Failover.	• Komplexer zu konfigurieren. • Konfiguration von Hardware außerhalb von StorageGRID erforderlich • Benötigt eine vom Kunden implementierte Zustandsprüfung.

Konfigurieren Sie Hochverfügbarkeitsgruppen

Sie können Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen) konfigurieren, um hochverfügbaren Zugriff auf die Services in Admin-Nodes oder Gateway-Nodes bereitzustellen.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben die Root-Zugriffsberechtigung.
- Wenn Sie eine VLAN-Schnittstelle in einer HA-Gruppe verwenden möchten, haben Sie die VLAN-Schnittstelle erstellt. Siehe Konfigurieren Sie die VLAN-Schnittstellen.
- Wenn Sie eine Zugriffsoberfläche für einen Node in einer HA-Gruppe verwenden möchten, haben Sie die Schnittstelle erstellt:
  - **Red hat Enterprise Linux oder CentOS (vor der Installation des Knotens)**: Erstellen von Node-Konfigurationsdateien
  - **Ubuntu oder Debian (vor der Installation des Knotens)**: Erstellen von Node-Konfigurationsdateien
  - **Linux (nach der Installation des Knotens)**: Linux: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node
  - **VMware (nach der Installation des Knotens)**: VMware: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node

Erstellen Sie eine Hochverfügbarkeitsgruppe

Wenn Sie eine Hochverfügbarkeitsgruppe erstellen, wählen Sie eine oder mehrere Schnittstellen aus und organisieren sie in Prioritätsreihenfolge. Anschließend weisen Sie der Gruppe eine oder mehrere VIP-Adressen zu.

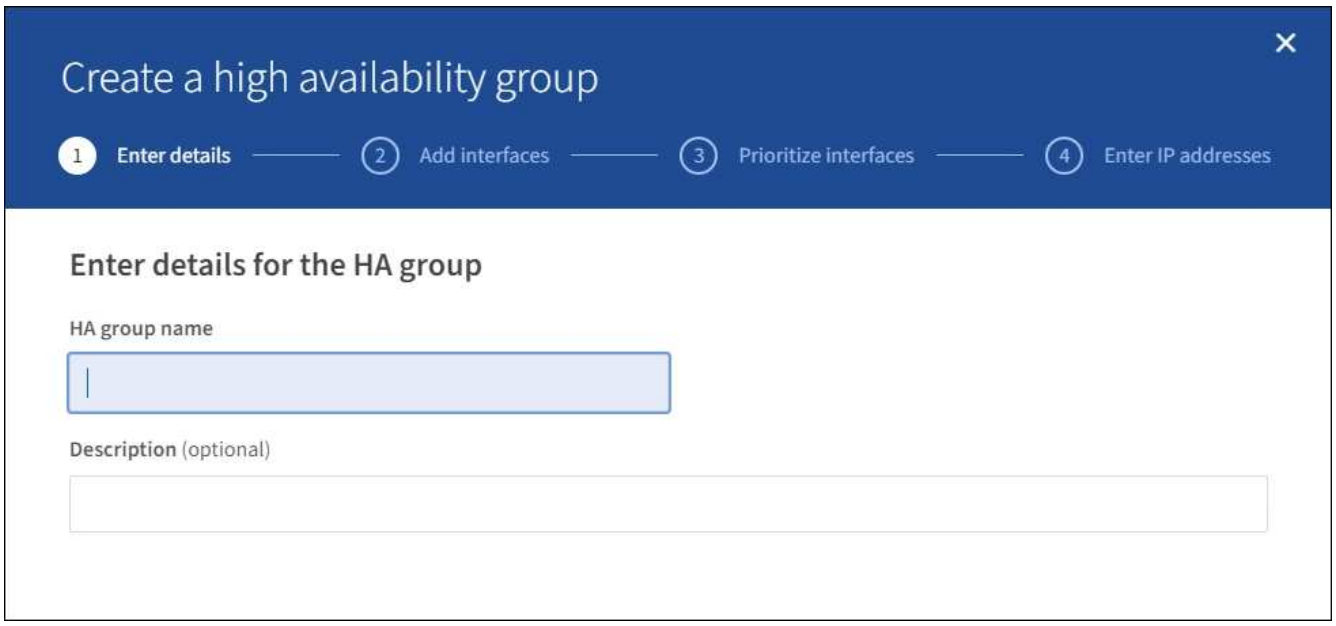
Eine Schnittstelle muss lauten, damit ein Gateway-Node oder ein Admin-Node in einer HA-Gruppe enthalten sein kann. Eine HA-Gruppe kann nur eine Schnittstelle für jeden angegebenen Node verwenden. Jedoch können andere Schnittstellen für denselben Node in anderen HA-Gruppen verwendet werden.

Greifen Sie auf den Assistenten zu

1. Wählen Sie **KONFIGURATION Netzwerk Hochverfügbarkeitsgruppen**.
2. Wählen Sie **Erstellen**.

Geben Sie Details für die HA-Gruppe ein

1. Geben Sie einen eindeutigen Namen für die HA-Gruppe ein.

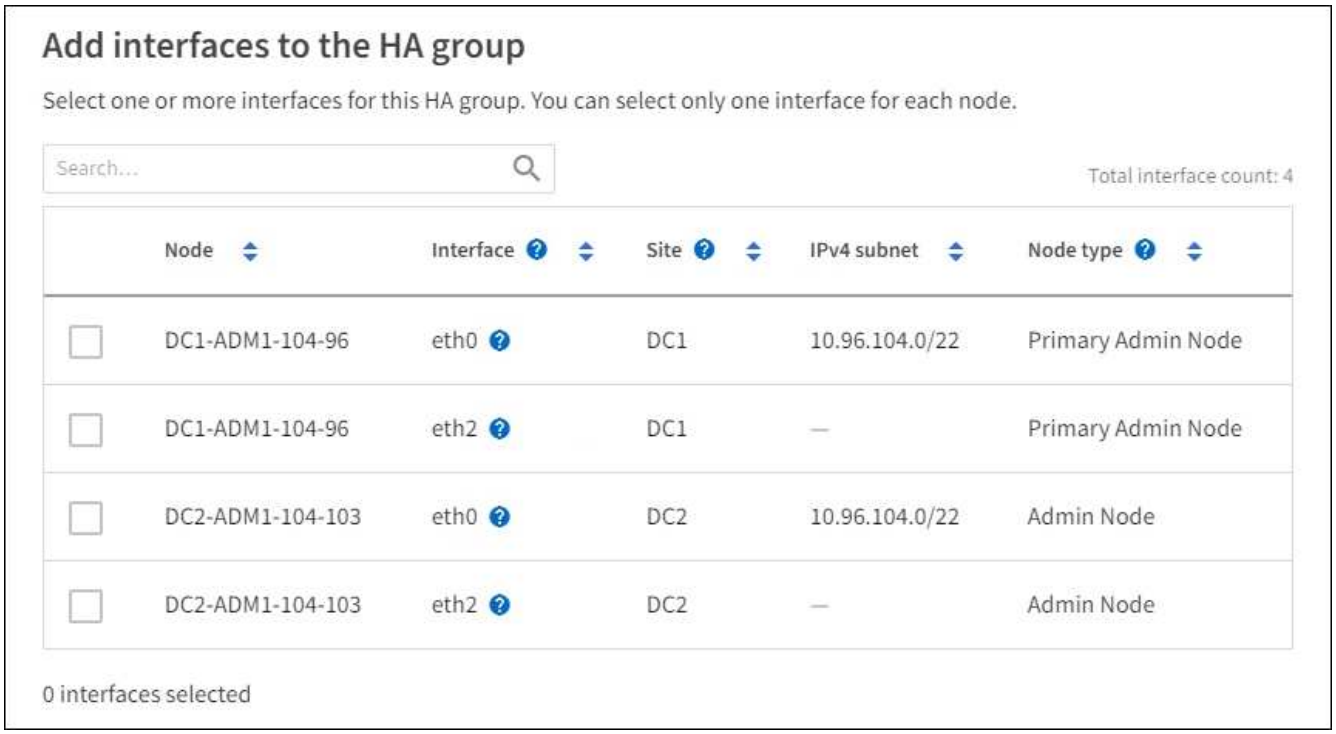


2. Geben Sie optional eine Beschreibung für die HA-Gruppe ein.
3. Wählen Sie **Weiter**.

Fügen Sie der HA-Gruppe Schnittstellen hinzu

1. Wählen Sie eine oder mehrere Schnittstellen aus, die dieser HA-Gruppe hinzugefügt werden sollen.

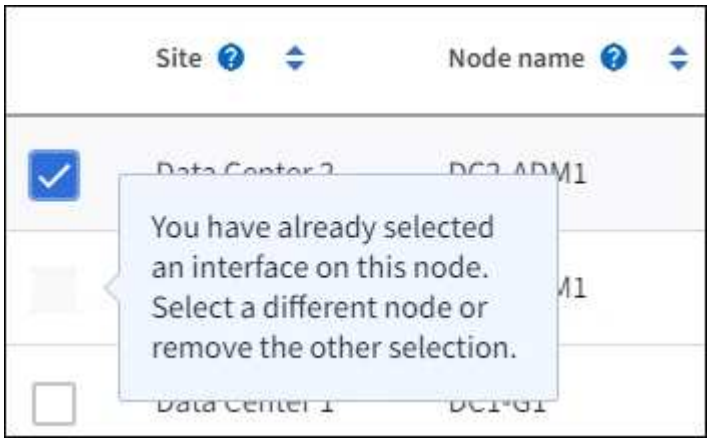
   Verwenden Sie die Spaltenüberschriften, um die Zeilen zu sortieren, oder geben Sie einen Suchbegriff ein, um Schnittstellen schneller zu finden.



Warten Sie nach dem Erstellen einer VLAN-Schnittstelle bis zu 5 Minuten, bis die neue Schnittstelle in der Tabelle angezeigt wird.

Richtlinien für die Auswahl von Schnittstellen

- Sie müssen mindestens eine Schnittstelle auswählen.
- Sie können nur eine Schnittstelle für einen Node auswählen.
- Wenn die HA-Gruppe den HA-Schutz von Admin Node-Services bietet, zu denen der Grid Manager und der MandantenManager gehören, wählen Sie nur Schnittstellen zu Admin-Nodes aus.
- Wenn die HA-Gruppe einen HA-Schutz für den Client-Datenverkehr von S3 oder Swift bietet, wählen Sie Schnittstellen an Admin-Nodes, Gateway Nodes oder beiden.
- Wenn die HA-Gruppe den HA-Schutz des veralteten CLB-Service bietet, wählen Sie nur Schnittstellen auf Gateway-Nodes aus.
- Wenn Sie Schnittstellen für verschiedene Node-Typen auswählen, wird ein Informationshinweis angezeigt. Sie werden daran erinnert, dass bei einem Failover Dienste, die vom zuvor aktiven Knoten bereitgestellt werden, möglicherweise auf dem neu aktiven Knoten nicht verfügbar sind. Beispielsweise kann ein Backup-Gateway-Node keinen HA-Schutz für Admin-Node-Services bereitstellen. Ebenso kann ein Backup-Admin-Node nicht alle Wartungsvorgänge ausführen, die der primäre Admin-Node bereitstellen kann.
- Wenn Sie keine Schnittstelle auswählen können, ist das Kontrollkästchen deaktiviert. Der QuickInfo enthält weitere Informationen.



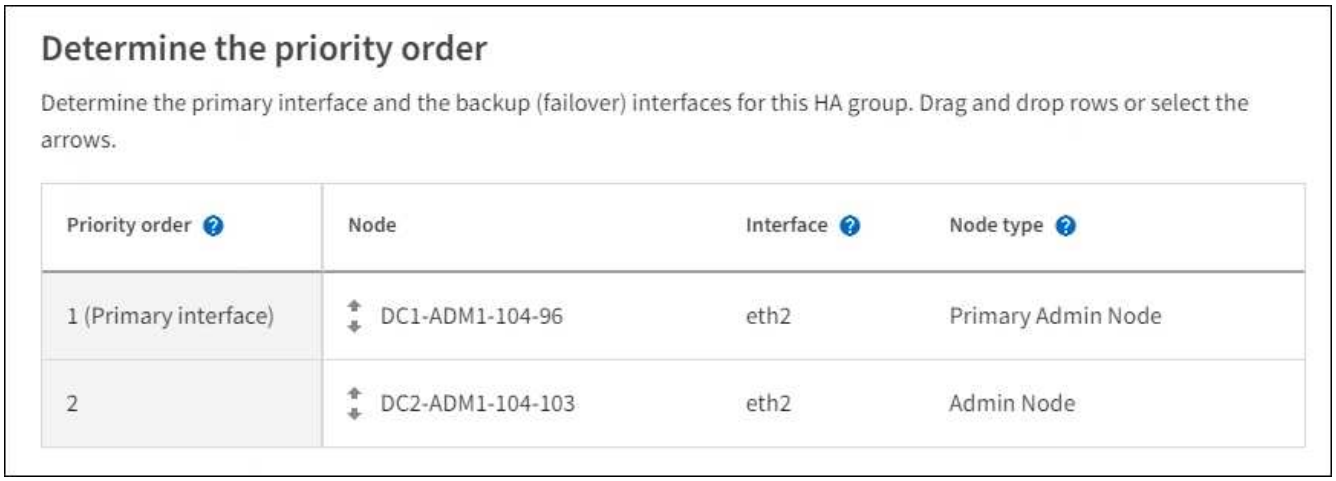
- Sie können keine Schnittstelle auswählen, wenn ihr Subnetz-Wert oder Gateway mit einer anderen ausgewählten Schnittstelle in Konflikt steht.
- Sie können keine konfigurierte Schnittstelle auswählen, wenn sie keine statische IP-Adresse hat.

2. Wählen Sie **Weiter**.

Legen Sie die Prioritätsreihenfolge fest

1. Ermitteln Sie die primäre Schnittstelle und alle Backup-Schnittstellen (Failover) für diese HA-Gruppe.

   Ziehen Sie Zeilen per Drag-and-Drop, um die Werte in der Spalte **Priority Order** zu ändern.



Wenn die HA-Gruppe Zugriff auf den Grid Manager bietet, müssen Sie eine Schnittstelle am primären Admin-Node als primäre Schnittstelle auswählen. Einige Wartungsvorgänge können nur vom primären Admin-Node ausgeführt werden.

Die erste Schnittstelle in der Liste ist die primäre Schnittstelle. Die primäre Schnittstelle ist die aktive Schnittstelle, sofern kein Fehler auftritt.

Wenn die HA-Gruppe mehr als eine Schnittstelle umfasst und die primäre Schnittstelle ausfällt, verschieben die VIP-Adressen auf die verfügbare Schnittstelle mit der höchsten Priorität. Wenn diese Schnittstelle ausfällt, werden die VIP-Adressen zur nächsten verfügbaren Schnittstelle mit der höchsten Priorität usw. verschoben.

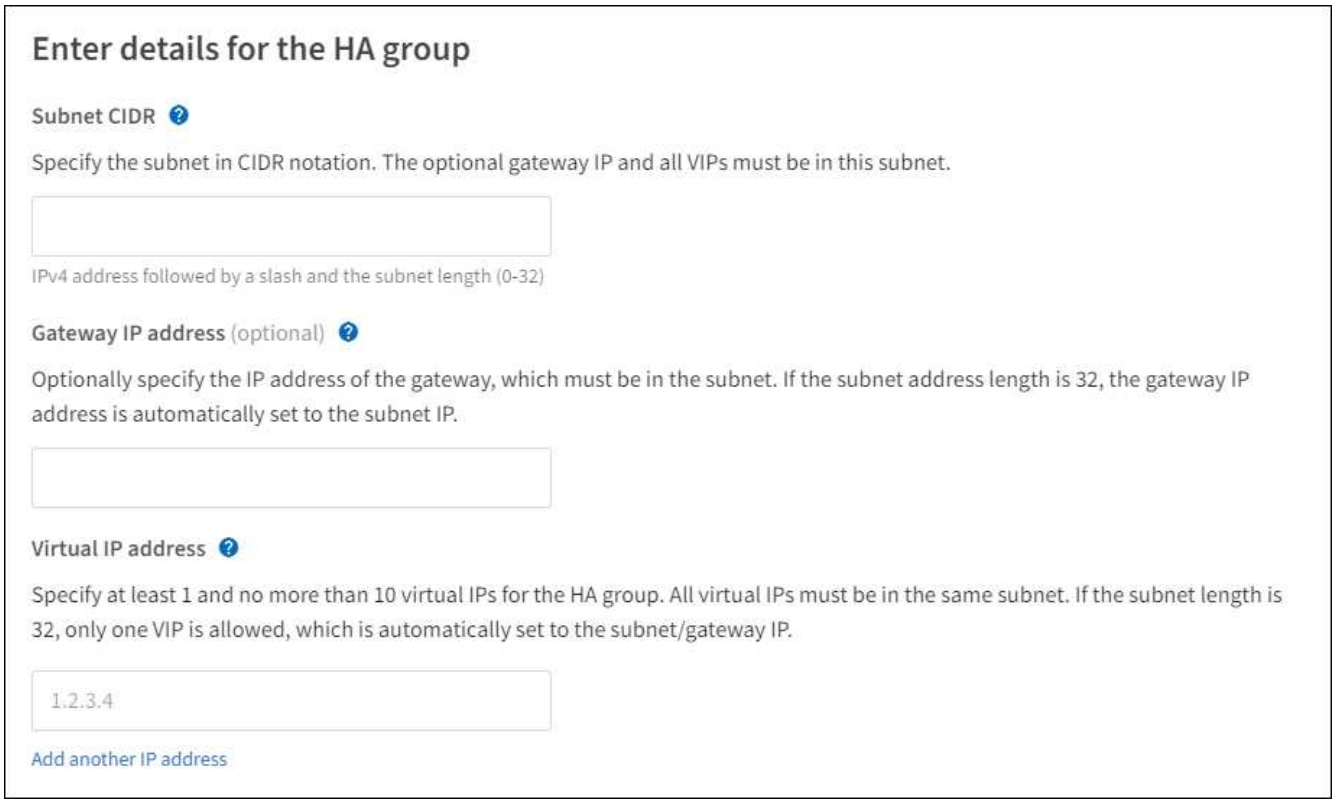
2. Wählen Sie **Weiter**.

Geben Sie die IP-Adressen ein

1. Geben Sie im Feld **Subnetz CIDR** das VIP-Subnetz in CIDR-Notation an - eine IPv4-Adresse gefolgt von einem Schrägstrich und der Subnetz-Länge (0-32).

   Die Netzwerkadresse darf keine Host-Bits festgelegt haben. Beispiel: `192.16.0.0/22`.

   Wenn Sie ein 32-Bit-Präfix verwenden, dient die VIP-Netzwerkadresse auch als Gateway-Adresse und VIP-Adresse.



2. Wenn auf diese VIP-Adressen von S3-, Swift-, Administrations- oder Mandantenclients aus einem anderen Subnetz zugegriffen wird, geben Sie die **Gateway IP-Adresse** ein. Die Gateway-Adresse muss sich im VIP-Subnetz befinden.

   Client- und Admin-Benutzer verwenden dieses Gateway, um auf die virtuellen IP-Adressen zuzugreifen.

3. Geben Sie eine oder mehrere **virtuelle IP-Adressen** für die HA-Gruppe ein. Sie können bis zu 10 IP-Adressen hinzufügen. Alle VIPs müssen sich im VIP-Subnetz befinden.

   Sie müssen mindestens eine IPv4-Adresse angeben. Optional können Sie weitere IPv4- und IPv6-Adressen angeben.

4. Wählen Sie **HA-Gruppe erstellen** und wählen Sie **Fertig**.

   Die HA-Gruppe wird erstellt. Sie können jetzt die konfigurierten virtuellen IP-Adressen verwenden.

> Warten Sie bis zu 15 Minuten, bis Änderungen an einer HA-Gruppe auf alle Nodes angewendet werden.

Nächste Schritte

Wenn Sie diese HA-Gruppe zum Lastausgleich verwenden möchten, erstellen Sie einen Endpunkt zum Load Balancer, um den Port und das Netzwerkprotokoll zu ermitteln und die erforderlichen Zertifikate anzuschließen. Siehe Konfigurieren von Load Balancer-Endpunkten.

Bearbeiten Sie eine Hochverfügbarkeitsgruppe

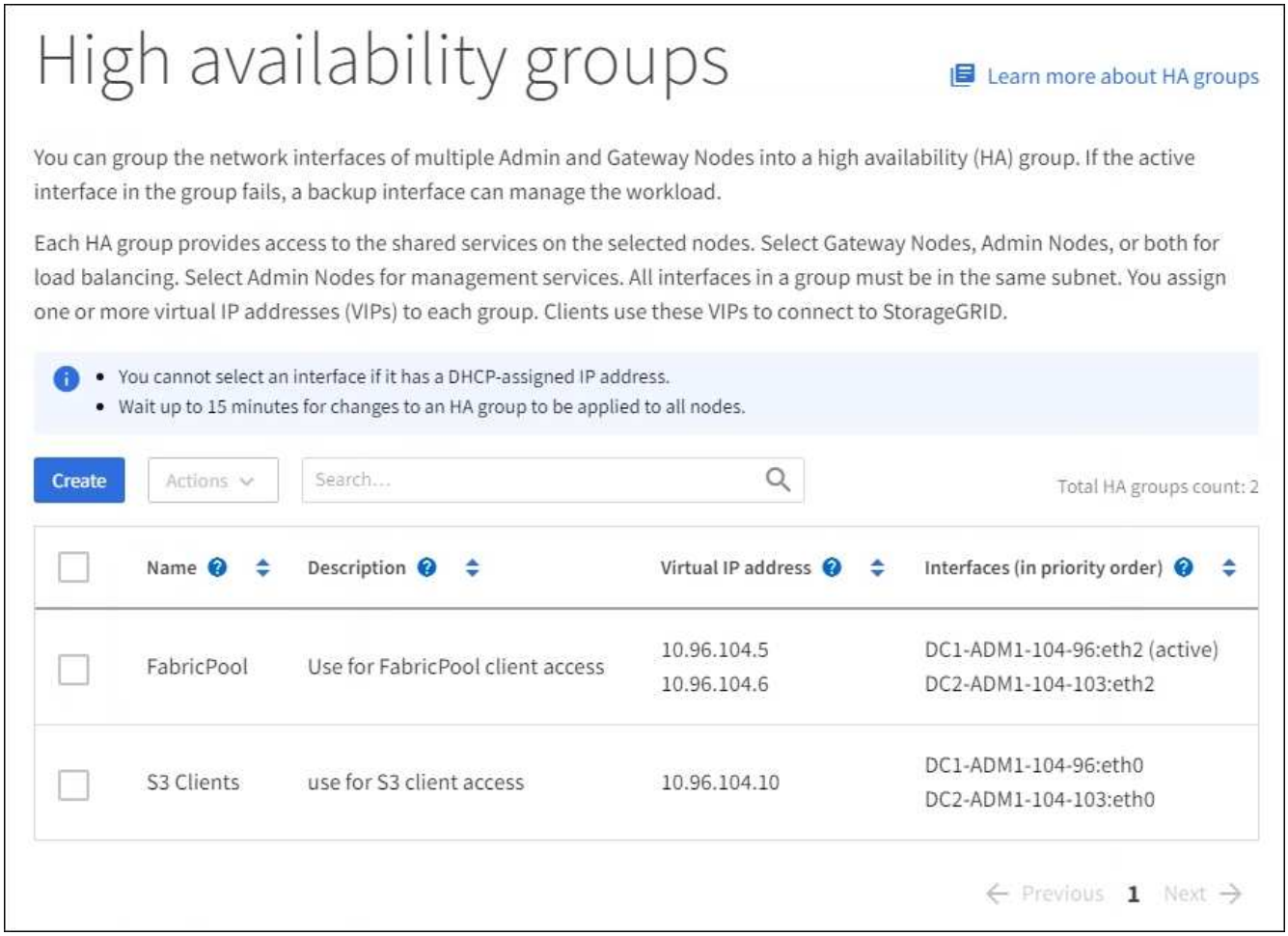
Sie können eine HA-Gruppe (High Availability, Hochverfügbarkeit) bearbeiten, um ihren Namen und ihre Beschreibung zu ändern, Schnittstellen hinzuzufügen oder zu entfernen, die Prioritätsreihenfolge zu ändern oder virtuelle IP-Adressen hinzuzufügen oder zu aktualisieren.

Beispielsweise müssen Sie möglicherweise eine HA-Gruppe bearbeiten, wenn Sie den Node, der einer ausgewählten Schnittstelle zugeordnet ist, entfernen möchten, wenn Sie ihn an einem Standort ausmustern oder einem Node entfernen möchten.

Schritte

1. Wählen Sie **KONFIGURATION Netzwerk Hochverfügbarkeitsgruppen**.

   Auf der Seite „Hochverfügbarkeitsgruppen“ werden alle vorhandenen HA-Gruppen angezeigt.



2. Aktivieren Sie das Kontrollkästchen für die HA-Gruppe, die Sie bearbeiten möchten.
3. Führen Sie einen der folgenden Schritte aus, je nachdem, was Sie aktualisieren möchten:
   - Wählen Sie **Aktionen virtuelle IP-Adresse bearbeiten**, um VIP-Adressen hinzuzufügen oder zu entfernen.
   - Wählen Sie **Aktionen HA-Gruppe bearbeiten** aus, um den Namen oder die Beschreibung der Gruppe zu aktualisieren, Schnittstellen hinzuzufügen oder zu entfernen, die Prioritätsreihenfolge zu ändern oder VIP-Adressen hinzuzufügen oder zu entfernen.
4. Wenn Sie **virtuelle IP-Adresse bearbeiten** ausgewählt haben:
   a. Aktualisieren Sie die virtuellen IP-Adressen für die HA-Gruppe.
   b. Wählen Sie **Speichern**.
   c. Wählen Sie **Fertig**.
5. Wenn Sie **HA-Gruppe bearbeiten** ausgewählt haben:

a. Optional können Sie den Namen oder die Beschreibung der Gruppe aktualisieren.
b. Aktivieren Sie optional die Kontrollkästchen, um Schnittstellen hinzuzufügen oder zu entfernen.

> Wenn die HA-Gruppe Zugriff auf den Grid Manager bietet, müssen Sie eine Schnittstelle am primären Admin-Node als primäre Schnittstelle auswählen. Einige Wartungsvorgänge können nur vom primären Admin-Node ausgeführt werden

c. Ziehen Sie optional Zeilen mit Drag-and-Drop, um die Prioritätsreihenfolge der primären Schnittstelle und aller Backup-Schnittstellen für diese HA-Gruppe zu ändern.
d. Optional können Sie die virtuellen IP-Adressen aktualisieren.
e. Wählen Sie **Speichern** und dann **Fertig stellen**.

> Warten Sie bis zu 15 Minuten, bis Änderungen an einer HA-Gruppe auf alle Nodes angewendet werden.

Entfernen Sie eine Hochverfügbarkeitsgruppe

Sie können eine oder mehrere HA-Gruppen (High Availability, Hochverfügbarkeit) gleichzeitig entfernen. Sie können jedoch keine HA-Gruppe entfernen, wenn sie an einen oder mehrere Load Balancer-Endpunkte gebunden ist.

Um Client-Unterbrechungen zu vermeiden, aktualisieren Sie die betroffenen S3- oder Swift-Client-Applikationen, bevor Sie eine HA-Gruppe entfernen. Aktualisieren Sie jeden Client, um eine Verbindung über eine andere IP-Adresse herzustellen, z. B. die virtuelle IP-Adresse einer anderen HA-Gruppe oder die IP-Adresse, die während der Installation für eine Schnittstelle konfiguriert wurde.

Schritte

1. Wählen Sie **KONFIGURATION Netzwerk Hochverfügbarkeitsgruppen**.
2. Aktivieren Sie das Kontrollkästchen für jede HA-Gruppe, die Sie entfernen möchten. Wählen Sie dann **Aktionen HA-Gruppe entfernen**.
3. Überprüfen Sie die Nachricht und wählen Sie **HA-Gruppe löschen**, um Ihre Auswahl zu bestätigen.

   Alle von Ihnen ausgewählten HA-Gruppen werden entfernt. Ein grünes Banner wird auf der Seite „Hochverfügbarkeitsgruppen“ angezeigt.

Managen Sie den Lastausgleich

Managen Sie den Lastausgleich: Übersicht

Die StorageGRID Lastausgleichfunktionen verarbeiten Aufnahme- und Abruf-Workloads von S3 und Swift Clients. Durch Verteilung der Workloads und Verbindungen auf mehrere Storage-Nodes maximiert der Lastausgleich die Geschwindigkeit und die Kapazität der Verbindungen.

Es gibt folgende Möglichkeiten für einen Lastenausgleich von Client-Workloads:

- Verwenden Sie den Lastverteilungsservice, der auf Admin Nodes und Gateway Nodes installiert ist. Der Lastverteilungsservice bietet Layer 7 Load Balancing und führt TLS-Terminierung von Client-Anfragen durch, prüft die Anfragen und stellt neue sichere Verbindungen zu den Storage Nodes her. Dies ist der

empfohlene Lastausgleichmechanismus.

Siehe Wie funktioniert der Lastausgleich? Load Balancer Service.

- Verwenden Sie den veralteten Verbindungs-Lastverteilungs-Service (CLB), der nur auf Gateway-Knoten installiert ist. Der CLB-Service bietet Layer 4-Lastenausgleich und unterstützt Verbindungskosten.

  Siehe Wie der Lastenausgleich funktioniert - CLB-Service (veraltet).

- Integration eines Load Balancer eines Drittanbieters: Genaue Informationen erhalten Sie bei Ihrem NetApp Ansprechpartner.

Wie funktioniert der Lastausgleich? Load Balancer Service

Der Load Balancer Service verteilt eingehende Netzwerkverbindungen von Client-Anwendungen auf Storage Nodes. Um den Lastenausgleich zu aktivieren, müssen Sie Load Balancer-Endpunkte mithilfe des Grid-Managers konfigurieren.

Sie können Load Balancer-Endpunkte nur für Admin-Nodes oder Gateway-Nodes konfigurieren, da diese Node-Typen den Load Balancer Service enthalten. Sie können keine Endpunkte für Speicherknoten oder Knoten archivieren konfigurieren.

Jeder Load Balancer-Endpunkt legt einen Port, ein Netzwerkprotokoll (HTTP oder HTTPS), einen Client-Typ (S3 oder Swift) und einen Bindungsmodus fest. HTTPS-Endpunkte erfordern ein Serverzertifikat. Bindungsmodi ermöglichen es Ihnen, die Zugriffsmöglichkeiten von Endpunktports auf folgende Arten zu beschränken:

- Die virtuellen IP-Adressen (VIPs) bestimmter Hochverfügbarkeitsgruppen (HA-Gruppen)
- Spezifische Netzwerkschnittstellen bestimmter Admin- und Gateway-Knoten

Überlegungen zu Ports

Clients können auf alle Endpunkte zugreifen, die Sie auf jedem Node konfigurieren, auf dem der Load Balancer Service ausgeführt wird. Es gibt zwei Ausnahmen: Die Ports 80 und 443 sind auf Admin-Nodes reserviert, sodass auf diesen Ports konfigurierte Endpunkte nur auf Gateway-Knoten Lastverteilungsvorgänge unterstützen.

Wenn Sie Ports neu zugeordnet haben, können Sie nicht dieselben Ports zum Konfigurieren von Load Balancer-Endpunkten verwenden. Sie können Endpunkte mit neu zugeordneten Ports erstellen, aber diese Endpunkte werden nicht dem Load Balancer-Service, sondern den ursprünglichen CLB-Ports und -Service neu zugeordnet. Befolgen Sie die Schritte unter Entfernen Sie die Port-Remaps.

Der CLB-Service ist veraltet.

CPU-Verfügbarkeit

Der Load Balancer Service läuft auf jedem Admin-Node und Gateway-Node unabhängig, wenn der S3- oder Swift-Datenverkehr zu den Storage-Nodes weitergeleitet wird. Durch eine Gewichtung leitet der Load Balancer-Service mehr Anfragen an Storage-Nodes mit höherer CPU-Verfügbarkeit weiter. Die Informationen zur CPU-Auslastung des Knotens werden alle paar Minuten aktualisiert. Die Gewichtung kann jedoch häufiger aktualisiert werden. Allen Storage-Nodes wird ein Mindestwert für das Basisgewicht zugewiesen, selbst wenn ein Node eine Auslastung von 100 % meldet oder seine Auslastung nicht meldet.

In manchen Fällen sind die Informationen zur CPU-Verfügbarkeit auf den Standort beschränkt, an dem sich

der Load Balancer Service befindet.

Konfigurieren von Load Balancer-Endpunkten

Load Balancer-Endpunkte bestimmen die Ports und Netzwerkprotokolle S3 und Swift-Clients können beim Herstellen einer Verbindung zum StorageGRID Load Balancer auf Gateway und Admin-Nodes verwendet werden.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben die Root-Zugriffsberechtigung.
- Wenn Sie zuvor einen Port neu zugeordnet haben, den Sie für den Load Balancer-Endpunkt verwenden möchten, haben Sie diesen Port-Remap wurde entfernt.
- Sie haben alle Hochverfügbarkeitsgruppen (High Availability groups, die Sie verwenden möchten, erstellt. HA-Gruppen werden empfohlen, jedoch nicht erforderlich. Siehe Management von Hochverfügbarkeitsgruppen.
- Wenn der Endpunkt des Load Balancer von verwendet wird S3 Mandanten für S3 Select, Es darf die IP-Adressen oder FQDNs von Bare-Metal-Knoten nicht verwenden. Für die bei S3 Select verwendeten Load Balancer-Endpunkte sind nur SG100- oder SG1000-Appliances und VMware-basierte Software-Nodes zulässig.
- Sie haben alle VLAN-Schnittstellen konfiguriert, die Sie verwenden möchten. Siehe Konfigurieren Sie die VLAN-Schnittstellen.
- Wenn Sie einen HTTPS-Endpunkt erstellen (empfohlen), haben Sie die Informationen für das Serverzertifikat.

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

  - Zum Hochladen eines Zertifikats benötigen Sie das Serverzertifikat, den privaten Zertifikatschlüssel und optional ein CA-Bundle.
  - Zum Generieren eines Zertifikats benötigen Sie alle Domain-Namen und IP-Adressen, die S3- oder Swift-Clients für den Zugriff auf den Endpunkt verwenden. Sie müssen auch das Thema (Distinguished Name) kennen.
  - Wenn Sie das StorageGRID S3- und Swift-API-Zertifikat verwenden möchten (das auch für direkte Verbindungen zu Speicherknoten verwendet werden kann), haben Sie das Standardzertifikat bereits durch ein benutzerdefiniertes Zertifikat ersetzt, das von einer externen Zertifizierungsstelle signiert ist. SieheKonfigurieren von S3- und Swift-API-Zertifikaten.

    Das Zertifikat kann Platzhalter verwenden, um die vollständig qualifizierten Domänennamen aller Admin-Nodes und Gateway-Nodes darzustellen, auf denen der Load Balancer Service ausgeführt wird. Beispiel: `*.storagegrid.example.com` Verwendet den Platzhalter * für die Darstellung `adm1.storagegrid.example.com` Und `gn1.storagegrid.example.com`. Siehe Konfigurieren von S3-API-Endpunkt-Domain-Namen.

Erstellen Sie einen Endpunkt für den Load Balancer

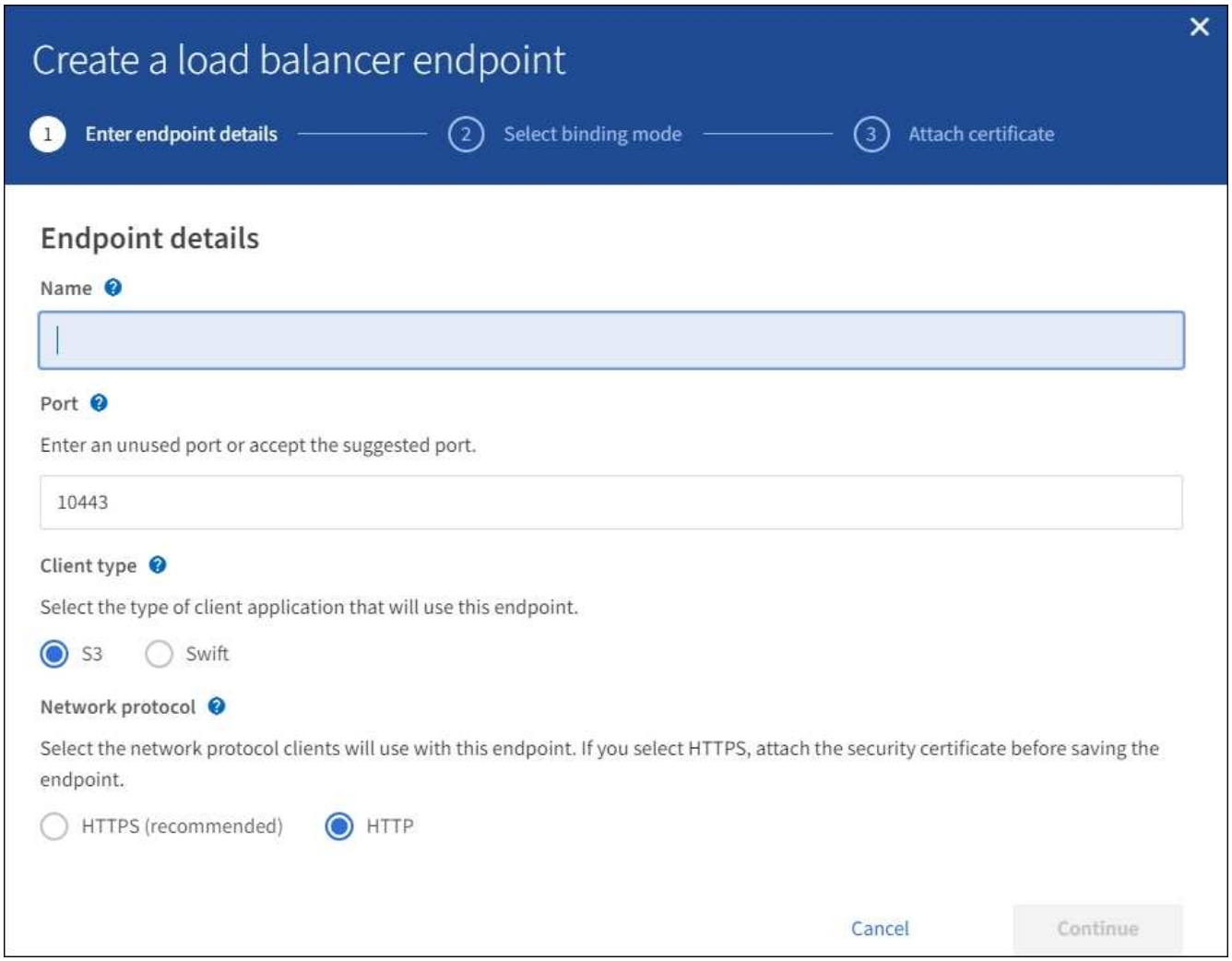
Jeder Load Balancer-Endpunkt gibt einen Port, einen Client-Typ (S3 oder Swift) und ein Netzwerkprotokoll (HTTP oder HTTPS) an.

Greifen Sie auf den Assistenten zu

1. Wählen Sie **KONFIGURATION Netzwerk Load Balancer-Endpunkte** aus.
2. Wählen Sie **Erstellen**.

Geben Sie Details zu Endpunkten ein

1. Geben Sie Details für den Endpunkt ein.



Feld	Beschreibung
Name	Ein beschreibbarer Name für den Endpunkt, der in der Tabelle auf der Seite Load Balancer Endpunkte angezeigt wird.

Feld	Beschreibung
Port	Die Port-Clients werden zum Herstellen einer Verbindung zum Load Balancer-Service auf Admin-Nodes und Gateway-Nodes verwendet. Akzeptieren Sie die vorgeschlagene Portnummer oder geben Sie einen externen Port ein, der nicht von einem anderen Grid-Service verwendet wird. Geben Sie einen Wert zwischen 1 und 65535 ein. Wenn Sie **80** oder **443** eingeben, wird der Endpunkt nur auf Gateway-Knoten konfiguriert. Diese Ports sind für Admin-Nodes reserviert. Siehe Netzwerkrichtlinien Weitere Informationen zu externen Ports.
Client-Typ	Der Typ der Client-Anwendung, die diesen Endpunkt verwenden wird, entweder **S3** oder **Swift**.
Netzwerkprotokoll	Das Netzwerkprotokoll, das Clients bei der Verbindung mit diesem Endpunkt verwenden werden. • Wählen Sie **HTTPS** für sichere, TLS verschlüsselte Kommunikation (empfohlen). Sie müssen ein Sicherheitszertifikat anhängen, bevor Sie den Endpunkt speichern können. • Wählen Sie **HTTP** für eine weniger sichere, unverschlüsselte Kommunikation. Verwenden Sie HTTP nur für ein Grid, das nicht produktionsbereit ist.

2. Wählen Sie **Weiter**.

Wählen Sie den Bindungsmodus aus

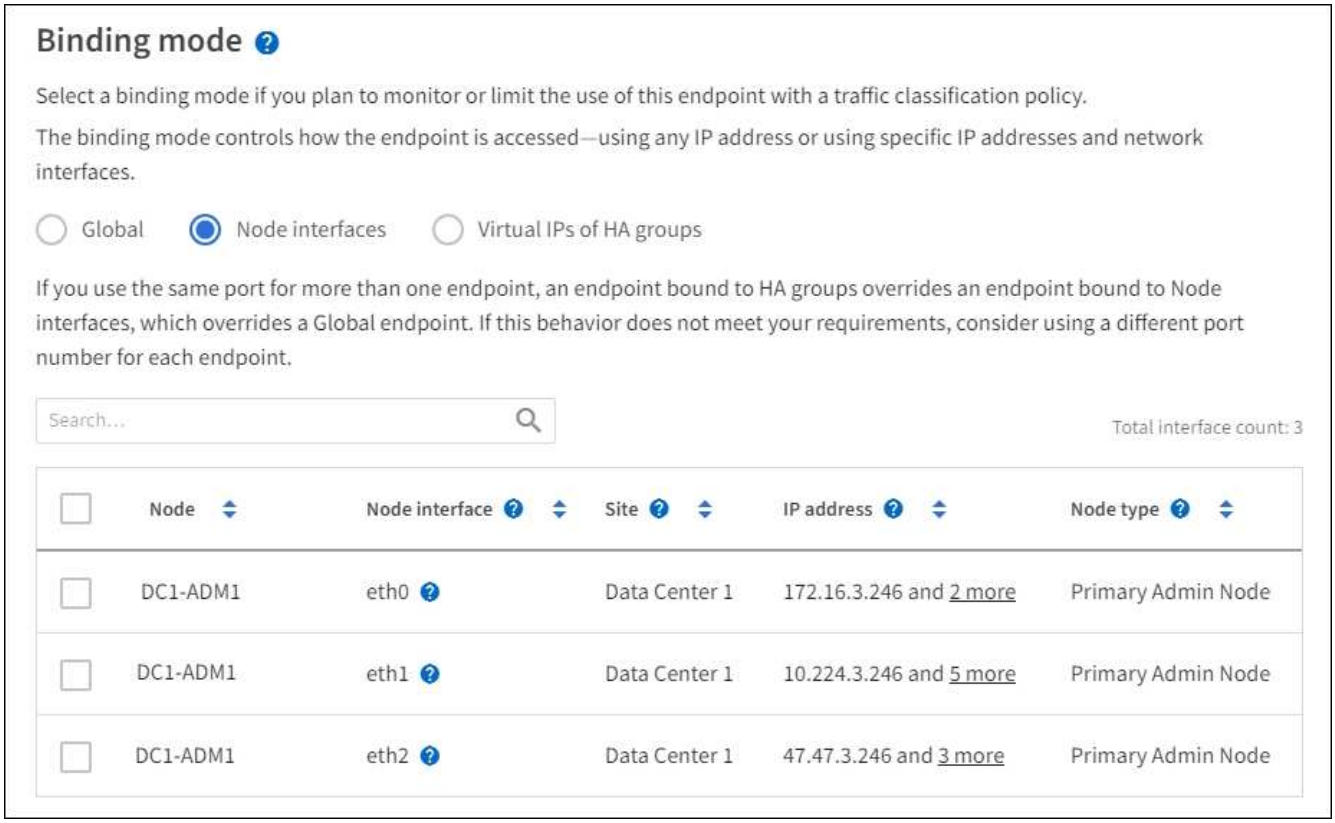
1. Wählen Sie einen Bindungsmodus für den Endpunkt aus, um den Zugriff auf den Endpunkt zu steuern.

Option	Beschreibung
Global (Standard)	Clients können über einen vollständig qualifizierten Domänennamen (FQDN), die IP-Adresse eines beliebigen Gateway-Node oder Admin-Nodes oder die virtuelle IP-Adresse einer beliebigen HA-Gruppe in einem beliebigen Netzwerk auf den Endpunkt zugreifen. Verwenden Sie die **Global**-Einstellung (Standard), es sei denn, Sie müssen die Zugriffsmöglichkeiten dieses Endpunkts einschränken.
Node-Schnittstellen	Clients müssen die IP-Adresse eines ausgewählten Knotens und einer ausgewählten Netzwerkschnittstelle verwenden, um auf diesen Endpunkt zugreifen zu können.

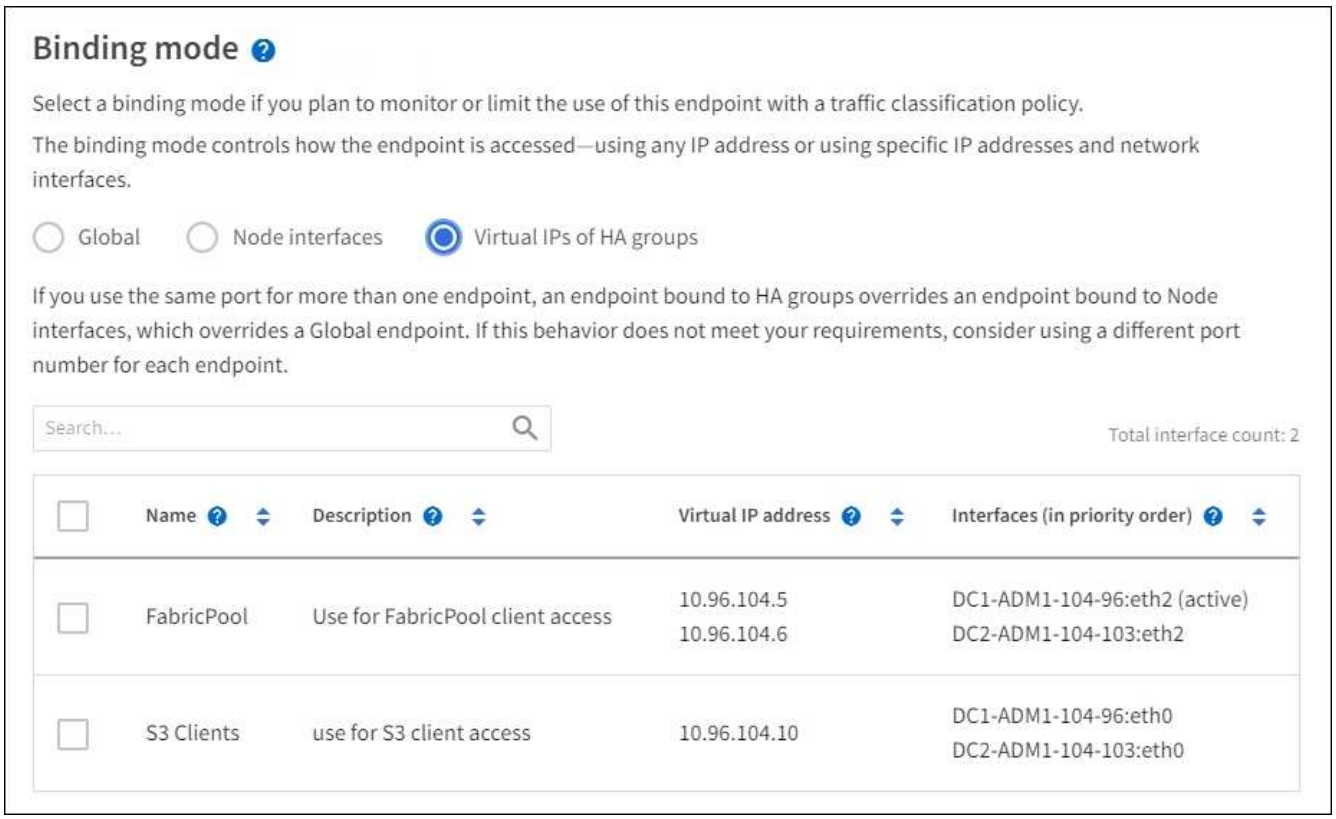
Option	Beschreibung
Virtuelle IPs von HA-Gruppen	Clients müssen für den Zugriff auf diesen Endpunkt eine virtuelle IP-Adresse einer HA-Gruppe verwenden. Endpunkte mit diesem Bindungsmodus können alle dieselbe Portnummer verwenden, solange sich die für die Endpunkte ausgewählten HA-Gruppen nicht überschneiden. Endpunkte mit diesem Modus können alle dieselbe Portnummer verwenden, solange sich die für die Endpunkte ausgewählten Schnittstellen nicht überschneiden.

Wenn Sie denselben Port für mehrere Endpunkte verwenden, überschreibt ein Endpunkt mit **Virtual IPs of HA groups** Mode einen Endpunkt mithilfe des **Node Interfaces**-Modus, der einen Endpunkt im **Global**-Modus überschreibt.

2. Wenn Sie **Node-Schnittstellen** ausgewählt haben, wählen Sie für jeden Admin-Node oder Gateway-Node eine oder mehrere Node-Schnittstellen aus, die mit diesem Endpunkt verknüpft werden sollen.



3. Wenn Sie **virtuelle IPs von HA-Gruppen** ausgewählt haben, wählen Sie eine oder mehrere HA-Gruppen aus.



4. Wenn Sie einen **HTTP**-Endpunkt erstellen, müssen Sie kein Zertifikat anhängen. Wählen Sie **Erstellen**, um den neuen Load Balancer-Endpunkt hinzuzufügen. Fahren Sie dann mit fort Nachdem Sie fertig sind. Andernfalls wählen Sie **Weiter**, um das Zertifikat anzuhängen.

Zertifikat anhängen

1. Wenn Sie einen **HTTPS**-Endpunkt erstellen, wählen Sie den Typ des Sicherheitszertifikats aus, das Sie an den Endpunkt anhängen möchten.

   Das Zertifikat sichert die Verbindungen zwischen S3- und Swift-Clients und dem Load Balancer-Service auf Admin-Node oder Gateway-Nodes.

   - **Zertifikat hochladen**. Wählen Sie diese Option aus, wenn Sie über benutzerdefinierte Zertifikate zum Hochladen verfügen.
   - **Zertifikat generieren**. Wählen Sie diese Option aus, wenn Sie über die Werte verfügen, die zum Generieren eines benutzerdefinierten Zertifikats erforderlich sind.
   - **Verwenden Sie StorageGRID S3 und Swift Zertifikat**. Wählen Sie diese Option aus, wenn Sie das globale S3- und Swift-API-Zertifikat verwenden möchten, das auch für direkte Verbindungen zu Storage-Nodes verwendet werden kann.

     Sie können diese Option nur auswählen, wenn Sie das von der Grid-CA signierte S3- und Swift-API-Standardzertifikat durch ein benutzerdefiniertes Zertifikat ersetzt haben, das von einer externen Zertifizierungsstelle signiert ist. SieheKonfigurieren von S3- und Swift-API-Zertifikaten.

2. Wenn Sie das StorageGRID S3- und Swift-Zertifikat nicht verwenden, laden Sie das Zertifikat hoch oder generieren Sie es.

Zertifikat hochladen

a. Wählen Sie **Zertifikat hochladen**.

b. Laden Sie die erforderlichen Serverzertifikatdateien hoch:

- **Server-Zertifikat**: Die benutzerdefinierte Server-Zertifikatdatei in PEM-Kodierung.
- **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 Zertifikatinhalt zum Einfügen an eine andere Stelle zu kopieren.

d. Wählen Sie **Erstellen**. + der Endpunkt des Load Balancer wird erstellt. Das individuelle Zertifikat wird für alle nachfolgenden neuen Verbindungen zwischen S3 und Swift Clients und dem Endpunkt verwendet.

Zertifikat wird generiert

a. Wählen Sie **Zertifikat erstellen**.

b. Geben Sie die Zertifikatsinformationen an:

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

c. Wählen Sie **Erzeugen**.

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

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

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

Beispiel: `storagegrid_certificate.pem`

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

e. Wählen Sie **Erstellen**.

Der Endpunkt des Load Balancer wird erstellt. Das individuelle Zertifikat wird für alle nachfolgenden neuen Verbindungen zwischen S3 und Swift Clients und diesem Endpunkt verwendet.

nach dem Ende

1. Wenn Sie ein Domain Name System (DNS) verwenden, stellen Sie sicher, dass der DNS einen Datensatz enthält, um den vollqualifizierten StorageGRID-Domänennamen jeder IP-Adresse zuzuordnen, die von Clients zum Herstellen von Verbindungen verwendet wird.

   Die IP-Adresse, die Sie im DNS-Datensatz eingeben, hängt davon ab, ob Sie eine HA-Gruppe von Load-Balancing-Nodes verwenden:

   - Wenn Sie eine HA-Gruppe konfiguriert haben, stellen Clients eine Verbindung zu den virtuellen IP-Adressen dieser HA-Gruppe her.
   - Wenn Sie keine HA-Gruppe verwenden, stellen die Clients unter Verwendung der IP-Adresse eines beliebigen Gateway-Node oder Admin-Node eine Verbindung zum StorageGRID Load Balancer-Service her.

     Außerdem müssen Sie sicherstellen, dass der DNS-Datensatz alle erforderlichen Endpunkt-Domain-Namen referenziert, einschließlich Platzhalternamen.

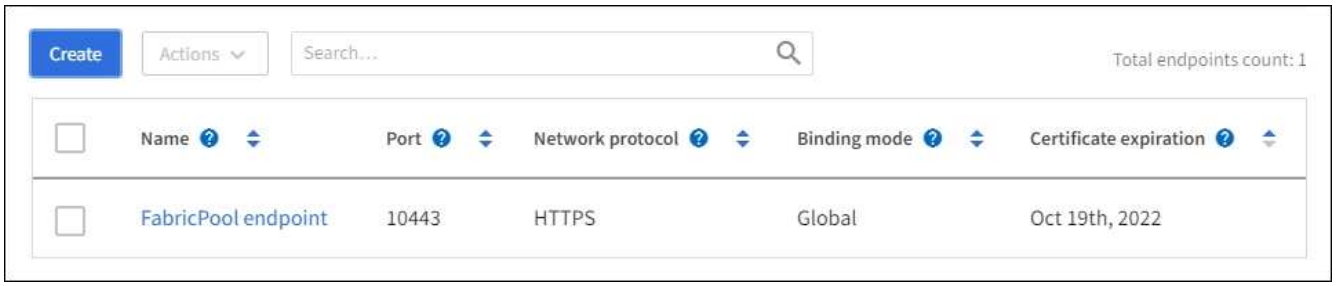
2. S3- und Swift-Clients erhalten die für die Verbindung mit dem Endpunkt erforderlichen Informationen:
   - Port-Nummer
   - Vollständig qualifizierter Domain-Name oder IP-Adresse
   - Alle erforderlichen Zertifikatsdetails

Load Balancer-Endpunkte anzeigen und bearbeiten

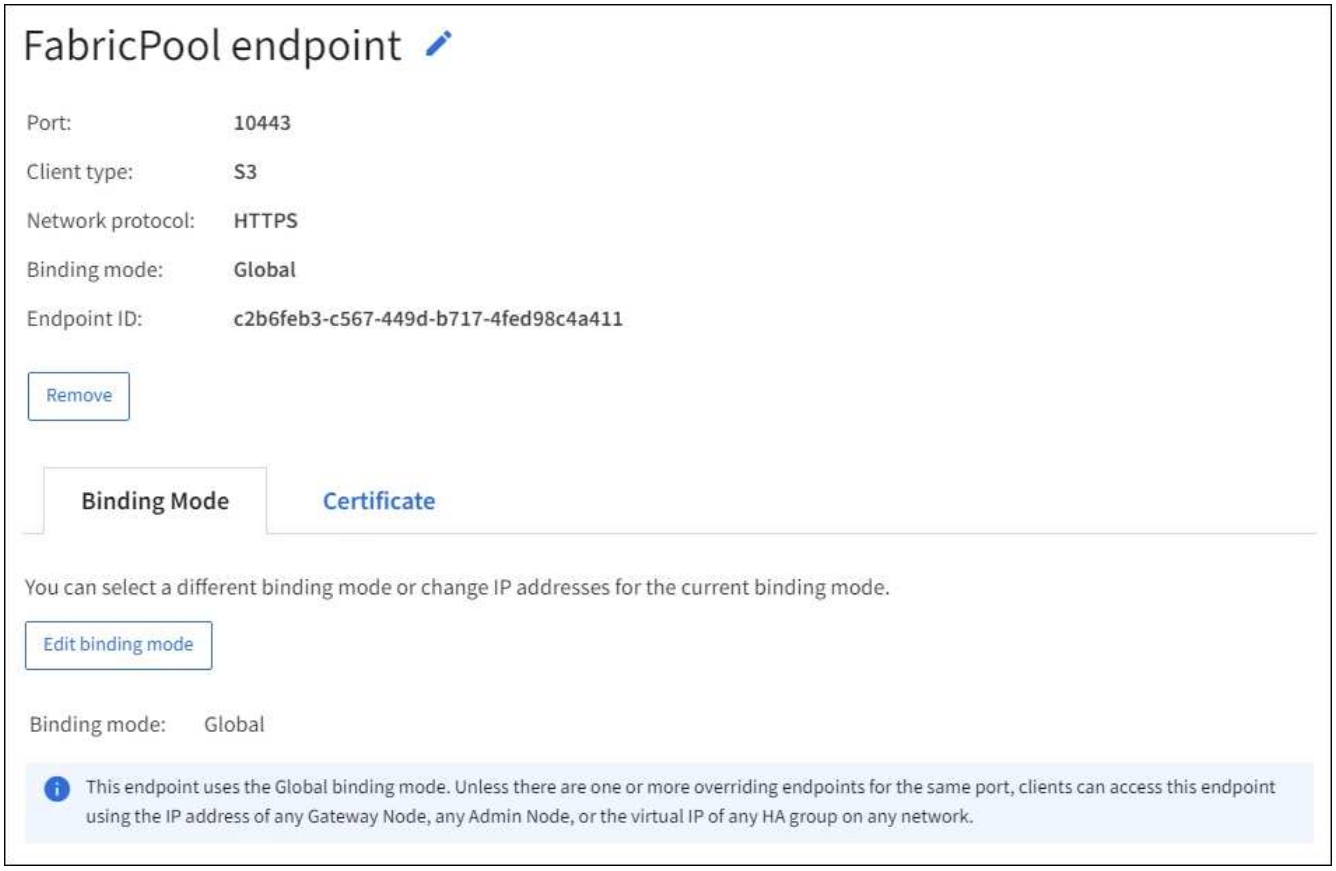
Sie können Details zu vorhandenen Load Balancer-Endpunkten anzeigen, einschließlich der Zertifikatmetadaten für einen gesicherten Endpunkt. Sie können auch den Namen oder den Bindungsmodus eines Endpunkts ändern und alle zugehörigen Zertifikate aktualisieren.

Sie können den Servicetyp (S3 oder Swift), den Port oder das Protokoll (HTTP oder HTTPS) nicht ändern.

- Um grundlegende Informationen für alle Load Balancer-Endpunkte anzuzeigen, lesen Sie die Tabelle auf der Seite Load Balancer Endpunkte durch.



- Um alle Details zu einem bestimmten Endpunkt einschließlich Zertifikatmetadaten anzuzeigen, wählen Sie in der Tabelle den Namen des Endpunkts aus.



- Um einen Endpunkt zu bearbeiten, verwenden Sie das Menü **Aktionen** auf der Seite Load Balancer Endpoints oder die Detailseite für einen bestimmten Endpunkt.

> Nach dem Bearbeiten eines Endpunkts müssen Sie möglicherweise bis zu 15 Minuten warten, bis Ihre Änderungen auf alle Nodes angewendet werden.

Aufgabe	Menü „Aktionen“	Detailseite
Endpunktname bearbeiten	a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie **Aktionen** **Endpunktname bearbeiten** aus. c. Geben Sie den neuen Namen ein. d. Wählen Sie **Speichern**.	a. Wählen Sie den Endpunktnamen aus, um die Details anzuzeigen. b. Wählen Sie das Bearbeitungssymbol . c. Geben Sie den neuen Namen ein. d. Wählen Sie **Speichern**.

Aufgabe	Menü „Aktionen“	Detailseite
Endpunktbindungsmodus bearbeiten	a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie **Aktionen Endpunktbindungsmodus bearbeiten**. c. Aktualisieren Sie den Bindungsmodus, falls erforderlich. d. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Endpunktnamen aus, um die Details anzuzeigen. b. Wählen Sie **Bindungsmodus bearbeiten**. c. Aktualisieren Sie den Bindungsmodus, falls erforderlich. d. Wählen Sie **Änderungen speichern**.
Endpunktzertifikat bearbeiten	a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie **Aktionen Endpunktzertifikat bearbeiten** aus. c. Laden Sie ein neues benutzerdefiniertes Zertifikat hoch oder erstellen Sie es, falls erforderlich, mit der Verwendung des globalen S3- und Swift-Zertifikats. d. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Endpunktnamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte **Zertifikat** aus. c. Wählen Sie **Zertifikat bearbeiten**. d. Laden Sie ein neues benutzerdefiniertes Zertifikat hoch oder erstellen Sie es, falls erforderlich, mit der Verwendung des globalen S3- und Swift-Zertifikats. e. Wählen Sie **Änderungen speichern**.

Entfernen Sie Load Balancer-Endpunkte

Sie können einen oder mehrere Endpunkte über das Menü **Aktionen** entfernen oder einen einzelnen Endpunkt von der Detailseite entfernen.

> Um Client-Unterbrechungen zu vermeiden, aktualisieren Sie die betroffenen S3- oder Swift-Client-Applikationen, bevor Sie einen Load Balancer-Endpunkt entfernen. Aktualisieren Sie jeden Client, um eine Verbindung über einen Port herzustellen, der einem anderen Load Balancer-Endpunkt zugewiesen ist. Aktualisieren Sie auch die erforderlichen Zertifikatsinformationen.

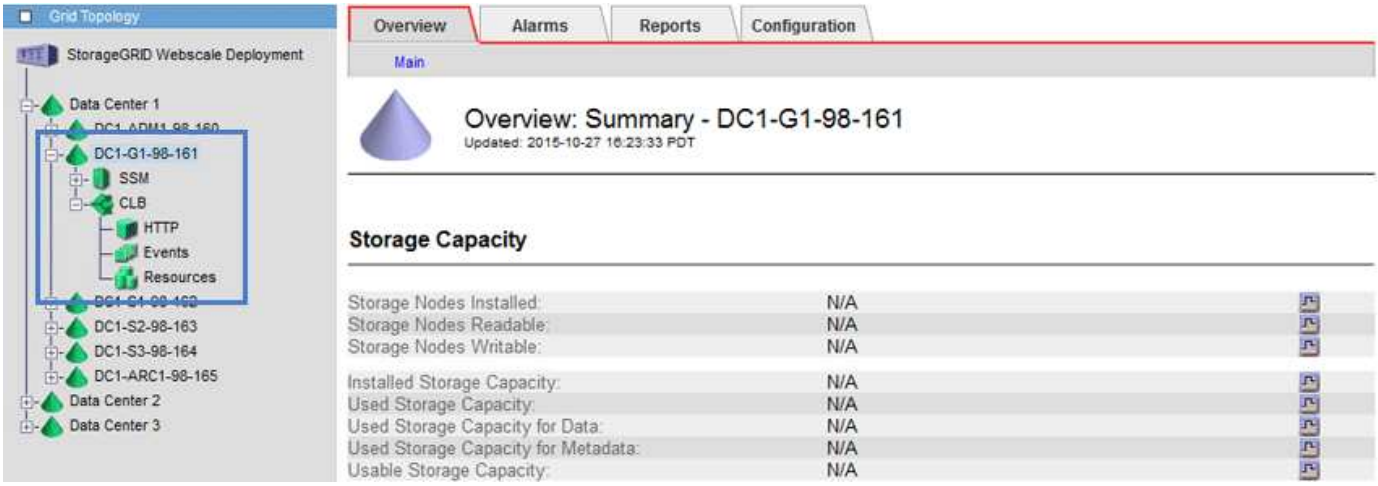
- So entfernen Sie einen oder mehrere Endpunkte:
  a. Aktivieren Sie auf der Seite Load Balancer das Kontrollkästchen für jeden zu entfernenden Endpunkt.
  b. Wählen Sie **Aktionen Entfernen**.
  c. Wählen Sie **OK**.
- So entfernen Sie einen Endpunkt auf der Detailseite:
  a. Auf der Seite Load Balancer. Wählen Sie den Endpunktnamen aus.
  b. Wählen Sie auf der Detailseite * Entfernen.
  c. Wählen Sie **OK**.

Wie der Lastenausgleich funktioniert - CLB-Service (veraltet)

Der CLB-Dienst (Connection Load Balancer) auf Gateway-Nodes ist veraltet. Der Lastausgleichsdienst ist jetzt der empfohlene Lastausgleichmechanismus.

Der CLB-Service nutzt Layer 4 Load Balancing zur Verteilung eingehender TCP-Netzwerkverbindungen von Client-Anwendungen auf den optimalen Storage Node basierend auf Verfügbarkeit, Systemlast und den vom Administrator konfigurierten Verbindungskosten. Wenn der optimale Speicherknoten ausgewählt wird, baut der CLB-Dienst eine zweiseitige Netzwerkverbindung auf und leitet den Datenverkehr vom und zum ausgewählten Knoten weiter. Beim CLB wird die Konfiguration des Grid-Netzwerks nicht berücksichtigt, wenn eingehende Netzwerkverbindungen geleitet werden.

Um Informationen zum CLB-Dienst anzuzeigen, wählen Sie **SUPPORT Tools Grid-Topologie** und erweitern Sie dann einen Gateway-Knoten, bis Sie **CLB** und die Optionen darunter auswählen können.



Wenn Sie den CLB-Service nutzen möchten, sollten Sie die Verbindungskosten für Ihr StorageGRID-System in Betracht ziehen.

- Was sind Verbindungskosten
- Verbindungskosten aktualisieren

Konfigurieren von S3-API-Endpunkt-Domain-Namen

Um virtuelle S3-Hosted-Style-Anforderungen zu unterstützen, müssen Sie die Liste der Endpunkt-Domain-Namen, mit denen S3-Clients verbunden werden, mit konfigurieren.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben bestätigt, dass ein Grid-Upgrade nicht ausgeführt wird.

> Nehmen Sie keine Änderungen an der Domänennamenkonfiguration vor, wenn ein Grid-Upgrade ausgeführt wird.

Über diese Aufgabe

Um Clients die Verwendung von S3-Endpunkt-Domain-Namen zu ermöglichen, müssen Sie folgende Aktionen

durchführen:

- Verwenden Sie den Grid-Manager, um dem StorageGRID System die S3-Endpunkt-Domain-Namen hinzuzufügen.
- Stellen Sie sicher, dass das Zertifikat, das der Client für HTTPS-Verbindungen zu StorageGRID verwendet, für alle vom Client erforderlichen Domänennamen signiert ist.

  Beispiel: Wenn der Endpunkt lautet `s3.company.com`, Sie müssen sicherstellen, dass das Zertifikat verwendet für HTTPS-Verbindungen enthält die `s3.company.com` endpunkt und Wildcard-alternativer Name (SAN) des Endpunkts: `*.s3.company.com`.

- Konfigurieren Sie den vom Client verwendeten DNS-Server. Fügen Sie DNS-Datensätze für die IP-Adressen ein, die von Clients zum Herstellen von Verbindungen verwendet werden, und stellen Sie sicher, dass die Datensätze auf alle erforderlichen Endpunkt-Domänennamen verweisen, einschließlich Platzhalternamen.

> Clients können sich mit StorageGRID über die IP-Adresse eines Gateway-Node, eines Admin-Nodes oder eines Storage-Nodes oder durch Verbindung mit der virtuellen IP-Adresse einer Hochverfügbarkeitsgruppe verbinden. Sie sollten verstehen, wie Client-Anwendungen eine Verbindung zum Raster herstellen, sodass Sie die richtigen IP-Adressen in die DNS-Einträge aufnehmen können.

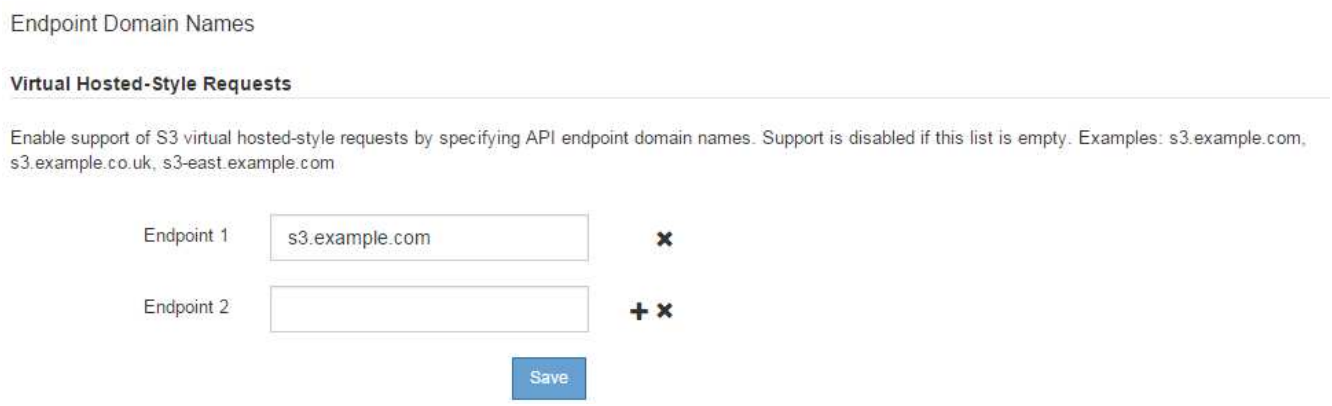
Clients, die HTTPS-Verbindungen (empfohlen) zum Raster verwenden, können eines der folgenden Zertifikate verwenden:

- Clients, die eine Verbindung zu einem Load Balancer-Endpunkt herstellen, können für diesen Endpunkt ein benutzerdefiniertes Zertifikat verwenden. Jeder Load Balancer-Endpunkt kann so konfiguriert werden, dass unterschiedliche Endpunkt-Domain-Namen erkannt werden.
- Clients, die eine Verbindung zu einem Load Balancer-Endpunkt, direkt zu einem Storage Node oder direkt zum veralteten CLB-Dienst auf einem Gateway-Node herstellen, können das globale S3- und Swift-API-Zertifikat so anpassen, dass alle erforderlichen Endpunkt-Domain-Namen berücksichtigt werden.

Schritte

1. Wählen Sie **KONFIGURATION Netzwerk Domain-Namen**.

   Die Seite „Endpoint Domain-Namen“ wird angezeigt.



2. Geben Sie in die Felder **Endpunkt** die Liste der S3-API-Endpunktdomänen ein. Verwenden Sie die + Symbol zum Hinzufügen weiterer Felder.

Wenn diese Liste leer ist, ist die Unterstützung für virtuelle S3-Hosted-Style-Anforderungen deaktiviert.

3. Wählen Sie **Speichern**.
4. Stellen Sie sicher, dass die Serverzertifikate, die Clients verwenden, mit den erforderlichen Endpunktdomänennamen übereinstimmen.
   - Wenn Clients eine Verbindung zu einem Load Balancer-Endpunkt herstellen, der sein eigenes Zertifikat verwendet, aktualisieren Sie das dem Endpunkt zugeordnete Zertifikat.
   - Wenn Clients eine Verbindung zu einem Endpunkt des Load Balancer herstellen, der das globale S3- und Swift-API-Zertifikat verwendet, direkt zu Storage-Nodes oder zum CLB-Service auf Gateway-Nodes, aktualisieren Sie das globale S3- und Swift-API-Zertifikat.
5. Fügen Sie die erforderlichen DNS-Einträge hinzu, um sicherzustellen, dass die Anforderungen für den Domänennamen des Endpunkts aufgelöst werden können.

Ergebnis

Wenn Clients nun den Endpunkt verwenden `bucket.s3.company.com`, Der DNS-Server löst sich auf den richtigen Endpunkt und das Zertifikat authentifiziert den Endpunkt wie erwartet.

Verwandte Informationen

- S3 verwenden
- Zeigen Sie IP-Adressen an
- Konfigurieren Sie Hochverfügbarkeitsgruppen
- Konfigurieren von S3- und Swift-API-Zertifikaten
- Konfigurieren von Load Balancer-Endpunkten

Aktivieren Sie HTTP für die Clientkommunikation

Standardmäßig verwenden Client-Anwendungen das HTTPS-Netzwerkprotokoll für alle Verbindungen zu Storage-Nodes oder zum veralteten CLB-Dienst auf Gateway-Nodes. Optional können Sie HTTP für diese Verbindungen aktivieren, z. B. beim Testen eines nicht produktiven Grids.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Führen Sie diese Aufgabe nur aus, wenn S3- und Swift-Clients HTTP-Verbindungen direkt zu Storage-Nodes oder zum veralteten CLB-Service auf Gateway-Nodes herstellen müssen.

Sie müssen diese Aufgabe nicht für Clients abschließen, die nur HTTPS-Verbindungen verwenden oder für Clients, die eine Verbindung zum Load Balancer-Dienst herstellen (da Sie jeden Load Balancer-Endpunkt so konfigurieren können, dass entweder HTTP oder HTTPS verwendet werden). Weitere Informationen finden Sie in den Informationen zum Konfigurieren von Load Balancer-Endpunkten.

Siehe Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen Um zu erfahren, welche S3- und Swift-Clients beim Herstellen einer Verbindung zu Storage-Nodes oder zum veralteten CLB-Dienst über HTTP oder HTTPS verwenden

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

Schritte

1. Wählen Sie **KONFIGURATION System Gitteroptionen**.
2. Aktivieren Sie im Abschnitt Netzwerkoptionen das Kontrollkästchen **HTTP-Verbindung aktivieren**.

3. Wählen Sie **Speichern**.

Verwandte Informationen

- Konfigurieren von Load Balancer-Endpunkten
- S3 verwenden
- Verwenden Sie Swift

Kontrollieren Sie, welche Client-Vorgänge zulässig sind

Sie können die Option „Client Modification Grid verhindern“ auswählen, um bestimmte HTTP-Client-Vorgänge zu verweigern.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

„Client-Änderung verhindern“ ist eine systemweite Einstellung. Wenn die Option „Client-Änderung verhindern“ ausgewählt ist, werden die folgenden Anfragen verweigert:

- **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

    Diese Einstellung gilt nicht für Buckets mit aktivierter Versionierung. Bei der Versionierung werden bereits Änderungen an Objektdaten, benutzerdefinierten Metadaten und Objekt-Tagging verhindert.

- **Swift REST API**
  - Container-Anforderungen löschen

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

Schritte

1. Wählen Sie **KONFIGURATION System Gitteroptionen**.
2. Aktivieren Sie im Abschnitt Netzwerkoptionen das Kontrollkästchen **Client-Änderung verhindern**.

3. Wählen Sie **Speichern**.

Netzwerke und Verbindungen verwalten

Richtlinien für StorageGRID-Netzwerke

Mit dem Grid Manager können Sie StorageGRID-Netzwerke und -Verbindungen konfigurieren und verwalten.

Siehe Konfiguration von S3- und Swift-Client-Verbindungen Informationen zum Verbinden von S3 oder Swift Clients

Standard-StorageGRID-Netzwerke

Standardmäßig unterstützt StorageGRID drei Netzwerkschnittstellen pro Grid Node. So können Sie das Netzwerk für jeden einzelnen Grid Node so konfigurieren, dass er Ihren Sicherheits- und Zugriffsanforderungen entspricht.

Weitere Informationen zur Netzwerktopologie finden Sie unter Netzwerkrichtlinien.

Grid-Netzwerk

Erforderlich. Das Grid-Netzwerk wird für den gesamten internen StorageGRID-Datenverkehr verwendet. Das System bietet Konnektivität zwischen allen Nodes im Grid und allen Standorten und Subnetzen.

Admin-Netzwerk

Optional Das Admin-Netzwerk wird in der Regel für die Systemadministration und -Wartung verwendet. Sie kann auch für den Zugriff auf das Client-Protokoll verwendet werden. Das Admin-Netzwerk ist in der Regel ein privates Netzwerk und muss nicht zwischen Standorten routingfähig sein.

Client-Netzwerk

Optional Das Client-Netzwerk ist ein offenes Netzwerk, das normalerweise für den Zugriff auf S3- und Swift-Client-Applikationen verwendet wird, sodass das Grid-Netzwerk isoliert und gesichert werden kann. Das Client-Netzwerk kann mit jedem Subnetz kommunizieren, das über das lokale Gateway erreichbar ist.

Richtlinien

- Jeder StorageGRID Grid Node benötigt für jedes ihm zugewiesene Netzwerk eine dedizierte Netzwerkschnittstelle, eine IP-Adresse, eine Subnetzmaske und ein Gateway.
- Ein Grid-Node kann nicht mehr als eine Schnittstelle in einem Netzwerk haben.
- Es wird ein einzelnes Gateway pro Netzwerk und pro Grid-Node unterstützt, das sich im gleichen Subnetz wie der Node befindet. Sie können bei Bedarf komplexere Routing-Lösungen im Gateway implementieren.
- Auf jedem Node ist jedes Netzwerk einer bestimmten Netzwerkschnittstelle zugeordnet.

Netzwerk	Schnittstellenname
Raster	Eth0
Admin (optional)	Eth1
Client (optional)	Eth2

- Wenn der Node mit einer StorageGRID Appliance verbunden ist, werden für jedes Netzwerk bestimmte Ports verwendet. Weitere Informationen finden Sie in den Installationsanweisungen für Ihr Gerät.
- Die Standardroute wird automatisch pro Knoten generiert. Wenn eth2 aktiviert ist, verwendet 0.0.0.0/0 das Client-Netzwerk auf eth2. Wenn eth2 nicht aktiviert ist, verwendet 0.0.0.0/0 das Grid-Netzwerk auf eth0.
- Das Client-Netzwerk ist erst betriebsbereit, wenn der Grid-Node dem Grid beigetreten ist
- Das Admin-Netzwerk kann während der Bereitstellung des Grid-Knotens konfiguriert werden, um den Zugriff auf die Installations-Benutzeroberfläche zu ermöglichen, bevor das Grid vollständig installiert ist.

Optionale Schnittstellen

Optional können Sie einem Node zusätzliche Schnittstellen hinzufügen. Beispielsweise möchten Sie einem Admin- oder Gateway-Node eine Trunk-Schnittstelle hinzufügen, sodass Sie verwenden können VLAN-Schnittstellen Zur Trennung des Datenverkehrs von unterschiedlichen Applikationen oder Mandanten. Oder Sie möchten möglicherweise eine Zugriffsschnittstelle hinzufügen, die in A verwendet werden soll Hochverfügbarkeitsgruppe (High Availability Group, HA-Gruppe.

Informationen zum Hinzufügen von Trunk- oder Access-Schnittstellen finden Sie unter:

- **VMware (nach der Installation des Knotens)**: VMware: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node
- **RHEL oder CentOS (vor dem Installieren des Knotens)**: Erstellen von Node-Konfigurationsdateien
- **Ubuntu oder Debian (vor der Installation des Knotens)**: Erstellen von Node-Konfigurationsdateien
- **RHEL, CentOS, Ubuntu oder Debian (nach der Installation des Knotens)**: Linux: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node

Zeigen Sie IP-Adressen an

Sie können die IP-Adresse für jeden Grid-Node im StorageGRID System anzeigen. Sie können diese IP-Adresse dann verwenden, um sich bei dem Grid-Node über die Befehlszeile anzumelden und verschiedene Wartungsvorgänge auszuführen.

Was Sie benötigen

Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.

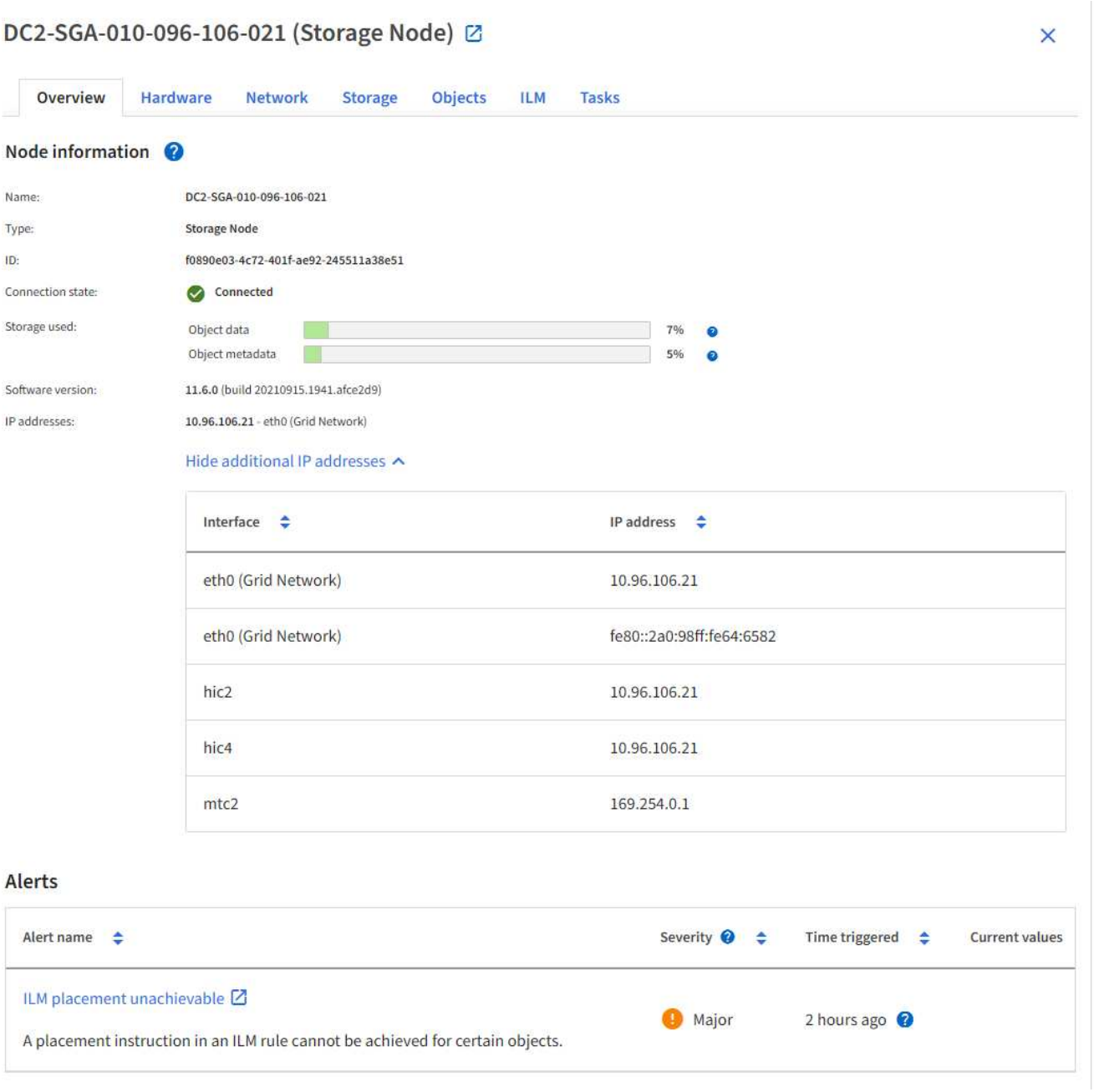
Über diese Aufgabe

Informationen zum Ändern von IP-Adressen finden Sie unter Recovery und Wartung.

Schritte

1. Wählen Sie **NODES** ***Grid Node*** **Übersicht** aus.
2. Wählen Sie **Mehr anzeigen** rechts neben dem Titel der IP-Adressen.

   Die IP-Adressen für diesen Grid-Node werden in einer Tabelle aufgeführt.



Unterstützte Chiffren für ausgehende TLS-Verbindungen

Das StorageGRID System unterstützt eine begrenzte Anzahl von Verschlüsselungssuiten für TLS-Verbindungen (Transport Layer Security) zu den externen Systemen, die für Identitätsföderation und Cloud-Storage-Pools verwendet werden.

Unterstützte Versionen von TLS

StorageGRID unterstützt TLS 1.2 und TLS 1.3 für Verbindungen zu externen Systemen, die für Identitätsföderation und Cloud-Storage-Pools verwendet werden.

Die zur Verwendung mit externen Systemen unterstützten TLS-Chiffren wurden ausgewählt, um die Kompatibilität mit verschiedenen externen Systemen sicherzustellen. Die Liste ist größer als die Liste der Chiffren, die zur Verwendung mit S3- oder Swift-Client-Applikationen unterstützt werden.

TLS-Konfigurationsoptionen wie Protokollversionen, Chiffren, Schlüsselaustausch-Algorithmen und MAC-Algorithmen sind in StorageGRID nicht konfigurierbar. Wenden Sie sich an Ihren NetApp Ansprechpartner, wenn Sie spezifische Anfragen zu diesen Einstellungen haben.

Unterstützte TLS 1.2-Cipher-Suiten

Die folgenden TLS 1.2-Chiffre-Suiten werden unterstützt:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

Unterstützte TLS 1.3-Cipher-Suiten

Die folgenden TLS 1.3-Chiffre-Suiten werden unterstützt:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

Netzwerkübertragungsverschlüsselung ändern

Das StorageGRID System verwendet Transport Layer Security (TLS) zum Schutz des internen Kontrolldatenverkehrs zwischen den Grid-Nodes. Die Option „Netzwerkübertragungsverschlüsselung“ legt den von TLS verwendeten Algorithmus zur Verschlüsselung der Datenverkehrskontrolle zwischen den Grid-Nodes fest. Diese Einstellung hat keine Auswirkung auf die Datenverschlüsselung.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Standardmäßig verwendet die Netzwerkübertragungsverschlüsselung den AES256-SHA-Algorithmus. Der Kontrolldatenverkehr kann auch mit dem AES128-SHA-Algorithmus verschlüsselt werden.

Schritte

1. Wählen Sie **KONFIGURATION System Gitteroptionen**.
2. Ändern Sie im Abschnitt Netzwerkoptionen die Netzwerkübertragungsverschlüsselung in **AES128-SHA** oder **AES256-SHA** (Standardeinstellung).

3. Wählen Sie **Speichern**.

Verwalten von Richtlinien zur Verkehrsklassifizierung

Verwalten von Richtlinien zur Verkehrsklassifizierung

Zur Verbesserung Ihrer QoS-Angebote (Quality of Service) können Sie Richtlinien zur Traffic-Klassifizierung erstellen, um verschiedene Arten von Netzwerkverkehr zu identifizieren und zu überwachen. Diese Richtlinien unterstützen die Begrenzung und das Monitoring des Datenverkehrs.

Richtlinien zur Traffic-Klassifizierung werden auf Endpunkte im StorageGRID Load Balancer Service für Gateway-Knoten und Admin-Nodes angewendet. Zum Erstellen von Richtlinien für die Verkehrsklassifizierung müssen Sie bereits Load Balancer Endpunkte erstellt haben.

Übereinstimmungsregeln

Jede Traffic-Klassifizierungsrichtlinie enthält mindestens eine übereinstimmende Regel, um den Netzwerkverkehr zu identifizieren, der mit einer oder mehreren der folgenden Einheiten in Verbindung steht:

- Buckets
- Mandanten
- Subnetze (IPv4-Subnetze, in denen der Client enthalten ist)
- Endpunkte (Load Balancer Endpunkte)

StorageGRID überwacht den Datenverkehr, der mit allen Regeln innerhalb der Richtlinie im Einklang mit den Zielen der Regel steht. Jeder Traffic, der einer Richtlinie entspricht, wird von dieser Richtlinie übernommen. Umgekehrt können Sie Regeln festlegen, die mit dem gesamten Verkehr übereinstimmen, außer einer angegebenen Einheit.

Traffic-Beschränkung

Optional können Sie Obergrenzen für eine Richtlinie auf Basis der folgenden Parameter festlegen:

- Aggregat-Bandbreite In
- Horizontale Aggregatbandbreite
- Gleichzeitige Leseanforderungen
- Anforderungen Für Gleichzeitige Schreibvorgänge
- Bandbreite Pro Anfrage In
- Bandbreitenausforderung Pro Anfrage

- Leseanforderungsrate
- Schreibanforderungen-Rate

Grenzwerte werden pro Load Balancer erzwungen. Wenn der Datenverkehr gleichzeitig auf mehrere Load Balancer verteilt wird, sind die maximalen Raten ein Vielfaches der von Ihnen angegebenen Ratenlimits.

> Sie können Richtlinien erstellen, um die aggregierte Bandbreite zu begrenzen oder die Bandbreite nach Bedarf zu begrenzen. StorageGRID kann jedoch nicht beide Bandbreitenarten gleichzeitig einschränken. Eine Einschränkung der Bandbreite im Aggregat kann eine zusätzliche geringfügige Auswirkung auf die Performance des nicht begrenzten Datenverkehrs haben.

Bei Bandbreitenbeschränkungen oder -Anforderungen werden die Anforderungen mit der von Ihnen festgelegten Rate in- oder Out-Streaming übertragen. StorageGRID kann nur eine Geschwindigkeit erzwingen. Daher ist die jeweils spezifischste Richtlinienabgleiche nach Matcher-Typ erzwungen. Bei allen anderen Grenzwerttypen werden Clientanforderungen um 250 Millisekunden verzögert und bei Anfragen, die die übereinstimmende Richtlinienbegrenzung überschreiten, eine langsame Antwort von 503 erhalten.

Im Grid Manager können Sie Traffic-Diagramme anzeigen und überprüfen, ob die Richtlinien die von Ihnen erwarteten Verkehrsgrenzen durchsetzen.

Richtlinien für die Verkehrsklassifizierung mit SLAs

Sie können Richtlinien für die Traffic-Klassifizierung in Verbindung mit Kapazitätsgrenzen und Datensicherung verwenden, um Service Level Agreements (SLAs) durchzusetzen, die Besonderheiten bei Kapazität, Datensicherung und Performance bieten.

Pro Load Balancer werden Einschränkungen für die Verkehrsklassifizierung implementiert. Wenn der Datenverkehr gleichzeitig auf mehrere Load Balancer verteilt wird, sind die maximalen Raten ein Vielfaches der von Ihnen angegebenen Ratenlimits.

Das folgende Beispiel zeigt drei SLA-Tiers. Sie können Traffic-Klassifizierungsrichtlinien erstellen, um die Performance-Ziele jeder SLA-Ebene zu erreichen.

Service Level-Ebene	Kapazität	Datensicherung	Leistung	Kosten
Gold	1 PB Speicherplatz zulässig	3 ILM-Regel für Kopien	25 K Anfragen/Sek. 5 GB/s (40 Gbit/s) Bandbreite	Kosten pro Monat
Silber	250 TB Speicherplatz zulässig	ILM-Regel für 2 Kopien	10 K Anfragen/Sek. 1.25 GB/s (10 Gbit/s) Bandbreite	Kosten pro Monat
Bronze	100 TB Speicherplatz zulässig	ILM-Regel für 2 Kopien	5 K Anfragen/Sek. 1 GB/s (8 Gbit/s) Bandbreite	Kosten pro Monat

Richtlinien für die Verkehrsklassifizierung erstellen

Sie erstellen Traffic-Klassifizierungsrichtlinien, wenn Sie den Netzwerkverkehr nach Bucket, Mandanten, IP-Subnetz oder Load Balancer-Endpunkt überwachen und optional begrenzen möchten. Optional können Sie Obergrenzen für eine Richtlinie basierend auf der Bandbreite, der Anzahl gleichzeitiger Anfragen oder der Anfragerate festlegen.

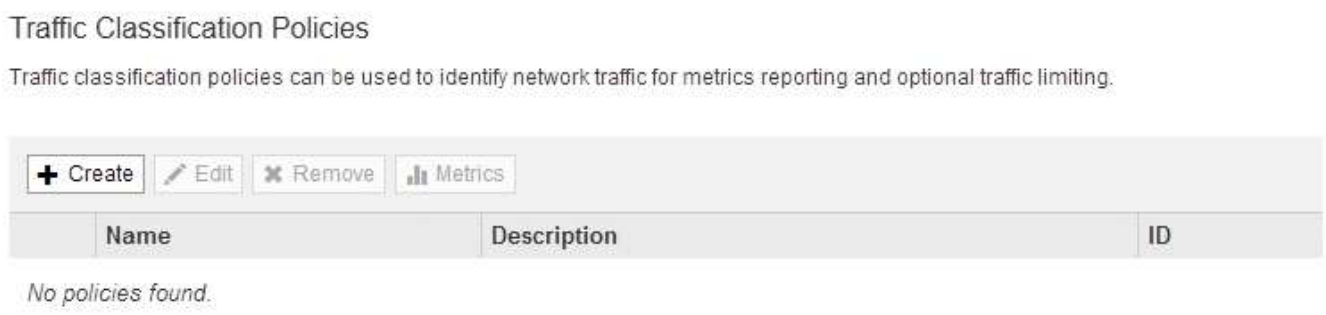
Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben die Root-Zugriffsberechtigung.
- Sie haben alle Load Balancer-Endpunkte erstellt, die übereinstimmen sollen.
- Sie haben alle Mandanten erstellt, denen Sie entsprechen möchten.

Schritte

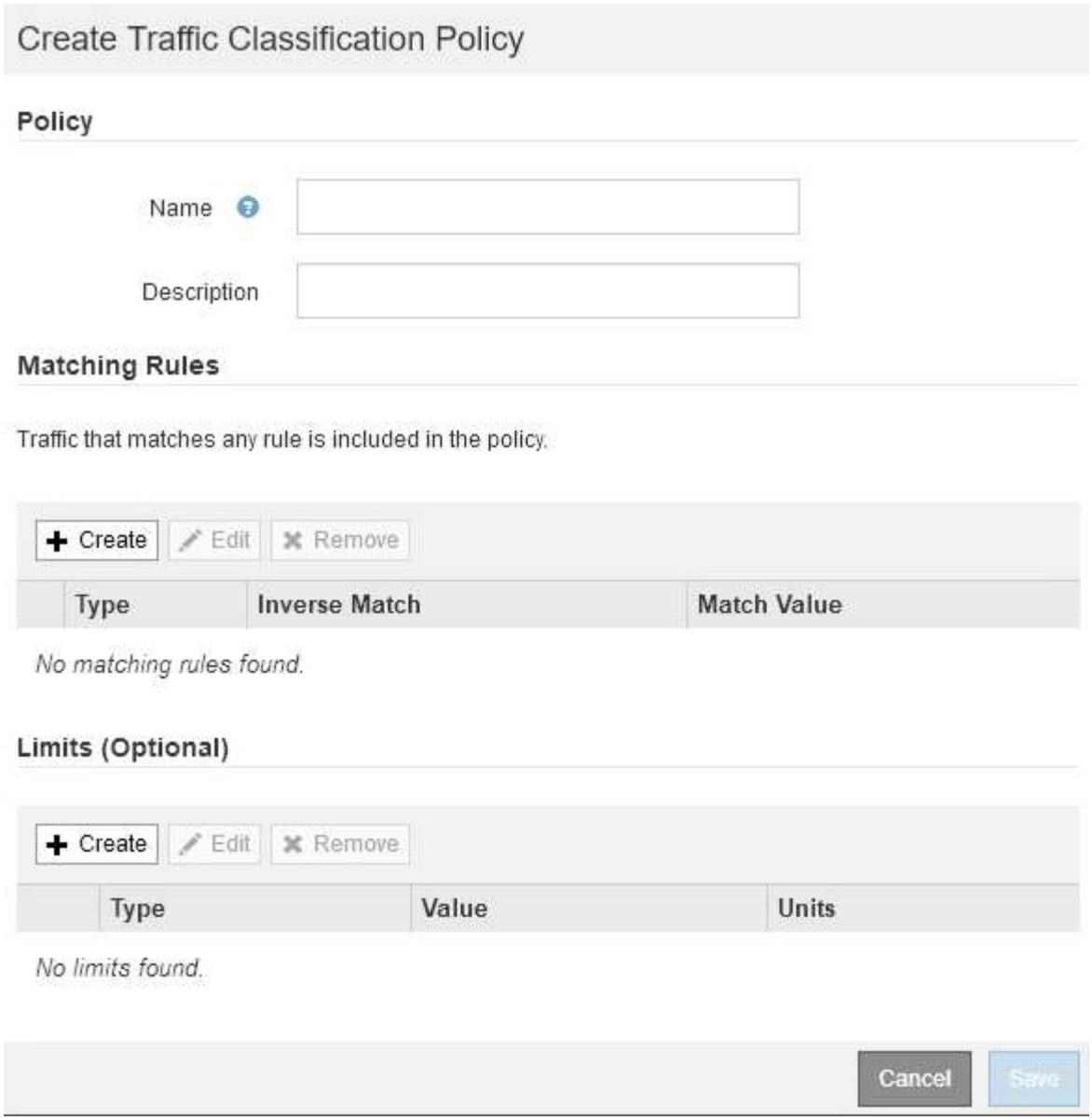
1. Wählen Sie **KONFIGURATION Netzwerk Verkehrsklassifizierung**.

   Die Seite Richtlinien zur Klassifizierung von Verkehrsdaten wird angezeigt.



2. Wählen Sie **Erstellen**.

   Das Dialogfeld Richtlinie zur Verkehrsklassifizierung erstellen wird angezeigt.



3. Geben Sie im Feld **Name** einen Namen für die Richtlinie ein.

   Geben Sie einen beschreibenden Namen ein, damit Sie die Richtlinie erkennen können.

4. Fügen Sie optional eine Beschreibung für die Richtlinie im Feld **Beschreibung** hinzu.

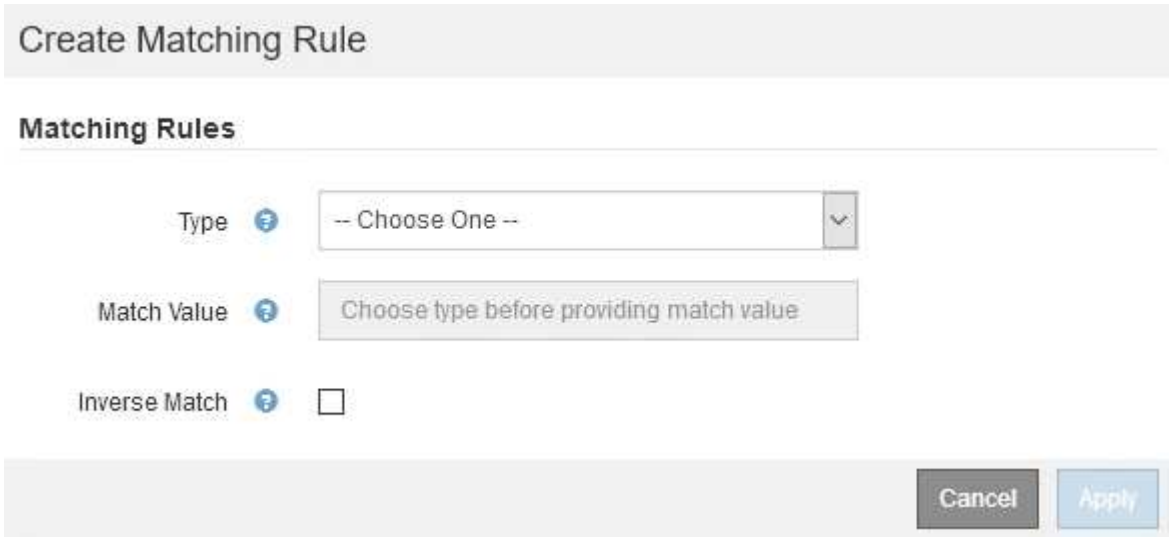
   Beschreiben Sie beispielsweise, auf welche Weise diese Richtlinie zur Klassifizierung von Verkehrsdaten zutrifft und welche Begrenzung sie hat.

5. Erstellen Sie eine oder mehrere passende Regeln für die Richtlinie.

   Die übereinstimmenden Regeln steuern, welche Einheiten von dieser Traffic-Klassifizierungsrichtlinie betroffen sein werden. Wählen Sie beispielsweise Tenant aus, wenn diese Richtlinie auf den Netzwerkverkehr für einen bestimmten Mandanten angewendet werden soll. Oder wählen Sie Endpunkt aus, wenn diese Richtlinie auf den Netzwerkverkehr auf einem bestimmten Load Balancer-Endpunkt angewendet werden soll.

   a. Wählen Sie im Abschnitt **passende Regeln** die Option **Erstellen** aus.

Das Dialogfeld „passende Regel erstellen“ wird angezeigt.



b. Wählen Sie im Dropdown-Menü **Typ** den Typ der Entität aus, die in die übereinstimmende Regel aufgenommen werden soll.

c. Geben Sie im Feld **Match-Wert** einen Match-Wert basierend auf dem gewählten Entitätstyp ein.

   - Bucket: Geben Sie einen Bucket-Namen ein.
   - Bucket-Regex: Geben Sie einen regulären Ausdruck ein, der für eine Reihe von Bucket-Namen verwendet wird.

     Der reguläre Ausdruck ist nicht verankert. Verwenden Sie den ^-Anker, um am Anfang des Bucket-Namens zu entsprechen, und verwenden Sie den €-Anker, um am Ende des Namens zu entsprechen.

   - CIDR: Geben Sie ein IPv4-Subnetz in CIDR-Notation ein, das dem gewünschten Subnetz entspricht.
   - Endpunkt: Wählen Sie einen Endpunkt aus der Liste der vorhandenen Endpunkte aus. Dies sind die Load Balancer Endpunkte, die Sie auf der Seite Load Balancer Endpoints definiert haben. Siehe Konfigurieren von Load Balancer-Endpunkten.
   - Mandant: Wählen Sie einen Mandanten aus der Liste der bestehenden Mandanten aus. Die Zuordnung von Mandanten basiert auf dem Besitz des Buckets, auf dem zugegriffen wird. Der anonyme Zugriff auf einen Bucket entspricht dem Mandanten, der den Bucket besitzt.

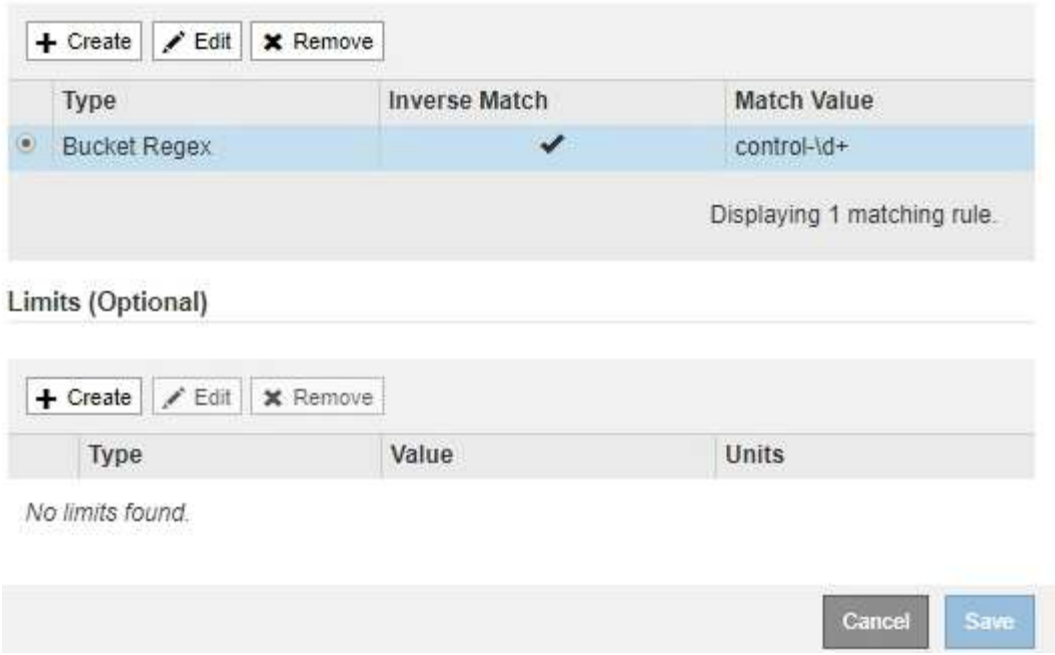
d. Wenn Sie dem gesamten Netzwerkverkehr *außer* Traffic entsprechen möchten, der mit dem gerade definierten Typ- und Vergleichswert übereinstimmt, aktivieren Sie das Kontrollkästchen **inverse**. Lassen Sie andernfalls das Kontrollkästchen nicht ausgewählt.

   Wenn diese Richtlinie beispielsweise auf alle Endpunkte des Load Balancer angewendet werden soll, geben Sie den zu ausgeschlossenen Endpunkt für den Load Balancer an und wählen Sie **Inverse** aus.

   > Bei einer Richtlinie, die mehrere Matriken enthält, bei denen mindestens eine inverse Matrix ist, sollten Sie darauf achten, keine Richtlinie zu erstellen, die allen Anforderungen entspricht.

e. Wählen Sie **Anwenden**.

   Die Regel wird erstellt und in der Tabelle Abpassende Regeln aufgeführt.



a. Wiederholen Sie diese Schritte für jede Regel, die Sie für die Richtlinie erstellen möchten.

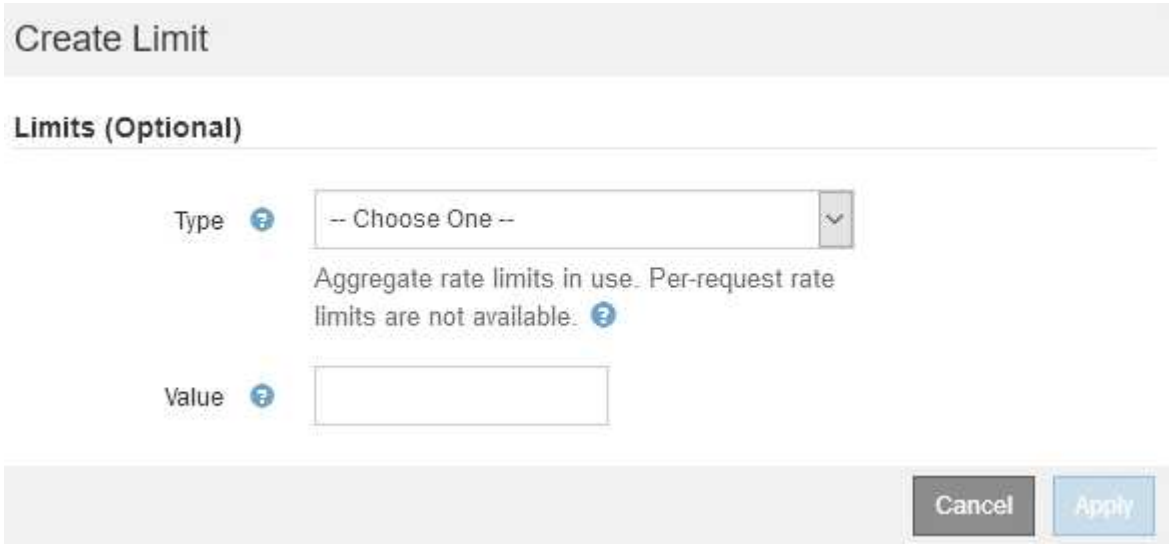
Datenverkehr, der einer Regel entspricht, wird von der Richtlinie übernommen.

6. Optional können Grenzen für die Richtlinie erstellt werden.

Selbst wenn Sie keine Grenzen erstellen, sammelt StorageGRID Metriken, sodass Sie den Netzwerk-Traffic, der der Richtlinie entspricht, überwachen können.

a. Wählen Sie im Abschnitt **Grenzwerte** die Option * Erstellen*.

Das Dialogfeld Limit erstellen wird angezeigt.



b. Wählen Sie im Dropdown-Menü **Typ** den Grenzwert aus, den Sie auf die Richtlinie anwenden möchten.

In der folgenden Liste bezieht sich **in** auf Datenverkehr von S3- oder Swift-Clients auf den StorageGRID-Load-Balancer, und **out** bezieht sich auf den Datenverkehr vom Load Balancer auf S3-

oder Swift-Clients.

- Aggregat-Bandbreite In
- Horizontale Aggregatbandbreite
- Gleichzeitige Leseanforderungen
- Anforderungen Für Gleichzeitige Schreibvorgänge
- Bandbreite Pro Anfrage In
- Bandbreitenausforderung Pro Anfrage
- Leseanforderungsrate
- Schreibanforderungen-Rate

> Sie können Richtlinien erstellen, um die aggregierte Bandbreite zu begrenzen oder die Bandbreite nach Bedarf zu begrenzen. StorageGRID kann jedoch nicht beide Bandbreitenarten gleichzeitig einschränken. Eine Einschränkung der Bandbreite im Aggregat kann eine zusätzliche geringfügige Auswirkung auf die Performance des nicht begrenzten Datenverkehrs haben.

Bei Bandbreitenbeschränkungen wendet StorageGRID die Richtlinie an, die der jeweils festgelegten Grenzwertart am besten entspricht. Wenn Sie beispielsweise eine Richtlinie haben, die Datenverkehr in nur eine Richtung begrenzt, ist der Datenverkehr in die entgegengesetzte Richtung unbegrenzt, selbst wenn der Datenverkehr mit zusätzlichen Richtlinien mit Bandbreitenbeschränkungen übereinstimmt. StorageGRID implementiert „`Best`“-Übereinstimmungen für Bandbreiteneinschränkungen in der folgenden Reihenfolge:

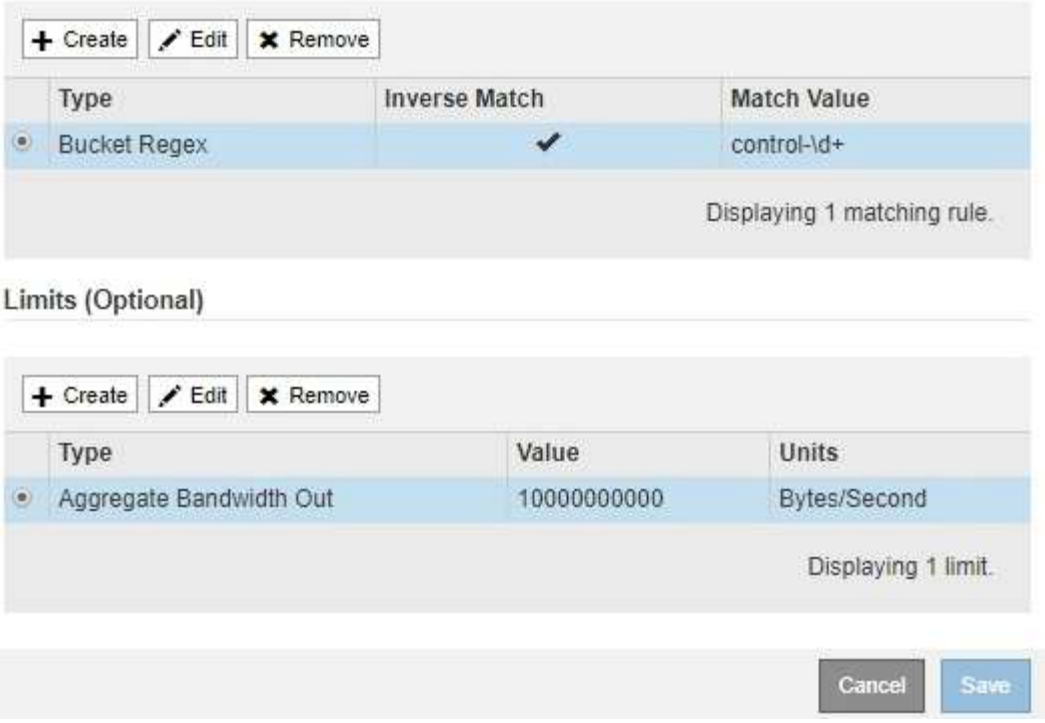
- Exakte IP-Adresse (/32-Maske)
- Exakter Bucket-Name
- Eimer-Regex
- Mandant
- Endpunkt
- Nicht exakte CIDR-Übereinstimmungen (nicht /32)
- Umgekehrte Übereinstimmungen

c. Geben Sie im Feld **Wert** einen numerischen Wert für den gewählten Grenzwert ein.

   Die erwarteten Einheiten werden angezeigt, wenn Sie ein Limit auswählen.

d. Wählen Sie **Anwenden**.

   Die Begrenzung wird erstellt und in der Grenzwertetabelle aufgelistet.



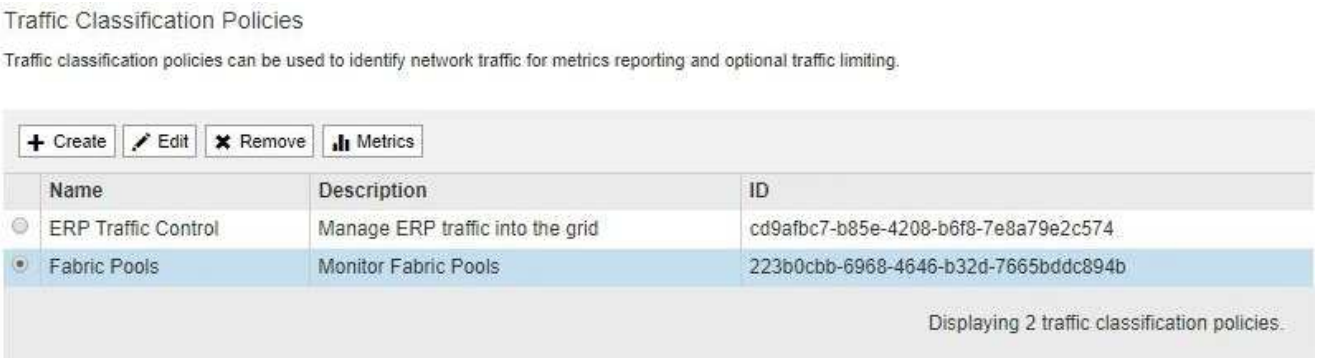
e. Wiederholen Sie diese Schritte für jedes Limit, das Sie der Richtlinie hinzufügen möchten.

   Wenn Sie beispielsweise ein Bandbreitenlimit von 40 Gbit/s für eine SLA-Ebene erstellen möchten, erstellen Sie eine aggregierte Bandbreitennutzung und ein Bandbreitenlimit und legen Sie jede auf 40 Gbit/s fest.

   Um Megabyte pro Sekunde in Gigabit pro Sekunde zu konvertieren, multiplizieren Sie mit acht. Beispielsweise entspricht 125 MB/s 1,000 Mbit/s oder 1 Gbit/s.

7. Wenn Sie mit dem Erstellen von Regeln und Limits fertig sind, wählen Sie **Speichern**.

   Die Richtlinie wird gespeichert und in der Tabelle „Richtlinien zur Klassifizierung von Verkehrsdaten“ aufgeführt.



   Der S3- und Swift-Client-Traffic wird nun gemäß den Traffic-Klassifizierungsrichtlinien gehandhabt. Sie können Verkehrsdiagramme anzeigen und überprüfen, ob die Richtlinien die von Ihnen erwarteten Verkehrsgrenzwerte durchsetzen. Siehe Zeigen Sie Metriken zum Netzwerkverkehr an.

Bearbeiten Sie eine Traffic-Klassifizierungsrichtlinie

Sie können eine Traffic-Klassifizierungsrichtlinie bearbeiten, um ihren Namen oder ihre Beschreibung zu ändern oder um Regeln oder Grenzen für die Richtlinie zu erstellen, zu bearbeiten oder zu löschen.

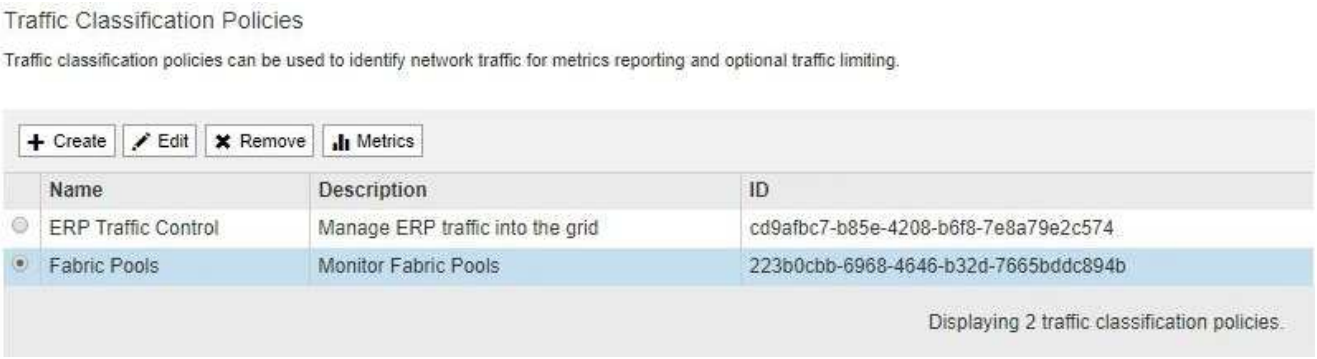
Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben die Root-Zugriffsberechtigung.

Schritte

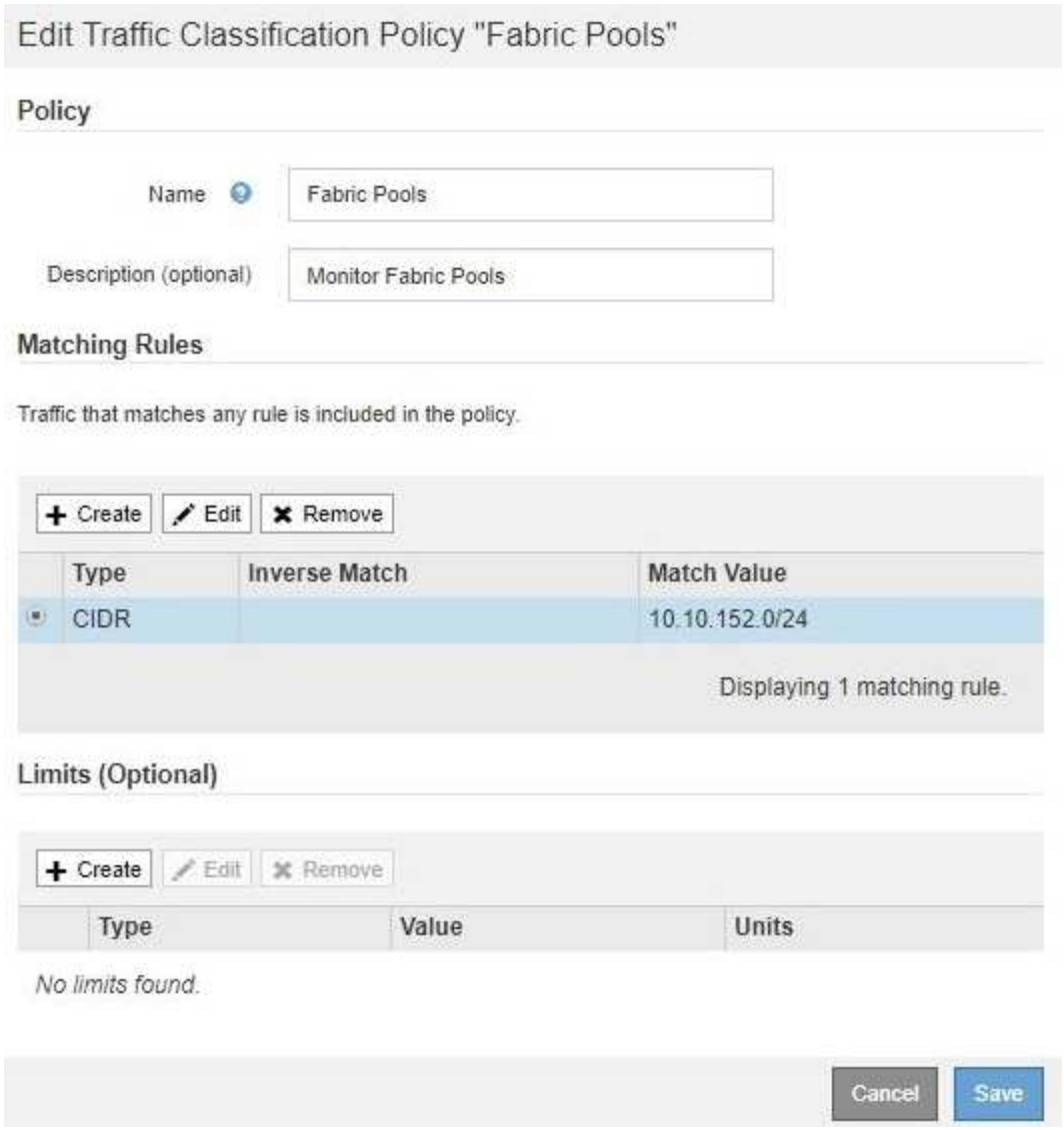
1. Wählen Sie **KONFIGURATION Netzwerk Verkehrsklassifizierung**.

   Die Seite Richtlinien zur Klassifizierung von Verkehrsdaten wird angezeigt, und die vorhandenen Richtlinien sind in der Tabelle aufgeführt.



2. Wählen Sie das Optionsfeld links neben der Richtlinie, die Sie bearbeiten möchten.
3. Wählen Sie **Bearbeiten**.

   Das Dialogfeld Richtlinie zur Klassifizierung von Datenverkehr bearbeiten wird angezeigt.



4. Erstellen, Bearbeiten oder Entfernen übereinstimmender Regeln und Grenzen nach Bedarf.
   a. Um eine übereinstimmende Regel oder ein entsprechendes Limit zu erstellen, wählen Sie **Erstellen** aus, und befolgen Sie die Anweisungen zum Erstellen einer Regel oder zum Erstellen eines Limits.
   b. Um eine passende Regel oder Grenze zu bearbeiten, wählen Sie die Optionsschaltfläche für die Regel oder die Begrenzung aus, wählen Sie im Abschnitt **passende Regeln** oder im Abschnitt **Grenzen** die Option **Bearbeiten** und befolgen Sie die Anweisungen zum Erstellen einer Regel oder zum Erstellen eines Limits.
   c. Um eine passende Regel oder Begrenzung zu entfernen, wählen Sie die Optionsschaltfläche für die Regel oder die Begrenzung aus, und wählen Sie **Entfernen**. Wählen Sie dann **OK** aus, um zu bestätigen, dass Sie die Regel oder das Limit entfernen möchten.
5. Wenn Sie mit dem Erstellen oder Bearbeiten einer Regel oder eines Limits fertig sind, wählen Sie **Anwenden**.
6. Wenn Sie mit der Bearbeitung der Richtlinie fertig sind, wählen Sie **Speichern**.

   Die an der Richtlinie vorgenommenen Änderungen werden gespeichert, und der Netzwerkverkehr wird nun gemäß den Richtlinien zur Klassifizierung von Verkehrsmeldungen verarbeitet. Sie können Verkehrsdiagramme anzeigen und überprüfen, ob die Richtlinien die von Ihnen erwarteten Verkehrsgrenzwerte durchsetzen.

Löschen einer Traffic-Klassifizierungsrichtlinie

Wenn Sie keine Traffic-Klassifizierungsrichtlinie mehr benötigen, können Sie sie löschen.

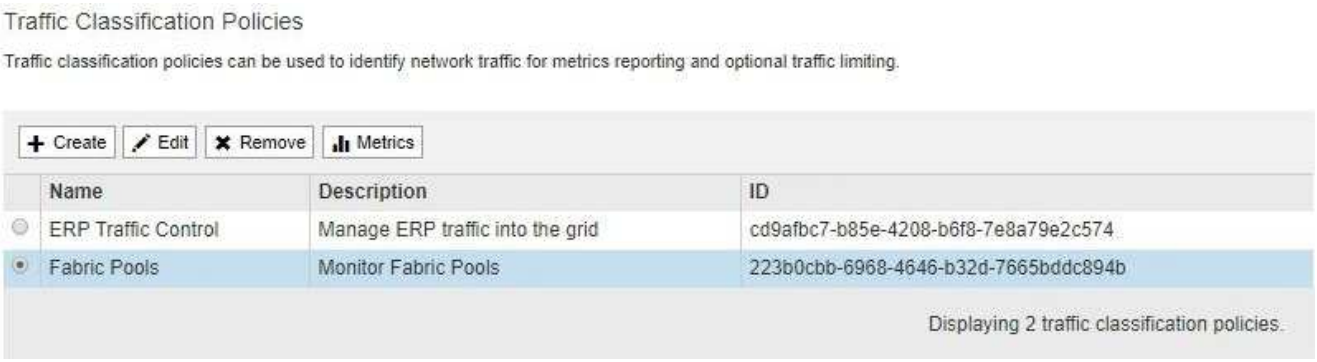
Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben die Root-Zugriffsberechtigung.

Schritte

1. Wählen Sie **KONFIGURATION Netzwerk Verkehrsklassifizierung**.

   Die Seite Richtlinien zur Klassifizierung von Verkehrsdaten wird angezeigt, und die vorhandenen Richtlinien sind in der Tabelle aufgeführt.



2. Wählen Sie das Optionsfeld links neben der Richtlinie, die Sie löschen möchten.
3. Wählen Sie **Entfernen**.

   Ein Warndialogfeld wird angezeigt.

4. Wählen Sie **OK**, um zu bestätigen, dass Sie die Richtlinie löschen möchten.

   Die Richtlinie wird gelöscht.

Zeigen Sie Metriken zum Netzwerkverkehr an

Sie können den Netzwerkverkehr überwachen, indem Sie die Diagramme aufrufen, die auf der Seite Richtlinien zur Klassifizierung von Verkehrsmeldungen verfügbar sind.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.

- Sie verfügen über die Berechtigung Root Access oder die Berechtigungen für Mandantenkonten.

Über diese Aufgabe

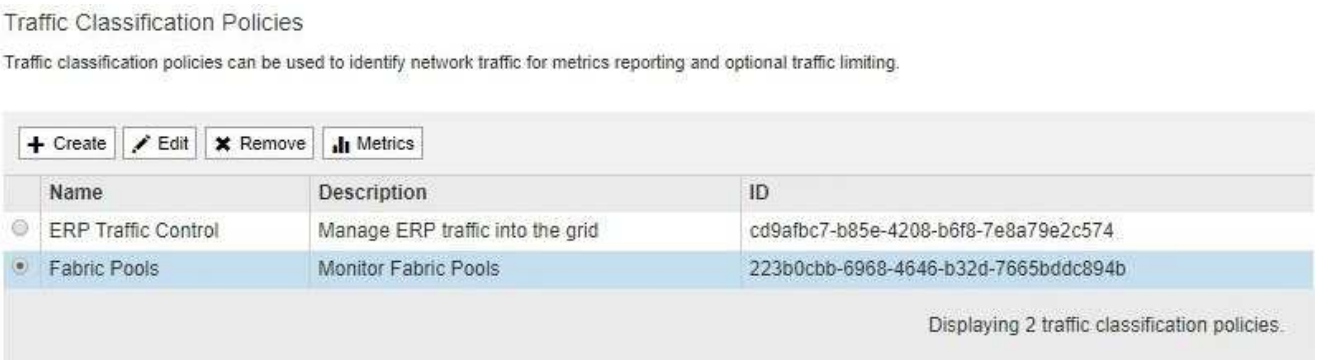
Für alle vorhandenen Traffic-Klassifizierungsrichtlinien können Sie Kennzahlen für den Load Balancer-Service anzeigen, um festzustellen, ob die Richtlinie den Datenverkehr im Netzwerk erfolgreich einschränkt. Anhand der Daten in den Diagrammen können Sie bestimmen, ob Sie die Richtlinie anpassen müssen.

Auch wenn für eine Richtlinie zur Klassifizierung von Datenverkehr keine Grenzen gesetzt wurden, werden Kennzahlen erfasst und die Diagramme bieten nützliche Informationen zum Verständnis von Verkehrstrends.

Schritte

1. Wählen Sie **KONFIGURATION Netzwerk Verkehrsklassifizierung**.

   Die Seite Richtlinien zur Klassifizierung von Verkehrsdaten wird angezeigt, und die vorhandenen Richtlinien sind in der Tabelle aufgeführt.



   Die Schaltflächen **Erstellen**, **Bearbeiten** und **Entfernen** sind deaktiviert, wenn Sie über die Berechtigung für Mandantenkonten verfügen, aber nicht über die Berechtigung Root-Zugriff verfügen.

2. Wählen Sie das Optionsfeld links neben der Richtlinie, für die Sie Metriken anzeigen möchten.
3. Wählen Sie **Metriken**.

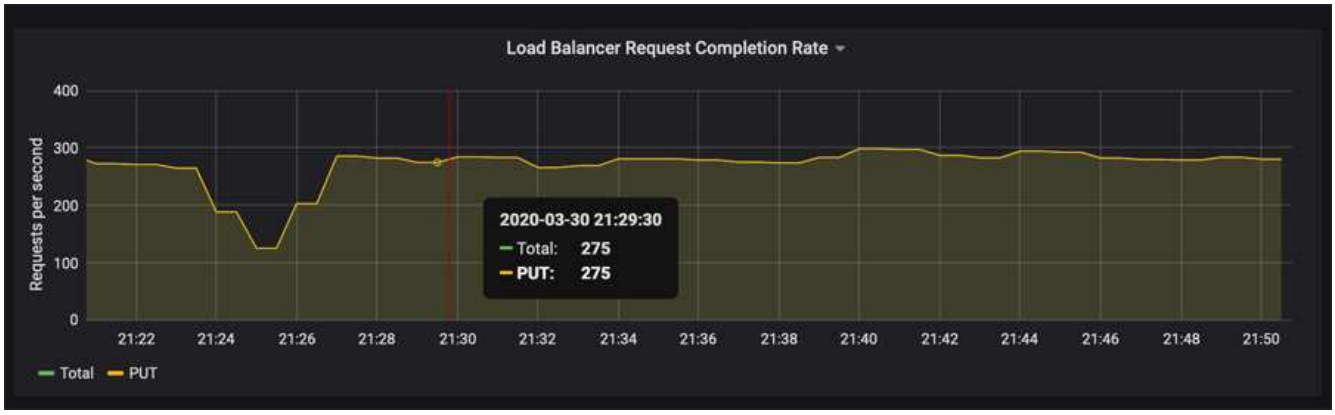
   Es wird ein neues Browserfenster geöffnet, und die Diagramme der Richtlinie zur Klassifizierung von Datenverkehr werden angezeigt. Die Diagramme zeigen Metriken nur für den Datenverkehr an, der mit der ausgewählten Richtlinie übereinstimmt.

   Sie können andere Richtlinien auswählen, die Sie anzeigen möchten, indem Sie das Pulldown-Menü **Policy** verwenden.

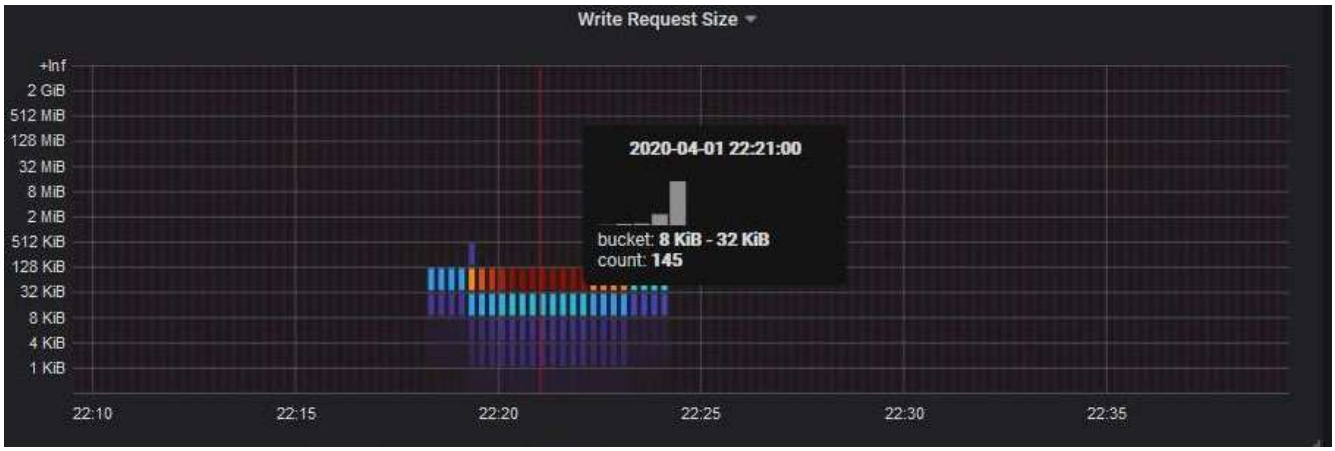
Die folgenden Diagramme sind auf der Webseite enthalten.

- Load Balancer Request Traffic: Dieses Diagramm liefert einen 3-minütigen Moving Average des Durchsatzes von Daten, die zwischen Load Balancer Endpunkten und den Clients, die die Anforderungen bearbeiten, in Bits pro Sekunde übertragen werden.
- Abschlusssatz für Lastbalancer-Anfragen: Dieses Diagramm bietet einen 3-minütigen Moving-Durchschnitt der Anzahl der abgeschlossenen Anfragen pro Sekunde, aufgeschlüsselt nach Anforderungstyp (GET, PUT, HEAD, DELETE). Dieser Wert wird aktualisiert, wenn die Kopfzeilen einer neuen Anfrage validiert wurden.
- Fehlerantwortzrate: Dieses Diagramm zeigt einen 3-minütigen Moving Average der Anzahl der an Kunden pro Sekunde zurückgegebenen Fehlerantworten, aufgeschlüsselt nach dem Fehlercode.
- Durchschnittliche Anfragedauer (nicht-Fehler): Dieses Diagramm bietet einen 3-minütigen Moving Average of Request durations, aufgeschlüsselt nach Anforderungstyp (GET, PUT, HEAD, DELETE). Jede Anforderungsdauer beginnt, wenn eine Anforderungs-Kopfzeile vom Lastbalancer-Dienst analysiert wird und endet, wenn der vollständige Antwortkörper an den Client zurückgesendet wird.
- Schreibanforderungsrate nach Objektgröße: Diese Heatmap bietet einen Moving Average von 3 Minuten für die Geschwindigkeit, mit der Schreibanforderungen basierend auf Objektgröße abgeschlossen werden. In diesem Zusammenhang beziehen sich Schreibanforderungen nur auf PUT-Anforderungen.
- Leseanforderungsrate nach Objektgröße: Dieser Heatmap bietet einen 3-minütigen Moving-Durchschnitt der Rate, mit der Leseanforderungen anhand der Objektgröße abgeschlossen werden. In diesem Zusammenhang beziehen sich Leseanforderungen nur auf ANFORDERUNGEN, DIE ABGERUFEN werden sollen. Die Farben in der Heatmap zeigen die relative Frequenz einer Objektgröße innerhalb eines einzelnen Diagramms an. Die kühleren Farben (z. B. violett und blau) zeigen niedrigere relative Raten an, und die wärmeren Farben (z. B. Orange und Rot) zeigen höhere relative Raten an.

4. Bewegen Sie den Cursor über ein Liniendiagramm, um ein Popup-Fenster mit Werten auf einem bestimmten Teil des Diagramms anzuzeigen.



5. Bewegen Sie den Mauszeiger über eine Heatmap, um ein Popup-Fenster mit Datum und Uhrzeit der Probe, Objektgrößen, die in die Anzahl aggregiert werden, und die Anzahl der Anfragen pro Sekunde in diesem Zeitraum anzuzeigen.



6. Verwenden Sie das Pull-down-Menü **Policy** oben links, um eine andere Richtlinie auszuwählen.

   Die Diagramme für die ausgewählte Richtlinie werden angezeigt.

7. Alternativ können Sie über das Menü * SUPPORT* auf die Diagramme zugreifen.
   a. Wählen Sie **SUPPORT Tools Kennzahlen** aus.
   b. Wählen Sie im Abschnitt **Grafana** der Seite die Option **Traffic Classification Policy** aus.
   c. Wählen Sie die Richtlinie aus der Dropdown-Liste oben links auf der Seite aus.

      Richtlinien für die Verkehrsklassifizierung werden anhand ihrer ID identifiziert. Richtlinien-IDs sind auf der Seite Richtlinien zur Klassifizierung von Verkehrsdaten aufgeführt.

8. Analysieren Sie die Diagramme, um zu ermitteln, wie oft die Richtlinie den Datenverkehr einschränkt und ob Sie die Richtlinie anpassen müssen.

Verwandte Informationen

Monitoring und Fehlerbehebung

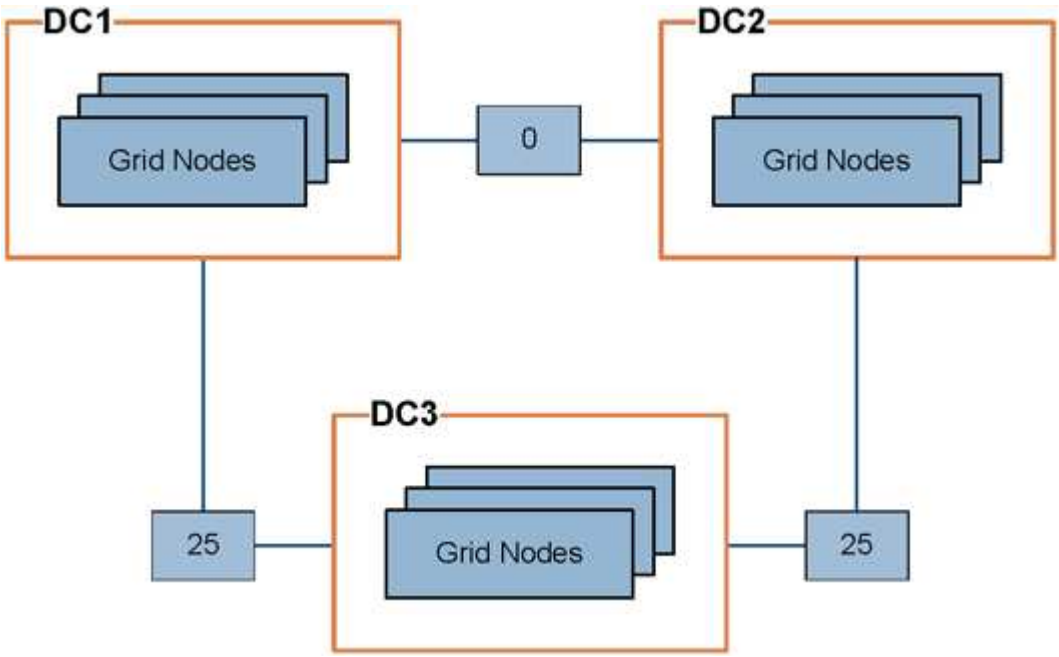
Verwalten Sie Verbindungskosten

Was sind Verbindungskosten

Durch die Verbindungskosten können Sie festlegen, welcher Datacenter-Standort einen angeforderten Service bereitstellt, wenn zwei oder mehr Datacenter-Standorte vorhanden sind. Sie können die Verbindungskosten anpassen, um die Latenz zwischen Standorten reflektieren.

- Die Link-Kosten werden verwendet, um Prioritäten zu setzen, welche Objektkopie für die Bearbeitung von Objektabrufungen verwendet wird.
- Die Link-Kosten werden von der Grid-Management-API und der Mandanten-Management-API verwendet, um festzustellen, welche internen StorageGRID-Services verwendet werden sollen.
- Die Verbindungskosten werden vom veralteten Connection Load Balancer (CLB)-Dienst auf Gateway-Knoten zur direkten Weiterleitung von Client-Verbindungen verwendet. Siehe Wie der Lastenausgleich funktioniert - CLB-Service.

Das Diagramm zeigt ein drei Standortraster mit Verbindungskosten, die zwischen Standorten konfiguriert sind:



- Der CLB-Service auf Gateway-Knoten verteilt Client-Verbindungen gleichermaßen auf alle Storage-Nodes am selben Datacenter-Standort und an beliebige Datacenter-Standorte mit einem Linkskosten von 0.

  Im Beispiel verteilt ein Gateway-Node am Datacenter-Standort 1 (DC1) Client-Verbindungen gleichmäßig auf Storage-Nodes an DC1 und Storage Nodes an DC2. Ein Gateway-Node bei DC3 sendet Client-Verbindungen nur zu Storage-Nodes an DC3.

- Beim Abrufen eines Objekts, das als mehrere replizierte Kopien vorhanden ist, ruft StorageGRID die Kopie im Datacenter ab, das die niedrigsten Verbindungskosten bietet.

  Wenn eine Client-Anwendung an DC2 ein Objekt abruft, das sowohl an DC1 als auch an DC3 gespeichert ist, wird das Objekt von DC1 abgerufen, da die Verbindungskosten von DC1 bis D2 0 sind, was niedriger ist als die Verbindungskosten von DC3 nach DC2 (25).

Verbindungskosten sind willkürliche relative Zahlen ohne spezifische Maßeinheit. So werden beispielsweise die Linkkosten von 50 weniger bevorzugt genutzt als eine Linkkosten von 25. In der Tabelle sind die häufig

verwendeten Verbindungskosten aufgeführt.

Verlinken	Verbindungskosten	Hinweise
Zwischen physischen Datacenter-Standorten zu wechseln	25 (Standard)	Über WAN-Verbindung verbundene Datacenter.
Zwischen logischen Datacenter-Standorten am selben physischen Standort	0	Logische Rechenzentren befinden sich in demselben physischen Gebäude oder Campus, das über ein LAN verbunden ist.

Verbindungskosten aktualisieren

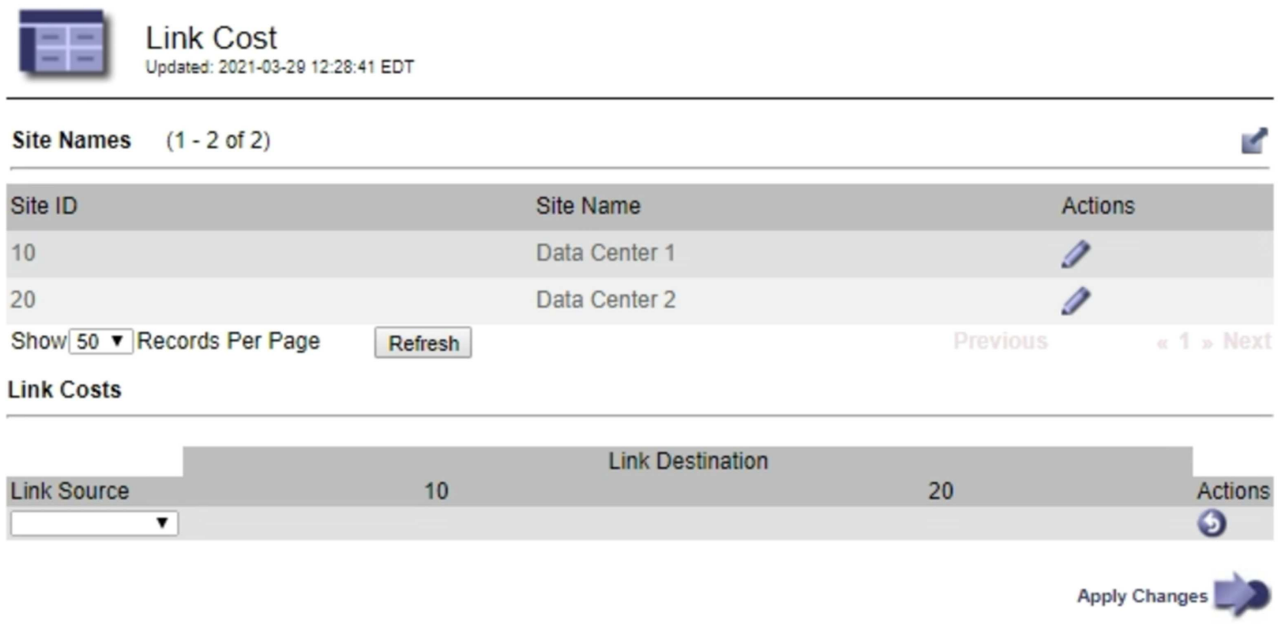
Sie können die Verbindungskosten zwischen Datacenter-Standorten aktualisieren, um die Latenz zwischen Standorten wiederzugeben.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben die Berechtigung für die Konfiguration der Seite Grid Topology.

Schritte

1. Wählen Sie **KONFIGURATION Netzwerk Link Cost**.



2. Wählen Sie eine Website unter **Link Source** aus, und geben Sie unter **Link Destination** einen Kostenwert zwischen 0 und 100 ein.

   Sie können die Verbindungskosten nicht ändern, wenn die Quelle mit dem Ziel identisch ist.

   Um Änderungen abzubrechen, wählen Sie „ **Zurücksetzen**.

3. Wählen Sie **Änderungen Anwenden**.

Verwenden Sie AutoSupport

Was ist AutoSupport?

Die AutoSupport-Funktion ermöglicht es Ihrem StorageGRID System, Gesundheits- und Statusmeldungen an den technischen Support zu senden.

Durch den Einsatz von AutoSupport werden die Problembestimmung und -Behebung erheblich beschleunigt. Der technische Support überwacht auch den Storage-Bedarf Ihres Systems und hilft Ihnen dabei zu ermitteln, ob Sie neue Nodes oder Standorte hinzufügen müssen. Optional können Sie AutoSupport Meldungen so konfigurieren, dass sie an ein zusätzliches Ziel gesendet werden.

Informationen, die in AutoSupport Meldungen enthalten sind

AutoSupport Meldungen enthalten Informationen, z. B. die folgenden:

- StorageGRID Softwareversion
- Betriebssystemversion
- Attributinformationen auf System- und Standortebene
- Aktuelle Warnmeldungen und Alarme (Altsystem)
- Aktueller Status aller Grid-Aufgaben, einschließlich historischer Daten
- Verwendung der Admin-Node-Datenbank
- Anzahl der verlorenen oder fehlenden Objekte
- Grid-Konfigurationseinstellungen
- NMS-Einheiten
- Aktive ILM-Richtlinie
- Bereitgestellte Grid-Spezifikations-Datei
- Diagnostische Metriken

Sie können die AutoSupport-Funktion und die einzelnen AutoSupport-Optionen bei der Erstinstallation von StorageGRID aktivieren oder später aktivieren. Wenn AutoSupport nicht aktiviert ist, wird eine Meldung im Grid-Manager-Dashboard angezeigt. Die Meldung enthält einen Link zur AutoSupport-Konfigurationsseite.

Wenn Sie die Nachricht schließen, wird sie erst wieder angezeigt, wenn Ihr Browser-Cache gelöscht wird, auch wenn AutoSupport deaktiviert bleibt.

Was ist Digital Advisor?

Digital Advisor ist Cloud-basiert und nutzt prädiktive Analysen und Community-Wissen der installierten Basis von NetApp. Kontinuierliche Risikobewertungen, prädiktive Warnungen, beschreibende Tipps und

automatisierte Aktionen helfen Ihnen, Probleme zu vermeiden, bevor sie auftreten. Dies führt zu verbesserter Systemintegrität und höherer Systemverfügbarkeit.

Wenn Sie die Digital Advisor Dashboards und Funktionen auf der NetApp Support-Website verwenden möchten, müssen Sie AutoSupport aktivieren.

"Digital Advisor-Dokumentation"

Protokolle zum Senden von AutoSupport Meldungen

Sie können eines von drei Protokollen zum Senden von AutoSupport Meldungen wählen:

- HTTPS
- HTTP
- SMTP

Wenn Sie AutoSupport-Meldungen über HTTPS oder HTTP senden, können Sie einen nicht transparenten Proxy-Server zwischen Admin-Knoten und dem technischen Support konfigurieren.

Wenn Sie SMTP als Protokoll für AutoSupport-Meldungen verwenden, müssen Sie einen SMTP-Mail-Server konfigurieren.

AutoSupport-Optionen

Sie können eine beliebige Kombination der folgenden Optionen verwenden, um AutoSupport Meldungen an den technischen Support zu senden:

- **Wöchentlich**: Senden Sie automatisch einmal pro Woche AutoSupport-Nachrichten. Standardeinstellung: Aktiviert.
- **Event-triggered**: Sendet automatisch AutoSupport jede Stunde oder wenn wichtige Systemereignisse auftreten. Standardeinstellung: Aktiviert.
- **Auf Anfrage**: Technischen Support erlauben, um zu verlangen, dass Ihr StorageGRID-System AutoSupport-Nachrichten automatisch sendet, was nützlich ist, wenn sie aktiv an einem Problem arbeiten (erfordert HTTPS AutoSupport Übertragungsprotokoll). Standardeinstellung: Deaktiviert.
- **Vom Benutzer ausgelöst**: Senden Sie AutoSupport-Nachrichten jederzeit manuell.

Verwandte Informationen

"NetApp Support"

Konfigurieren Sie AutoSupport

Sie können die AutoSupport-Funktion und die einzelnen AutoSupport-Optionen bei der Erstinstallation von StorageGRID aktivieren oder später aktivieren.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben die Berechtigung Root-Zugriff oder andere Grid-Konfigurationen.
- Wenn Sie das HTTPS- oder HTTP-Protokoll für das Senden von AutoSupport-Meldungen verwenden, haben Sie Outbound-Internetzugang für den primären Admin-Node entweder direkt oder über einen Proxy-Server bereitgestellt (eingehende Verbindungen sind nicht erforderlich).

- Wenn Sie das HTTPS- oder HTTP-Protokoll verwenden und einen Proxy-Server verwenden möchten, haben Sie die Möglichkeit Administrator-Proxy-Server konfiguriert.
- Wenn Sie SMTP als Protokoll für AutoSupport-Meldungen verwenden, haben Sie einen SMTP-Mail-Server konfiguriert. Die gleiche E-Mail-Serverkonfiguration wird für Benachrichtigungen über Alarm E-Mails verwendet (altes System).

Geben Sie das Protokoll für AutoSupport Meldungen an

Sie können eines der folgenden Protokolle zum Senden von AutoSupport Meldungen verwenden:

- **HTTPS**: Dies ist die Standard-Einstellung und wird für Neuinstallationen empfohlen. Das HTTPS-Protokoll verwendet Port 443. Wenn Sie die Funktion AutoSupport On Demand aktivieren möchten, müssen Sie das HTTPS-Protokoll verwenden.
- **HTTP**: Dieses Protokoll ist nicht sicher, es sei denn, es wird in einer vertrauenswürdigen Umgebung verwendet, in der der Proxyserver beim Senden von Daten über das Internet in HTTPS konvertiert. Das HTTP-Protokoll verwendet Port 80.
- **SMTP**: Verwenden Sie diese Option, wenn Sie AutoSupport-Nachrichten per E-Mail versenden möchten. Wenn Sie SMTP als Protokoll für AutoSupport-Meldungen verwenden, müssen Sie auf der Seite Legacy E-Mail-Einrichtung einen SMTP-Mail-Server konfigurieren (**SUPPORT Alere) Legacy-E-Mail-Setup**).

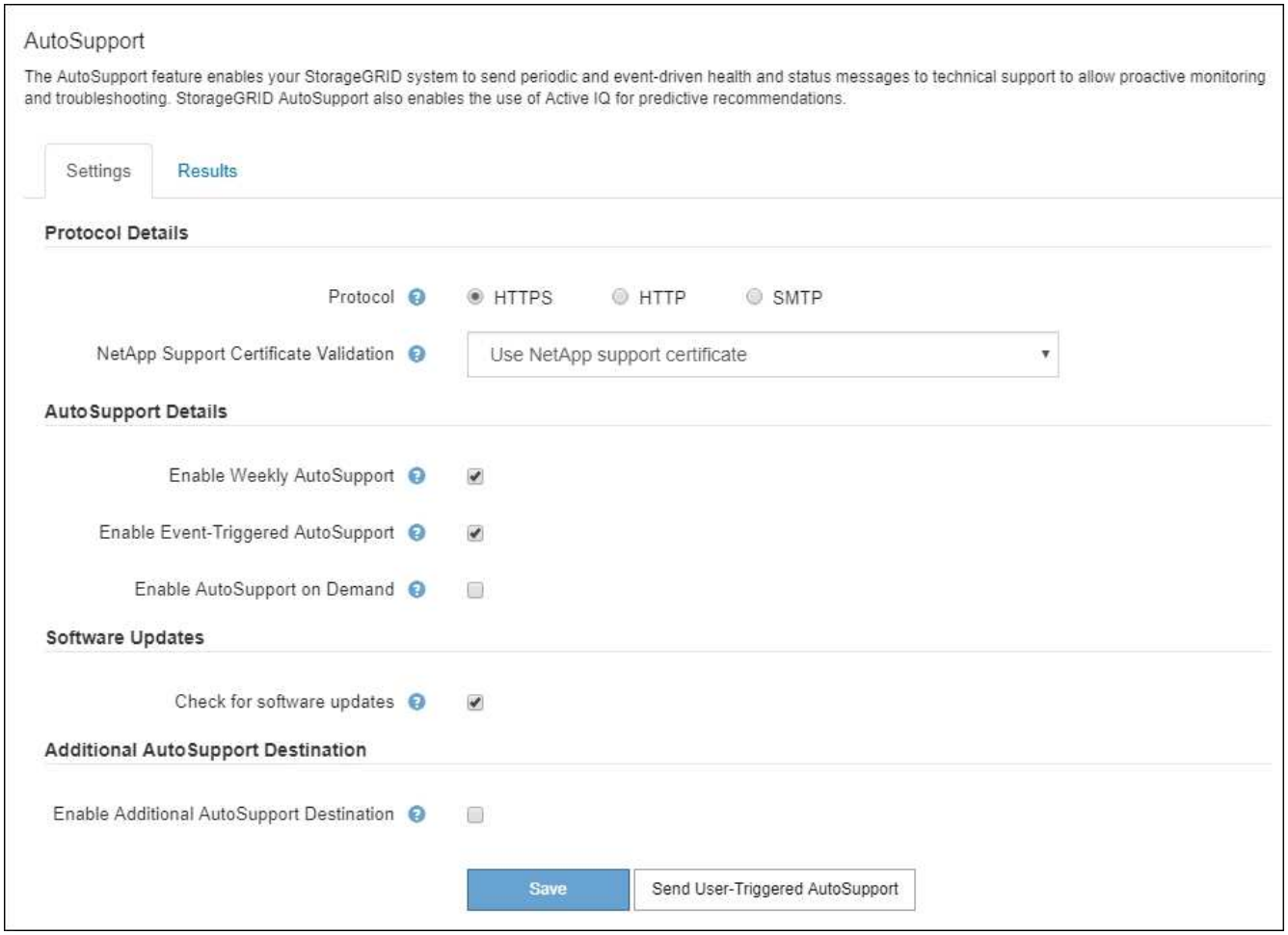
> SMTP war das einzige Protokoll, das vor der StorageGRID 11.2-Version für AutoSupport-Meldungen verfügbar war. Wenn Sie zunächst eine frühere Version von StorageGRID installiert haben, ist SMTP möglicherweise das ausgewählte Protokoll.

Das von Ihnen festgelegte Protokoll wird für das Senden aller Typen von AutoSupport Meldungen verwendet.

Schritte

1. Wählen Sie **SUPPORT Tools AutoSupport**.

   Die Seite AutoSupport wird angezeigt, und die Registerkarte **Einstellungen** ist ausgewählt.



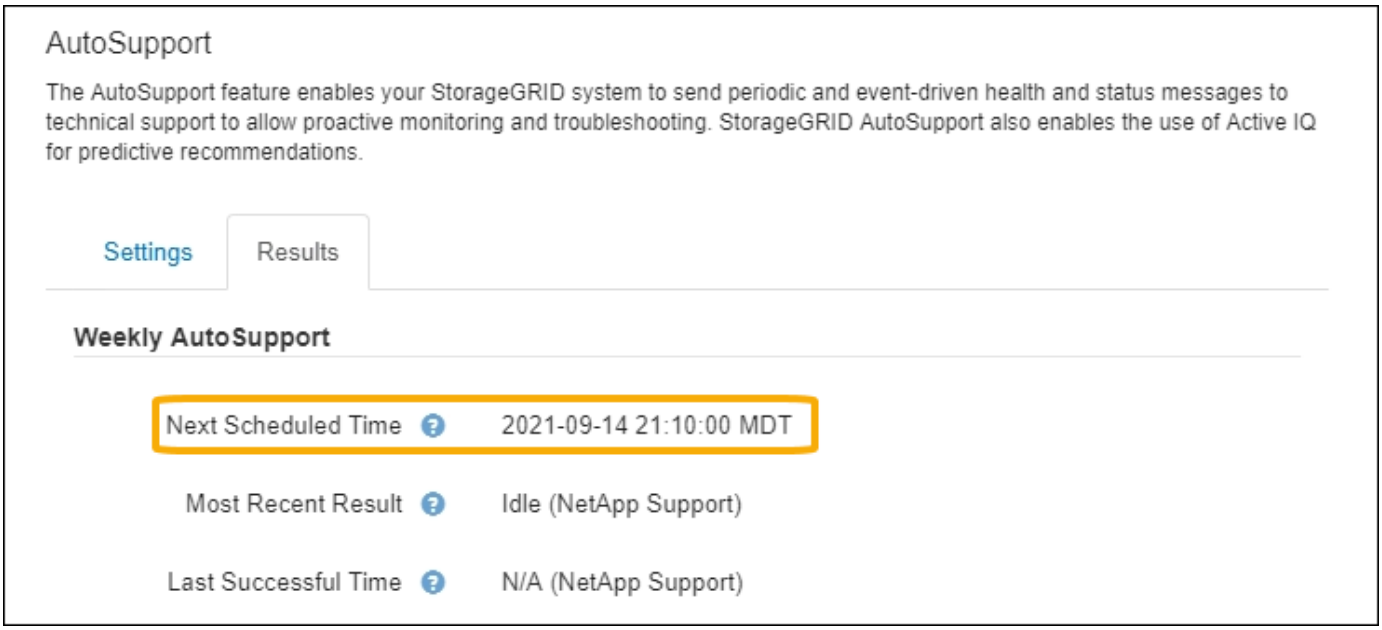
2. Wählen Sie das Protokoll aus, das Sie zum Senden von AutoSupport Meldungen verwenden möchten.
3. Wenn Sie **HTTPS** ausgewählt haben, wählen Sie aus, ob die Verbindung zum NetApp Support Server mit einem TLS-Zertifikat gesichert werden soll.
   - **NetApp Supportzertifikat verwenden** (Standard): Die Zertifikatvalidierung stellt sicher, dass die Übertragung von AutoSupport Meldungen sicher ist. Das NetApp Supportzertifikat ist bereits mit der StorageGRID Software installiert.
   - **Zertifikat nicht überprüfen**: Wählen Sie diese Option nur aus, wenn Sie einen guten Grund haben, keine Zertifikatvalidierung zu verwenden, z.B. wenn es ein vorübergehendes Problem mit einem Zertifikat gibt.
4. Wählen Sie **Speichern**.

   Alle wöchentlichen, vom Benutzer ausgelösten und von Ereignissen ausgelösten Meldungen werden über das ausgewählte Protokoll gesendet.

Deaktivieren Sie wöchentliche AutoSupport-Meldungen

Standardmäßig wird das StorageGRID System so konfiguriert, dass einmal pro Woche eine AutoSupport Meldung an den NetApp Support gesendet wird.

Um festzustellen, wann die wöchentliche AutoSupport-Nachricht gesendet wird, gehen Sie zur Registerkarte **AutoSupport results**. Sehen Sie im Abschnitt **Wöchentliche AutoSupport** den Wert für **Nächste geplante Zeit** an.



Sie können das automatische Senden von wöchentlichen AutoSupport Meldungen jederzeit deaktivieren.

Schritte

1. Wählen Sie **SUPPORT Tools AutoSupport**.
2. Deaktivieren Sie das Kontrollkästchen **wöchentlicher AutoSupport** aktivieren.
3. Wählen Sie **Speichern**.

Deaktivieren Sie ereignisgesteuerte AutoSupport Meldungen

Standardmäßig wird das StorageGRID System so konfiguriert, dass es eine AutoSupport Meldung an den NetApp Support sendet, wenn eine wichtige Meldung oder ein anderes bedeutendes Systemereignis auftritt.

Sie können AutoSupport Meldungen, bei denen Ereignisse ausgelöst wurden, jederzeit deaktivieren.

> Auch bei Event-ausgelösten AutoSupport-Meldungen werden diese unterdrückt, wenn Sie E-Mail-Benachrichtigungen systemweit unterdrücken. (Wählen Sie **KONFIGURATION System Anzeigeoptionen**. Wählen Sie dann **Benachrichtigung Alle unterdrücken**.)

Schritte

1. Wählen Sie **SUPPORT Tools AutoSupport**.
2. Deaktivieren Sie das Kontrollkästchen * Event-Triggered AutoSupport* aktivieren.
3. Wählen Sie **Speichern**.

AutoSupport-on-Demand aktivieren

AutoSupport On Demand kann Ihnen bei der Lösung von Problemen helfen, an denen der technische Support aktiv arbeitet.

AutoSupport-on-Demand ist standardmäßig deaktiviert. Wenn Sie diese Funktion aktivieren, kann der technische Support von Ihrem StorageGRID System automatisch AutoSupport Meldungen senden. Der technische Support kann auch das Abfrageintervall für AutoSupport-on-Demand-Abfragen festlegen.

Der technische Support kann AutoSupport bei Bedarf nicht aktivieren oder deaktivieren.

Schritte

1. Wählen Sie **SUPPORT Tools AutoSupport**.
2. Wählen Sie **HTTPS** für das Protokoll aus.
3. Aktivieren Sie das Kontrollkästchen **Wochenendfach-AutoSupport aktivieren**.
4. Aktivieren Sie das Kontrollkästchen * AutoSupport on Demand aktivieren*.
5. Wählen Sie **Speichern**.

   AutoSupport-on-Demand ist aktiviert, und der technische Support kann AutoSupport-on-Demand-Anfragen an StorageGRID senden.

Deaktivieren Sie die Prüfung auf Softwareupdates

Standardmäßig wendet sich StorageGRID an NetApp, um zu ermitteln, ob Software-Updates für Ihr System verfügbar sind. Wenn ein StorageGRID-Hotfix oder eine neue Version verfügbar ist, wird die neue Version auf der Seite StorageGRID-Aktualisierung angezeigt.

Bei Bedarf können Sie optional die Prüfung auf Softwareupdates deaktivieren. Wenn Ihr System beispielsweise keinen WAN-Zugriff hat, sollten Sie die Prüfung deaktivieren, um Download-Fehler zu vermeiden.

Schritte

1. Wählen Sie **SUPPORT Tools AutoSupport**.
2. Deaktivieren Sie das Kontrollkästchen **nach Softwareupdates suchen**.
3. Wählen Sie **Speichern**.

Fügen Sie ein weiteres AutoSupport Ziel hinzu

Wenn Sie AutoSupport aktivieren, werden Zustandsmeldungen und Statusmeldungen an den NetApp Support gesendet. Sie können ein zusätzliches Ziel für alle AutoSupport Meldungen angeben.

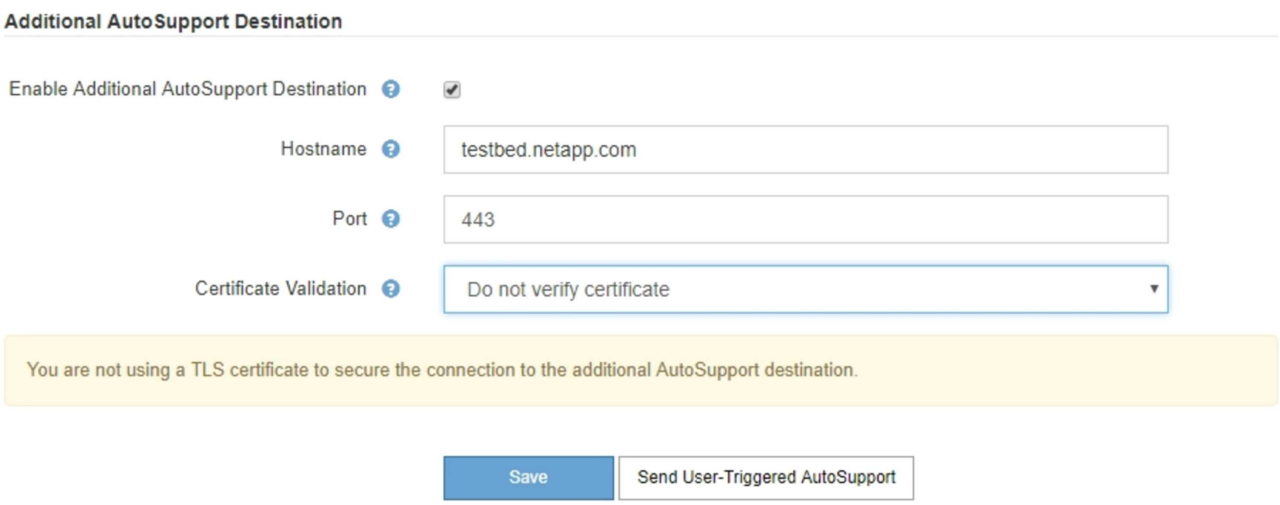
Informationen zum Überprüfen oder Ändern des Protokolls zum Senden von AutoSupport Meldungen finden Sie in den Anweisungen an Geben Sie das Protokoll für AutoSupport Meldungen an.

> Sie können das SMTP-Protokoll nicht zum Senden von AutoSupport Meldungen an ein zusätzliches Ziel verwenden.

Schritte

1. Wählen Sie **SUPPORT Tools AutoSupport**.
2. Wählen Sie **zusätzliches AutoSupport-Ziel aktivieren**.

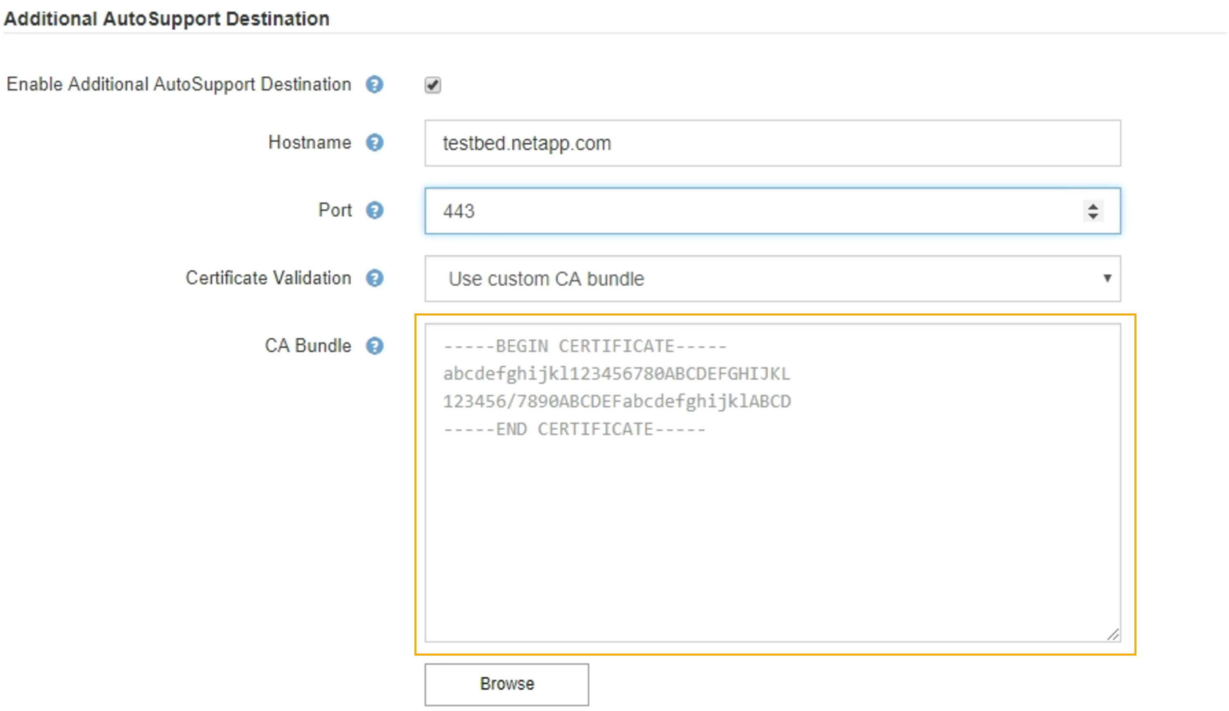
   Die Felder „zusätzliche AutoSupport-Zieladresse“ werden angezeigt.



3. Geben Sie den Hostnamen oder die IP-Adresse des Servers eines zusätzlichen AutoSupport-Zielservers ein.

   Sie können nur ein weiteres Ziel eingeben.

4. Geben Sie den Port ein, der für die Verbindung zu einem zusätzlichen AutoSupport-Zielserver verwendet wird (standardmäßig ist Port 80 für HTTP oder Port 443 für HTTPS).
5. Um Ihre AutoSupport-Nachrichten mit Zertifikatvalidierung zu senden, wählen Sie im Dropdown-Menü **Zertifikatvalidierung Custom CA-Bundle verwenden** aus. Führen Sie dann einen der folgenden Schritte aus:
   - Verwenden Sie ein Bearbeitungswerkzeug, um alle Inhalte jeder PEM-kodierten CA-Zertifikatdatei in das Feld **CA Bundle** zu kopieren und einzufügen, das in der Reihenfolge der Zertifikatskette verkettet ist. Sie müssen Folgendes einschließen `----BEGIN CERTIFICATE----` Und `----END CERTIFICATE----` Wählen Sie aus.



◦ Wählen Sie **Durchsuchen**, navigieren Sie zu der Datei mit den Zertifikaten und wählen Sie dann **Öffnen**, um die Datei hochzuladen. Die Zertifikatvalidierung stellt sicher, dass die Übertragung von AutoSupport Meldungen sicher ist.

6. Um Ihre AutoSupport-Nachrichten ohne Zertifikatvalidierung zu senden, wählen Sie im Dropdown-Menü * Zertifikatvalidierung* * * * nicht verifizieren aus.

   Wählen Sie diese Option nur aus, wenn Sie einen guten Grund haben, die Zertifikatvalidierung nicht zu verwenden, z. B. wenn ein vorübergehendes Problem mit einem Zertifikat vorliegt.

   Eine Warnung: "Sie verwenden kein TLS-Zertifikat, um die Verbindung zum zusätzlichen AutoSupport-Ziel zu sichern."

7. Wählen Sie **Speichern**.

   Alle zukünftigen wöchentlichen, ereignisgesteuert und vom Benutzer ausgelösten AutoSupport Meldungen werden an das zusätzliche Ziel gesendet.

Senden Sie manuell eine AutoSupport Meldung aus

Um den technischen Support bei der Fehlerbehebung bei Problemen mit Ihrem StorageGRID System zu unterstützen, können Sie manuell eine AutoSupport Meldung auslösen, die gesendet werden soll.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben die Berechtigung Root-Zugriff oder andere Grid-Konfigurationen.

Schritte

1. Wählen Sie **SUPPORT Tools AutoSupport**.

   Die Seite AutoSupport wird angezeigt, wobei die Registerkarte **Einstellungen** ausgewählt ist.

2. Wählen Sie **vom Benutzer ausgelöste AutoSupport senden** aus.

   StorageGRID versucht, eine AutoSupport Nachricht an den technischen Support zu senden. Wenn der Versuch erfolgreich ist, werden die **aktuellsten Ergebnisse** und **Letzte erfolgreiche Zeit** Werte auf der Registerkarte **Ergebnisse** aktualisiert. Wenn ein Problem auftritt, werden die **neuesten Ergebnisse**-Werte auf „Fehlgeschlagen“ aktualisiert, und StorageGRID versucht nicht, die AutoSupport-Nachricht erneut zu senden.

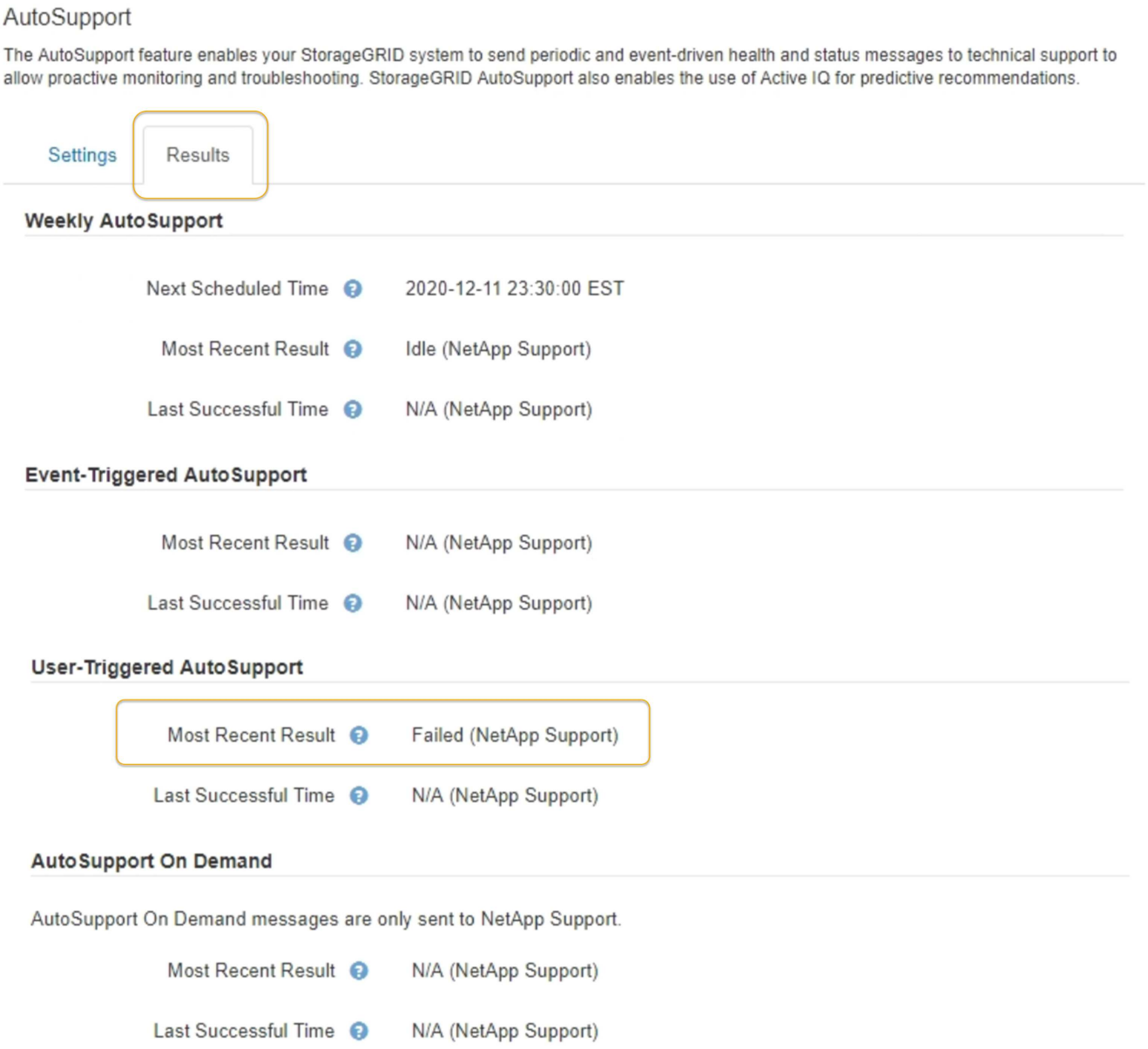
   > Nachdem Sie eine vom Benutzer ausgelöste AutoSupport-Nachricht gesendet haben, aktualisieren Sie die AutoSupport-Seite im Browser nach 1 Minute, um auf die neuesten Ergebnisse zuzugreifen.

Fehlerbehebung für AutoSupport Meldungen

Wenn das Senden einer AutoSupport Meldung fehlschlägt, führt das StorageGRID System abhängig vom Typ der AutoSupport Meldung unterschiedliche Aktionen durch. Sie können den Status von AutoSupport-Meldungen überprüfen, indem Sie **SUPPORT Tools AutoSupport Ergebnisse** auswählen.

Wenn Sie E-Mail-Benachrichtigungen im gesamten System unterdrücken, werden ereignisgesteuerte AutoSupport Meldungen unterdrückt. (Wählen Sie **KONFIGURATION System Anzeigeoptionen**. Wählen Sie dann **Benachrichtigung Alle unterdrücken**.)

Wenn die AutoSupport-Meldung nicht gesendet wird, wird „`failed`“ auf der Registerkarte **Results** der Seite **AutoSupport** angezeigt.



Wöchentlicher AutoSupport-Nachrichtenfehler

Wenn eine wöchentliche AutoSupport-Meldung nicht gesendet werden kann, werden im StorageGRID System folgende Aktionen ausgeführt:

1. Aktualisiert das Attribut für das aktuellste Ergebnis, um es erneut zu versuchen.
2. Versucht, die AutoSupport Meldung alle vier Minuten für eine Stunde 15 Mal erneut zu senden.
3. Nach einer Stunde des Sendefehlens aktualisiert das Attribut „Aktuelles Ergebnis“ auf „Fehlgeschlagen“.

4. Versucht, eine AutoSupport-Nachricht zum nächsten geplanten Zeitpunkt erneut zu senden.
5. Behält den regulären AutoSupport-Zeitplan bei, wenn die Meldung fehlschlägt, weil der NMS-Dienst nicht verfügbar ist und wenn eine Meldung vor sieben Tagen gesendet wird.
6. Wenn der NMS-Dienst wieder verfügbar ist, sendet sofort eine AutoSupport-Nachricht, wenn eine Nachricht für sieben Tage oder länger nicht gesendet wurde.

Vom Benutzer ausgelöste oder ereignisgesteuerte AutoSupport-Meldung ist fehlgeschlagen

Wenn eine vom Benutzer ausgelöste oder eine AutoSupport Meldung, die aufgrund eines Ereignisses ausgelöst wird, nicht gesendet wird, ergreift das StorageGRID System folgende Maßnahmen:

1. Zeigt eine Fehlermeldung an, wenn der Fehler bekannt ist. Wenn z. B. ein Benutzer das SMTP-Protokoll auswählt, ohne korrekte E-Mail-Konfigurationseinstellungen vorzunehmen, wird der folgende Fehler angezeigt: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. Versucht nicht, die Nachricht erneut zu senden.
3. Protokolliert den Fehler in `nms.log`.

Wenn ein Fehler auftritt und SMTP das ausgewählte Protokoll ist, überprüfen Sie, ob der E-Mail-Server des StorageGRID-Systems korrekt konfiguriert ist und Ihr E-Mail-Server ausgeführt wird (**SUPPORT Alered)** * Legacy E-Mail Setup*). Die folgende Fehlermeldung kann auf der AutoSupport-Seite angezeigt werden: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Erfahren Sie, wie Sie die Einstellungen für E-Mail-Server im konfigurieren Anweisungen zum Monitoring und zur Fehlerbehebung.

Korrigieren Sie einen Fehler bei der AutoSupport-Meldung

Wenn ein Fehler auftritt und SMTP das ausgewählte Protokoll ist, überprüfen Sie, ob der E-Mail-Server des StorageGRID-Systems korrekt konfiguriert ist und Ihr E-Mail-Server ausgeführt wird. Die folgende Fehlermeldung kann auf der AutoSupport-Seite angezeigt werden: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Senden Sie AutoSupport Nachrichten aus der E-Series über StorageGRID

Sie können AutoSupport Meldungen von E-Series SANtricity System Manager über einen StorageGRID Admin-Node anstelle des Storage Appliance Management-Ports an den technischen Support senden.

Was Sie benötigen

- Sie sind im Grid Manager mit einem angemeldet Unterstützter Webbrowser.
- Sie verfügen über die Berechtigung zum Administrator oder Root-Zugriff.

> Sie müssen über die SANtricity-Firmware 8.70 (11.7) oder höher verfügen, um mithilfe des Grid-Managers auf den SANtricity-System-Manager zuzugreifen.

Über diese Aufgabe

E-Series AutoSupport-Meldungen enthalten Details zur Storage Hardware und sind spezifischer als andere AutoSupport-Meldungen, die vom StorageGRID System gesendet werden.

Konfigurieren Sie eine spezielle Proxy-Server-Adresse in SANtricity System Manager, damit die AutoSupport-Meldungen ohne Verwendung des Managementports der Appliance über einen StorageGRID-Admin-Node übertragen werden. Auf diese Weise übertragene AutoSupport-Nachrichten gelten für die Proxyeinstellungen für bevorzugte Sender und Admin, die möglicherweise im Grid Manager konfiguriert wurden.

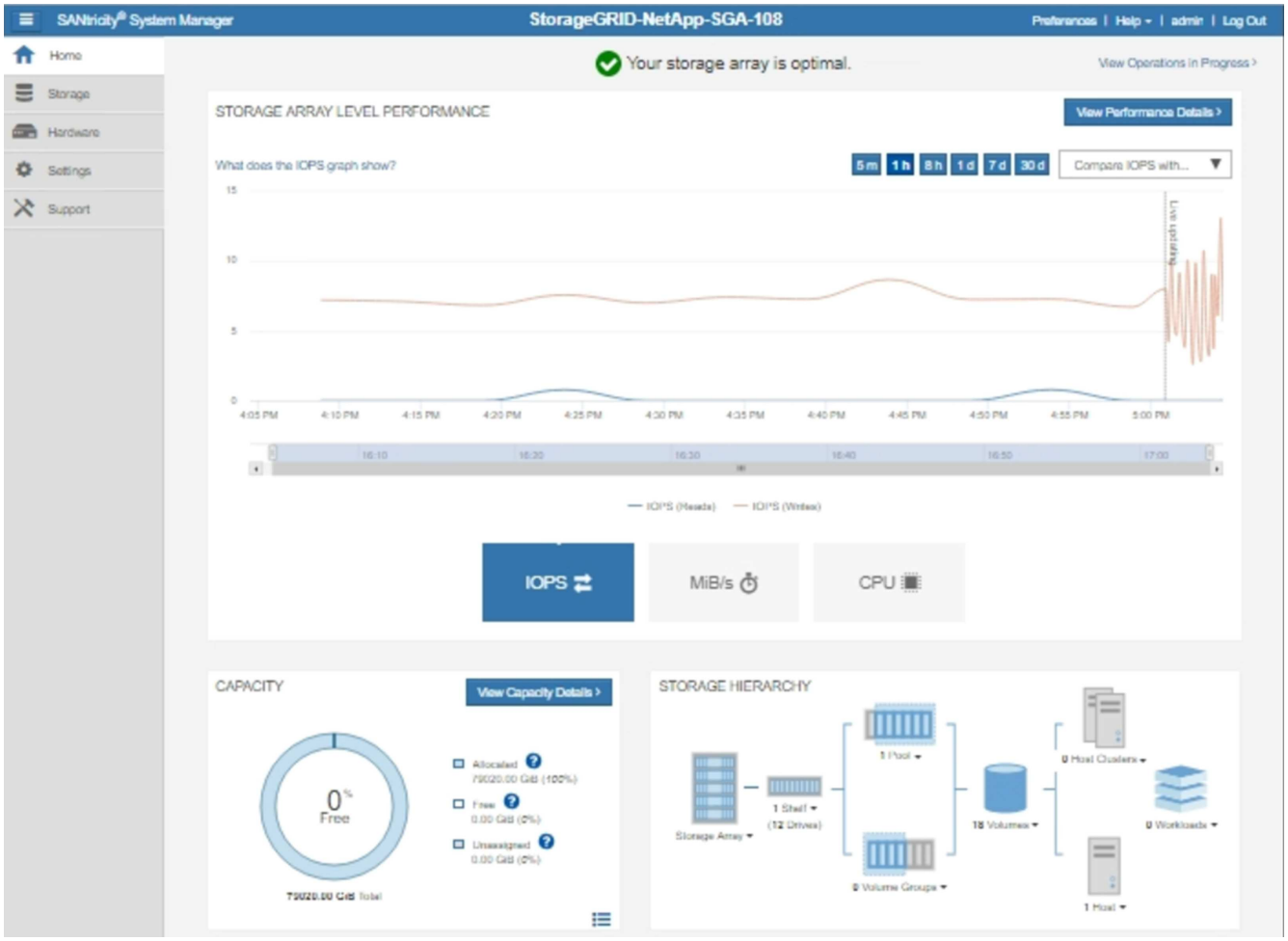
Informationen zum Konfigurieren des Admin-Proxyservers in Grid Manager finden Sie unter Konfigurieren Sie die Administrator-Proxy-Einstellungen.

> Dieses Verfahren dient nur zur Konfiguration eines StorageGRID-Proxyservers für AutoSupport-Meldungen der E-Serie. Weitere Informationen zur Konfiguration der E-Series AutoSupport finden Sie unter "NetApp E-Series und SANtricity Dokumentation".

Schritte

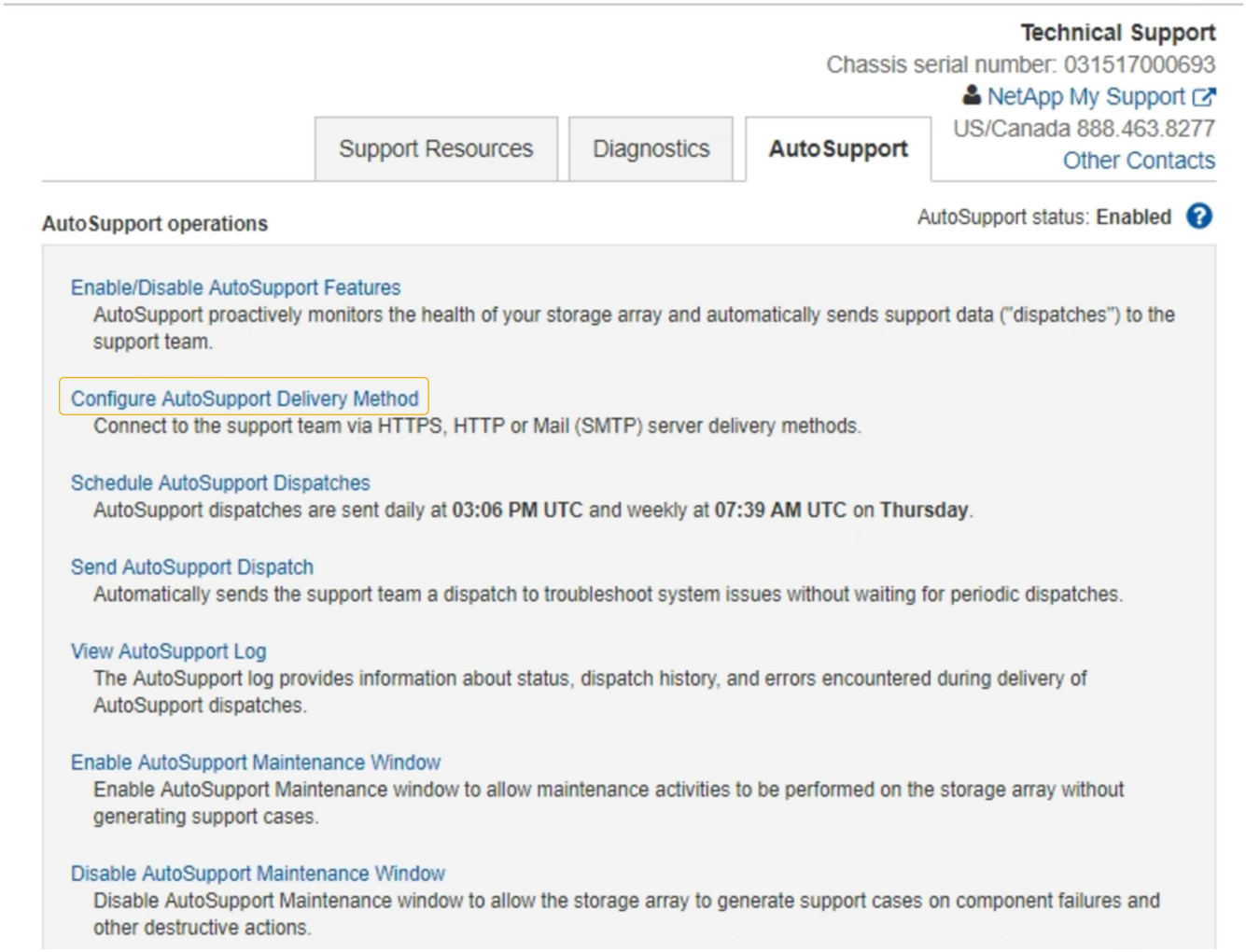
1. Wählen Sie im Grid Manager die Option **NODES** aus.
2. Wählen Sie in der Liste der Knoten links den Speicher-Appliance-Node aus, den Sie konfigurieren möchten.
3. Wählen Sie **SANtricity System Manager**.

   Die Startseite von SANtricity System Manager wird angezeigt.



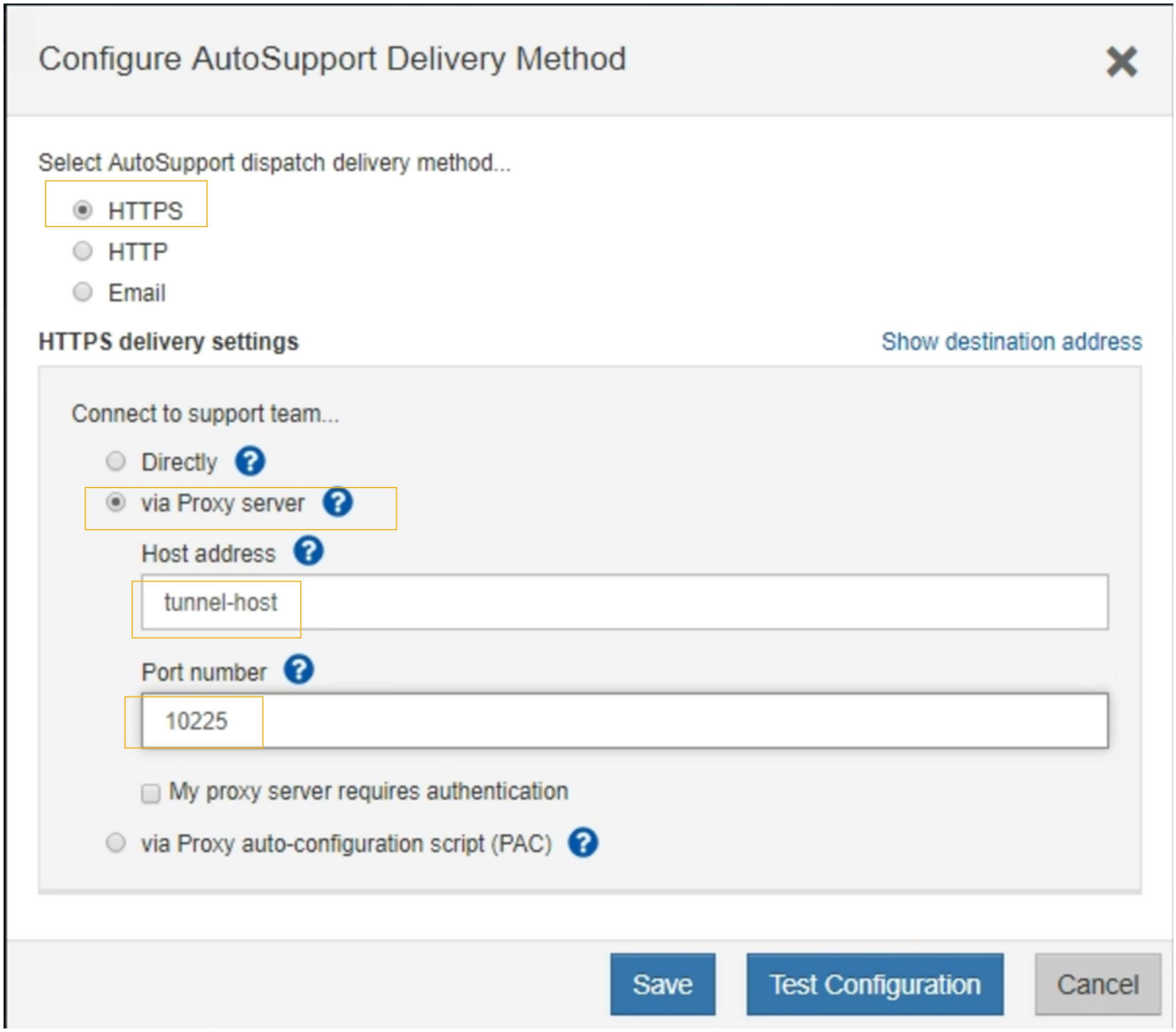
4. Wählen Sie **SUPPORT Support Center AutoSupport**.

   Die Seite AutoSupport-Vorgänge wird angezeigt.



5. Wählen Sie **AutoSupport-Bereitstellungsmethode konfigurieren**.

   Die Seite AutoSupport-Bereitstellungsmethode konfigurieren wird angezeigt.



6. Wählen Sie **HTTPS** für die Liefermethode aus.

   Das Zertifikat, das das HTTPS-Protokoll aktiviert, ist vorinstalliert.

7. Wählen Sie **über Proxy-Server**.
8. Eingabe `tunnel-host` Für die **Host-Adresse**.

   `tunnel-host` Hat die besondere Adresse, um einen Admin-Node zum Senden von E-Series AutoSupport Meldungen zu verwenden.

9. Eingabe `10225` Für die * Portnummer*.

   `10225` Ist die Portnummer auf dem StorageGRID Proxy-Server, der AutoSupport Meldungen vom E-Series Controller in der Appliance empfängt.

10. Wählen Sie **Testkonfiguration** aus, um die Routing- und Konfigurationseinstellungen Ihres AutoSupport Proxy-Servers zu testen.

Falls richtig, erscheint eine Meldung in einem grünen Banner: „`Ihre AutoSupport-Konfiguration wurde verifiziert.`“

Wenn der Test fehlschlägt, wird eine Fehlermeldung in einem roten Banner angezeigt. Überprüfen Sie Ihre StorageGRID DNS-Einstellungen und Netzwerke. Stellen Sie sicher, dass der bevorzugte Sender Admin-Node eine Verbindung zur NetApp Support-Website herstellen kann, und versuchen Sie es erneut.

11. Wählen Sie **Speichern**.

    Die Konfiguration wird gespeichert, und es wird eine Bestätigungsmeldung angezeigt: „`AutoSupport-Bereitstellungsmethode wurde konfiguriert.`“

Managen Sie Storage-Nodes

Allgemeines zum Verwalten von Storage-Nodes

Storage-Nodes stellen Festplattenkapazität und Services zur Verfügung. Das Verwalten von Storage-Nodes umfasst Folgendes:

- Management der Storage-Optionen
- Um zu verstehen, welche Wasserzeichen für das Storage-Volume sind und wie Sie mit Wasserzeichen-Überschreibungen steuern können, wann Storage-Nodes schreibgeschützt sind
- Monitoring und Management des Speicherplatzes, der für Objektmetadaten verwendet wird
- Globale Einstellungen für gespeicherte Objekte konfigurieren
- Konfigurationseinstellungen für Speicherknoten werden angewendet
- Verwalten vollständiger Speicherknoten

Was ist ein Storage-Node?

Storage-Nodes managen und speichern Objektdaten und Metadaten. Jedes StorageGRID System muss mindestens drei Storage-Nodes aufweisen. Wenn Sie über mehrere Standorte verfügen, muss jeder Standort im StorageGRID System auch drei Storage-Nodes aufweisen.

Ein Storage Node umfasst die Services und Prozesse, die zum Speichern, Verschieben, Überprüfen und Abrufen von Objektdaten und Metadaten auf der Festplatte erforderlich sind. Auf der Seite **NODES** können Sie detaillierte Informationen zu den Speicherknoten anzeigen.

Was ist der ADC-Dienst?

Der Dienst Administrative Domain Controller (ADC) authentifiziert Grid-Knoten und ihre Verbindungen miteinander. Der ADC-Service wird auf jedem der ersten drei Storage-Nodes an einem Standort gehostet.

Der ADC-Dienst verwaltet Topologiedaten, einschließlich Standort und Verfügbarkeit von Diensten. Wenn ein Grid-Knoten Informationen von einem anderen Grid-Knoten benötigt oder eine Aktion von einem anderen Grid-Knoten ausgeführt werden muss, kontaktiert er einen ADC-Service, um den besten Grid-Knoten für die Bearbeitung seiner Anforderung zu finden. Darüber hinaus behält der ADC-Dienst eine Kopie der Konfigurationspakete der StorageGRID-Bereitstellung bei, sodass jeder Grid-Knoten aktuelle Konfigurationsinformationen abrufen kann.ADC-Informationen für einen Speicherknoten können Sie auf der

Seite Grid Topology anzeigen (**SUPPORT Grid Topology**).

Zur Erleichterung von verteilten und isanded-Operationen synchronisiert jeder ADC-Dienst Zertifikate, Konfigurationspakete und Informationen über Services und Topologie mit den anderen ADC-Diensten im StorageGRID-System.

Im Allgemeinen unterhalten alle Rasterknoten eine Verbindung zu mindestens einem ADC-Dienst. So wird sichergestellt, dass die Grid-Nodes immer auf die neuesten Informationen zugreifen. Wenn Grid-Nodes verbunden sind, speichern sie Zertifikate anderer Grid-Nodes`, sodass die Systeme auch dann weiterhin mit bekannten Grid-Nodes funktionieren können, wenn ein ADC-Service nicht verfügbar ist. Neue Grid-Knoten können nur Verbindungen über einen ADC-Dienst herstellen.

Durch die Verbindung jedes Grid-Knotens kann der ADC-Service Topologiedaten erfassen. Die Informationen zu diesem Grid-Node umfassen die CPU-Last, den verfügbaren Festplattenspeicher (wenn der Storage vorhanden ist), unterstützte Services und die Standort-ID des Grid-Node. Andere Dienste fragen den ADC-Service nach Topologiedaten durch Topologieabfragen. Der ADC-Dienst reagiert auf jede Abfrage mit den neuesten Informationen, die vom StorageGRID-System empfangen wurden.

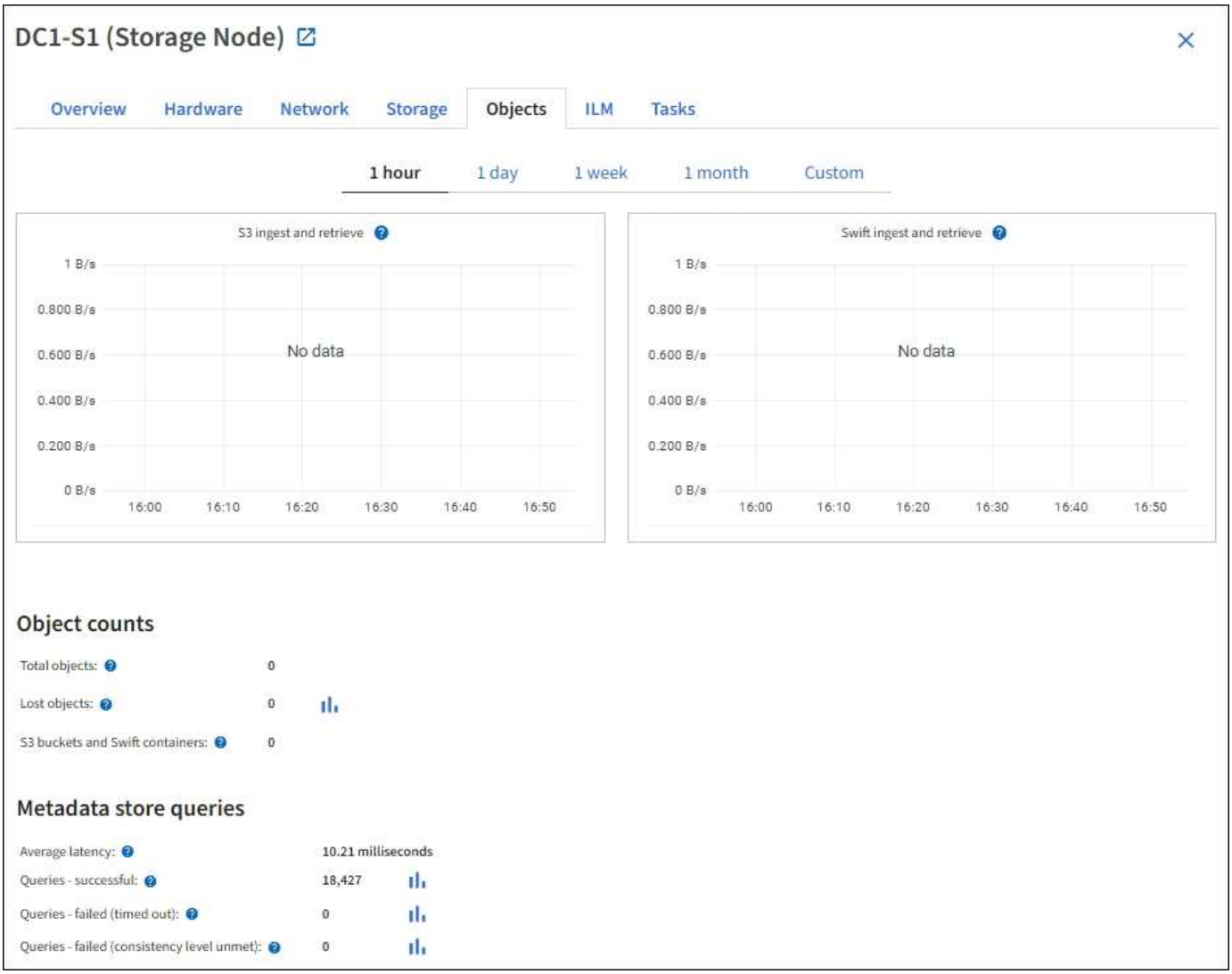
Was ist der DDS-Service?

Der DDS-Service (Distributed Data Store) wird von einem Storage-Node gehostet und führt Hintergrundaufgaben zu den im StorageGRID-System gespeicherten Objektmetadaten durch.

Anzahl der Objekte

Der DDS-Dienst verfolgt die Gesamtzahl der im StorageGRID-System aufgenommenen Objekte sowie die Gesamtzahl der über die unterstützten Schnittstellen (S3 oder Swift) des Systems aufgenommenen Objekte.

Die Gesamtzahl der Objekte wird auf der Registerkarte Objekte auf der Registerkarte Knoten für jeden Speicherknoten angezeigt.



Abfragen

Sie können die durchschnittliche Zeit für die Ausführung einer Abfrage zum Metadatenspeicher durch den spezifischen DDS-Dienst, die Gesamtzahl der erfolgreichen Abfragen und die Gesamtanzahl der fehlgeschlagenen Abfragen für ein Timeout-Problem identifizieren.

Vielleicht möchten Sie nach Abfrageinformationen suchen, um den Zustand des Metadatenspeichers, Cassandra, zu überwachen. Dies hat Auswirkungen auf die Aufnahme- und Abrufleistung des Systems. Wenn beispielsweise die Latenz für eine durchschnittliche Abfrage langsam ist und die Anzahl fehlgeschlagener Abfragen aufgrund von Timeouts hoch ist, kann der Metadatenspeicher zu einer höheren Last führen oder einen anderen Vorgang ausführen.

Sie können auch die Gesamtzahl der Abfragen anzeigen, die aufgrund von Konsistenzfehlern fehlgeschlagen sind. Fehler auf Konsistenzebene resultieren aus einer unzureichenden Anzahl von verfügbaren Metadatenspeichern zum Zeitpunkt der Durchführung einer Abfrage durch den spezifischen DDS-Service.

Auf der Diagnoseseite können Sie weitere Informationen zum aktuellen Status Ihres Rasters abrufen. Siehe Führen Sie eine Diagnose aus.

Konsistenzgarantien und -Kontrollen

StorageGRID garantiert die Konsistenz zwischen Lese- und Schreibvorgängen bei neu erstellten Objekten.

Jeder GET-Vorgang nach einem erfolgreich abgeschlossenen PUT-Vorgang kann die neu geschriebenen Daten lesen. Überschreibungen vorhandener Objekte, Metadatenaktualisierungen und -Löschungen bleiben irgendwann konsistent.

Was ist der LDR-Service?

Der Service Local Distribution Router (LDR) wird von jedem Speicherknoten gehostet und übernimmt den Content-Transport des StorageGRID-Systems. Der Content-Transport umfasst viele Aufgaben, einschließlich Datenspeicherung, Routing und Bearbeitung von Anfragen. Der LDR-Service erledigt den Großteil der harten Arbeit des StorageGRID-Systems durch die Handhabung von Datenübertragungslasten und Datenverkehrsfunktionen.

Der LDR-Service übernimmt folgende Aufgaben:

- Abfragen
- Information Lifecycle Management-Aktivitäten (ILM
- Löschen von Objekten
- Objekt-Storage
- Objektdatenübertragung von einem anderen LDR-Service (Storage Node)
- Datenspeicher-Management
- Protokollschnittstellen (S3 und Swift)

Der LDR-Service managt auch die Zuordnung von S3- und Swift-Objekten zu den eindeutigen „`Content Handles`“ (UUIDs), die das StorageGRID System jedem aufgenommene Objekt zuweist.

Abfragen

LDR-Abfragen umfassen Abfragen zum Objektspeicherort während Abruf- und Archivierungsvorgängen. Sie können die durchschnittliche Zeit zum Ausführen einer Abfrage, die Gesamtzahl der erfolgreichen Abfragen und die Gesamtzahl der Abfragen, die aufgrund eines Timeout-Problems fehlgeschlagen sind, identifizieren.

Sie können Abfrageinformationen prüfen, um den Zustand des Metadatenspeichers zu überwachen und die Aufnahme- und Abrufleistung des Systems zu beeinträchtigen. Wenn beispielsweise die Latenz für eine durchschnittliche Abfrage langsam ist und die Anzahl fehlgeschlagener Abfragen aufgrund von Timeouts hoch ist, kann der Metadatenspeicher zu einer höheren Last führen oder einen anderen Vorgang ausführen.

Sie können auch die Gesamtzahl der Abfragen anzeigen, die aufgrund von Konsistenzfehlern fehlgeschlagen sind. Fehler auf Konsistenzebene resultieren aus einer unzureichenden Anzahl an verfügbaren Metadatenspeichern zum Zeitpunkt einer Abfrage durch den spezifischen LDR-Service.

Auf der Diagnoseseite können Sie weitere Informationen zum aktuellen Status Ihres Rasters abrufen. Siehe Führen Sie eine Diagnose aus.

ILM-Aktivität

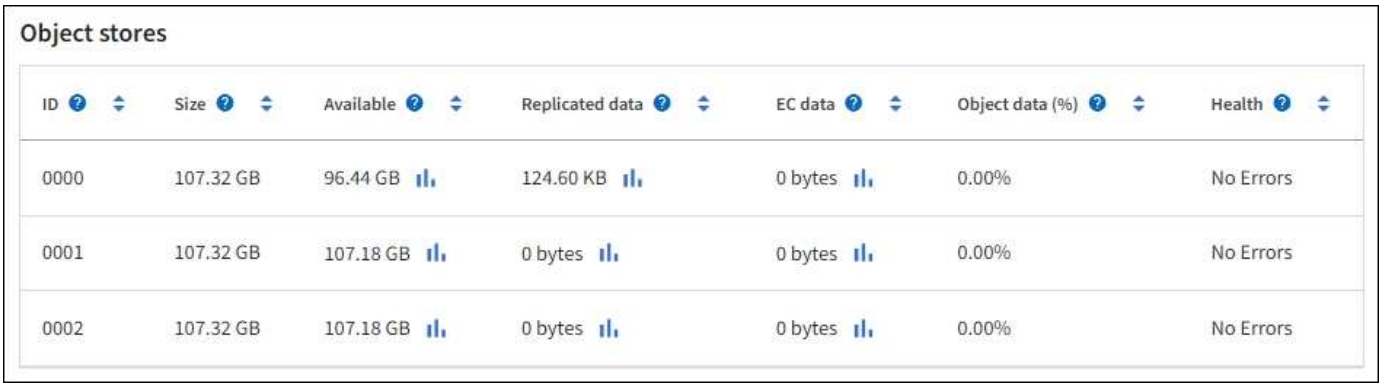
Mithilfe der ILM-Metriken (Information Lifecycle Management) können Sie die Bewertung von Objekten für die ILM-Implementierung durchführen. Sie können diese Kennzahlen auf dem Dashboard oder auf **NODES** ***Storage Node*** **ILM** anzeigen.

Objektspeicher

Der zugrunde liegende Datenspeicher eines LDR-Service wird in eine feste Anzahl an Objektspeichern (auch

Storage-Volumes genannt) unterteilt. Jeder Objektspeicher ist ein separater Bereitstellungspunkt.

Auf der Seite Knoten Speicher sehen Sie die Objektspeicher für einen Speicherknoten.



Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Das Objekt speichert in einem Storage-Node werden durch eine Hexadezimalzahl zwischen 0000 und 002F identifiziert, die als Volume-ID bezeichnet wird. Der Speicherplatz ist im ersten Objektspeicher (Volume 0) für Objekt-Metadaten in einer Cassandra-Datenbank reserviert. Für Objektdaten werden alle verbleibenden Speicherplatz auf diesem Volume verwendet. Alle anderen Objektspeichern werden ausschließlich für Objektdaten verwendet, zu denen replizierte Kopien und nach dem Erasure-Coding-Verfahren Fragmente gehören.

Um sicherzustellen, dass selbst der Speicherplatz für replizierte Kopien genutzt wird, werden Objektdaten für ein bestimmtes Objekt auf Basis des verfügbaren Storage in einem Objektspeicher gespeichert. Wenn ein oder mehrere Objektspeichern die Kapazität voll haben, speichern die übrigen Objektspeicher weiterhin Objekte, bis kein Platz mehr auf dem Speicherknoten vorhanden ist.

Metadatensicherung

Objektmetadaten sind Informationen mit oder eine Beschreibung eines Objekts, z. B. Änderungszeit des Objekts oder der Storage-Standort. StorageGRID speichert Objekt-Metadaten in einer Cassandra-Datenbank, die über eine Schnittstelle zum LDR-Service verfügt.

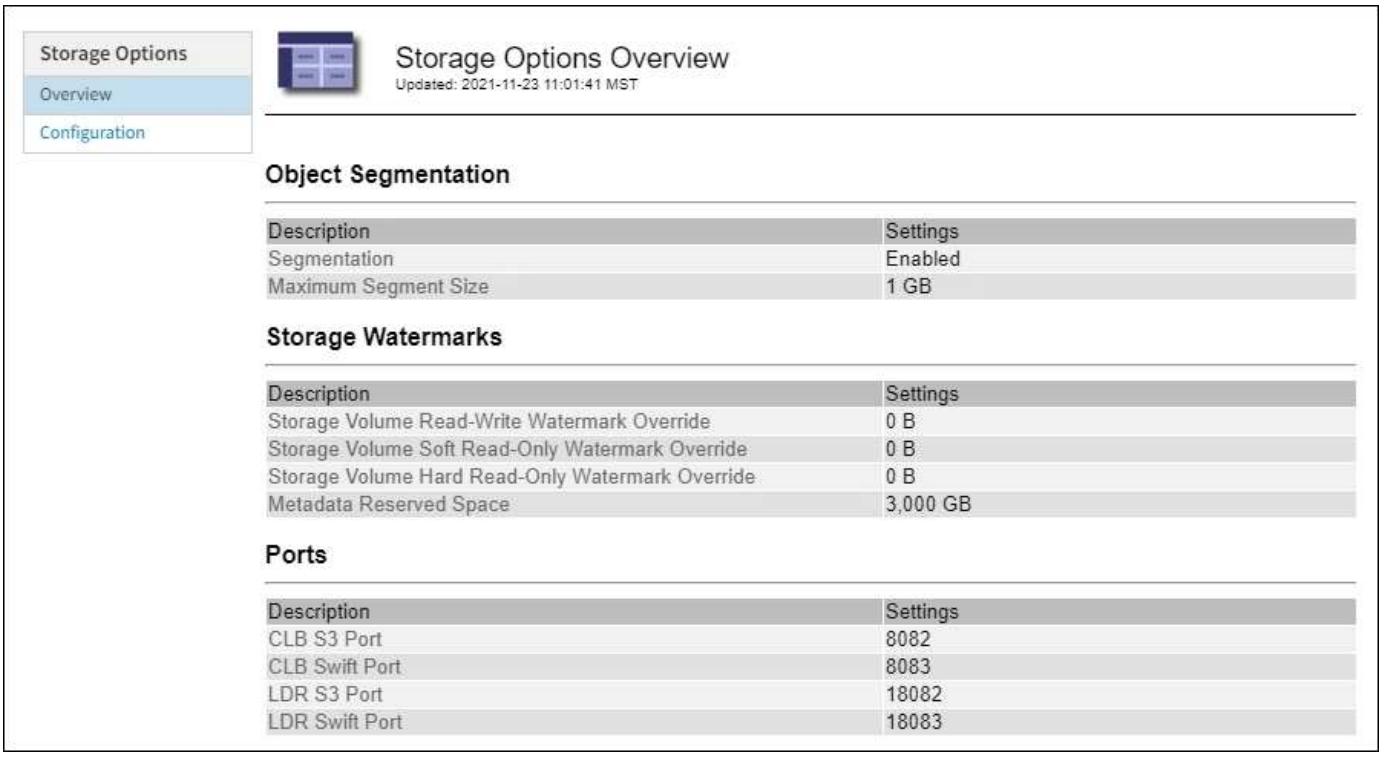
Um Redundanz sicherzustellen und so vor Verlust zu schützen, werden an jedem Standort drei Kopien von Objekt-Metadaten aufbewahrt. Die Kopien werden gleichmäßig auf alle Storage-Nodes an jedem Standort verteilt. Diese Replikation ist nicht konfigurierbar und wird automatisch ausgeführt.

Management von Objekt-Metadaten-Storage

Storage-Optionen managen

Storage-Optionen umfassen die Einstellungen für die Objektsegmentierung, die aktuellen Werte für Storage-Volume-Wasserzeichen und die Einstellung für reservierten Speicherplatz. Sie können auch die S3- und Swift-Ports anzeigen, die vom veralteten CLB-Dienst auf Gateway-Nodes und vom LDR-Service auf Storage-Nodes verwendet werden.

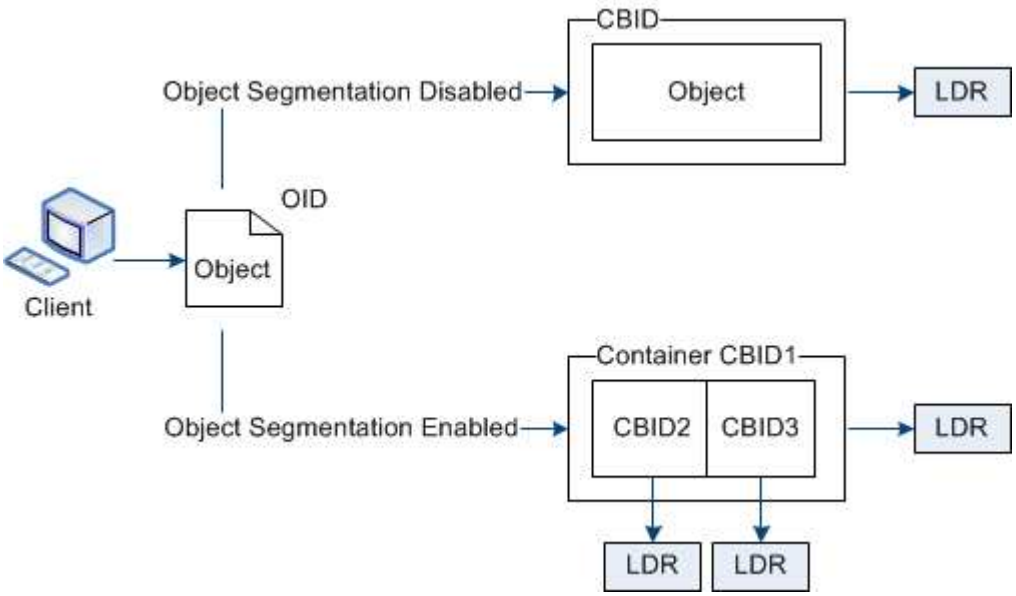
Informationen zu Port-Zuweisungen finden Sie unter Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen.



Was ist Objektsegmentierung?

Objektsegmentierung ist der Vorgang, ein Objekt in eine Sammlung kleinerer Objekte mit fester Größe aufzuteilen, um die Speicherung und Ressourcennutzung für große Objekte zu optimieren. Auch beim S3-Multi-Part-Upload werden segmentierte Objekte erstellt, wobei ein Objekt die einzelnen Teile darstellt.

Wenn ein Objekt in das StorageGRID-System aufgenommen wird, teilt der LDR-Service das Objekt in Segmente auf und erstellt einen Segment-Container, der die Header-Informationen aller Segmente als Inhalt auflistet.



Beim Abruf eines Segment-Containers fasst der LDR-Service das ursprüngliche Objekt aus seinen Segmenten zusammen und gibt das Objekt dem Client zurück.

Der Container und die Segmente werden nicht notwendigerweise auf demselben Storage-Node gespeichert. Container und Segmente können auf jedem Storage-Node innerhalb des in der ILM-Regel angegebenen Speicherpools gespeichert werden.

Jedes Segment wird vom StorageGRID System unabhängig behandelt und trägt zur Anzahl der Attribute wie verwaltete Objekte und gespeicherte Objekte bei. Wenn ein im StorageGRID System gespeichertes Objekt beispielsweise in zwei Segmente aufgeteilt wird, erhöht sich der Wert von verwalteten Objekten nach Abschluss der Aufnahme um drei Segmente:

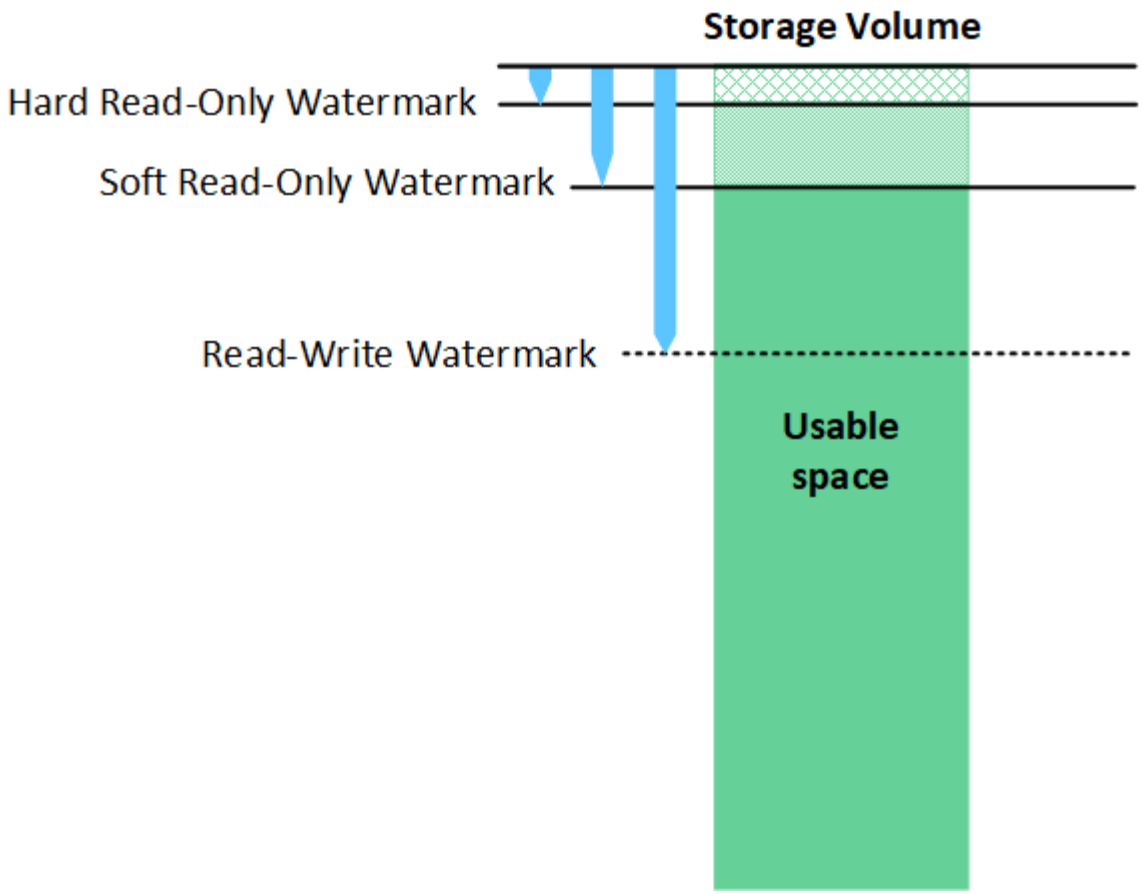
Segmentcontainer + Segment 1 + Segment 2 = drei gespeicherte Objekte

Die Performance beim Umgang mit großen Objekten lässt sich verbessern, indem Folgendes sichergestellt wird:

- Jedes Gateway und jeder Storage-Node verfügt über eine ausreichende Netzwerkbandbreite für den erforderlichen Durchsatz. Konfigurieren Sie beispielsweise separate Grid- und Client-Netzwerke auf 10-Gbit/s-Ethernet-Schnittstellen.
- Für den erforderlichen Durchsatz werden ausreichend Gateway und Storage-Nodes implementiert.
- Jeder Storage-Node verfügt über eine ausreichende Festplatten-I/O-Performance für den erforderlichen Durchsatz.

Was sind Wasserzeichen für Storage-Volumes?

StorageGRID verwendet drei Storage-Volume-Wasserzeichen, um sicherzustellen, dass Storage-Nodes sicher in einen schreibgeschützten Zustand überführt werden, bevor deren Speicherplatz kritisch knapp wird. Damit können Storage-Nodes, die aus einem schreibgeschützten Zustand migriert wurden, erneut Lese- und Schreibvorgänge werden.



Storage Volume-Wasserzeichen gelten nur für den Speicherplatz, der für replizierte und nach Datenkonsistenz (Erasure Coding) verwendet wird. Weitere Informationen über den Speicherplatz, der für Objekt-Metadaten auf Volume 0 reserviert ist, finden Sie unterManagement von Objekt-Metadaten-Storage.

Was ist das Soft Read-Only Watermark?

Das **Speichervolumen Soft Read-Only Watermark** ist das erste Wasserzeichen, das angibt, dass der für Objektdaten nutzbare Speicherplatz eines Speicherknoten voll wird.

Wenn jedes Volume in einem Storage-Node weniger freien Speicherplatz als das Soft Read-Only-Wasserzeichen dieses Volumes besitzt, wechselt der Storage-Node in den Modus *read-only*. Schreibgeschützter Modus bedeutet, dass der Storage Node für den Rest des StorageGRID Systems schreibgeschützte Dienste anbietet, aber alle ausstehenden Schreibanforderungen erfüllt.

Angenommen, jedes Volume in einem Speicherknoten hat einen Soft Read-Only-Wasserzeichen von 10 GB. Sobald jedes Volume weniger als 10 GB freien Speicherplatz hat, wechselt der Storage-Node in den Modus „Soft Read“.

Was ist die Hard Read-Only Watermark?

Das **Speichervolumen Hard Read-Only Watermark** ist das nächste Wasserzeichen, um anzuzeigen, dass der nutzbare Speicherplatz eines Knotens für Objektdaten voll wird.

Wenn der freie Speicherplatz auf einem Volume kleiner ist als das harte Read-Only-Wasserzeichen dieses Volumes, schlägt das Schreiben auf das Volume fehl. Schreibvorgänge auf anderen Volumes können jedoch fortgesetzt werden, bis der freie Speicherplatz auf diesen Volumes kleiner als ihre Hard Read-Only-

Wasserzeichen ist.

Angenommen, jedes Volume in einem Speicherknoten hat einen Hard Read-Only-Wasserzeichen von 5 GB. Sobald jedes Volume weniger als 5 GB freien Speicherplatz hat, akzeptiert der Speicherknoten keine Schreibanforderungen mehr.

Der Hard Read-Only-Wasserzeichen ist immer kleiner als der Soft Read-Only-Wasserzeichen.

Was ist der Read-Write-Wasserzeichen?

Das **Storage Volume Read-Write Watermark** gilt nur für Storage-Nodes, die in den schreibgeschützten Modus gewechselt sind. Er bestimmt, wann der Node wieder Lese-/Schreibzugriff werden kann. Wenn der freie Speicherplatz auf einem Speichervolumen in einem Speicherknoten größer ist als das Read-Write-Wasserzeichen dieses Volumes, wechselt der Knoten automatisch zurück in den Lese-Schreib-Zustand.

Angenommen, der Storage-Node ist in den schreibgeschützten Modus migriert. Nehmen Sie auch an, dass jedes Volume ein Read-Write-Wasserzeichen von 30 GB hat. Sobald der freie Speicherplatz eines beliebigen Volumes auf 30 GB ansteigt, wird der Node erneut zum Lesen/Schreiben.

Der Read-Write-Wasserzeichen ist immer größer als der Soft Read-Only-Wasserzeichen und der Hard Read-Only-Wasserzeichen.

Anzeigen von Wasserzeichen für Speichervolumen

Sie können die aktuellen Einstellungen für Wasserzeichen und die systemoptimierten Werte anzeigen. Wenn keine optimierten Wasserzeichen verwendet werden, können Sie festlegen, ob Sie die Einstellungen anpassen können oder sollten.

Was Sie benötigen

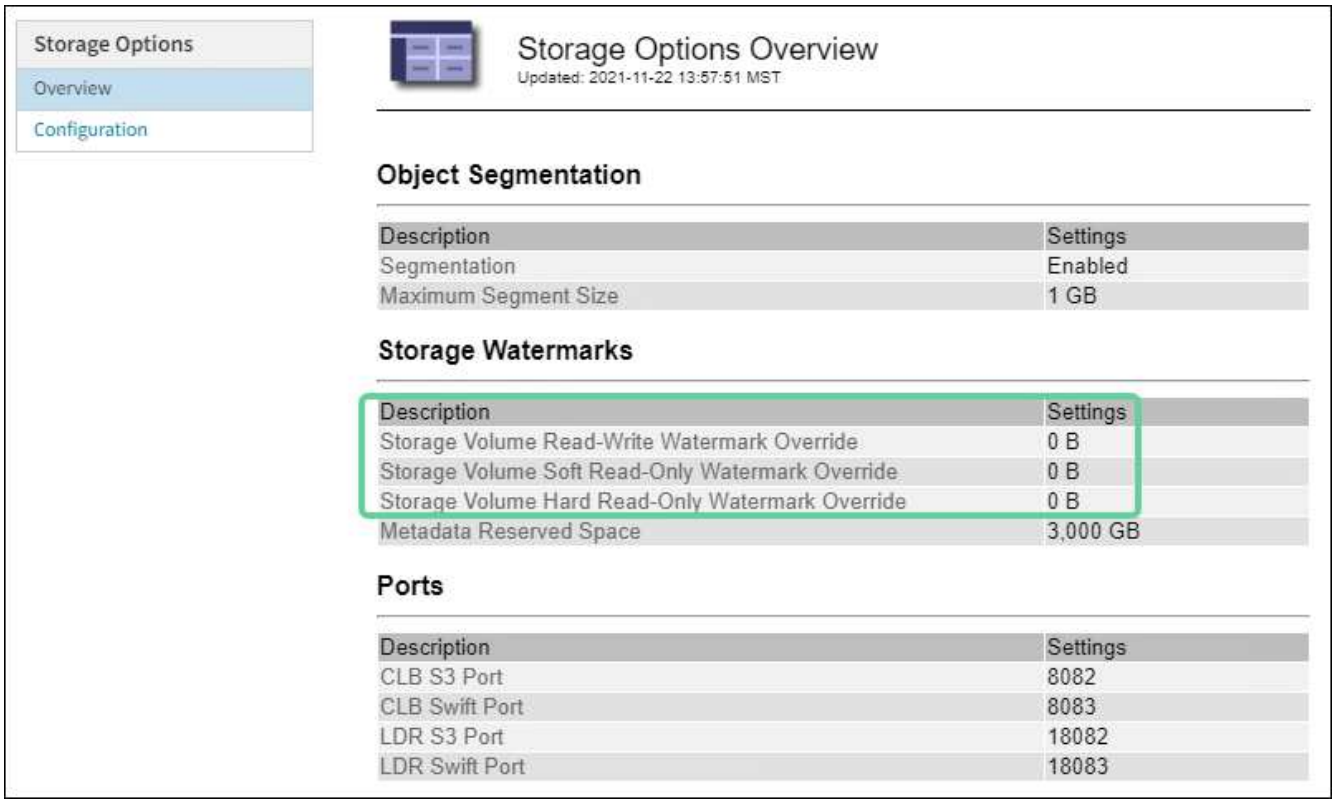
- Sie haben das Upgrade auf StorageGRID 11.6 abgeschlossen.
- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben die Root-Zugriffsberechtigung.

Aktuelle Wasserzeichen-Einstellungen anzeigen

Im Grid Manager können Sie die aktuellen Einstellungen für Speicherwasserzeichen anzeigen.

Schritte

1. Wählen Sie **KONFIGURATION System Speicheroptionen**.
2. Sehen Sie sich im Abschnitt Speicherwasserzeichen die Einstellungen für die drei Überschreibungen der Speichervolumen an.



- Wenn die Wasserzeichen **0** überschreiben, sind alle drei Wasserzeichen für jedes Speichervolumen auf jedem Speicherknoten optimiert, basierend auf der Größe des Speicherknoten und der relativen Kapazität des Volumes.

  Dies ist die Standardeinstellung und die empfohlene Einstellung. Sie sollten diese Werte nicht aktualisieren. Nach Bedarf können Sie optional Anzeigen optimierter Speicherabdrücke.

- Wenn es sich bei den Wasserzeichen um nicht-0-Werte handelt, werden benutzerdefinierte (nicht optimierte) Wasserzeichen verwendet. Es wird nicht empfohlen, benutzerdefinierte Wasserzeichen zu verwenden. Befolgen Sie die Anweisungen für Fehlerbehebung Warnungen bei niedriger Schreibschutzmarke überschreiben Um zu bestimmen, ob Sie die Einstellungen anpassen können oder sollen.

Anzeigen optimierter Speicherabdrücke

StorageGRID verwendet zwei Prometheus-Kennzahlen, um die optimierten Werte anzuzeigen, die es für das **Speichervolumen Soft Read-Only Watermark** berechnet hat. Sie können die minimalen und maximalen optimierten Werte für jeden Speicherknoten in Ihrem Raster anzeigen.

1. Wählen Sie **SUPPORT Tools Kennzahlen** aus.
2. Wählen Sie im Abschnitt Prometheus den Link aus, um auf die Benutzeroberfläche von Prometheus zuzugreifen.
3. Um das empfohlene Mindestwasserzeichen für weichen, schreibgeschützten Wert anzuzeigen, geben Sie die folgende Prometheus-Metrik ein, und wählen Sie **Ausführen**:

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   In der letzten Spalte wird der mindestens optimierte Wert des „Soft Read-Only“-Wasserzeichens für alle Storage-Volumes auf jedem Storage-Node angezeigt. Wenn dieser Wert größer ist als die benutzerdefinierte Einstellung für das **Speichervolumen-Soft-Read-Only-Wasserzeichen**, wird für den

Speicherknoten die Warnung **Low read-only Watermark override** ausgelöst.

4. Um das empfohlene maximale Softread-only-Wasserzeichen anzuzeigen, geben Sie die folgende Prometheus-Metrik ein und wählen Sie **Ausführen**:

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   In der letzten Spalte wird der maximal optimierte Wert des „Soft Read-Only“-Wasserzeichens für alle Storage-Volumes auf jedem Storage-Node angezeigt.

Management von Objekt-Metadaten-Storage

Die Kapazität der Objektmetadaten eines StorageGRID Systems steuert die maximale Anzahl an Objekten, die auf diesem System gespeichert werden können. Um sicherzustellen, dass Ihr StorageGRID System über ausreichend Platz zum Speichern neuer Objekte verfügt, müssen Sie wissen, wo und wie StorageGRID Objekt-Metadaten speichert.

Was sind Objekt-Metadaten?

Objektmetadaten sind alle Informationen, die ein Objekt beschreiben. StorageGRID verwendet Objektmetadaten, um die Standorte aller Objekte im Grid zu verfolgen und den Lebenszyklus eines jeden Objekts mit der Zeit zu managen.

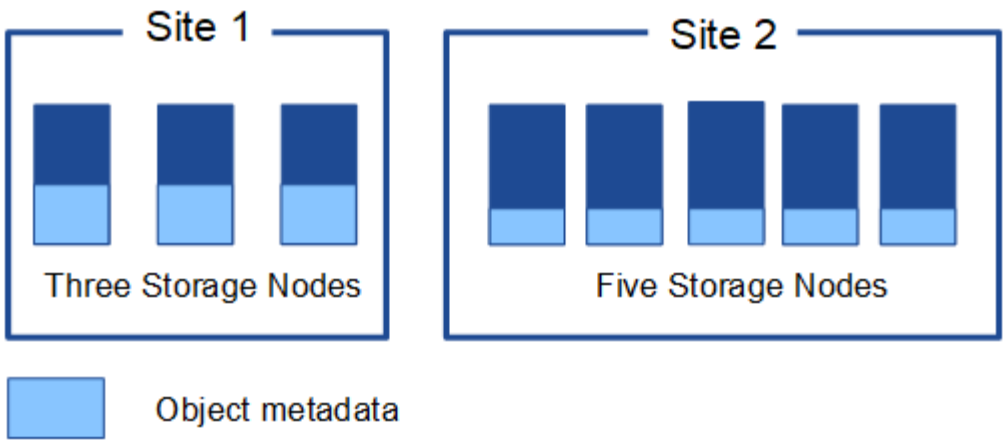
Für ein Objekt in StorageGRID enthalten die Objektmetadaten die folgenden Informationstypen:

- Systemmetadaten, einschließlich einer eindeutigen ID für jedes Objekt (UUID), dem Objektnamen, dem Namen des S3-Buckets oder Swift-Containers, dem Mandanten-Kontonamen oder -ID, der logischen Größe des Objekts, dem Datum und der Uhrzeit der ersten Erstellung des Objekts Und Datum und Uhrzeit der letzten Änderung des Objekts.
- Alle mit dem Objekt verknüpften Schlüssel-Wert-Paare für benutzerdefinierte Benutzer-Metadaten.
- Bei S3-Objekten sind alle dem Objekt zugeordneten Objekt-Tag-Schlüsselwert-Paare enthalten.
- Der aktuelle Storage-Standort jeder Kopie für replizierte Objektkopien
- Für Objektkopien mit Erasure-Coding-Verfahren wird der aktuelle Speicherort der einzelnen Fragmente gespeichert.
- Bei Objektkopien in einem Cloud Storage Pool befindet sich der Speicherort des Objekts, einschließlich des Namens des externen Buckets und der eindeutigen Kennung des Objekts.
- Für segmentierte Objekte und mehrteilige Objekte, Segment-IDs und Datengrößen.

Wie werden Objekt-Metadaten gespeichert?

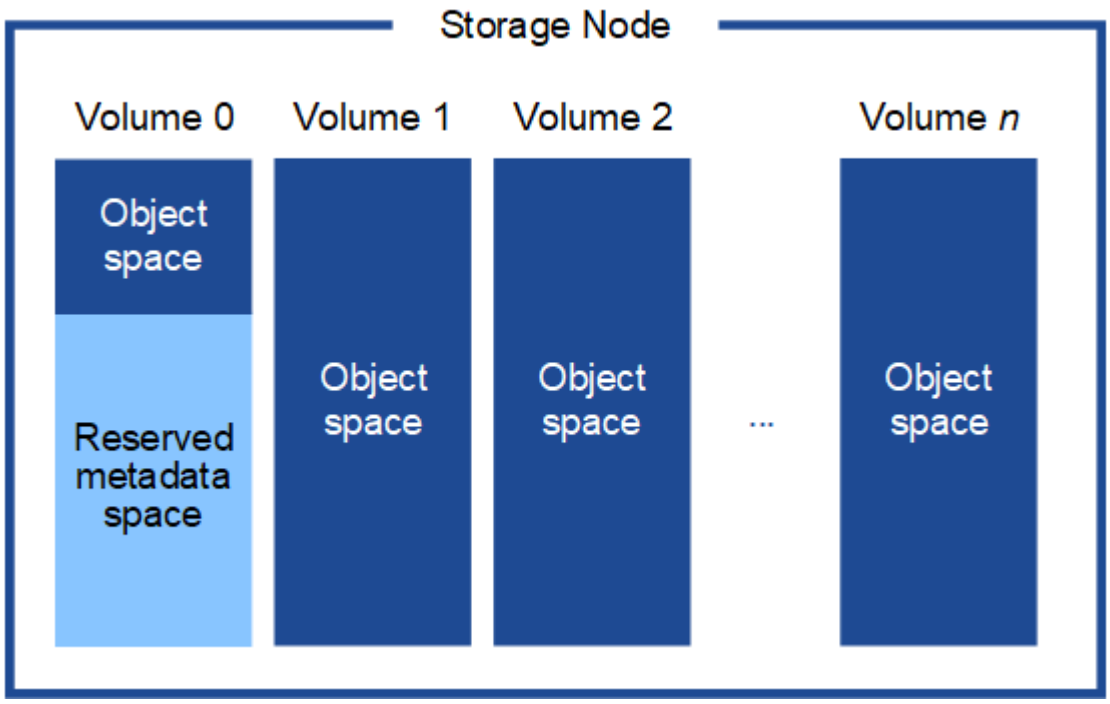
StorageGRID speichert Objektmetadaten in einer Cassandra-Datenbank, die unabhängig von Objektdaten gespeichert werden. Um Redundanz zu gewährleisten und Objekt-Metadaten vor Verlust zu schützen, speichert StorageGRID drei Kopien der Metadaten für alle Objekte im System an jedem Standort. Die drei Kopien der Objektmetadaten werden gleichmäßig auf alle Storage-Nodes an jedem Standort verteilt.

Diese Abbildung zeigt die Speicherknoten an zwei Standorten. Jeder Standort verfügt über die gleiche Menge an Objektmetadaten, die auf die Storage-Nodes an diesem Standort verteilt werden.



Wo werden Objekt-Metadaten gespeichert?

Diese Abbildung zeigt die Storage Volumes für einen einzelnen Storage-Node.



Wie in der Abbildung dargestellt, reserviert StorageGRID Speicherplatz für Objekt-Metadaten auf dem Storage Volume 0 jedes Storage-Nodes. Sie verwendet den reservierten Speicherplatz zum Speichern von Objektmetadaten und zum Ausführen wichtiger Datenbankvorgänge. Alle übrigen Speicherplatz auf dem Storage Volume 0 und allen anderen Storage Volumes im Storage Node werden ausschließlich für Objektdaten (replizierte Kopien und nach Datenkonsistenz) verwendet.

Die Menge an Speicherplatz, die für Objektmetadaten auf einem bestimmten Storage-Node reserviert ist, hängt von einer Reihe von Faktoren ab, die im Folgenden beschrieben werden.

Einstellung für reservierten Speicherplatz für Metadaten

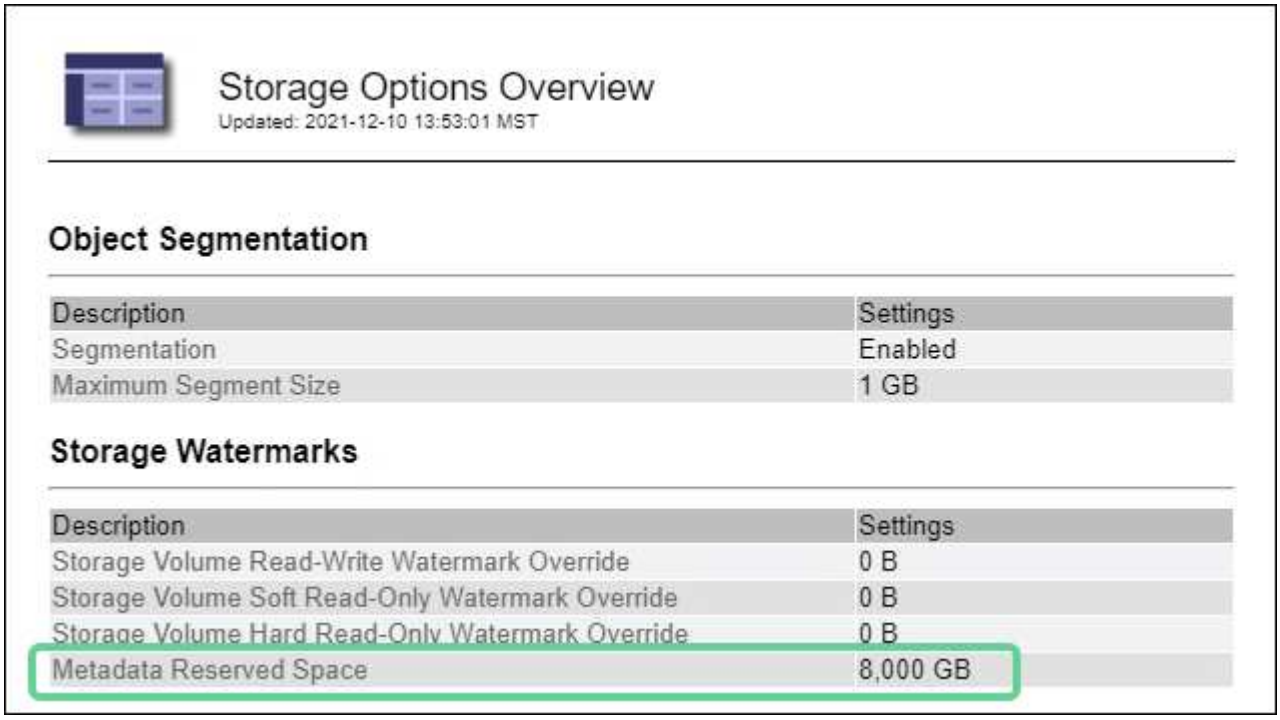
Die Einstellung *Metadaten Reserved Space* stellt die Menge an Speicherplatz dar, die für Metadaten auf Volume 0 jedes Storage-Node reserviert wird. Wie in der Tabelle dargestellt, basiert der Standardwert dieser Einstellung für StorageGRID 11.6 auf dem folgenden:

- Die Softwareversion, die Sie bei der Erstinstallation von StorageGRID verwendet haben.
- Die RAM-Menge auf jedem Storage-Node.

Für die Erstinstallation von StorageGRID verwendete Version	RAM-Größe auf Speicherknoten	Standardeinstellung für reservierten Speicherplatz bei Metadaten für StorageGRID 11.6
11.5/11.6	128 GB oder mehr auf jedem Storage-Node im Grid	8 TB (8,000 GB)
	Weniger als 128 GB auf jedem Storage-Node im Grid	3 TB (3,000 GB)
11.1 bis 11.4	128 GB oder mehr auf jedem Speicherknoten an einem beliebigen Standort	4 TB (4,000 GB)
	Weniger als 128 GB auf jedem Speicherknoten an jedem Standort	3 TB (3,000 GB)
11.0 oder früher	Beliebiger Betrag	2 TB (2,000 GB)

So zeigen Sie die Einstellung für den reservierten Metadatenspeicherplatz für Ihr StorageGRID-System an:

1. Wählen Sie **KONFIGURATION System Speicheroptionen**.
2. Suchen Sie in der Tabelle Speicherwasserzeichen **Metadatenreservierter Speicherplatz**.



Im Screenshot beträgt der Wert **Metadaten reservierter Speicherplatz** 8,000 GB (8 TB). Dies ist die Standardeinstellung für eine neue StorageGRID 11.6-Installation, bei der jeder Speicherknoten 128 GB oder

mehr RAM hat.

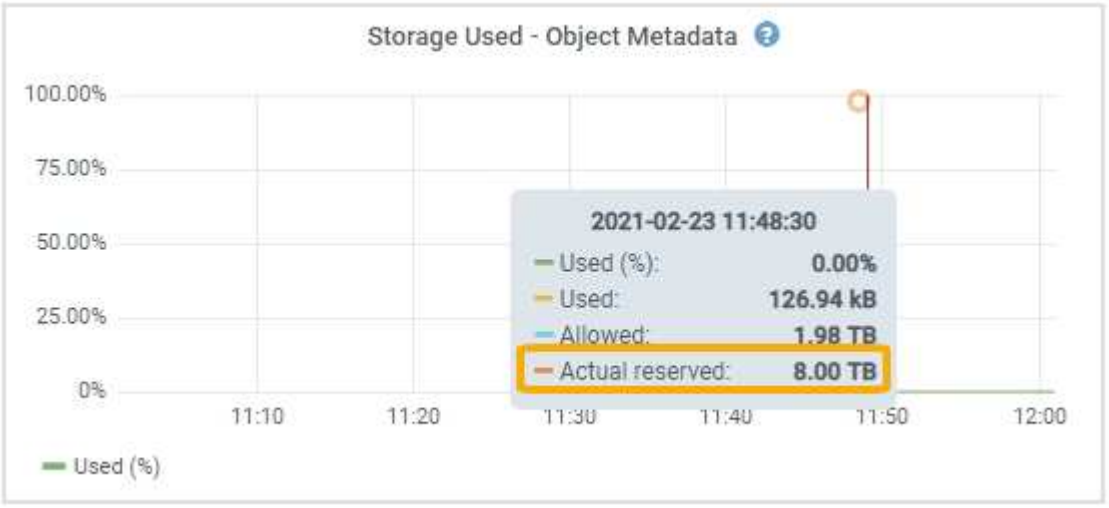
Tatsächlich reservierter Speicherplatz für Metadaten

Im Gegensatz zur Einstellung „systemweiter reservierter Speicherplatz für Metadaten“ wird für jeden Storage-Node der_tatsächlich reservierte Speicherplatz_ für Objektmetadaten ermittelt. Für jeden bestimmten Storage-Node hängt der tatsächlich reservierte Speicherplatz für Metadaten von der Größe des Volumes 0 für den Node und der systemweiten Einstellung **Metadaten reservierter Speicherplatz** ab.

Größe von Volume 0 für den Node	Tatsächlich reservierter Speicherplatz für Metadaten
Weniger als 500 GB (nicht in der Produktion)	10% des Volumens 0
500 GB oder mehr	Die kleineren Werte: • Lautstärke 0 • Einstellung für reservierten Speicherplatz für Metadaten

So zeigen Sie den tatsächlich reservierten Speicherplatz für Metadaten auf einem bestimmten Speicherknoten an:

1. Wählen Sie im Grid Manager **NODES** ***Storage Node*** aus.
2. Wählen Sie die Registerkarte **Storage** aus.
3. Bewegen Sie den Cursor über das Diagramm verwendete Speicherdaten — Objektmetadaten und suchen Sie den Wert **tatsächlich reserviert**.



Im Screenshot beträgt der **tatsächliche reservierte** Wert 8 TB. Dieser Screenshot ist für einen großen Speicherknoten in einer neuen StorageGRID 11.6 Installation. Da die Einstellung für den systemweiten reservierten Speicherplatz für Metadaten kleiner als das Volume 0 für diesen Storage-Node ist, entspricht der tatsächlich reservierte Speicherplatz für diesen Node der Einstellung für den reservierten Speicherplatz.

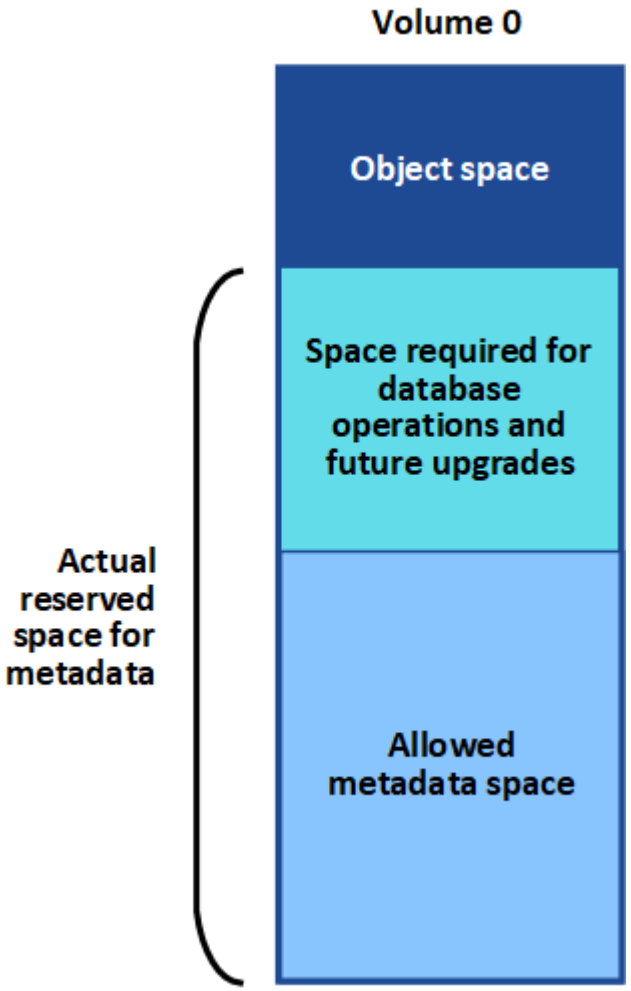
Beispiel für den tatsächlich reservierten Metadatenspeicherplatz

Angenommen, Sie installieren ein neues StorageGRID System unter Verwendung der Version 11.6. Nehmen Sie in diesem Beispiel an, dass jeder Speicherknoten mehr als 128 GB RAM und dieses Volume 0 von Speicherknoten 1 (SN1) 6 TB hat. Basierend auf diesen Werten:

- Der systemweite **Metadaten reservierter Platz** ist auf 8 TB eingestellt. (Dies ist der Standardwert für eine neue StorageGRID 11.6-Installation, wenn jeder Speicherknoten über mehr als 128 GB RAM verfügt.)
- Der tatsächlich reservierte Speicherplatz für Metadaten von SN1 beträgt 6 TB. (Das gesamte Volume ist reserviert, da Volume 0 kleiner ist als die Einstellung **Metadaten reservierter Speicherplatz**.)

Zulässiger Metadatenspeicherplatz

Der tatsächlich reservierte Speicherplatz jedes Storage-Node für Metadaten wird in den Speicherplatz für Objekt-Metadaten (den „ *zulässigen Metadatenspeicherplatz*“) und den Platzbedarf für wichtige Datenbankvorgänge (wie Data-Compaction und Reparatur) sowie zukünftige Hardware- und Software-Upgrades unterteilt. Der zulässige Metadatenspeicherplatz bestimmt die gesamte Objektkapazität.

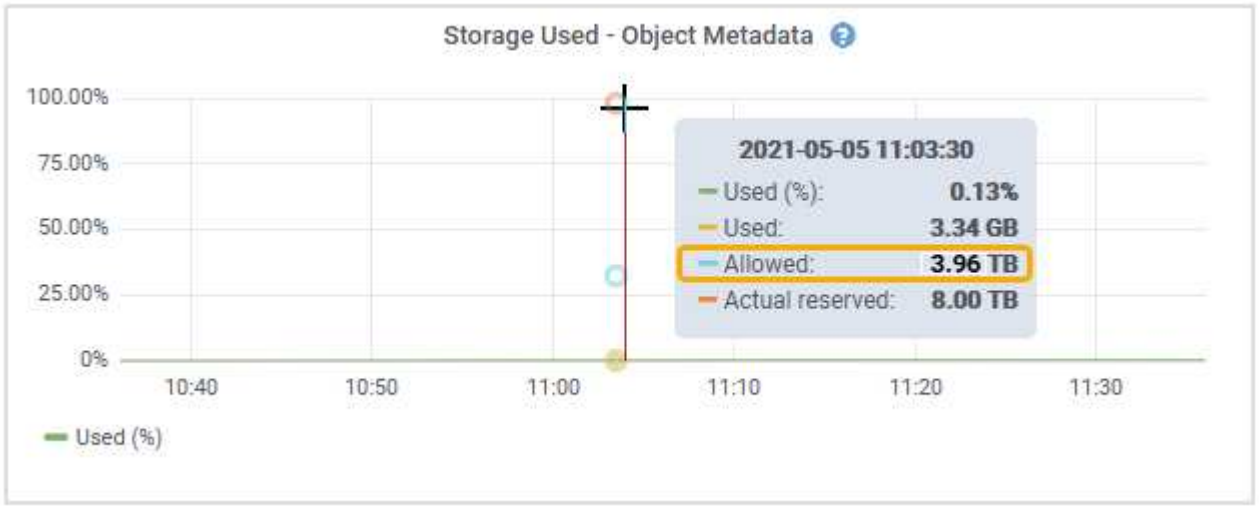


Die folgende Tabelle zeigt, wie StorageGRID den **zulässigen Metadatenspeicherplatz** für verschiedene Storage-Nodes berechnet, basierend auf der Speichermenge für den Node und dem tatsächlich reservierten Speicherplatz für Metadaten.

		Speichermenge auf Speicherknoten	
	lt; 128 GB	gt;= 128 GB	**Tatsächlich reservierter Platz für Metadaten**
lt;= 4 TB	60 % des tatsächlich reservierten Speicherplatzes für Metadaten maximal 1.32 TB	60 % des tatsächlich reservierten Speicherplatzes für Metadaten maximal 1.98 TB	gt; 4 TB

So zeigen Sie den zulässigen Metadatenspeicherplatz für einen Speicherknoten an:

1. Wählen Sie im Grid Manager die Option **NODES** aus.
2. Wählen Sie den Speicherknoten aus.
3. Wählen Sie die Registerkarte **Storage** aus.
4. Bewegen Sie den Cursor über das Diagramm verwendete Speicherdaten — Objektmetadaten und suchen Sie den Wert **zulässig**.



Im Screenshot beträgt der **zulässige**-Wert 3.96 TB, was der maximale Wert für einen Storage Node ist, dessen tatsächlicher reservierter Speicherplatz für Metadaten mehr als 4 TB beträgt.

Der **zulässige**-Wert entspricht dieser Prometheus-Metrik:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Beispiel für zulässigen Metadatenspeicherplatz

Angenommen, Sie installieren ein StorageGRID System mit Version 11.6. Nehmen Sie in diesem Beispiel an, dass jeder Speicherknoten mehr als 128 GB RAM und dieses Volume 0 von Speicherknoten 1 (SN1) 6 TB hat. Basierend auf diesen Werten:

- Der systemweite **Metadaten reservierter Platz** ist auf 8 TB eingestellt. (Dies ist der Standardwert für StorageGRID 11.6, wenn jeder Speicherknoten mehr als 128 GB RAM hat.)
- Der tatsächlich reservierte Speicherplatz für Metadaten von SN1 beträgt 6 TB. (Das gesamte Volume ist reserviert, da Volume 0 kleiner ist als die Einstellung **Metadaten reservierter Speicherplatz**.)
- Der zulässige Speicherplatz für Metadaten auf SN1 beträgt 3 TB, basierend auf der im angegebenen Berechnung Tabelle für zulässigem Speicherplatz für Metadaten: (Tatsächlich reservierter Platz für Metadaten − 1 TB) × 60%, bis zu einem Maximum von 3.96 TB.

Storage-Nodes unterschiedlicher Größen beeinflussen die Objektkapazität

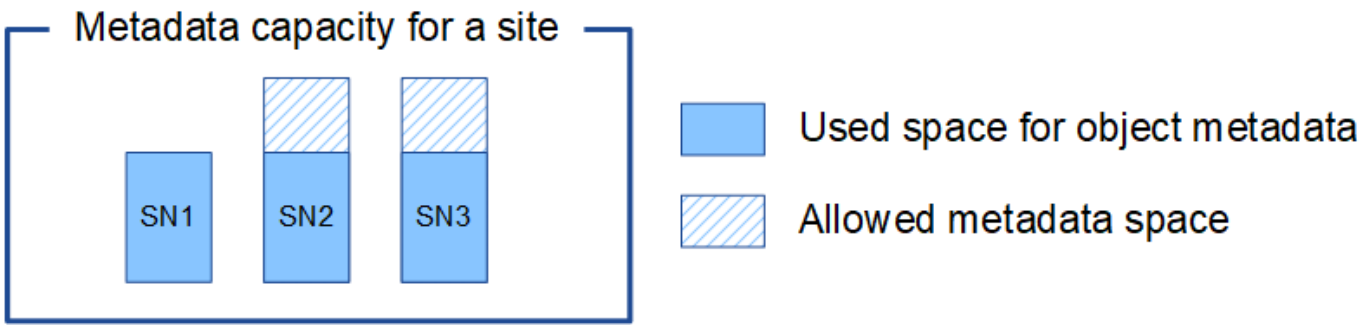
Wie oben beschrieben, verteilt StorageGRID Objektmetadaten gleichmäßig über Storage-Nodes an jedem Standort. Wenn ein Standort Storage-Nodes unterschiedlicher Größen enthält, bestimmt der kleinste Node am Standort die Metadaten-Kapazität des Standorts.

Beispiel:

- Sie haben ein Raster mit drei Storage Nodes unterschiedlicher Größe an einem einzigen Standort.
- Die Einstellung **Metadaten reservierter Platz** beträgt 4 TB.
- Die Storage-Nodes haben die folgenden Werte für den tatsächlich reservierten Metadatenspeicherplatz und den zulässigen Metadatenspeicherplatz.

Storage-Node	Größe von Volumen 0	Tatsächlich reservierter Metadatenspeicherplatz	Zulässiger Metadatenspeicherplatz
SN1	2.2 TB	2.2 TB	1.32 TB
SN2	5 TB	4 TB	1.98 TB
SN3	6 TB	4 TB	1.98 TB

Da Objektmetadaten gleichmäßig auf die Storage-Nodes an einem Standort verteilt werden, kann jeder Node in diesem Beispiel nur 1.32 TB Metadaten enthalten. Der zusätzlich zulässige Metadatenspeicherplatz von 0.66 TB für SN2 und SN3 kann nicht verwendet werden.



Da StorageGRID alle Objektmetadaten für ein StorageGRID System an jedem Standort speichert, wird die Gesamtkapazität der Metadaten eines StorageGRID Systems durch die Objektmetadaten des kleinsten Standorts bestimmt.

Und da die Objektmetadaten die maximale Objektanzahl steuern, wenn einem Node die Metadatenkapazität ausgeht, ist das Grid effektiv voll.

Verwandte Informationen

- Informationen zum Monitoring der Objektmetadaten für jeden Storage-Node finden Sie unter Monitoring und Fehlerbehebung.
- Um die Kapazität der Objektmetadaten für Ihr System zu erhöhen, fügen Sie neue Storage-Nodes hinzu. Gehen Sie zu Erweitern Sie Ihr Raster.

Globale Einstellungen für gespeicherte Objekte konfigurieren

Gespeicherte Objektkomprimierung konfigurieren

Über die Grid-Option „gespeicherte Objekte komprimieren“ lässt sich die Größe der in StorageGRID gespeicherten Objekte reduzieren, sodass Objekte weniger Storage belegen.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Die Grid-Option „gespeicherte Objekte komprimieren“ ist standardmäßig deaktiviert. Wenn Sie diese Option aktivieren, versucht StorageGRID, jedes Objekt beim Speichern mit verlustfreier Komprimierung zu komprimieren.

> 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.

Bevor Sie diese Option aktivieren, beachten Sie Folgendes:

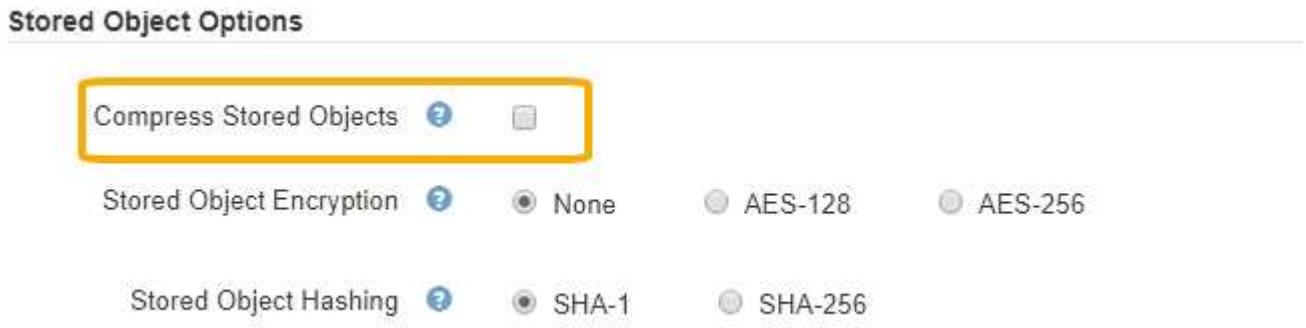
- Die Komprimierung sollte nur aktiviert werden, wenn die gespeicherten Daten komprimierbar sind.
- Applikationen, die Objekte in StorageGRID speichern, komprimieren möglicherweise Objekte, bevor sie gespeichert werden. Wenn bereits eine Client-Applikation ein Objekt komprimiert hat, bevor sie in StorageGRID gespeichert wird, wird die Komprimierung gespeicherter Objekte die Größe eines Objekts nicht weiter verringert.
- Aktivieren Sie die Komprimierung nicht, wenn Sie NetApp FabricPool mit StorageGRID verwenden.
- Wenn die Grid-Option „gespeicherte Objekte komprimieren“ aktiviert ist, sollten S3- und Swift-Client-Applikationen die AUSFÜHRUNG VON GET-Objektoperationen vermeiden, die einen Bereich von Bytes angeben. Diese Vorgänge „`range Read`“ sind ineffizient, da StorageGRID die Objekte effektiv dekomprimieren muss, um auf die angeforderten Bytes zugreifen zu können. VORGÄNGE ZUM ABRUFEN von Objekten, die einen kleinen Byte-Bereich von einem sehr großen Objekt anfordern, sind besonders ineffizient, beispielsweise ist es ineffizient, einen Bereich von 10 MB von einem komprimierten 50-GB-Objekt zu lesen.

  Wenn Bereiche von komprimierten Objekten gelesen werden, können Client-Anforderungen eine Zeitdauer haben.

  > Wenn Sie Objekte komprimieren müssen und Ihre Client-Applikation Bereichslesevorgänge verwenden muss, erhöhen Sie die Zeitüberschreitung beim Lesen der Anwendung.

Schritte

1. Wählen Sie **KONFIGURATION System Gitteroptionen**.
2. Aktivieren Sie im Abschnitt Optionen für gespeicherte Objekte das Kontrollkästchen **gespeicherte Objekte komprimieren**.



3. Wählen Sie **Speichern**.

Gespeicherte Objektverschlüsselung konfigurieren

Sie können gespeicherte Objekte verschlüsseln, wenn Sie sicherstellen möchten, dass die Daten bei einer Gefährdung eines Objektspeichers nicht in lesbarer Form abgerufen werden können. Objekte sind standardmäßig nicht verschlüsselt.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Die gespeicherte Objektverschlüsselung ermöglicht die Verschlüsselung aller Objektdaten bei der Aufnahme durch S3 oder Swift. 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 aktuell verschlüsselte Objekte verschlüsselt, neu aufgenommene Objekte werden jedoch nicht verschlüsselt.

> 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.

Gespeicherte Objekte können mit dem Verschlüsselungsalgorithmus AES-128 oder AES-256 verschlüsselt werden.

Die Einstellung „gespeicherte Objektverschlüsselung“ gilt nur für S3 Objekte, die nicht durch Verschlüsselung auf Bucket- oder Objektebene verschlüsselt wurden.

Schritte

1. Wählen Sie **KONFIGURATION System Gitteroptionen**.
2. Ändern Sie im Abschnitt Speicherte Objektoptionen die gespeicherte Objektverschlüsselung in **Keine** (Standard), **AES-128** oder **AES-256**.

3. Wählen Sie **Speichern**.

Konfigurieren Sie die gespeicherte Objekt-Hashing

Die Option „Speichertes Objekt-Hashing“ gibt den Hash-Algorithmus an, der zur Überprüfung der Objektintegrität verwendet wird.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Standardmäßig werden Objektdaten mit dem SHA-1-Algorithmus gehasht. Der SHA-256-Algorithmus erfordert zusätzliche CPU-Ressourcen und wird im Allgemeinen nicht für die Integritätsprüfung empfohlen.

> 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.

Schritte

1. Wählen Sie **KONFIGURATION System Gitteroptionen**.
2. Ändern Sie im Abschnitt „Optionen für gespeicherte Objekte“ die Option „gespeicherte Objekt-Hashing“ in **SHA-1** (Standardeinstellung) oder **SHA-256**.

3. Wählen Sie **Speichern**.

Konfigurationseinstellungen für Storage-Nodes

Jeder Storage Node verwendet eine Reihe von Konfigurationseinstellungen und Zählern. Möglicherweise müssen Sie die aktuellen Einstellungen anzeigen oder Zähler zurücksetzen, um Alarme zu löschen (Legacy-System).

> Mit Ausnahme der in der Dokumentation ausdrücklich enthaltenen Anweisungen sollten Sie sich mit dem technischen Support in Verbindung setzen, bevor Sie die Konfigurationseinstellungen für den Storage-Node ändern. Nach Bedarf können Sie Ereigniszähler zurücksetzen, um ältere Alarme zu löschen.

So greifen Sie auf die Konfigurationseinstellungen und Zähler eines Speicherknotens zu:

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***site Storage Node*** aus.
3. Erweitern Sie den Speicherknoten, und wählen Sie den Dienst oder die Komponente aus.
4. Wählen Sie die Registerkarte **Konfiguration**.

In den folgenden Tabellen sind die Konfigurationseinstellungen für Storage Node zusammengefasst.

LDR

Attributname	Codieren	Beschreibung
HTTP-Status	HSTE	Der aktuelle Status des HTTP-Protokolls für S3, Swift und andere interne StorageGRID-Zugriffe: • Offline: Es sind keine Vorgänge zulässig. Jede Client-Anwendung, die versucht, eine HTTP-Sitzung für den LDR-Dienst zu öffnen, erhält eine Fehlermeldung. Aktive Sitzungen werden ordnungsgemäß geschlossen. • Online: Der Vorgang wird normal fortgesetzt
Automatisches Starten von HTTP	HTAS	• Wenn diese Option ausgewählt ist, hängt der Zustand des Systems bei Neustart vom Zustand der **LDR Storage**-Komponente ab. Wenn die **LDR Storage**-Komponente beim Neustart schreibgeschützt ist, ist auch die HTTP-Schnittstelle schreibgeschützt. Wenn die **LDR Storage** Komponente Online ist, ist HTTP auch Online. Andernfalls bleibt die HTTP-Schnittstelle im Status Offline. • Wenn diese Option nicht aktiviert ist, bleibt die HTTP-Schnittstelle offline, bis sie explizit aktiviert ist.

LDR-Datenspeicher

Attributname	Codieren	Beschreibung
Anzahl Verlorener Objekte Zurücksetzen	RCOR	Setzen Sie den Zähler für die Anzahl der verlorenen Objekte dieses Dienstes zurück.

LDR-Speicher

Attributname	Codieren	Beschreibung
Storage-Zustand - Gewünscht	SSDS	Eine vom Benutzer konfigurierbare Einstellung für den gewünschten Status der Speicherkomponente. Der LDR-Dienst liest diesen Wert und versucht, den durch dieses Attribut angegebenen Status zu entsprechen. Der Wert wird bei Neustarts dauerhaft verwendet. Mit dieser Einstellung können Sie beispielsweise dazu zwingen, dass Speicher schreibgeschützt wird, selbst wenn genügend Speicherplatz vorhanden ist. Dies kann bei der Fehlerbehebung hilfreich sein. Das Attribut kann einen der folgenden Werte annehmen: • Offline: Wenn der gewünschte Status Offline ist, schaltet der LDR-Dienst die **LDR Storage** -Komponente offline. • Schreibgeschützt: Wenn der gewünschte Status schreibgeschützt ist, verschiebt der LDR-Service den Speicherstatus auf schreibgeschützt und hört auf, neue Inhalte zu akzeptieren. Beachten Sie, dass Inhalte möglicherweise noch für kurze Zeit im Speicherknoten gespeichert werden, bis offene Sitzungen geschlossen sind. • Online: Den Wert bei Online während des normalen Systembetriebs belassen. Der Speicherstatus – der aktuelle Status der Speicherkomponente wird durch den Service dynamisch festgelegt, basierend auf dem Zustand des LDR-Service, z. B. der Menge des verfügbaren Objektspeicherspeichers. Wenn der Speicherplatz knapp ist, ist die Komponente schreibgeschützt.
Zeitüberschreitung Bei Der Integritätsprüfung	SHCT	Die Zeitgrenze in Sekunden, innerhalb derer ein Integritätstest abgeschlossen werden muss, damit ein Speichervolumen als ordnungsgemäß angesehen wird. Ändern Sie diesen Wert nur, wenn Sie dazu vom Support aufgefordert werden.

LDR-Überprüfung

Attributname	Codieren	Beschreibung
Fehlende Objekte Zurücksetzen Anzahl	VCMI	Setzt die Anzahl der erkannten fehlenden Objekte zurück (OMIS). Nur nach Abschluss der Objektprüfung verwenden. Fehlende replizierte Objektdaten werden vom StorageGRID System automatisch wiederhergestellt.
Verifizierungsrate	VPRI	Legen Sie die Geschwindigkeit fest, mit der die Hintergrundüberprüfung durchgeführt wird. Weitere Informationen zur Konfiguration der Hintergrundverifizierungsrate finden Sie unter.
Anzahl Der Beschädigten Objekte Zurücksetzen	VCCR	Setzen Sie den Zähler für beschädigte, replizierte Objektdaten zurück, die während der Hintergrundüberprüfung gefunden wurden. Mit dieser Option können Sie den Alarmzustand der beschädigten Objekte löschen, die erkannt wurden (OCOR). Weitere Informationen finden Sie in den Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID.
Objekte In Quarantäne Löschen	OQRT	Löschen Sie beschädigte Objekte aus dem Quarantäneverzeichnis, setzen Sie die Anzahl der isolierten Objekte auf Null zurück und löschen Sie den Alarm „Quarantäne Objekte erkannt“ (OQRT). Diese Option wird verwendet, nachdem beschädigte Objekte vom StorageGRID-System automatisch wiederhergestellt wurden. Wenn ein Alarm „Lost Objects“ ausgelöst wird, kann der technische Support auf die isolierten Objekte zugreifen. In manchen Fällen können isolierte Objekte für die Datenwiederherstellung oder das Debuggen der zugrunde liegenden Probleme, die die beschädigten Objektkopien verursacht haben, nützlich sein.

LDR Erasure Coding

Attributname	Codieren	Beschreibung
Zurücksetzen Der Fehleranzahl Für Schreibvorgänge	RWF.	Setzen Sie den Zähler auf Schreibfehler von Objektdaten mit Erasure-Coding-Verfahren auf den Storage-Node zurück.
Anzahl Der Fehlgeschlagene Lesevorgänge Zurücksetzen	RSRF	Setzen Sie den Zähler für Leseausfälle von Objektdaten mit Erasure-Coding-Verfahren vom Storage-Node zurück.

Attributname	Codieren	Beschreibung
Zurücksetzen Löschen Fehleranzahl	RSDF	Setzen Sie den Zähler für Löschfehler von Objektdaten mit Erasure-Coding-Verfahren vom Storage-Node zurück.
Beschädigte Kopien Erkannte Anzahl Zurücksetzen	RSCC	Setzen Sie den Zähler für die Anzahl beschädigter Kopien von Objektdaten, die nach dem Erasure-Coding-Verfahren codiert wurden, auf dem Storage-Node zurück.
Beschädigte Fragmente Erkannte Anzahl Zurücksetzen	RCD	Setzen Sie den Zähler auf beschädigte Fragmente von Objektdaten mit Erasure-Coding-Verfahren auf dem Storage-Node zurück.
Fehlende Fragmente Erkannt Anzahl Zurücksetzen	RSMD	Setzen Sie den Zähler auf fehlende Fragmente von Objektdaten mit Erasure-Coding-Verfahren auf dem Storage Node zurück. Nur nach Abschluss der Objektprüfung verwenden.

LDR-Replizierung

Attributname	Codieren	Beschreibung
Fehleranzahl Inbound Replication Zurücksetzen	RICR	Setzen Sie den Zähler auf Fehler bei eingehender Replikation zurück. Dies kann verwendet werden, um den RIRF-Alarm (Inbound Replication — failed) zu löschen.
Fehleranzahl Für Ausgehende Replikation Zurücksetzen	ROCR	Setzen Sie den Zähler auf Fehler bei ausgehenden Replikationen zurück. Dies kann verwendet werden, um den RORF-Alarm (ausgehende Replikationen — fehlgeschlagen) zu löschen.
Deaktivieren Sie Inbound Replication	DSIR	Wählen Sie diese Option aus, um die eingehende Replikation im Rahmen eines Wartungs- oder Testverfahrens zu deaktivieren. Während des normalen Betriebs nicht aktiviert lassen. Wenn die eingehende Replikation deaktiviert ist, können Objekte vom Speicherknoten zum Kopieren an andere Speicherorte im StorageGRID-System abgerufen werden, Objekte können jedoch nicht von anderen Speicherorten aus zu diesem Speicherknoten kopiert werden: Der LDR-Dienst ist schreibgeschützt.

Attributname	Codieren	Beschreibung
Deaktivieren Sie Ausgehende Replikation	DSOR	Wählen Sie diese Option aus, um die ausgehende Replikation (einschließlich Inhaltsanforderungen für HTTP-Abrufvorgänge) im Rahmen eines Wartungs- oder Testverfahrens zu deaktivieren. Während des normalen Betriebs nicht aktiviert lassen. Wenn die ausgehende Replikation deaktiviert ist, können Objekte auf diesen Speicherknoten kopiert werden. Objekte können jedoch nicht vom Speicherknoten abgerufen werden, um sie an andere Speicherorte im StorageGRID-System zu kopieren. Der LDR-Service ist schreibgeschützt.

Verwandte Informationen

Monitoring und Fehlerbehebung

Management vollständiger Storage-Nodes

Wenn Storage-Nodes die Kapazität erreichen, müssen Sie das StorageGRID System durch Hinzufügen eines neuen Storage erweitern. Es sind drei Optionen verfügbar: Das Hinzufügen von Storage Volumes, das Hinzufügen von Shelfs zur Storage-Erweiterung und das Hinzufügen von Storage-Nodes.

Hinzufügen von Storage-Volumes

Jeder Storage-Node unterstützt eine maximale Anzahl an Storage-Volumes. Der definierte Höchstwert variiert je nach Plattform. Wenn ein Storage-Node weniger als die maximale Anzahl an Storage-Volumes enthält, können Sie Volumes hinzufügen, um seine Kapazität zu erhöhen. Siehe Anweisungen für Erweitern eines StorageGRID Systems.

Hinzufügen von Shelfs zur Storage-Erweiterung

Einige Storage-Nodes von StorageGRID Appliances, z. B. SG6060, können zusätzliche Storage-Shelfs unterstützen. Bei StorageGRID Appliances mit Erweiterungsfunktionen, die nicht bereits auf die maximale Kapazität erweitert wurden, können Sie Storage-Shelfs zur Steigerung der Kapazität hinzufügen. Siehe Anweisungen für Erweitern eines StorageGRID Systems.

Storage-Nodes Hinzufügen

Sie können die Storage-Kapazität durch Hinzufügen von Storage-Nodes erhöhen. Beim Hinzufügen von Storage müssen die aktuell aktiven ILM-Regeln und Kapazitätsanforderungen sorgfältig berücksichtigt werden. Siehe Anweisungen für Erweitern eines StorageGRID Systems.

Managen Sie Admin-Nodes

Was ist ein Admin-Node

Admin Nodes stellen Managementservices wie Systemkonfiguration, Monitoring und Protokollierung bereit. Jedes Grid muss einen primären Admin-Node haben und kann

eine beliebige Anzahl nicht primärer Admin-Nodes für Redundanz aufweisen.

Wenn Sie sich beim Grid Manager oder dem Tenant Manager anmelden, stellen Sie eine Verbindung zu einem Admin-Node her. Sie können eine Verbindung zu einem beliebigen Admin-Knoten herstellen, und jeder Admin-Knoten zeigt eine ähnliche Ansicht des StorageGRID-Systems an. Wartungsverfahren müssen jedoch mit dem primären Admin-Node durchgeführt werden.

Admin-Nodes können auch verwendet werden, um den S3- und Swift-Client-Datenverkehr auszugleichen.

Admin-Nodes hosten die folgenden Services:

- AMS-Service
- CMN-Service
- NMS-Service
- Prometheus Service
- Load Balancer- und High Availability-Services (zur Unterstützung von S3- und Swift-Client-Datenverkehr)

Admin-Nodes unterstützen außerdem die Management Application Program Interface (Management-API) zur Verarbeitung von Anfragen aus der Grid Management API und der Mandanten-Management-API. Siehe Verwenden Sie die Grid-Management-API.

Was ist der AMS-Service

Der Audit Management System (AMS)-Dienst verfolgt Systemaktivität und -Ereignisse.

Was der CMN-Service ist

Der Configuration Management Node (CMN)-Dienst verwaltet systemweite Konfigurationen von Konnektivität und Protokollfunktionen, die von allen Diensten benötigt werden. Darüber hinaus wird der CMN-Dienst zur Ausführung und Überwachung von Grid-Aufgaben verwendet. Es gibt nur einen CMN-Service pro StorageGRID-Implementierung. Der Admin-Node, der den CMN-Service hostet, wird als primärer Admin-Node bezeichnet.

Was ist der NMS-Service

Der NMS-Dienst (Network Management System) steuert die Überwachungs-, Reporting- und Konfigurationsoptionen, die über den Grid Manager, die browserbasierte Schnittstelle des StorageGRID-Systems, angezeigt werden.

Was der Prometheus Service ist

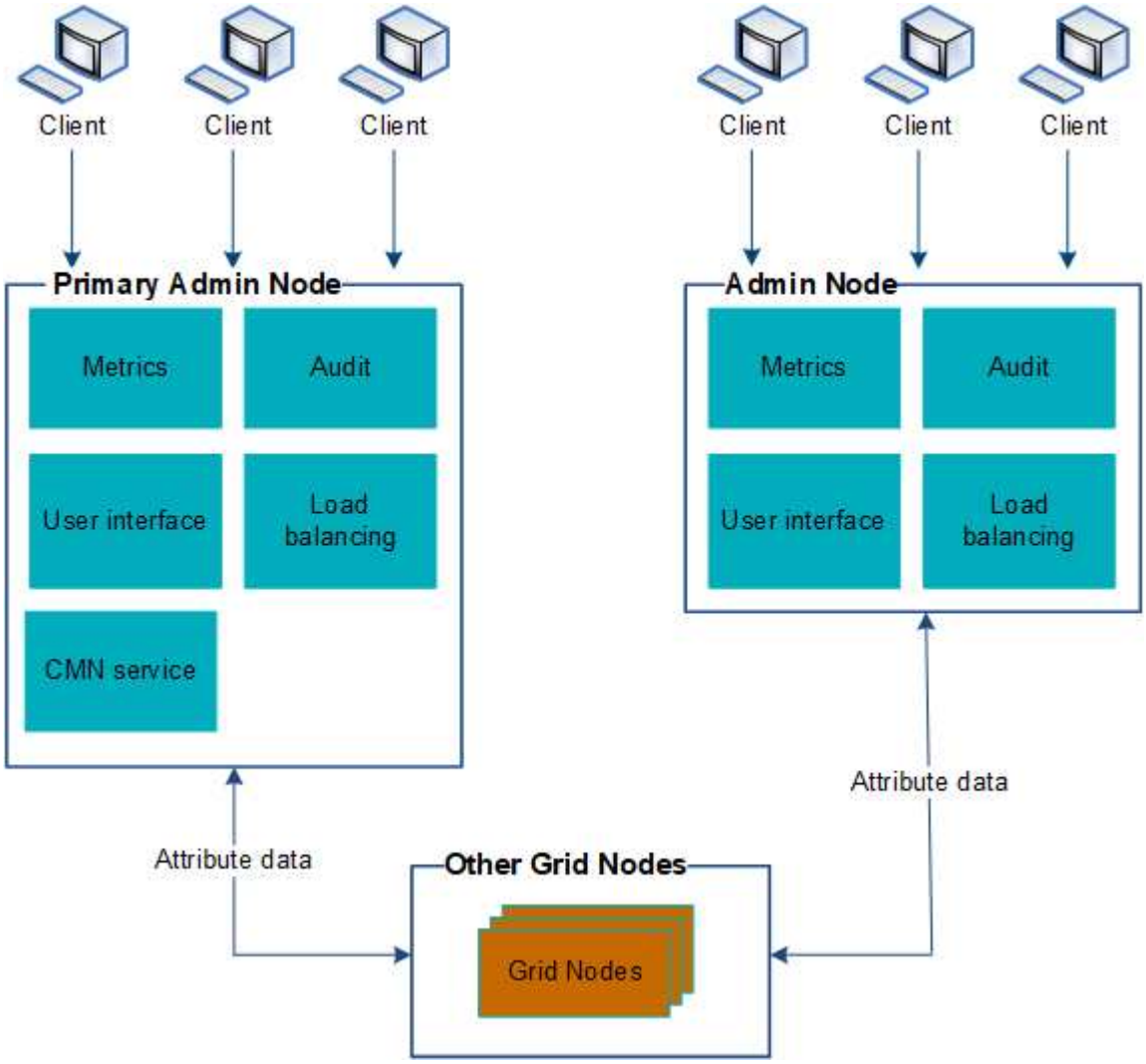
Der Prometheus Service sammelt Zeitreihungsmetriken aus den Services auf allen Knoten.

Verwenden Sie mehrere Admin-Nodes

Ein StorageGRID-System kann mehrere Admin-Knoten enthalten, damit Sie Ihr StorageGRID-System kontinuierlich überwachen und konfigurieren können, auch wenn ein Admin-Knoten ausfällt.

Wenn ein Admin-Knoten nicht mehr verfügbar ist, wird die Attributverarbeitung fortgesetzt, Alarme und Alarme (Legacy-System) werden immer noch ausgelöst und E-Mail-Benachrichtigungen und AutoSupport-Meldungen werden weiterhin gesendet. Das Vorhandensein mehrerer Admin-Nodes bietet jedoch keinen Failover-Schutz

außer Benachrichtigungen und AutoSupport-Meldungen. Insbesondere werden die von einem Admin-Knoten ausgemachten Alarmbestätigungen nicht auf andere Admin-Knoten kopiert.



Es gibt zwei Optionen, um das StorageGRID-System weiterhin anzuzeigen und zu konfigurieren, wenn ein Admin-Knoten ausfällt:

- Webclients können sich mit jedem anderen verfügbaren Admin-Node verbinden.
- Wenn ein Systemadministrator eine Hochverfügbarkeitsgruppe von Admin-Nodes konfiguriert hat, können Webclients unter Verwendung der virtuellen IP-Adresse der HA-Gruppe weiterhin auf den Grid Manager oder den Mandanten Manager zugreifen. Siehe Management von Hochverfügbarkeitsgruppen.

> Bei Verwendung einer HA-Gruppe wird der Zugriff unterbrochen, wenn der Master Admin-Node ausfällt. Benutzer müssen sich erneut anmelden, nachdem die virtuelle IP-Adresse der HA-Gruppe auf einen anderen Admin-Node in der Gruppe Failover erfolgt.

Einige Wartungsarbeiten können nur mit dem primären Admin-Node ausgeführt werden. Wenn der primäre Admin-Node ausfällt, muss er wiederhergestellt werden, bevor das StorageGRID System wieder voll funktionsfähig ist.

Identifizieren Sie den primären Admin-Node

Der primäre Admin-Node hostet den CMN-Service. Einige Wartungsarbeiten können nur mit dem primären Admin-Node durchgeführt werden.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***site* Admin Node**, und wählen Sie dann + So erweitern Sie die Topologiestruktur und zeigen die auf diesem Admin-Node gehosteten Services an.

   Der primäre Admin-Node hostet den CMN-Service.

3. Wenn dieser Admin-Node den CMN-Dienst nicht hostet, prüfen Sie die anderen Admin-Nodes.

Wählen Sie einen bevorzugten Sender aus

Wenn Ihre StorageGRID-Bereitstellung mehrere Administratorknoten enthält, können Sie auswählen, welcher Admin-Knoten der bevorzugte Absender von Benachrichtigungen sein soll. Standardmäßig ist der primäre Admin-Node ausgewählt, aber jeder Admin-Node kann der bevorzugte Absender sein.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Die Seite **CONFIGURATION System Anzeigeoptionen** zeigt an, welcher Admin-Node derzeit als bevorzugter Absender ausgewählt wurde. Der primäre Admin-Node ist standardmäßig ausgewählt.

Bei normalen Systemvorgängen sendet nur der bevorzugte Absender folgende Benachrichtigungen:

- AutoSupport Nachrichten
- SNMP-Benachrichtigungen
- E-Mails benachrichtigen
- Alarm-E-Mails (älteres System)

Alle anderen Admin-Knoten (Standby-Sender) überwachen jedoch den bevorzugten Sender. Wenn ein Problem erkannt wird, kann ein Standby-Sender diese Benachrichtigungen auch senden.

In diesen Fällen können sowohl der bevorzugte Sender als auch ein Standby-Sender Benachrichtigungen senden:

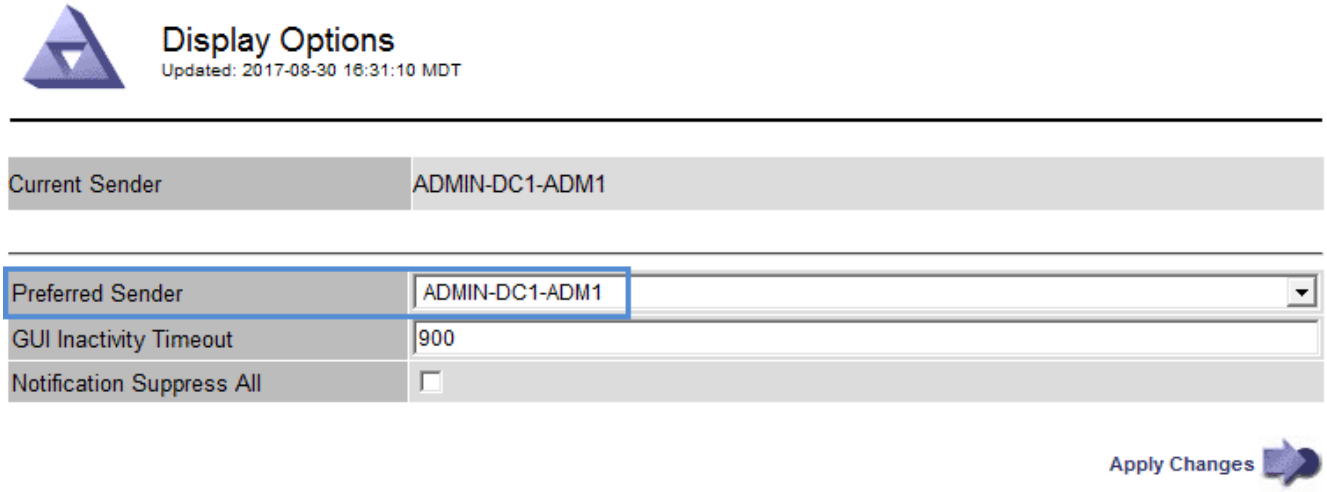
- Wenn Admin-Knoten von einander “islanded” werden, werden sowohl der bevorzugte Sender als auch die Standby-Sender versuchen, Benachrichtigungen zu senden, und mehrere Kopien von Benachrichtigungen können empfangen werden.

- Nachdem ein Standby-Sender Probleme mit dem bevorzugten Sender erkannt hat und mit dem Senden von Benachrichtigungen beginnt, kann der bevorzugte Sender seine Fähigkeit zum Senden von Benachrichtigungen wiederherstellen. In diesem Fall können doppelte Benachrichtigungen gesendet werden. Der Standby-Sender hört auf, Benachrichtigungen zu senden, wenn Fehler auf dem bevorzugten Sender nicht mehr erkannt werden.

> Wenn Sie Alarmbenachrichtigungen und AutoSupport-Meldungen testen, senden alle Admin-Knoten die Test-E-Mail. Wenn Sie die Warnbenachrichtigungen testen, müssen Sie sich bei jedem Admin-Knoten anmelden, um die Verbindung zu überprüfen.

Schritte

1. Wählen Sie **KONFIGURATION System Anzeigeoptionen**.
2. Wählen Sie im Menü Anzeigeoptionen die Option **Optionen**.
3. Wählen Sie in der Dropdown-Liste den Admin-Knoten aus, den Sie als bevorzugten Sender festlegen möchten.



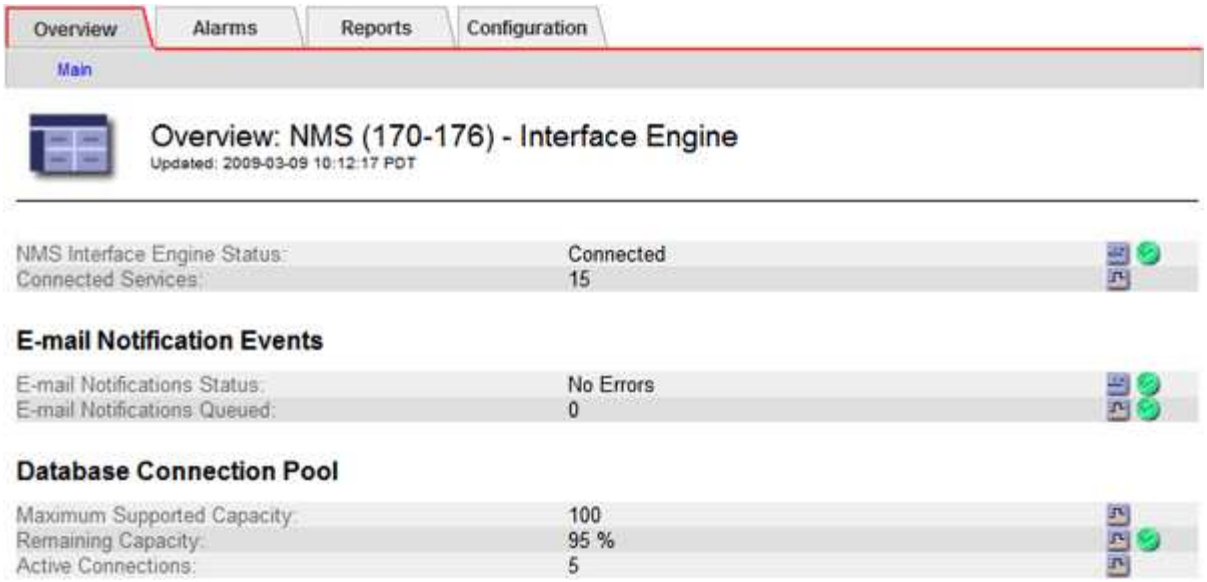
4. Wählen Sie **Änderungen Anwenden**.

   Der Admin-Node wird als bevorzugter Absender von Benachrichtigungen festgelegt.

Benachrichtigungsstatus und -Warteschlangen anzeigen

Der NMS-Dienst (Network Management System) auf Admin Nodes sendet Benachrichtigungen an den Mail-Server. Sie können den aktuellen Status des NMS-Dienstes und die Größe der Benachrichtigungswarteschlange auf der Seite Interface Engine anzeigen.

Um auf die Seite Interface Engine zuzugreifen, wählen Sie **SUPPORT Tools Grid-Topologie**. Wählen Sie abschließend ***site Admin Node* NMS Interface Engine** aus.

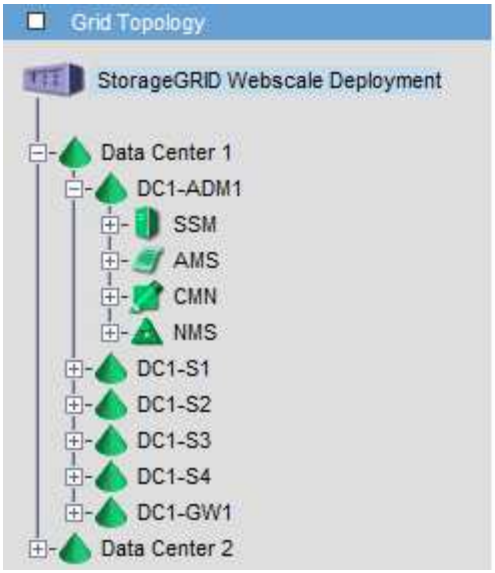


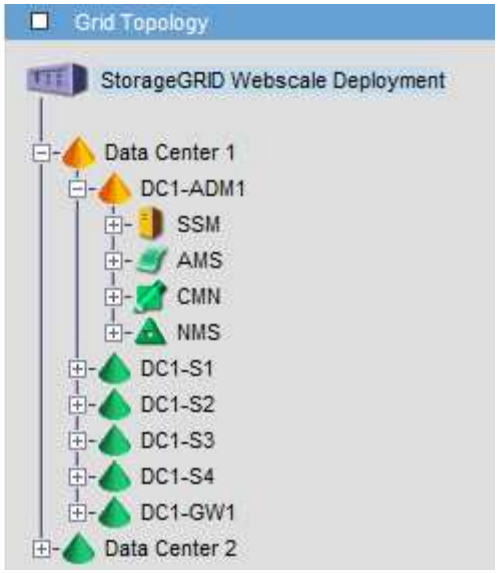
Benachrichtigungen werden über die E-Mail-Benachrichtigungswarteschlange verarbeitet und an den Mail-Server gesendet, einer nach dem anderen in der Reihenfolge, in der sie ausgelöst werden. Wenn ein Problem auftritt (z. B. ein Netzwerkverbindungsfehler) und der Mail-Server nicht verfügbar ist, wenn versucht wird, die Benachrichtigung zu senden, wird der Versuch unternommen, die Benachrichtigung an den Mailserver erneut zu senden, 60 Sekunden lang fortgesetzt. Wenn die Benachrichtigung nach 60 Sekunden nicht an den Mailserver gesendet wird, wird die Benachrichtigung aus der Benachrichtigungswarteschlange gelöscht und es wird versucht, die nächste Benachrichtigung in der Warteschlange zu senden. Da Benachrichtigungen aus der Benachrichtigungswarteschlange gelöscht werden können, ohne gesendet zu werden, ist es möglich, dass ein Alarm ausgelöst werden kann, ohne dass eine Benachrichtigung gesendet wird. Wenn eine Benachrichtigung aus der Warteschlange gelöscht wird, ohne gesendet zu werden, wird der Minor-Alarm FÜR MINUTEN (E-Mail-Benachrichtigungsstatus) ausgelöst.

So zeigen Admin-Knoten bestätigte Alarme an (Legacy-System)

Wenn Sie einen Alarm an einem Admin-Knoten bestätigen, wird der bestätigte Alarm nicht auf einen anderen Admin-Knoten kopiert. Da Danksagungen nicht auf andere Admin-Knoten kopiert werden, sieht die Struktur der Grid Topology für jeden Admin-Knoten möglicherweise nicht gleich aus.

Dieser Unterschied kann nützlich sein, wenn Web-Clients verbunden werden. Web-Clients können je nach Administratoranforderungen unterschiedliche Ansichten des StorageGRID-Systems haben.





Beachten Sie, dass Benachrichtigungen vom Admin-Knoten gesendet werden, wo die Bestätigung erfolgt.

Konfigurieren des Zugriffs auf Audit-Clients

Der Admin-Knoten protokolliert über den Service Audit Management System (AMS) alle überprüften Systemereignisse in eine Protokolldatei, die über die Revisionsfreigabe verfügbar ist und die zu jedem Admin-Knoten bei der Installation hinzugefügt wird. Um einfachen Zugriff auf Audit-Protokolle zu ermöglichen, lässt sich der Client-Zugriff auf Audit-Freigaben für CIFS und NFS konfigurieren.

Das StorageGRID System verwendet eine positive Bestätigung, um den Verlust von Audit-Meldungen zu verhindern, bevor sie in die Protokolldatei geschrieben werden. Eine Meldung bleibt an einem Dienst in der Warteschlange, bis der AMS-Dienst oder ein Zwischenaudit-Relaisdienst die Kontrolle über ihn bestätigt hat.

Weitere Informationen finden Sie unter Prüfung von Audit-Protokollen.

> Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt. Wenn Sie CIFS oder NFS verwenden möchten, wählen Sie NFS.

Audit-Clients für CIFS konfigurieren

Das Verfahren zum Konfigurieren eines Audit-Clients hängt von der Authentifizierungsmethode ab: Windows Workgroup oder Windows Active Directory (AD). Wenn diese Option hinzugefügt wird, wird die Revisionsfreigabe automatisch als schreibgeschützte Freigabe aktiviert.

> Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

Konfigurieren von Audit-Clients für Workgroup

Führen Sie dieses Verfahren für jeden Admin-Knoten in einer StorageGRID-Bereitstellung durch, von der aus Sie Audit-Nachrichten abrufen möchten.

Was Sie benötigen

- Sie haben die `Passwords.txt` Datei mit dem Root-/Admin-Passwort (im GENANNTEN Paket verfügbar).
- Sie haben die `Configuration.txt` Datei (im GENANNTEN Paket verfügbar).

Über diese Aufgabe

Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

Schritte

1. 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 `#`.

2. Vergewissern Sie sich, dass alle Dienste den Status „ausgeführt“ oder „geprüft“ aufweisen: `storagegrid-status`

   Wenn nicht alle Dienste ausgeführt oder verifiziert werden, beheben Sie Probleme, bevor Sie fortfahren.

3. Kehren Sie zur Befehlszeile zurück und drücken Sie **Strg+C**.
4. Starten Sie das CIFS-Konfigurationsprogramm: `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                 | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share        | set-authentication     | validate-config |
| enable-disable-share   | set-netbios-name       | help            |
| add-user-to-share      | join-domain            | exit            |
| remove-user-from-share | add-password-server    |                 |
| modify-group           | remove-password-server |                 |
|                        | add-wins-server        |                 |
|                        | remove-wins-server     |                 |
------------------------------------------------------------------
```

5. Legen Sie die Authentifizierung für die Windows Workgroup fest:

   Wenn die Authentifizierung bereits festgelegt wurde, wird eine Beratungsmeldung angezeigt. Wenn die Authentifizierung bereits festgelegt wurde, fahren Sie mit dem nächsten Schritt fort.

   a. Geben Sie Ein: `set-authentication`
   b. Wenn Sie zur Installation von Windows Workgroup oder Active Directory aufgefordert werden, geben Sie Folgendes ein: `workgroup`
   c. Geben Sie bei der entsprechenden Aufforderung einen Namen für die Arbeitsgruppe ein:

workgroup_name

d. Erstellen Sie bei Aufforderung einen aussagekräftigen NetBIOS-Namen: *netbios_name*

   Oder

   Drücken Sie **Enter**, um den Hostnamen des Admin-Knotens als NetBIOS-Name zu verwenden.

Das Skript startet den Samba-Server neu und es werden Änderungen vorgenommen. Dies sollte weniger als eine Minute dauern. Fügen Sie nach dem Festlegen der Authentifizierung einen Audit-Client hinzu.

a. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

   Das CIFS-Konfigurationsprogramm wird angezeigt.

6. Hinzufügen eines Audit-Clients:

   a. Geben Sie Ein: `add-audit-share`

      Die Freigabe wird automatisch als schreibgeschützt hinzugefügt.

   b. Wenn Sie dazu aufgefordert werden, fügen Sie einen Benutzer oder eine Gruppe hinzu: *user*
   c. Geben Sie bei der entsprechenden Aufforderung den Benutzernamen für die Prüfung ein: *audit_user_name*
   d. Wenn Sie dazu aufgefordert werden, geben Sie ein Kennwort für den Benutzer der Prüfung ein: *password*
   e. Geben Sie bei der entsprechenden Aufforderung dasselbe Passwort erneut ein, um es zu bestätigen: *password*
   f. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

      Das CIFS-Konfigurationsprogramm wird angezeigt.

      Es ist nicht erforderlich, ein Verzeichnis einzugeben. Der Name des Überwachungsverzeichnisses ist vordefiniert.

7. Wenn mehr als ein Benutzer oder eine Gruppe auf die Revisionsfreigabe zugreifen darf, fügen Sie die zusätzlichen Benutzer hinzu:

   a. Geben Sie Ein: `add-user-to-share`

      Es wird eine nummerierte Liste mit aktivierten Freigaben angezeigt.

   b. Geben Sie bei der entsprechenden Aufforderung die Nummer der Freigabe für den Audit-Export ein: *share_number*
   c. Wenn Sie dazu aufgefordert werden, fügen Sie einen Benutzer oder eine Gruppe hinzu: `user`

      Oder `group`

   d. Geben Sie bei Aufforderung den Namen des Audit-Benutzers oder der Gruppe ein: *audit_user or audit_group*
   e. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das CIFS-Konfigurationsprogramm wird angezeigt.

f. Wiederholen Sie diese Teilschritte für jeden weiteren Benutzer oder jede Gruppe, die Zugriff auf die Revisionsfreigabe hat.

8. Überprüfen Sie optional die Konfiguration: `validate-config`

   Die Dienste werden überprüft und angezeigt. Sie können die folgenden Meldungen ohne Bedenken ignorieren:

   ```
   Can't find include file /etc/samba/includes/cifs-interfaces.inc
   Can't find include file /etc/samba/includes/cifs-filesystem.inc
   Can't find include file /etc/samba/includes/cifs-custom-config.inc
   Can't find include file /etc/samba/includes/cifs-shares.inc
   rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
   (16384)
   ```

   a. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

      Die Konfiguration des Audit-Clients wird angezeigt.

   b. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

      Das CIFS-Konfigurationsprogramm wird angezeigt.

9. Schließen Sie das CIFS-Konfigurationsprogramm: `exit`
10. Starten Sie den Samba-Dienst: `service smbd start`
11. Wenn es sich bei der StorageGRID-Implementierung um einen einzelnen Standort handelt, mit dem nächsten Schritt fortfahren.

    Oder

    Wenn die StorageGRID-Bereitstellung Admin-Nodes an anderen Standorten enthält, aktivieren Sie diese Revisionsfreigabe nach Bedarf:

    a. Remote-Anmeldung beim Admin-Node eines Standorts:
       i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
       ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
       iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
       iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
    b. Wiederholen Sie die Schritte, um die Revisionsfreigabe für jeden zusätzlichen Admin-Knoten zu konfigurieren.
    c. Schließen Sie die sichere Remote-Shell-Anmeldung am Remote-Admin-Node: `exit`
12. Melden Sie sich aus der Befehlsshell ab: `exit`

Führen Sie dieses Verfahren für jeden Admin-Knoten in einer StorageGRID-Bereitstellung durch, von der aus Sie Audit-Nachrichten abrufen möchten.

Was Sie benötigen

- Sie haben die `Passwords.txt` Datei mit dem Root-/Admin-Passwort (im GENANNTEN Paket verfügbar).
- Sie haben den Benutzernamen und das Kennwort für das CIFS Active Directory.
- Sie haben die `Configuration.txt` Datei (im GENANNTEN Paket verfügbar).

> Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

Schritte

1. 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 `#`.

2. Vergewissern Sie sich, dass alle Dienste den Status „ausgeführt“ oder „geprüft“ aufweisen: `storagegrid-status`

   Wenn nicht alle Dienste ausgeführt oder verifiziert werden, beheben Sie Probleme, bevor Sie fortfahren.

3. Kehren Sie zur Befehlszeile zurück und drücken Sie **Strg+C**.
4. Starten Sie das CIFS-Konfigurationsprogramm: `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share       | set-authentication     | validate-config |
| enable-disable-share  | set-netbios-name       | help            |
| add-user-to-share     | join-domain            | exit            |
| remove-user-from-share| add-password-server    |                 |
| modify-group          | remove-password-server |                 |
|                       | add-wins-server        |                 |
|                       | remove-wins-server     |                 |
------------------------------------------------------------------
```

5. Legen Sie die Authentifizierung für Active Directory fest: `set-authentication`

   In den meisten Bereitstellungen müssen Sie die Authentifizierung festlegen, bevor Sie den Audit-Client

hinzufügen. Wenn die Authentifizierung bereits festgelegt wurde, wird eine Beratungsmeldung angezeigt. Wenn die Authentifizierung bereits festgelegt wurde, fahren Sie mit dem nächsten Schritt fort.

a. Bei Aufforderung zur Workgroup- oder Active Directory-Installation: `ad`
b. Geben Sie bei der entsprechenden Aufforderung den Namen der AD-Domäne ein (kurzer Domain-Name).
c. Geben Sie bei entsprechender Aufforderung die IP-Adresse oder den DNS-Hostnamen des Domänencontrollers ein.
d. Geben Sie bei entsprechender Aufforderung den vollständigen Domänennamen ein.

   Verwenden Sie Großbuchstaben.

e. Geben Sie bei Aufforderung zur Aktivierung der Winbindunterstützung **y** ein.

   Winbind wird verwendet, um Benutzer- und Gruppeninformationen von AD-Servern zu lösen.

f. Geben Sie bei entsprechender Aufforderung den NetBIOS-Namen ein.
g. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

   Das CIFS-Konfigurationsprogramm wird angezeigt.

6. Treten Sie der Domäne bei:
   a. Wenn noch nicht gestartet, starten Sie das CIFS-Konfigurationsprogramm: `config_cifs.rb`
   b. Treten Sie der Domäne bei: `join-domain`
   c. Sie werden aufgefordert zu testen, ob der Admin-Knoten derzeit ein gültiges Mitglied der Domain ist. Wenn dieser Admin-Node der Domäne noch nicht beigetreten ist, geben Sie Folgendes ein: `no`
   d. Geben Sie bei entsprechender Aufforderung den Benutzernamen des Administrators an: *`administrator_username`*

      Wo *`administrator_username`* Ist der Benutzername für das CIFS Active Directory, nicht der StorageGRID-Benutzername.

   e. Geben Sie bei entsprechender Aufforderung das Administratorpasswort an: *`administrator_password`*

      Waren *`administrator_password`* Ist der Benutzername für das CIFS-Active-Verzeichnis und nicht das StorageGRID-Kennwort.

   f. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

      Das CIFS-Konfigurationsprogramm wird angezeigt.

7. Vergewissern Sie sich, dass Sie der Domäne ordnungsgemäß beigetreten sind:
   a. Treten Sie der Domäne bei: `join-domain`
   b. Wenn Sie aufgefordert werden, zu testen, ob der Server derzeit ein gültiges Mitglied der Domäne ist, geben Sie Folgendes ein: `y`

      Wenn Sie die Meldung „`Join is OK,`“ erhalten, haben Sie sich erfolgreich der Domäne angeschlossen. Wenn diese Antwort nicht angezeigt wird, versuchen Sie, die Authentifizierung zu aktivieren und die Domain erneut anzuschließen.

c. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

   Das CIFS-Konfigurationsprogramm wird angezeigt.

8. Hinzufügen eines Audit-Clients: `add-audit-share`
   a. Wenn Sie aufgefordert werden, einen Benutzer oder eine Gruppe hinzuzufügen, geben Sie Folgendes ein: `user`
   b. Wenn Sie zur Eingabe des Benutzernamens für die Prüfung aufgefordert werden, geben Sie den Benutzernamen für die Prüfung ein.
   c. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

      Das CIFS-Konfigurationsprogramm wird angezeigt.

9. Wenn mehr als ein Benutzer oder eine Gruppe auf die Revisionsfreigabe zugreifen darf, fügen Sie weitere Benutzer hinzu: `add-user-to-share`

   Es wird eine nummerierte Liste mit aktivierten Freigaben angezeigt.

   a. Geben Sie die Nummer der Freigabe für den Audit-Export ein.
   b. Wenn Sie aufgefordert werden, einen Benutzer oder eine Gruppe hinzuzufügen, geben Sie Folgendes ein: `group`

      Sie werden aufgefordert, den Namen der Überwachungsgruppe anzugeben.

   c. Wenn Sie zur Eingabe des Namens der Überwachungsgruppe aufgefordert werden, geben Sie den Namen der Benutzergruppe für die Prüfung ein.
   d. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

      Das CIFS-Konfigurationsprogramm wird angezeigt.

   e. Wiederholen Sie diesen Schritt für jeden weiteren Benutzer oder jede Gruppe, der Zugriff auf die Revisionsfreigabe hat.

10. Überprüfen Sie optional die Konfiguration: `validate-config`

    Die Dienste werden überprüft und angezeigt. Sie können die folgenden Meldungen ohne Bedenken ignorieren:

    - Die include-Datei kann nicht gefunden werden `/etc/samba/includes/cifs-interfaces.inc`
    - Die include-Datei kann nicht gefunden werden `/etc/samba/includes/cifs-filesystem.inc`
    - Die include-Datei kann nicht gefunden werden `/etc/samba/includes/cifs-interfaces.inc`
    - Die include-Datei kann nicht gefunden werden `/etc/samba/includes/cifs-custom-config.inc`
    - Die include-Datei kann nicht gefunden werden `/etc/samba/includes/cifs-shares.inc`
    - Rlimit_max: Anstieg von rlimit_max (1024) auf Windows-Minimum (16384)

    > Kombinieren Sie die Einstellung 'security=ads' nicht mit dem Parameter 'Password Server'. (Standardmäßig erkennt Samba das korrekte DC, um automatisch Kontakt aufzunehmen).

i. Wenn Sie dazu aufgefordert werden, drücken Sie **Enter**, um die Konfiguration des Audit-Clients anzuzeigen.

ii. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das CIFS-Konfigurationsprogramm wird angezeigt.

11. Schließen Sie das CIFS-Konfigurationsprogramm: `exit`
12. Wenn es sich bei der StorageGRID-Implementierung um einen einzelnen Standort handelt, mit dem nächsten Schritt fortfahren.

    Oder

    Wenn die StorageGRID-Bereitstellung Admin-Nodes an anderen Standorten enthält, aktivieren Sie optional die folgenden Audit-Shares nach Bedarf:

    a. Remote-Anmeldung beim Admin-Node eines Standorts:
        i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
        ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
        iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
        iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
    b. Wiederholen Sie diese Schritte, um die Revisionsfreigaben für jeden Admin-Knoten zu konfigurieren.
    c. Schließen Sie die sichere Remote-Shell-Anmeldung beim Admin-Node: `exit`
13. Melden Sie sich aus der Befehlsshell ab: `exit`

Fügen Sie einen Benutzer oder eine Gruppe zu einer CIFS-Revisionsfreigabe hinzu

Sie können einen Benutzer oder eine Gruppe zu einer CIFS-Revisionsfreigabe hinzufügen, die in die AD-Authentifizierung integriert ist.

Was Sie benötigen

- Sie haben die `Passwords.txt` Datei mit dem Root-/Admin-Passwort (im GENANNTEN Paket verfügbar).
- Sie haben die `Configuration.txt` Datei (im GENANNTEN Paket verfügbar).

Über diese Aufgabe

Das folgende Verfahren gilt für eine mit AD-Authentifizierung integrierte Audit-Freigabe.

> Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

Schritte

1. 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 `#`.

2. Vergewissern Sie sich, dass alle Dienste den Status „ausgeführt“ oder „verifiziert“ aufweisen. Geben Sie Ein: `storagegrid-status`

   Wenn nicht alle Dienste ausgeführt oder verifiziert werden, beheben Sie Probleme, bevor Sie fortfahren.

3. Kehren Sie zur Befehlszeile zurück und drücken Sie **Strg+C**.
4. Starten Sie das CIFS-Konfigurationsprogramm: `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------
```

5. Beginnen Sie mit dem Hinzufügen eines Benutzers oder einer Gruppe: `add-user-to-share`

   Eine nummerierte Liste der konfigurierten Audit-Shares wird angezeigt.

6. Wenn Sie dazu aufgefordert werden, geben Sie die Nummer für die Revisionsfreigabe ein (Audit-Export): *`audit_share_number`*

   Sie werden gefragt, ob Sie einem Benutzer oder einer Gruppe Zugriff auf diese Revisionsfreigabe gewähren möchten.

7. Wenn Sie dazu aufgefordert werden, fügen Sie einen Benutzer oder eine Gruppe hinzu: `user` Oder `group`
8. Wenn Sie zur Eingabe des Benutzer- oder Gruppennamens für diese AD-Revisionsfreigabe aufgefordert werden, geben Sie den Namen ein.

   Der Benutzer oder die Gruppe wird als schreibgeschützt für die Revisionsfreigabe sowohl im Betriebssystem des Servers als auch im CIFS-Dienst hinzugefügt. Die Samba-Konfiguration wird neu geladen, damit der Benutzer oder die Gruppe auf die Audit-Client-Freigabe zugreifen können.

9. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

   Das CIFS-Konfigurationsprogramm wird angezeigt.

10. Wiederholen Sie diese Schritte für jeden Benutzer oder jede Gruppe, der Zugriff auf die Revisionsfreigabe hat.
11. Überprüfen Sie optional die Konfiguration: `validate-config`

    Die Dienste werden überprüft und angezeigt. Sie können die folgenden Meldungen ohne Bedenken

ignorieren:

- Kann die Datei /etc/samba/includes/cifs-interfaces.inc nicht finden
- Kann die Datei /etc/samba/includes/cifs-filesystem.inc nicht finden
- Kann die Datei /etc/samba/includes/cifs-custom-config.inc nicht finden
- Kann die Datei /etc/samba/includes/cifs-shares.inc nicht finden

  i. Wenn Sie dazu aufgefordert werden, drücken Sie **Enter**, um die Konfiguration des Audit-Clients anzuzeigen.

  ii. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

12. Schließen Sie das CIFS-Konfigurationsprogramm: `exit`
13. Ermitteln Sie wie folgt, ob zusätzliche Audit-Shares aktiviert werden müssen:
    - Wenn es sich bei der StorageGRID-Implementierung um einen einzelnen Standort handelt, mit dem nächsten Schritt fortfahren.
    - Wenn die StorageGRID-Bereitstellung Admin-Nodes an anderen Standorten umfasst, aktivieren Sie die folgenden Audit-Freigaben nach Bedarf:

      i. Remote-Anmeldung beim Admin-Node eines Standorts:

      A. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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:

      ii. Wiederholen Sie diese Schritte, um die Revisionsfreigaben für jeden Admin-Knoten zu konfigurieren.

      iii. Schließen Sie die sichere Remote-Shell-Anmeldung am Remote-Admin-Node: `exit`
14. Melden Sie sich aus der Befehlsshell ab: `exit`

Entfernen Sie einen Benutzer oder eine Gruppe aus einer CIFS-Revisionsfreigabe

Sie können den letzten Benutzer oder die letzte Gruppe, der Zugriff auf die Revisionsfreigabe hat, nicht entfernen.

Was Sie benötigen

- Sie haben die `Passwords.txt` Datei mit den Passwörtern des Root-Kontos (im GENANNTEN Paket verfügbar).
- Sie haben die `Configuration.txt` Datei (im GENANNTEN Paket verfügbar).

Über diese Aufgabe

Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

Schritte

1. 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 `#`.

2. Starten Sie das CIFS-Konfigurationsprogramm: `config_cifs.rb`

```
----------------------------------------------------------------------
| Shares                 | Authentication         | Config          |
----------------------------------------------------------------------
| add-audit-share        | set-authentication     | validate-config |
| enable-disable-share   | set-netbios-name       | help            |
| add-user-to-share      | join-domain            | exit            |
| remove-user-from-share | add-password-server    |                 |
| modify-group           | remove-password-server |                 |
|                        | add-wins-server        |                 |
|                        | remove-wins-server     |                 |
----------------------------------------------------------------------
```

3. Starten Sie das Entfernen eines Benutzers oder einer Gruppe: `remove-user-from-share`

   Eine nummerierte Liste der verfügbaren Audit-Shares für den Admin-Knoten wird angezeigt. Die Revisionsfreigabe wird als Audit-Export bezeichnet.

4. Geben Sie die Nummer der Revisionsfreigabe ein: *`audit_share_number`*

5. Wenn Sie aufgefordert werden, einen Benutzer oder eine Gruppe zu entfernen: `user` Oder `group`

   Eine nummerierte Liste von Benutzern oder Gruppen für die Revisionsfreigabe wird angezeigt.

6. Geben Sie die Nummer für den Benutzer oder die Gruppe ein, die Sie entfernen möchten: *`number`*

   Die Revisionsfreigabe wird aktualisiert, und der Benutzer oder die Gruppe ist nicht mehr berechtigt, auf die Revisionsfreigabe zuzugreifen. Beispiel:

```
Enabled shares
 1. audit-export
Select the share to change: 1
Remove user or group? [User/group]: User
Valid users for this share
1. audituser
2. newaudituser
Select the user to remove: 1

Removed user "audituser" from share "audit-export".

Press return to continue.
```

7. Schließen Sie das CIFS-Konfigurationsprogramm: `exit`
8. Wenn die StorageGRID-Bereitstellung Admin-Nodes an anderen Standorten umfasst, deaktivieren Sie die Revisionsfreigabe an jedem Standort nach Bedarf.
9. Melden Sie sich bei Abschluss der Konfiguration von jeder Befehlshaber ab: `exit`

Ändern Sie einen CIFS-Benutzer- oder Gruppennamen für die Revisionsfreigabe

Sie können den Namen eines Benutzers oder einer Gruppe für eine CIFS-Revisionsfreigabe ändern, indem Sie einen neuen Benutzer oder eine neue Gruppe hinzufügen und dann den alten löschen.

Über diese Aufgabe

Der Audit-Export über CIFS/Samba wurde veraltet und wird in einer zukünftigen StorageGRID-Version entfernt.

Schritte

1. Fügen Sie einen neuen Benutzer oder eine neue Gruppe mit dem aktualisierten Namen zur Revisionsfreigabe hinzu.
2. Löschen Sie den alten Benutzer- oder Gruppennamen.

Verwandte Informationen

- Fügen Sie einen Benutzer oder eine Gruppe zu einer CIFS-Revisionsfreigabe hinzu
- Entfernen Sie einen Benutzer oder eine Gruppe aus einer CIFS-Revisionsfreigabe

Prüfung der CIFS-Audit-Integration

Die Revisionsfreigabe ist schreibgeschützt. Die Protokolldateien sind für Computeranwendungen gedacht, und die Überprüfung beinhaltet nicht das Öffnen einer Datei. Es wird als ausreichend überprüft, ob die Audit-Log-Dateien in einem Windows Explorer-Fenster angezeigt werden. Schließen Sie nach der Verbindungsüberprüfung alle Fenster.

Konfigurieren Sie den Audit-Client für NFS

Die Revisionsfreigabe wird automatisch als schreibgeschützte Freigabe aktiviert.

Was Sie benötigen

- Sie haben die `Passwords.txt` Datei mit dem Root-/Admin-Passwort (im GENANNTEN Paket verfügbar).
- Sie haben die `Configuration.txt` Datei (im GENANNTEN Paket verfügbar).
- Der Audit-Client verwendet die NFS-Version 3 (NFSv3).

Über diese Aufgabe

Führen Sie dieses Verfahren für jeden Admin-Knoten in einer StorageGRID-Bereitstellung durch, von der aus Sie Audit-Nachrichten abrufen möchten.

Schritte

1. 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 `#`.

2. Vergewissern Sie sich, dass alle Dienste den Status „ausgeführt“ oder „verifiziert“ aufweisen. Geben Sie Ein: `storagegrid-status`

   Wenn Dienste nicht als aktiv oder verifiziert aufgeführt sind, beheben Sie Probleme, bevor Sie fortfahren.

3. Zurück zur Kommandozeile. Drücken Sie **Strg+C**.
4. Starten Sie das NFS-Konfigurationsprogramm. Geben Sie Ein: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares               | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share      | add-ip-to-share      | validate-config |
| enable-disable-share | remove-ip-from-share | refresh-config  |
|                      |                      | help            |
|                      |                      | exit            |
------------------------------------------------------------------
```

5. Fügen Sie den Audit-Client hinzu: `add-audit-share`
   a. Geben Sie bei entsprechender Aufforderung die IP-Adresse oder den IP-Adressbereich des Audit-Clients für die Revisionsfreigabe ein: `client_IP_address`
   b. Drücken Sie auf der entsprechenden Aufforderung **Enter**.
6. Wenn mehr als ein Audit-Client auf die Revisionsfreigabe zugreifen darf, fügen Sie die IP-Adresse des zusätzlichen Benutzers hinzu: `add-ip-to-share`

a. Geben Sie die Nummer der Revisionsfreigabe ein: *audit_share_number*

b. Geben Sie bei entsprechender Aufforderung die IP-Adresse oder den IP-Adressbereich des Audit-Clients für die Revisionsfreigabe ein: *client_IP_address*

c. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

   Das NFS-Konfigurationsprogramm wird angezeigt.

d. Wiederholen Sie diese Teilschritte für jeden zusätzlichen Audit-Client, der Zugriff auf die Revisionsfreigabe hat.

7. Überprüfen Sie optional Ihre Konfiguration.

   a. Geben Sie Folgendes ein: `validate-config`

      Die Dienste werden überprüft und angezeigt.

   b. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

      Das NFS-Konfigurationsprogramm wird angezeigt.

   c. Schließen Sie das NFS-Konfigurationsdienstprogramm: `exit`

8. Legen Sie fest, ob die Revisionsfreigaben an anderen Standorten aktiviert werden müssen.

   - Wenn es sich bei der StorageGRID-Implementierung um einen einzelnen Standort handelt, mit dem nächsten Schritt fortfahren.
   - Wenn die StorageGRID-Bereitstellung Admin-Nodes an anderen Standorten umfasst, aktivieren Sie die folgenden Audit-Freigaben nach Bedarf:

     i. Remote-Anmeldung beim Admin-Node des Standorts:

        A. Geben Sie den folgenden Befehl ein: `ssh admin@grid_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:

     ii. Wiederholen Sie diese Schritte, um die Revisionsfreigaben für jeden zusätzlichen Admin-Node zu konfigurieren.

     iii. Schließen Sie die sichere Remote-Shell-Anmeldung am Remote-Admin-Node. Geben Sie Ein: `exit`

9. Melden Sie sich aus der Befehlsshell ab: `exit`

NFS-Audit-Clients erhalten auf Basis ihrer IP-Adresse Zugriff auf eine Revisionsfreigabe. Gewähren Sie einem neuen NFS-Audit-Client Zugriff auf die Revisionsfreigabe, indem Sie der Freigabe ihre IP-Adresse hinzufügen oder einen vorhandenen Audit-Client entfernen, indem Sie seine IP-Adresse entfernen.

Fügen Sie einem Audit-Share einen NFS-Audit-Client hinzu

NFS-Audit-Clients erhalten auf Basis ihrer IP-Adresse Zugriff auf eine Revisionsfreigabe. Gewähren Sie einem neuen NFS-Audit-Client Zugriff auf die Revisionsfreigabe, indem Sie dessen IP-Adresse zur Revisionsfreigabe hinzufügen.

Was Sie benötigen

- Sie haben die `Passwords.txt` Datei mit dem Root-/Admin-Passwort (im GENANNTEN Paket verfügbar).
- Sie haben die `Configuration.txt` Datei (im GENANNTEN Paket verfügbar).
- Der Audit-Client verwendet die NFS-Version 3 (NFSv3).

Schritte

1. 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 `#`.

2. Starten Sie das NFS-Konfigurationsprogramm: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

3. Geben Sie Ein: `add-ip-to-share`

   Es wird eine Liste der auf dem Admin-Knoten aktivierten NFS-Audit-Freigaben angezeigt. Die Revisionsfreigabe ist wie folgt aufgelistet: `/var/local/audit/export`

4. Geben Sie die Nummer der Revisionsfreigabe ein: *`audit_share_number`*
5. Geben Sie bei entsprechender Aufforderung die IP-Adresse oder den IP-Adressbereich des Audit-Clients für die Revisionsfreigabe ein: *`client_IP_address`*

   Der Audit-Client wird der Revisionsfreigabe hinzugefügt.

6. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

   Das NFS-Konfigurationsprogramm wird angezeigt.

7. Wiederholen Sie die Schritte für jeden Audit-Client, der zur Revisionsfreigabe hinzugefügt werden soll.
8. Überprüfen Sie optional die Konfiguration: `validate-config`

   Die Dienste werden überprüft und angezeigt.

   a. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das NFS-Konfigurationsprogramm wird angezeigt.

9. Schließen Sie das NFS-Konfigurationsdienstprogramm: `exit`
10. Wenn es sich bei der StorageGRID-Implementierung um einen einzelnen Standort handelt, mit dem nächsten Schritt fortfahren.

    Wenn die StorageGRID-Bereitstellung Admin-Nodes an anderen Standorten umfasst, aktivieren Sie andernfalls optional diese Audit-Shares nach Bedarf:

    a. Remote-Anmeldung beim Admin-Node eines Standorts:
        i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
        ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
        iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
        iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
    b. Wiederholen Sie diese Schritte, um die Revisionsfreigaben für jeden Admin-Knoten zu konfigurieren.
    c. Schließen Sie die sichere Remote-Shell-Anmeldung am Remote-Admin-Node: `exit`
11. Melden Sie sich aus der Befehlsshell ab: `exit`

Prüfung der NFS-Audit-Integration

Nachdem Sie eine Audit-Freigabe konfiguriert und einen NFS-Audit-Client hinzugefügt haben, können Sie die Audit-Client-Freigabe mounten und überprüfen, ob die Dateien über die Audit-Freigabe verfügbar sind.

Schritte

1. Überprüfen Sie die Konnektivität (oder Variante für das Clientsystem) mithilfe der clientseitigen IP-Adresse des Admin-Knotens, der den AMS-Dienst hostet. Geben Sie Ein: `ping IP_address`

   Stellen Sie sicher, dass der Server antwortet, und geben Sie die Konnektivität an.

2. Mounten Sie die schreibgeschützte Revisionsfreigabe mit einem dem Client-Betriebssystem entsprechenden Befehl. Ein Beispiel für Linux lautet (geben Sie in einer Zeile ein):

   `mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/audit/export myAudit`

   Verwenden Sie die IP-Adresse des Admin-Knotens, der den AMS-Dienst hostet, und den vordefinierten Freigabennamen für das Audit-System. Der Mount-Punkt kann ein beliebiger Name sein, der vom Client ausgewählt wurde (z. B. `myAudit` Im vorherigen Befehl).

3. Stellen Sie sicher, dass die Dateien über die Revisionsfreigabe verfügbar sind. Geben Sie Ein: `ls myAudit /*`

   Wo `myAudit` Ist der Bereitstellungspunkt der Revisionsfreigabe. Es sollte mindestens eine Protokolldatei aufgeführt sein.

Entfernen Sie einen NFS-Audit-Client aus der Revisionsfreigabe

NFS-Audit-Clients erhalten auf Basis ihrer IP-Adresse Zugriff auf eine Revisionsfreigabe. Sie können einen vorhandenen Audit-Client entfernen, indem Sie seine IP-Adresse entfernen.

Was Sie benötigen

- Sie haben die `Passwords.txt` Datei mit dem Root-/Admin-Passwort (im GENANNTEN Paket verfügbar).
- Sie haben die `Configuration.txt` Datei (im GENANNTEN Paket verfügbar).

Über diese Aufgabe

Sie können die letzte IP-Adresse, die für den Zugriff auf die Revisionsfreigabe zulässig ist, nicht entfernen.

Schritte

1. 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 `#`.

2. Starten Sie das NFS-Konfigurationsprogramm: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares               | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share      | add-ip-to-share      | validate-config |
| enable-disable-share | remove-ip-from-share | refresh-config  |
|                      |                      | help            |
|                      |                      | exit            |
------------------------------------------------------------------
```

3. Entfernen Sie die IP-Adresse aus der Revisionsfreigabe: `remove-ip-from-share`

   Eine nummerierte Liste der auf dem Server konfigurierten Audit-Freigaben wird angezeigt. Die Revisionsfreigabe ist wie folgt aufgelistet: `/var/local/audit/export`

4. Geben Sie die Nummer für die Revisionsfreigabe ein: *`audit_share_number`*

   Eine nummerierte Liste mit IP-Adressen, die Zugriff auf die Revisionsfreigabe ermöglichen, wird angezeigt.

5. Geben Sie die Nummer für die IP-Adresse ein, die Sie entfernen möchten.

   Die Revisionsfreigabe wird aktualisiert, und der Zugriff ist von keinem Audit-Client mit dieser IP-Adresse mehr gestattet.

6. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

   Das NFS-Konfigurationsprogramm wird angezeigt.

7. Schließen Sie das NFS-Konfigurationsdienstprogramm: `exit`
8. Wenn es sich bei Ihrer StorageGRID-Bereitstellung um mehrere Datacenter-Standortimplementierungen mit zusätzlichen Admin-Nodes an anderen Standorten handelt, deaktivieren Sie diese Revisionsfreigaben nach Bedarf:
   a. Remote-Anmeldung bei jedem Standort Admin-Node:
      i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
      ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
      iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
      iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
   b. Wiederholen Sie diese Schritte, um die Revisionsfreigaben für jeden zusätzlichen Admin-Node zu konfigurieren.
   c. Schließen Sie die sichere Remote-Shell-Anmeldung am Remote-Admin-Node: `exit`
9. Melden Sie sich aus der Befehlsshell ab: `exit`

Ändern der IP-Adresse eines NFS-Audit-Clients

Führen Sie diese Schritte aus, wenn Sie die IP-Adresse eines NFS-Audit-Clients ändern müssen.

Schritte

1. Fügen Sie einer vorhandenen NFS-Revisionsfreigabe eine neue IP-Adresse hinzu.
2. Entfernen Sie die ursprüngliche IP-Adresse.

Verwandte Informationen

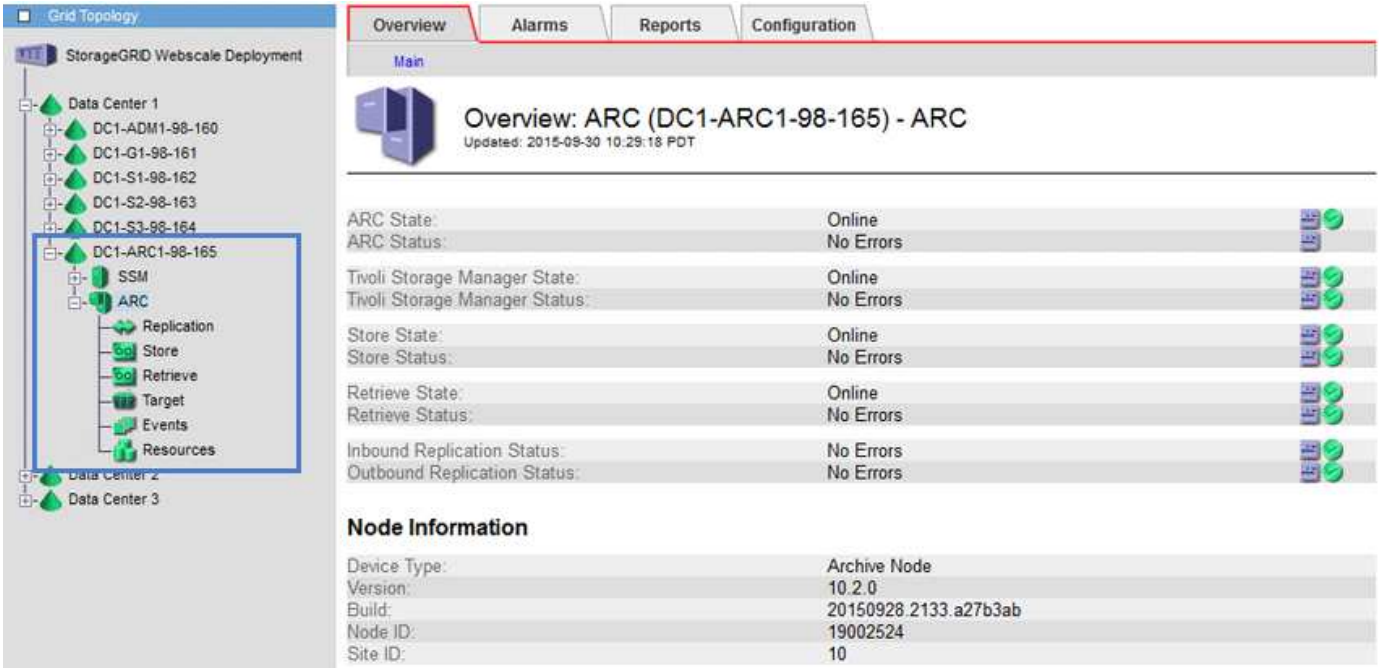
- Fügen Sie einem Audit-Share einen NFS-Audit-Client hinzu
- Entfernen Sie einen NFS-Audit-Client aus der Revisionsfreigabe

Archiv-Nodes Managen

Was ist ein Archivknoten

Optional kann jeder StorageGRID Datacenter-Standort mit einem Archiv-Node implementiert werden, sodass eine Verbindung zu einem externen Archiv-Storage-System wie Tivoli Storage Manager (TSM) hergestellt werden kann.

Der Archive Node bietet eine Schnittstelle, über die Sie ein externes Archiv-Storage-System zur langfristigen Speicherung von Objektdaten gezielt einsetzen können. Der Archivknoten überwacht darüber hinaus diese Verbindung und die Übertragung von Objektdaten zwischen dem StorageGRID System und dem angestrebten externen Archiv-Storage-System.



Nachdem Sie Verbindungen zum externen Ziel konfiguriert haben, können Sie den Archiv-Node so konfigurieren, dass die TSM-Performance optimiert wird, einen Archiv-Node offline schalten, wenn sich ein TSM-Server der Kapazität nähert oder nicht mehr verfügbar ist, und Einstellungen für Replikation und Abruf konfigurieren. Sie können auch benutzerdefinierte Alarme für den Knoten Archiv einstellen.

Objektdaten, die nicht gelöscht, aber nicht regelmäßig abgerufen werden können, können jederzeit von den rotierenden Festplatten eines Storage Node auf einen externen Archiv-Storage wie die Cloud oder auf Tapes verschoben werden. Diese Archivierung von Objektdaten erfolgt durch die Konfiguration des Archiv-Nodes eines Datacenter-Standorts und anschließend die Konfiguration von ILM-Regeln, bei denen dieser Archivknoten als „Ziel“ für Anweisungen zur Content-Platzierung ausgewählt wird. Der Archivknoten verwaltet die archivierten Objektdaten nicht selbst; dies wird durch das externe Archivgerät erreicht.

Objektmetadaten werden nicht archiviert, bleiben aber auf Storage-Nodes erhalten.

Was der ARC-Service ist

Der ARC-Dienst (Archive Nodes) stellt die Managementoberfläche bereit, über die Sie Verbindungen zu externen Archivspeichern konfigurieren können, z. B. Bandmedien über TSM Middleware.

Der ARC-Service interagiert mit einem externen Archivspeichersystem, sendet Objektdaten für Nearline-Speicherung und führt Abrufvorgänge durch, wenn eine Client-Anwendung ein archiviertes Objekt anfordert. Wenn eine Client-Anwendung ein archiviertes Objekt anfordert, fordert ein Storage Node die Objektdaten vom ARC-Service an. Der ARC-Dienst stellt eine Anfrage an das externe Archiv-Speichersystem, das die angeforderten Objektdaten abruft und diese an den ARC-Dienst sendet. Der ARC-Dienst überprüft die Objektdaten und leitet sie an den Speicherknoten weiter, der wiederum das Objekt an die anfordernde Client-Anwendung zurückgibt.

Anfragen nach über TSM Middleware auf Tape archivierten Objektdaten werden für eine effiziente Abrufvorgänge verwaltet. Anfragen können so bestellt werden, dass Objekte, die nacheinander auf Band gespeichert sind, in derselben sequenziellen Reihenfolge angefordert werden. Anforderungen werden dann in die Warteschlange gestellt, um sie an das Speichergerät zu übertragen. Je nach Archivgerät können mehrere Anfragen für Objekte auf verschiedenen Volumes gleichzeitig verarbeitet werden.

Archivierung in der Cloud über die S3-API

Ein Archivierungs-Node kann so konfiguriert werden, dass er eine direkte Verbindung zu Amazon Web Services (AWS) oder einem anderen System herstellt, das über die S3-API mit dem StorageGRID-System verbunden werden kann.

> Das Verschieben von Objekten vom Archiv-Node auf ein externes Archiv-Storage-System über die S3-API wurde durch ILM Cloud Storage-Pools ersetzt, die mehr Funktionen bieten. Die **Cloud Tiering - Simple Storage Service (S3)** Option wird weiterhin unterstützt, aber Sie könnten stattdessen Cloud Storage Pools implementieren.

Wenn Sie derzeit einen Archiv-Node mit der Option **Cloud Tiering - Simple Storage Service (S3)** verwenden, sollten Sie Ihre Objekte in einen Cloud-Storage-Pool migrieren. Siehe Anweisungen für Objektmanagement mit ILM.

Konfigurieren Sie die Verbindungseinstellungen für die S3-API

Wenn Sie über die S3-Schnittstelle eine Verbindung zu einem Archiv-Node herstellen, müssen Sie die Verbindungseinstellungen für die S3-API konfigurieren. Bis diese Einstellungen konfiguriert sind, bleibt der ARC-Dienst in einem wichtigen Alarmzustand, da er nicht mit dem externen Archivspeichersystem kommunizieren kann.

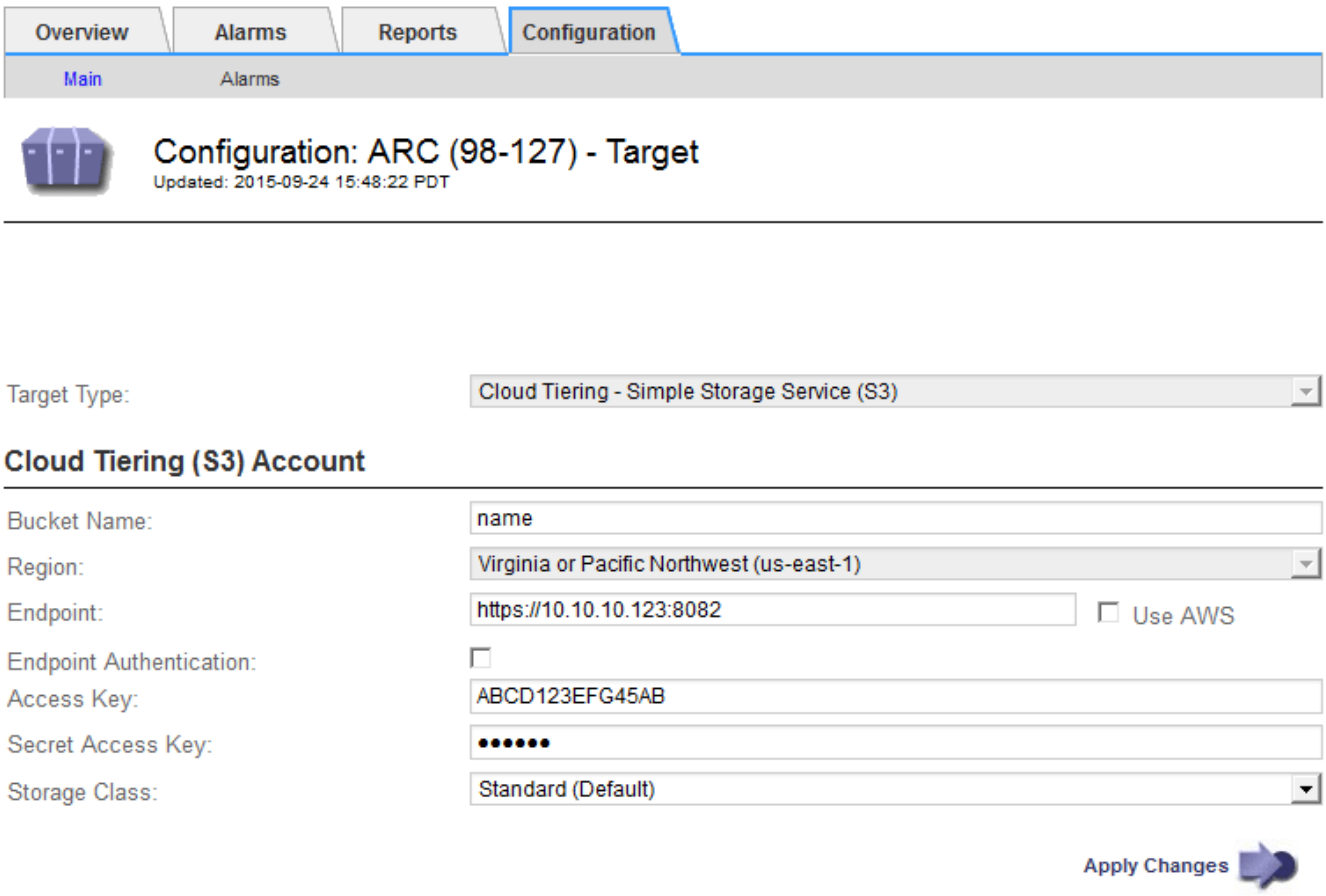
> Das Verschieben von Objekten vom Archiv-Node auf ein externes Archiv-Storage-System über die S3-API wurde durch ILM Cloud Storage-Pools ersetzt, die mehr Funktionen bieten. Die **Cloud Tiering - Simple Storage Service (S3)** Option wird weiterhin unterstützt, aber Sie könnten stattdessen Cloud Storage Pools implementieren.
>
> Wenn Sie derzeit einen Archiv-Node mit der Option **Cloud Tiering - Simple Storage Service (S3)** verwenden, sollten Sie Ihre Objekte in einen Cloud-Storage-Pool migrieren. Siehe Objektmanagement mit ILM.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben auf dem Ziel-Archiv-Storage-System einen Bucket erstellt:
  - Der Bucket ist einem einzelnen Archiv-Node zugewiesen. Sie kann nicht von anderen Archiv-Nodes oder anderen Anwendungen verwendet werden.
  - Der Bucket hat die für Ihren Standort ausgewählte Region.
  - Der Bucket sollte mit der Versionierung als ausgesetzt konfiguriert werden.
- Objektsegmentierung ist aktiviert, und die maximale Segmentgröße beträgt weniger als oder gleich 4.5 gib (4,831,838,208 Byte). S3-API-Anfragen, die diesen Wert überschreiten, schlagen fehl, wenn S3 als externes Archiv-Storage-System verwendet wird.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie **Archivknoten** > **ARC** > **Ziel**.
3. Wählen Sie **Konfiguration Main**.



4. Wählen Sie in der Dropdown-Liste Zieltyp * Cloud Tiering - Simple Storage Service (S3)* aus.

   Konfigurationseinstellungen sind erst verfügbar, wenn Sie einen Zieltyp auswählen.

5. Konfigurieren Sie das Cloud-Tiering-Konto (S3), über das der Archive-Node eine Verbindung zum externen S3-fähigen Archiv-Storage-System herstellen soll.

   Die meisten Felder auf dieser Seite sind selbsterklärend. Im folgenden werden die Felder beschrieben, für die Sie möglicherweise Hinweise benötigen.

   - **Region**: Nur verfügbar, wenn **AWS verwenden** ausgewählt ist. Die ausgewählte Region muss mit der Region des Buckets übereinstimmen.
   - **Endpunkt** und **AWS verwenden**: Für Amazon Web Services (AWS) wählen Sie **AWS verwenden**. **Endpunkt** wird dann automatisch mit einer Endpunkt-URL auf der Grundlage der Attribute Bucket-Name und Region ausgefüllt. Beispiel:

     ```
     https://bucket.region.amazonaws.com
     ```

     Geben Sie bei einem nicht von AWS stammenden Ziel die URL des Systems ein, das den Bucket hostet, einschließlich der Portnummer. Beispiel:

```
https://system.com:1080
```

   - **Endpunktauthentifizierung**: Standardmäßig aktiviert. Wenn das Netzwerk dem externen Archivspeichersystem vertraut ist, können Sie das Kontrollkästchen deaktivieren, um das SSL-Zertifikat und die hostname-Überprüfung des Zielsystems für die externe Archivierung zu deaktivieren. Wenn eine andere Instanz eines StorageGRID-Systems das Zielspeichergerät für die Archivierung ist und

das System mit öffentlich signierten Zertifikaten konfiguriert ist, können Sie das Kontrollkästchen aktivieren.

- **Speicherklasse**: Wählen Sie **Standard (Standard)** für die normale Lagerung. Wählen Sie **reduzierte Redundanz** nur für Objekte, die einfach neu erstellt werden können. **Reduzierte Redundanz** bietet kostengünstige Speicherung mit weniger Zuverlässigkeit. Wenn das zielgerichtete Archivspeichersystem eine weitere Instanz des StorageGRID-Systems ist, steuert **Speicherklasse**, wie viele Zwischenkopien des Objekts bei der Aufnahme auf das Zielsystem erstellt werden, wenn bei Aufnahme von Objekten Dual Commit verwendet wird.

6. Wählen Sie **Änderungen Anwenden**.

   Die angegebenen Konfigurationseinstellungen werden validiert und auf Ihr StorageGRID System angewendet. Nach der Konfiguration kann das Ziel nicht mehr geändert werden.

Ändern der Verbindungseinstellungen für die S3-API

Nachdem der Archivknoten über die S3 API für die Verbindung zu einem externen Archiv-Storage-System konfiguriert wurde, können Sie einige Einstellungen ändern, wenn sich die Verbindung ändert.

Was Sie benötigen

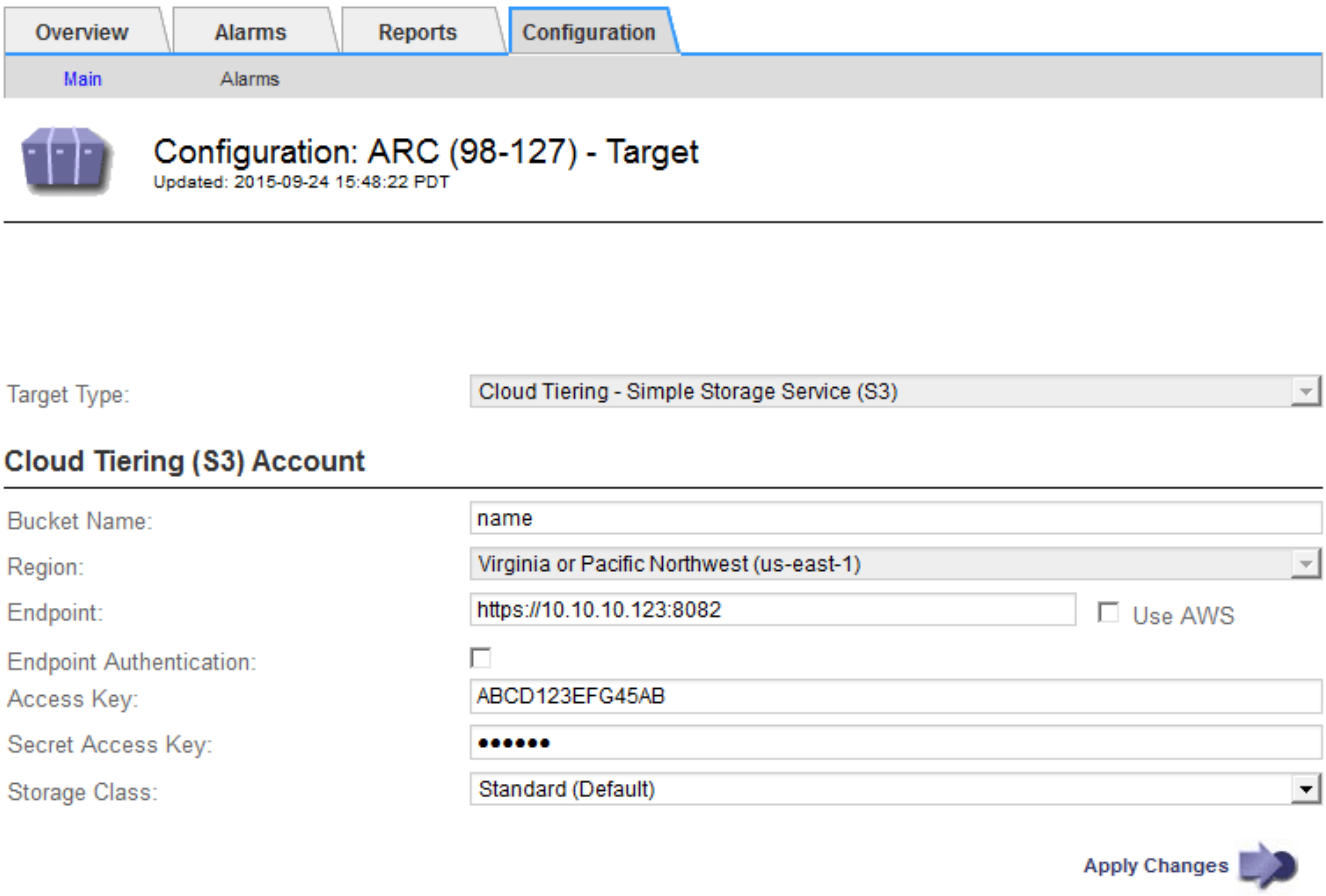
- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Wenn Sie das Cloud Tiering (S3) Konto ändern, müssen Sie sicherstellen, dass die Anmeldedaten für Benutzerzugriff auch auf den Bucket Lese-/Schreibzugriff haben, einschließlich aller Objekte, die zuvor vom Archiv-Node in den Bucket aufgenommen wurden.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***Archivknoten*** **ARC Ziel** aus.
3. Wählen Sie **Konfiguration Main**.



4. Ändern Sie ggf. die Kontoinformationen.

   Wenn Sie die Storage-Klasse ändern, werden neue Objektdaten mit der neuen Storage-Klasse gespeichert. Vorhandene Objekte werden bei der Aufnahme weiterhin unter dem Storage-Klassensatz gespeichert.

   Bucket-Name, -Region und -Endpunkt verwenden AWS-Werte und können nicht geändert werden.

5. Wählen Sie **Änderungen Anwenden**.

Ändern Sie den Status des Cloud Tiering Service

Sie können die Lese- und Schreibvorgänge des Archiv-Nodes auf das externe Archiv-Storage-System steuern, das über die S3 API verbunden ist, indem Sie den Status des Cloud Tiering Service ändern.

Was Sie benötigen

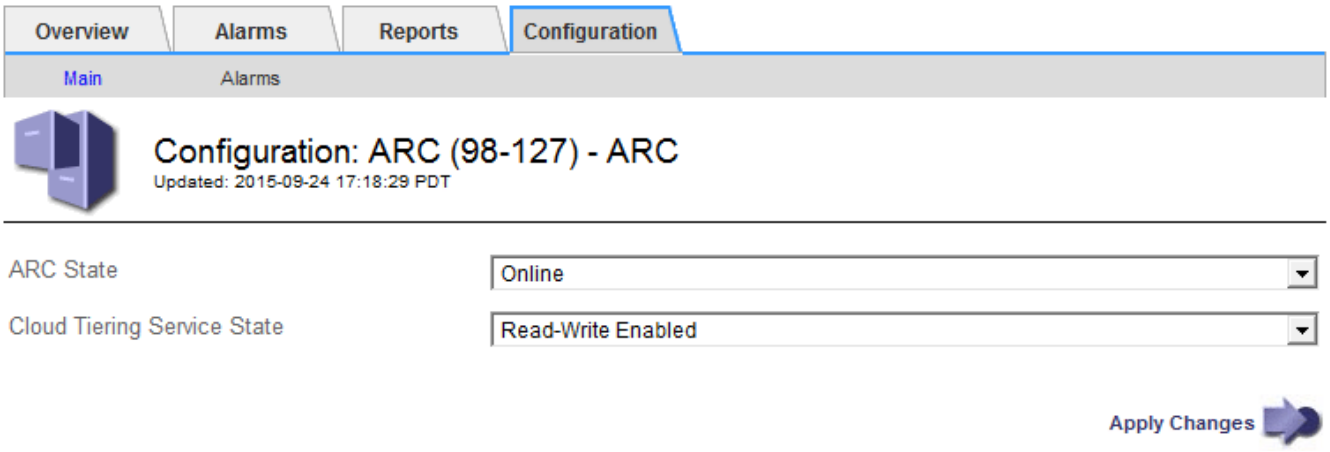
- Sie müssen mit einem beim Grid Manager angemeldet sein Unterstützter Webbrowser.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Der Archivknoten muss konfiguriert sein.

Über diese Aufgabe

Sie können den Archiv-Knoten effektiv offline setzen, indem Sie den Cloud-Tiering-Servicenstatus in **Lesen-Schreiben deaktiviert** ändern.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***Archivknoten*** **ARC** aus.
3. Wählen Sie **Konfiguration Main**.



4. Wählen Sie einen **Cloud Tiering Service-Status** aus.
5. Wählen Sie **Änderungen Anwenden**.

Zurücksetzen der Speicherfehler-Anzahl für S3-API-Verbindung

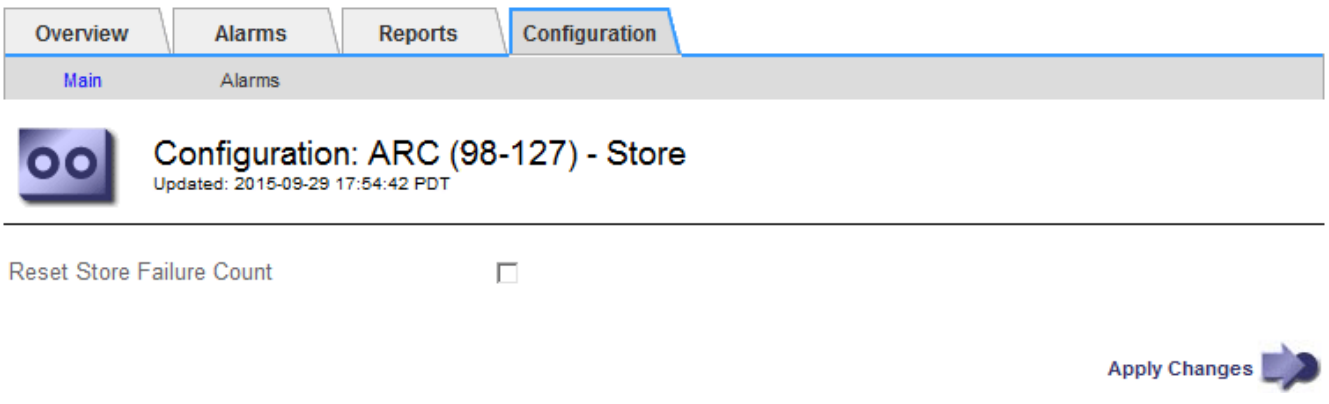
Wenn Ihr Archiv-Node über die S3-API eine Verbindung zu einem Archivspeichersystem herstellt, können Sie die Anzahl der Speicherfehler zurücksetzen, die zum Löschen des ARVF-Alarms (Store Failures) verwendet werden kann.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***Archivknoten*** **ARC Store** aus.
3. Wählen Sie **Konfiguration Main**.



4. Wählen Sie **Anzahl Der Fehler Im Store Zurücksetzen** Aus.

5. Wählen Sie **Änderungen Anwenden**.

   Das Attribut Fehler speichern wird auf Null zurückgesetzt.

Migrieren Sie Objekte von Cloud Tiering – S3 zu einem Cloud-Storage-Pool

Wenn Sie derzeit die Funktion **Cloud Tiering - Simple Storage Service (S3)** verwenden, um Objektdaten auf einen S3-Bucket zu verschieben, sollten Sie stattdessen Ihre Objekte in einen Cloud-Storage-Pool migrieren. Cloud Storage Pools bieten einen skalierbaren Ansatz, der alle Storage-Nodes in Ihrem StorageGRID System nutzt.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben bereits Objekte im S3-Bucket gespeichert, der für Cloud Tiering konfiguriert ist.

> Vor der Migration von Objektdaten sollten Sie den NetApp Ansprechpartner kontaktieren, um die damit verbundenen Kosten zu verstehen und zu managen.

Über diese Aufgabe

Aus einer ILM-Perspektive ähnelt ein Cloud-Storage-Pool einem Storage-Pool. Während Storage-Pools jedoch aus Storage-Nodes oder Archiv-Nodes innerhalb des StorageGRID Systems bestehen, besteht ein Cloud Storage-Pool aus einem externen S3-Bucket.

Vor der Migration von Objekten aus Cloud Tiering – S3 zu einem Cloud-Storage-Pool müssen Sie zuerst einen S3-Bucket erstellen und dann den Cloud-Storage-Pool in StorageGRID erstellen. Dann können Sie eine neue ILM-Richtlinie erstellen und die ILM-Regel ersetzen, die zum Speichern von Objekten im Cloud Tiering Bucket verwendet wird, durch eine geklonte ILM-Regel, die dieselben Objekte im Cloud-Storage-Pool speichert.

> Wenn Objekte in einem Cloud-Storage-Pool gespeichert werden, können im StorageGRID keine Kopien dieser Objekte gespeichert werden. Wenn die ILM-Regel, die Sie derzeit für Cloud Tiering verwenden, so konfiguriert ist, um Objekte an mehreren Standorten gleichzeitig zu speichern, sollten Sie bedenken, ob Sie diese optionale Migration dennoch durchführen möchten, da diese Funktion verloren geht. Wenn Sie mit dieser Migration fortfahren, müssen Sie neue Regeln erstellen, anstatt die vorhandenen zu klonen.

Schritte

1. Erstellen Sie einen Cloud-Storage-Pool.

   Verwenden Sie einen neuen S3-Bucket für den Cloud-Storage-Pool, um sicherzustellen, dass er nur die Daten enthält, die vom Cloud-Storage-Pool gemanagt werden.

2. Suchen Sie alle ILM-Regeln der aktiven ILM-Richtlinie, die dazu führen, dass Objekte im Cloud Tiering Bucket gespeichert werden.
3. Jede dieser Regeln klonen.
4. Ändern Sie in den geklonten Regeln den Speicherort in den neuen Cloud-Storage-Pool.
5. Speichern Sie die geklonten Regeln.
6. Erstellen Sie eine neue Richtlinie, die die neuen Regeln verwendet.

7. Simulieren und aktivieren Sie die neue Richtlinie.

   Wenn die neue Richtlinie aktiviert ist und eine ILM-Bewertung erfolgt, werden die Objekte vom für Cloud Tiering konfigurierten S3-Bucket in den für den Cloud-Storage-Pool konfigurierten S3-Bucket verschoben. Der nutzbare Speicherplatz im Raster ist nicht betroffen. Nachdem die Objekte in den Cloud Storage Pool verschoben wurden, werden sie aus dem Cloud Tiering Bucket entfernt.

Verwandte Informationen

Objektmanagement mit ILM

Archivierung auf Band über TSM Middleware

Sie können einen Archiv-Node so konfigurieren, dass er als Ziel für einen Tivoli Storage Manager (TSM)-Server dient, der eine logische Schnittstelle zum Speichern und Abrufen von Objektdaten an Random- oder Sequential-Access-Speichergeräten, einschließlich Tape Libraries, bereitstellt.

Der ARC-Service des Archivknotens fungiert als Client zum TSM-Server und verwendet Tivoli Storage Manager als Middleware zur Kommunikation mit dem Archivspeichersystem.

TSM Management-Klassen

Durch die TSM Middleware definierte Managementklassen beschreiben, wie die TSM's Backup- und Archivierungsvorgänge funktionieren und können verwendet werden, um Regeln für Inhalte festzulegen, die vom TSM-Server angewendet werden. Diese Regeln laufen unabhängig von der ILM-Richtlinie des StorageGRID Systems und müssen im Einklang mit der Anforderung des StorageGRID Systems stehen, dass Objekte dauerhaft gespeichert und für den Abruf durch den Archivierungs-Node immer verfügbar sind. Nachdem die Objektdaten vom Archiv-Node an einen TSM-Server gesendet wurden, werden die Regeln für den TSM Lebenszyklus und die Aufbewahrung angewendet, während die Objektdaten auf dem vom TSM-Server verwalteten Band gespeichert werden.

Die TSM-Managementklasse wird vom TSM-Server verwendet, um Regeln für den Datenspeicherort oder die Aufbewahrung anzuwenden, nachdem Objekte vom Archiv-Node an den TSM-Server gesendet wurden. So können beispielsweise als Datenbank-Backups identifizierte Objekte (temporärer Content, der mit neueren Daten überschrieben werden kann) anders behandelt werden als Applikationsdaten (unveränderlicher Inhalt, der unendlich lange aufbewahrt werden muss).

Konfigurieren Sie Verbindungen zur TSM Middleware

Bevor der Archivknoten mit der Tivoli Storage Manager (TSM) Middleware kommunizieren kann, müssen Sie eine Reihe von Einstellungen konfigurieren.

Was Sie benötigen

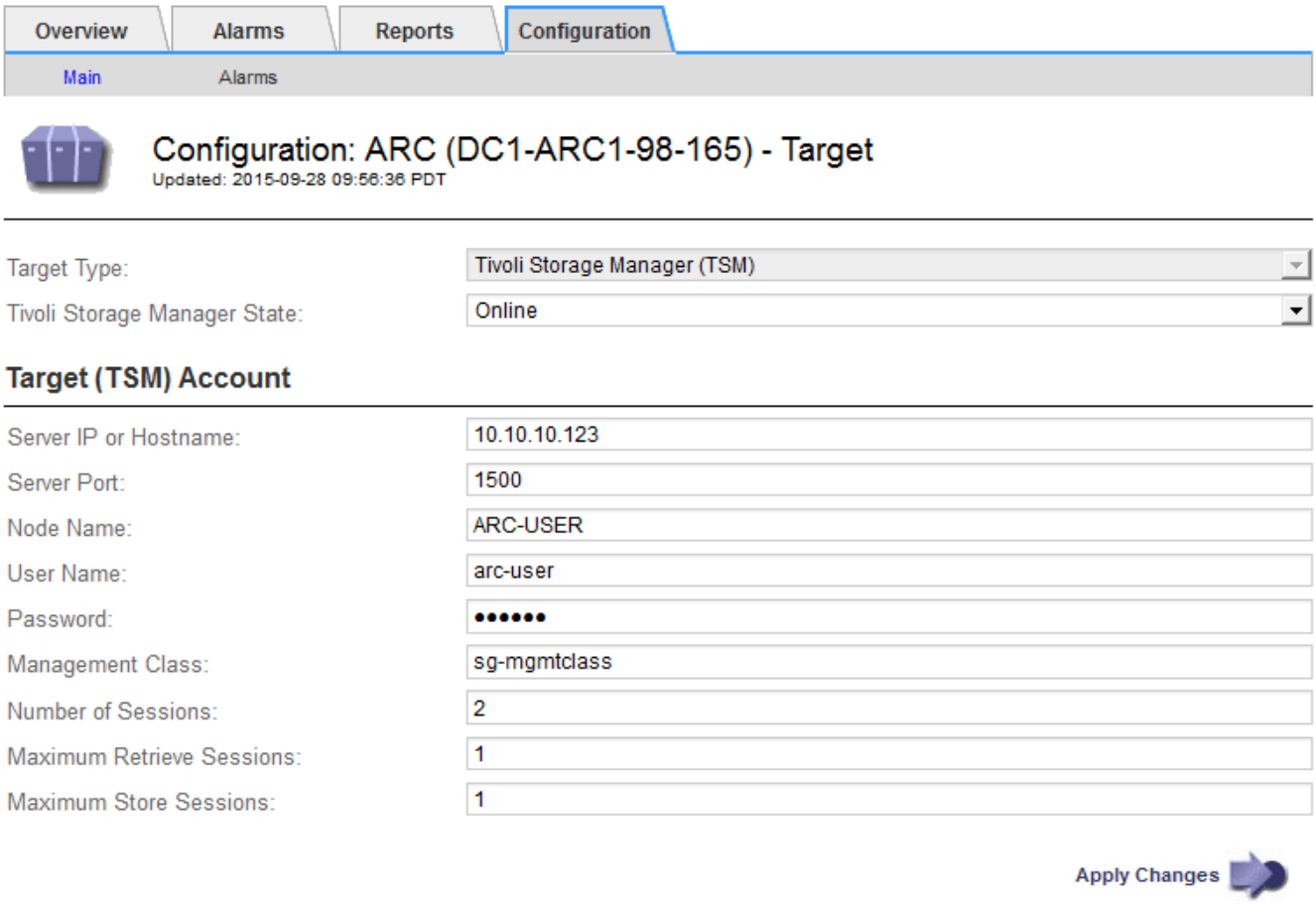
- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Bis diese Einstellungen konfiguriert sind, bleibt der ARC-Dienst in einem wichtigen Alarmzustand, da er nicht mit dem Tivoli Storage Manager kommunizieren kann.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***Archivknoten*** **ARC Ziel** aus.
3. Wählen Sie **Konfiguration Main**.



4. Wählen Sie aus der Dropdown-Liste **Zieltyp** die Option **Tivoli Storage Manager (TSM)** aus.
5. Wählen Sie für den **Tivoli Storage Manager State Offline** aus, um Rückrufe vom TSM Middleware-Server zu verhindern.

   Standardmäßig ist der Status von Tivoli Storage Manager auf Online eingestellt, was bedeutet, dass der Archive Node Objektdaten vom TSM Middleware-Server abrufen kann.

6. Geben Sie die folgenden Informationen an:

   - **Server IP oder Hostname**: Geben Sie die IP-Adresse oder den vollqualifizierten Domänennamen des TSM Middleware-Servers an, der vom ARC-Dienst verwendet wird. Die Standard-IP-Adresse ist 127.0.0.1.
   - **Server-Port**: Geben Sie die Portnummer auf dem TSM Middleware-Server an, mit dem der ARC-Dienst eine Verbindung herstellen wird. Der Standardwert ist 1500.
   - **Knotenname**: Geben Sie den Namen des Archiv-Knotens an. Sie müssen den Namen (Arc-user) eingeben, den Sie auf dem TSM Middleware-Server registriert haben.
   - **Benutzername**: Geben Sie den Benutzernamen an, den der ARC-Dienst zur Anmeldung am TSM-Server verwendet. Geben Sie den Standardbenutzernamen (Arc-user) oder den administrativen Benutzer ein, den Sie für den Archiv-Node angegeben haben.
   - **Passwort**: Geben Sie das Passwort an, das der ARC-Dienst zur Anmeldung am TSM-Server

verwendet.

- **Managementklasse**: Geben Sie die Standardverwaltungsklasse an, die verwendet werden soll, wenn beim Speichern des Objekts auf dem StorageGRID-System keine Managementklasse angegeben ist oder die angegebene Managementklasse nicht auf dem TSM Middleware-Server definiert ist.
- **Anzahl der Sitzungen**: Geben Sie die Anzahl der Bandlaufwerke auf dem TSM Middleware-Server an, die dem Archiv-Knoten gewidmet sind. Der Archivknoten erstellt gleichzeitig maximal eine Sitzung pro Bereitstellungspunkt plus eine kleine Anzahl zusätzlicher Sitzungen (weniger als fünf).

  Sie müssen diesen Wert ändern, um den für MAXNUMMP festgelegten Wert (maximale Anzahl von Mount-Punkten) zu erhalten, wenn der Archivknoten registriert oder aktualisiert wurde. (Im Register-Befehl ist der Standardwert von MAXNUMMP verwendet 1, wenn kein Wert festgelegt ist.)

Außerdem müssen Sie den Wert von MAXSESSIONS für den TSM-Server auf eine Zahl ändern, die mindestens so groß ist wie die Anzahl der Sitzungen, die für den ARC-Dienst festgelegt wurden. Der Standardwert von MAXSESSIONS auf dem TSM-Server ist 25.

- **Maximum Retrieve Sessions**: Geben Sie die maximale Anzahl von Sitzungen an, die der ARC-Dienst für den TSM Middleware-Server für Abrufvorgänge öffnen kann. In den meisten Fällen ist der entsprechende Wert die Anzahl der Sitzungen abzüglich der maximalen Speichersitzungen. Wenn Sie ein Bandlaufwerk für die Speicherung und den Abruf freigeben möchten, geben Sie einen Wert an, der der Anzahl der Sitzungen entspricht.
- **Maximum Store Sessions**: Geben Sie die maximale Anzahl gleichzeitiger Sitzungen an, die der ARC-Dienst für den TSM Middleware-Server für Archivierungsvorgänge öffnen kann.

  Dieser Wert sollte auf eins gesetzt werden, außer wenn das gezielte Archivspeichersystem voll ist und nur Abrufvorgänge durchgeführt werden können. Setzen Sie diesen Wert auf Null, um alle Sitzungen für Abrufvorgänge zu verwenden.

7. Wählen Sie **Änderungen Anwenden**.

Optimieren Sie einen Archiv-Node für TSM Middleware-Sitzungen

Sie können die Performance eines Archivierungs-Knotens, der sich mit Tivoli Server Manager (TSM) verbindet, optimieren, indem Sie die Sitzungen des Archivierungs-Nodes konfigurieren.

Was Sie benötigen

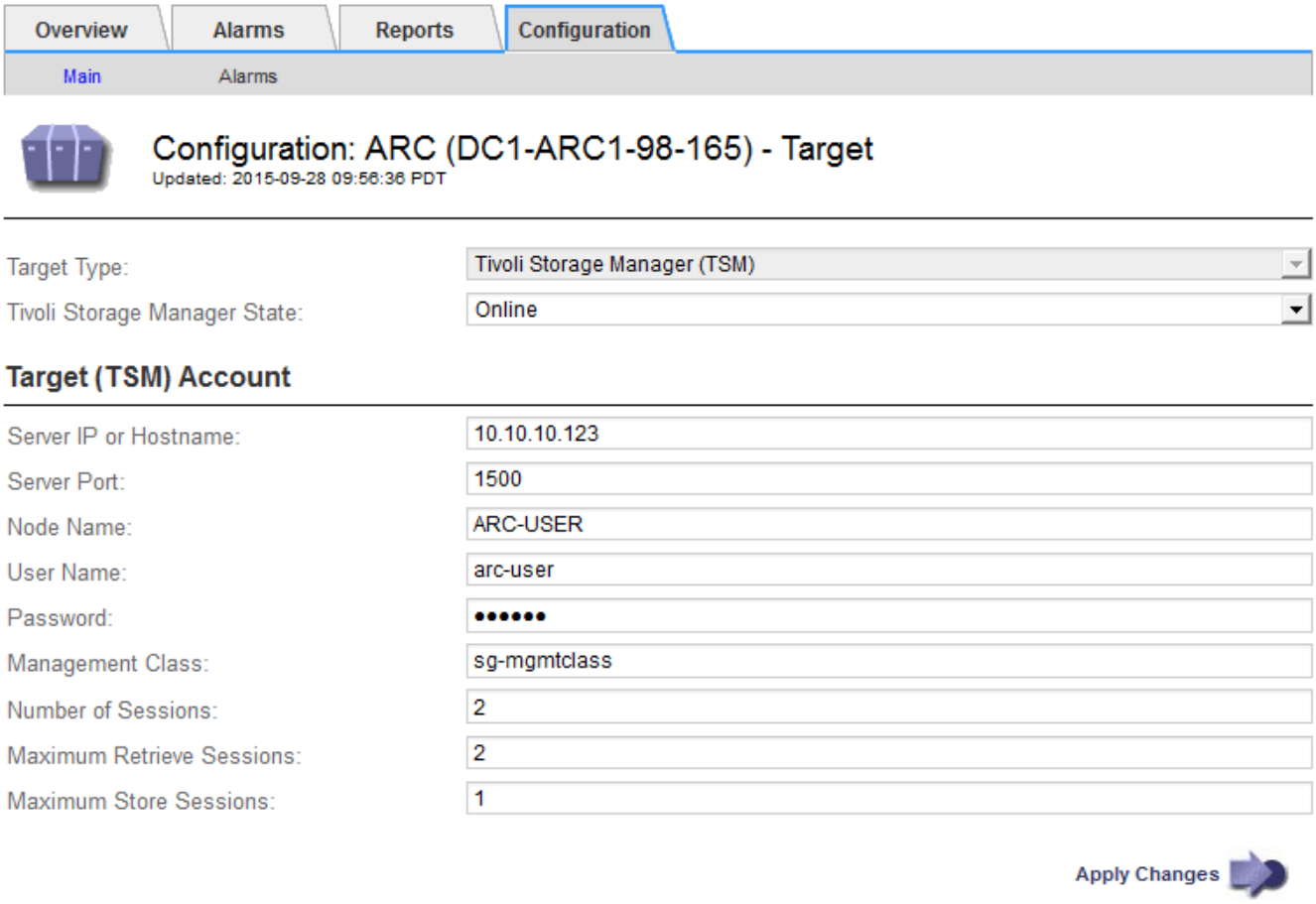
- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

In der Regel ist die Anzahl der gleichzeitigen Sitzungen, die der Archivknoten für den TSM Middleware-Server offen hat, auf die Anzahl der Bandlaufwerke eingestellt, die der TSM-Server dem Archiv-Node zugewiesen hat. Ein Bandlaufwerk wird für den Speicher zugewiesen, während der Rest für den Abruf zugewiesen wird. Wenn jedoch ein Speicherknoten aus Archive Node Kopien neu aufgebaut wird oder der Archivknoten im schreibgeschützten Modus arbeitet, können Sie die TSM-Serverleistung optimieren, indem Sie die maximale Anzahl der Abrufsitzungen so einstellen, dass sie mit der Anzahl der gleichzeitigen Sitzungen identisch sind. Das Ergebnis ist, dass alle Laufwerke gleichzeitig für den Abruf genutzt werden können. Höchstens kann eines dieser Laufwerke zur Lagerung verwendet werden.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***Archivknoten*** **ARC Ziel** aus.
3. Wählen Sie **Konfiguration Main**.
4. Ändern Sie **Maximum Retrieve Sessions** als **Anzahl der Sitzungen**.



5. Wählen Sie **Änderungen Anwenden**.

Konfigurieren Sie den Archivierungsstatus und die Zähler für TSM

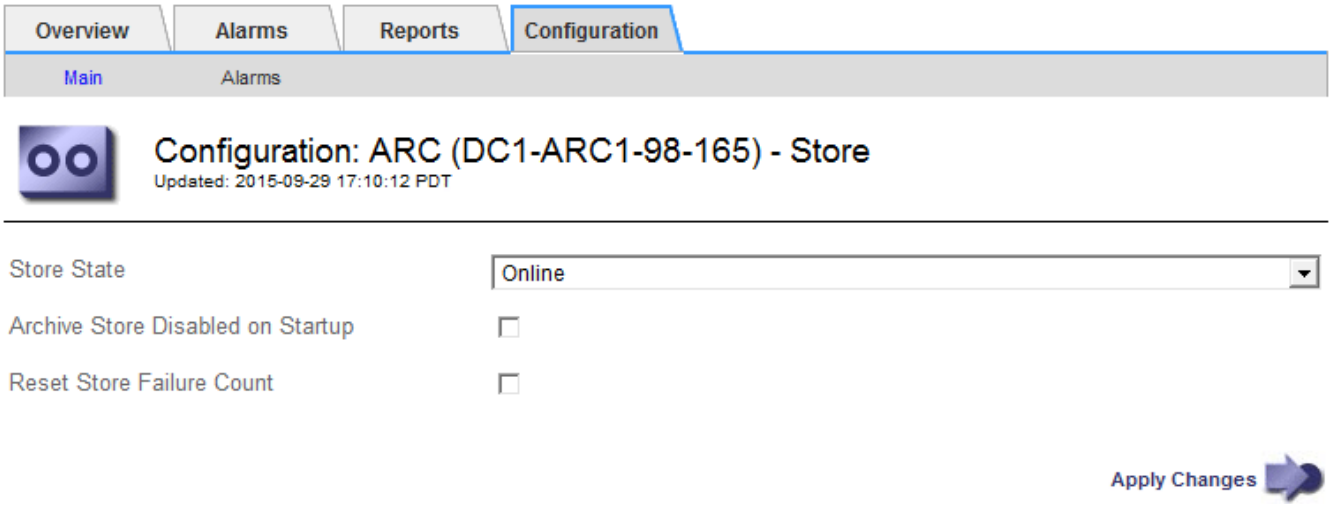
Wenn der Archivknoten eine Verbindung zu einem TSM Middleware-Server herstellt, können Sie den Status des Archivspeichers eines Archiv-Knotens in Online oder Offline konfigurieren. Sie können den Archivspeicher auch deaktivieren, wenn der Archivknoten zum ersten Mal gestartet wird, oder die Fehleranzahl, die für den zugehörigen Alarm nachverfolgt wird, zurücksetzen.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***Archivknoten*** **ARC Store** aus.
3. Wählen Sie **Konfiguration Main**.



4. Ändern Sie bei Bedarf die folgenden Einstellungen:
   - Speicherstatus: Legen Sie den Komponentenstatus auf entweder:
     - Online: Der Archiv-Node ist zur Verarbeitung von Objektdaten zum Speichern im Archiv-Storage-System verfügbar.
     - Offline: Der Archiv-Node ist nicht verfügbar, um Objektdaten zum Speichern im Archiv-Storage-System zu verarbeiten.
   - Archivspeicher beim Start deaktiviert: Wenn diese Option ausgewählt ist, bleibt die Komponente Archivspeicher beim Neustart im schreibgeschützten Zustand. Wird verwendet, um Speicher dauerhaft für das Zielspeichersystem zu deaktivieren. Nützlich, wenn das ausgewählte Archivspeichersystem keine Inhalte akzeptieren kann.
   - Reset Store Failure Count: Setzt den Zähler für Store Failures zurück. Dies kann verwendet werden, um den ARVF-Alarm (Stores Failure) zu löschen.
5. Wählen Sie **Änderungen Anwenden**.

Verwandte Informationen

Verwalten Sie einen Archiv-Node, wenn der TSM-Server die Kapazität erreicht

Verwalten Sie einen Archiv-Node, wenn der TSM-Server die Kapazität erreicht

Der TSM-Server hat keine Möglichkeit, den Archiv-Node zu benachrichtigen, wenn sich die Kapazität der TSM-Datenbank oder des vom TSM-Server verwalteten Archivmedienspeichers befindet. Dies kann durch proaktive Überwachung des TSM-Servers vermieden werden.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Der Archivknoten akzeptiert weiterhin Objektdaten für die Übertragung an den TSM-Server, nachdem der TSM-Server keine neuen Inhalte mehr akzeptiert. Dieser Inhalt kann nicht auf Medien geschrieben werden, die vom TSM-Server verwaltet werden. In diesem Fall wird ein Alarm ausgelöst.

Verhindern, dass der ARC-Dienst Inhalte an den TSM-Server sendet

Um zu verhindern, dass der ARC-Service weitere Inhalte an den TSM-Server sendet, können Sie den Archiv-Node offline schalten, indem Sie die **ARC Store**-Komponente offline schalten. Dieses Verfahren kann auch nützlich sein, um Alarme zu vermeiden, wenn der TSM-Server nicht zur Wartung verfügbar ist.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***Archivknoten* ARC Store** aus.
3. Wählen Sie **Konfiguration Main**.

4. Ändern Sie **Store State** in `Offline`.
5. Wählen Sie * Archivspeicher beim Start deaktiviert* aus.
6. Wählen Sie **Änderungen Anwenden**.

Stellen Sie Archive Node auf „Read-Only“ ein, wenn die TSM Middleware die Kapazität erreicht

Wenn der angestrebte TSM Middleware-Server seine Kapazität erreicht, kann der Archivknoten optimiert werden, um nur die Abrufvorgänge durchzuführen.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***Archivknoten* ARC Ziel** aus.
3. Wählen Sie **Konfiguration Main**.
4. Ändern Sie die maximale Anzahl der Abruf-Sitzungen auf dieselbe Weise wie die Anzahl der gleichzeitigen Sitzungen, die in der Anzahl der Sitzungen aufgeführt sind.
5. Ändern Sie die maximale Anzahl von Sitzungen im Store auf 0.

> Das Ändern der maximalen Speichersitzungen auf 0 ist nicht erforderlich, wenn der Archivknoten schreibgeschützt ist. Speichersitzungen werden nicht erstellt.

6. Wählen Sie **Änderungen Anwenden**.

Konfigurieren Sie die Einstellungen für den Abruf von Archivknoten

Sie können die Einstellungen für den Abruf eines Archiv-Knotens so konfigurieren, dass

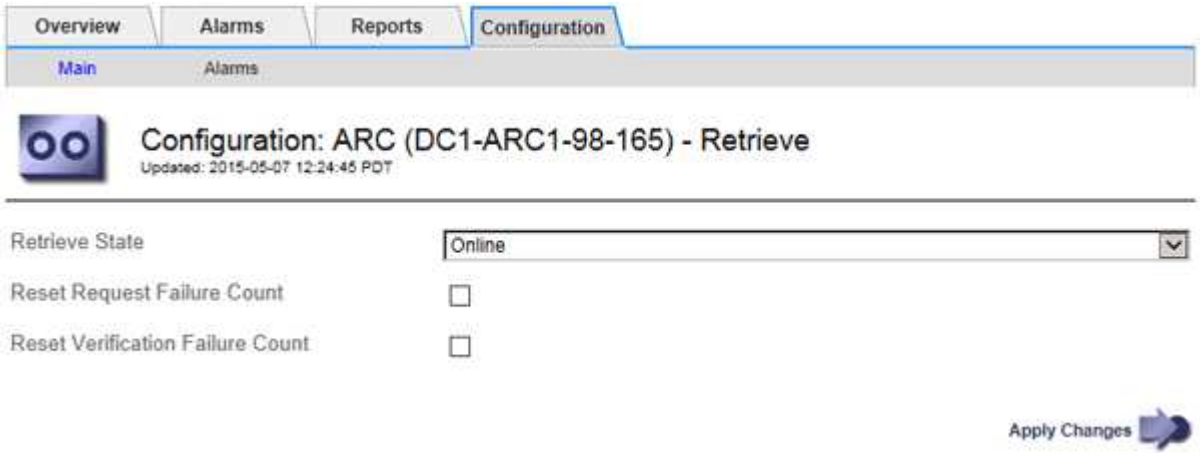
der Status auf Online oder Offline gesetzt wird, oder die Fehleranzahl, die für die zugehörigen Alarme nachverfolgt wird, zurücksetzen.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie **Archivknoten ARC Abruf**.
3. Wählen Sie **Konfiguration Main**.



4. Ändern Sie bei Bedarf die folgenden Einstellungen:
   - **Retrieve Status**: Den Komponentenzustand auf entweder einstellen:
     - Online: Der Grid-Node ist verfügbar, um Objektdaten vom Archivierungsmedium abzurufen.
     - Offline: Der Grid-Node ist zum Abrufen von Objektdaten nicht verfügbar.
   - Reset Request Failures Count: Aktivieren Sie das Kontrollkästchen, um den Zähler für Anforderungsfehler zurückzusetzen. Dieser kann verwendet werden, um den ARRF-Alarm (Request Failures) zu löschen.
   - Zurücksetzen Fehleranzahl der Überprüfung: Aktivieren Sie das Kontrollkästchen, um den Zähler auf Überprüfungsfehler bei abgerufenen Objektdaten zurückzusetzen. Dies kann verwendet werden, um den ARRV-Alarm (Verifizierungsfehler) zu löschen.
5. Wählen Sie **Änderungen Anwenden**.

Konfigurieren Sie die Replikation des Archivierungs-Knotens

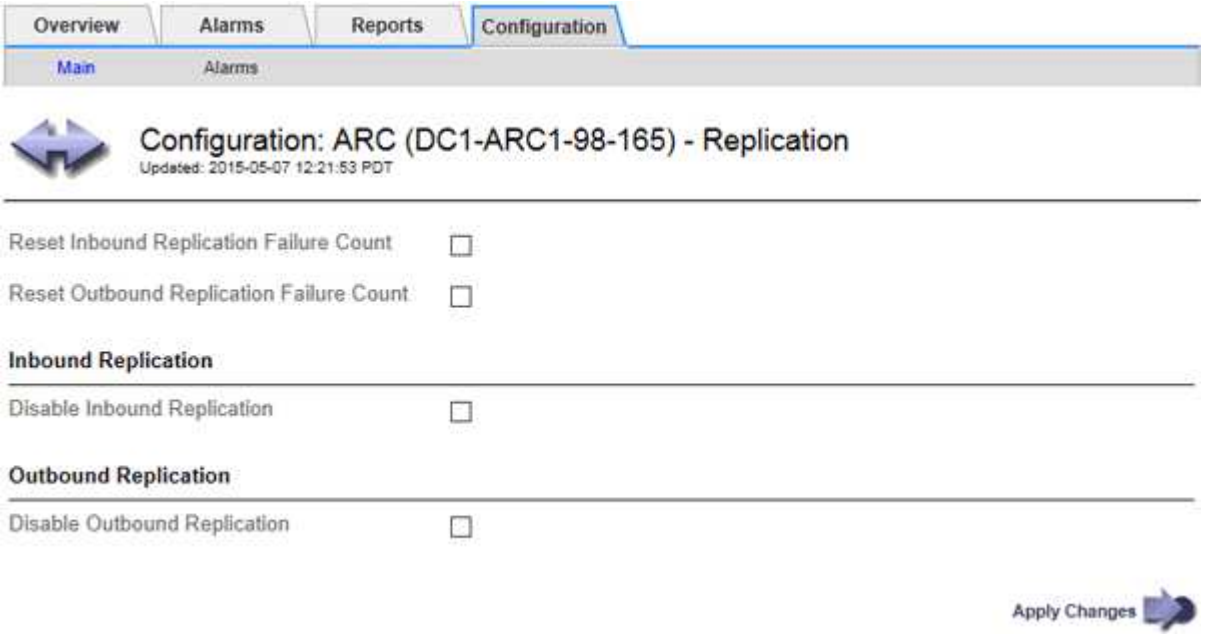
Sie können die Replikationseinstellungen für einen Archivknoten konfigurieren und die ein- und ausgehende Replikation deaktivieren oder die für die zugehörigen Alarme zu protokollierenden Fehlerzählungen zurücksetzen.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***Archivknoten*** **ARC Replikation** aus.
3. Wählen Sie **Konfiguration Main**.



4. Ändern Sie bei Bedarf die folgenden Einstellungen:
   - **Fehleranzahl Inbound Replication zurücksetzen**: Wählen Sie, um den Zähler für eingehende Replikationsfehler zurückzusetzen. Dies kann verwendet werden, um den RIRF-Alarm (eingehende Replikationen — fehlgeschlagen) zu löschen.
   - **Fehleranzahl bei ausgehenden Replikationsfehlern zurücksetzen**: Wählen Sie, um den Zähler für ausgehende Replikationsfehler zurückzusetzen. Dies kann verwendet werden, um den RORF-Alarm (ausgehende Replikationen — fehlgeschlagen) zu löschen.
   - **Inbound Replication** deaktivieren: Wählen Sie aus, um die eingehende Replikation im Rahmen eines Wartungs- oder Testverfahrens zu deaktivieren. Während des normalen Betriebs löschen lassen.

     Wenn die eingehende Replikation deaktiviert ist, können Objektdaten vom ARC-Dienst zur Replikation an andere Standorte im StorageGRID-System abgerufen werden. Objekte können jedoch von anderen Systemstandorten nicht zu diesem ARC-Dienst repliziert werden. Der ARC-Dienst wird-only gelesen.

   - **Ausgehende Replikation deaktivieren**: Aktivieren Sie das Kontrollkästchen, um die ausgehende Replikation (einschließlich Inhaltsanforderungen für HTTP-Abruf) im Rahmen eines Wartungs- oder Testverfahrens zu deaktivieren. Während des normalen Betriebs nicht aktiviert lassen.

     Wenn die ausgehende Replikation deaktiviert ist, können Objektdaten in diesen ARC-Dienst kopiert werden, um ILM-Regeln zu erfüllen. Objektdaten können jedoch nicht vom ARC-Dienst abgerufen werden, um sie an andere Speicherorte im StorageGRID-System zu kopieren. Der ARC-Dienst ist nur schreiben-.

5. Wählen Sie **Änderungen Anwenden**.

Legen Sie benutzerdefinierte Alarme für den Knoten Archiv fest

Sie sollten benutzerdefinierte Alarme für die ARQL- und ARRL-Attribute einrichten, die zur Überwachung der Geschwindigkeit und Effizienz des Datenabrufs von Objektdaten vom Archivspeichersystem durch den Knoten Archiv verwendet werden.

- ARQL: Durchschnittliche Warteschlangenlänge. Die durchschnittliche Zeit in Mikrosekunden dieser Objektdaten wird zum Abruf aus dem Archivspeichersystem in die Warteschlange verschoben.
- ARRL: Durchschnittliche Anfragelatenz. Die durchschnittliche Zeit in Mikrosekunden, die der Archive-Node benötigt, um Objektdaten aus dem Archiv-Storage-System abzurufen.

Die akzeptablen Werte dieser Attribute hängen davon ab, wie das Archivspeichersystem konfiguriert und verwendet wird. (Weiter zu **ARC Retrieve Übersicht Main**.) Die Werte, die für die Timeouts von Anfragen festgelegt sind, und die Anzahl der Sitzungen, die für Abrufanfragen zur Verfügung gestellt werden, haben einen besonderen Einfluss.

Nach Abschluss der Integration überwachen Sie die Abfrage der Objektdaten des Archivknoten, um Werte für die normalen Abrufzeiten und Warteschlangenlänge zu ermitteln. Erstellen Sie dann benutzerdefinierte Alarme für ARQL und ARRL, die ausgelöst werden, wenn eine anormale Betriebsbedingung auftritt. Siehe Monitoring und Fehlerbehebung.

Integration Von Tivoli Storage Manager

Konfiguration und Betrieb des Archivierungs-Node

Ihr StorageGRID-System managt den Archiv-Node als Speicherort, an dem Objekte unendlich gespeichert werden und stets zugänglich sind.

Bei der Aufnahme eines Objekts werden auf Basis der für das StorageGRID System definierten Regeln für das Information Lifecycle Management Kopien an allen erforderlichen Speicherorten, einschließlich Archiv-Nodes, erstellt. Der Archivknoten fungiert als Client auf einem TSM-Server, und die TSM-Clientbibliotheken sind auf dem Archiv-Knoten durch den Installationsvorgang der StorageGRID-Software installiert. Objektdaten, die zum Archiv-Node für Speicher geleitet werden, werden beim Empfang direkt auf dem TSM-Server gespeichert. Der Archivknoten stellt keine Objektdaten vor dem Speichern auf dem TSM-Server dar und führt auch keine Objektaggregation durch. Der Archivknoten kann jedoch in einer einzigen Transaktion mehrere Kopien an den TSM-Server senden, wenn die Datenraten dies erfordern.

Nachdem der Archivknoten Objektdaten auf dem TSM-Server speichert, werden die Objektdaten unter Anwendung der Lifecycle-/Aufbewahrungsrichtlinien vom TSM-Server gemanagt. Diese Aufbewahrungsrichtlinien müssen definiert werden, damit sie mit dem Vorgang des Archivierungs-Nodes kompatibel sind. Das bedeutet, dass vom Archiv-Node gespeicherte Objektdaten unbegrenzt gespeichert werden müssen und vom Archiv-Node immer darauf zugegriffen werden muss, es sei denn, sie werden vom Archiv-Node gelöscht.

Es besteht keine Verbindung zwischen den ILM-Regeln des StorageGRID Systems und den Lifecycle-/Aufbewahrungsrichtlinien des TSM Servers. Jeder arbeitet unabhängig voneinander. Wenn jedoch jedes Objekt in das StorageGRID System aufgenommen wird, kann ihm eine TSM Management-Klasse zugewiesen werden. Diese Managementklasse wird gemeinsam mit Objektdaten an den TSM Server übergeben. Durch das Zuweisen verschiedener Managementklassen zu unterschiedlichen Objekttypen können Sie den TSM-Server so konfigurieren, dass Objektdaten in verschiedenen Storage-Pools gespeichert werden, oder unterschiedliche Migrations- oder Aufbewahrungsrichtlinien anwenden. Beispielsweise können als Datenbank-Backups identifizierte Objekte (temporärer Content als mit neueren Daten überschrieben werden kann) anders als Applikationsdaten behandelt werden (unveränderlicher Inhalt, der für unbegrenzte Zeit aufbewahrt werden

muss).

Der Archivknoten kann in einen neuen oder vorhandenen TSM-Server integriert werden; es ist kein dedizierter TSM-Server erforderlich. TSM-Server können mit anderen Clients gemeinsam genutzt werden, vorausgesetzt, der TSM-Server ist für die erwartete maximale Last angemessen dimensioniert. TSM muss auf einem vom Archiv-Node getrennten Server oder einer virtuellen Maschine installiert sein.

Es ist möglich, mehr als einen Archivknoten zu konfigurieren, um auf denselben TSM-Server zu schreiben; diese Konfiguration wird jedoch nur empfohlen, wenn die Archiv-Knoten unterschiedliche Datensätze auf den TSM-Server schreiben. Die Konfiguration von mehr als einem Archiv-Node zum Schreiben auf denselben TSM-Server wird nicht empfohlen, wenn jeder Archiv-Node Kopien derselben Objektdaten in das Archiv schreibt. Bei einem letzteren Szenario unterliegen beide Kopien einem Single Point of Failure (dem TSM-Server), da sie unabhängige, redundante Kopien von Objektdaten sind.

Archive Nodes nutzen die hierarchische Storage Management (HSM) Komponente von TSM nicht.

Best Practices für die Konfiguration

Wenn Sie den TSM-Server dimensionieren und konfigurieren, gibt es Best Practices, die Sie anwenden sollten, um ihn für die Arbeit mit dem Archiv-Knoten zu optimieren.

Bei der Dimensionierung und Konfiguration des TSM-Servers sollten folgende Faktoren berücksichtigt werden:

- Da der Archivknoten keine Objekte aggregiert, bevor sie auf dem TSM-Server gespeichert werden, muss die TSM-Datenbank so dimensioniert sein, dass sie Verweise auf alle Objekte enthält, die auf den Archiv-Node geschrieben werden.
- Die Archivierungs-Node-Software kann die Latenz beim Schreiben von Objekten direkt auf Tapes oder andere Wechseldatenträger nicht tolerieren. Daher muss der TSM-Server mit einem Festplatten-Speicherpool für den ursprünglichen Speicher der Daten konfiguriert werden, die vom Archiv-Node gespeichert werden, wenn Wechseldatenträger verwendet werden.
- Sie müssen TSM-Aufbewahrungsrichtlinien konfigurieren, um die ereignisbasierte Aufbewahrung zu verwenden-. Der Archivierungs-Node unterstützt keine auf der Erstellung basierenden TSM-Aufbewahrungsrichtlinien. Verwenden Sie in der Aufbewahrungsrichtlinie die folgenden empfohlenen Einstellungen von remin=0 und rever=0 (dies bedeutet, dass die Aufbewahrung beginnt, wenn der Archivknoten ein Archivierungsereignis auslöst und danach 0 Tage lang aufbewahrt wird). Diese Werte für Remin und Rever sind jedoch optional.

Der Laufwerk-Pool muss so konfiguriert sein, dass Daten in den Bandpool migriert werden (das heißt, der Bandpool muss NXTSTGPOOL des Laufwerk-Pools sein). Der Bandpool darf nicht als Copy-Pool des Disk-Pools konfiguriert werden, wobei gleichzeitig in beide Pools geschrieben wird (das heißt, der Bandpool kann kein COPYSTGPOL für den Laufwerk-Pool sein). Um Offline-Kopien der Bänder zu erstellen, die Daten von Archivierungs-Nodes enthalten, konfigurieren Sie den TSM-Server mit einem zweiten Bandpool, der ein Kopie-Pool des für Archiv-Node-Daten verwendeten Bandpools ist.

Schließen Sie die Konfiguration des Archivierungs-Knotens ab

Der Archivknoten funktioniert nicht, nachdem Sie den Installationsprozess abgeschlossen haben. Bevor das StorageGRID-System Objekte auf dem TSM-Archivknoten speichern kann, müssen Sie die Installation und Konfiguration des TSM-Servers abschließen und den Archivknoten für die Kommunikation mit dem TSM-Server konfigurieren.

Beachten Sie bei Bedarf die folgende IBM-Dokumentation, wenn Sie Ihren TSM-Server für die Integration mit dem Archiv-Node in einem StorageGRID-System vorbereiten:

- "IBM Bandgerätetreiber – Installations- und Benutzerhandbuch"
- "Programmierreferenz für IBM Bandgerätetreiber"

Installieren Sie einen neuen TSM-Server

Sie können den Archiv-Knoten entweder mit einem neuen oder einem vorhandenen TSM-Server integrieren. Wenn Sie einen neuen TSM-Server installieren, befolgen Sie die Anweisungen in der TSM-Dokumentation, um die Installation abzuschließen.

Ein Archivknoten kann nicht mit einem TSM-Server Co-gehostet werden.

Konfigurieren Sie den TSM-Server

Dieser Abschnitt enthält Beispielanweisungen zur Vorbereitung eines TSM-Servers gemäß den Best Practices von TSM.

Die folgenden Anweisungen führen Sie durch den Prozess von:

- Definieren eines Festplatten-Speicherpools und eines Bandspeicherpools (falls erforderlich) auf dem TSM-Server
- Definieren einer Domänenrichtlinie, die die TSM-Managementklasse für die Daten verwendet, die im Knoten Archiv gespeichert sind, und Registrieren eines Knotens für diese Domänenrichtlinie

Diese Anweisungen dienen nur zu Ihrer Orientierung. Sie dienen nicht als Ersatz für die TSM Dokumentation oder zur Bereitstellung der vollständigen und umfassenden Anweisungen für alle Konfigurationen. Eine Anleitung zur Implementierung sollte von einem TSM-Administrator bereitgestellt werden, der sowohl mit Ihren detaillierten Anforderungen als auch mit dem vollständigen Satz der TSM-Server-Dokumentation vertraut ist.

Definieren Sie TSM Tape- und Festplatten-Storage-Pools

Der Archivknoten schreibt in einen Festplatten-Speicherpool. Um Inhalte auf Band zu archivieren, müssen Sie den Festplatten-Speicherpool konfigurieren, um Inhalte in einen Bandspeicher-Pool zu verschieben.

Über diese Aufgabe

Bei einem TSM-Server müssen Sie einen Bandspeicher-Pool und einen Festplatten-Speicherpool in Tivoli Storage Manager definieren. Erstellen Sie nach Definition des Laufwerk-Pools ein Laufwerk-Volume und weisen Sie es dem Laufwerk-Pool zu. Ein Bandpool-nicht erforderlich, wenn Ihr TSM-Server nur Festplatten-Storage verwendet.

Sie müssen eine Reihe von Schritten auf Ihrem TSM-Server durchführen, bevor Sie einen Bandspeicher-Pool erstellen können. (Erstellen Sie eine Bandbibliothek und mindestens ein Laufwerk in der Bandbibliothek. Definieren Sie einen Pfad vom Server zur Bibliothek und vom Server zu den Laufwerken und definieren Sie dann eine Geräteklasse für die Laufwerke.) Die Details dieser Schritte können je nach Hardwarekonfiguration und Storage-Anforderungen des Standorts variieren. Weitere Informationen finden Sie in der TSM-Dokumentation.

Die folgenden Anweisungen veranschaulichen den Prozess. Sie sollten beachten, dass die Anforderungen an Ihren Standort je nach Bereitstellungsanforderungen unterschiedlich sein können. Weitere Informationen zur Konfiguration und zu Anweisungen finden Sie in der TSM-Dokumentation.

Sie müssen sich mit Administratorrechten auf dem Server anmelden und das dsmadmc-Tool verwenden, um die folgenden Befehle auszuführen.

Schritte

1. Erstellen einer Tape Library

   `define library tapelibrary libtype=scsi`

   Wo *tapelibrary* Ist ein willkürlicher Name, der für die Bandbibliothek und den Wert von ausgewählt wurde `libtype` Je nach Art der Tape Library kann es variieren.

2. Definieren Sie einen Pfad vom Server zur Bandbibliothek.

   `define path servername tapelibrary srctype=server desttype=library device=lib-devicename`

   - *servername* Ist der Name des TSM-Servers
   - *tapelibrary* Ist der von Ihnen definierte Bandbibliothek
   - *lib-devicename* Ist der Gerätename für die Bandbibliothek

3. Legen Sie ein Laufwerk für die Bibliothek fest.

   `define drive tapelibrary drivename`

   - *drivename* Ist der Name, den Sie für das Laufwerk angeben möchten
   - *tapelibrary* Ist der von Ihnen definierte Bandbibliothek

     Je nach Hardwarekonfiguration möchten Sie möglicherweise ein zusätzliches Laufwerk oder weitere Laufwerke konfigurieren. (Wenn beispielsweise der TSM-Server mit einem Fibre Channel-Switch verbunden ist, der über zwei Eingaben aus einer Bandbibliothek verfügt, sollten Sie für jede Eingabe möglicherweise ein Laufwerk definieren.)

4. Definieren Sie einen Pfad vom Server zum Laufwerk, das Sie definiert haben.

   `define path servername drivename srctype=server desttype=drive library=tapelibrary device=drive-dname`

   - *drive-dname* Ist der Gerätename für das Laufwerk
   - *tapelibrary* Ist der von Ihnen definierte Bandbibliothek

     Wiederholen Sie diesen Vorgang für jedes Laufwerk, das Sie für die Bandbibliothek definiert haben, mit einem separaten Laufwerk *drivename* Und *drive-dname* Für jedes Laufwerk.

5. Definieren Sie eine Geräteklasse für die Laufwerke.

   `define devclass DeviceClassName devtype=lto library=tapelibrary format=tapetype`

   - *DeviceClassName* Ist der Name der Geräteklasse
   - *lto* Ist der Laufwerkstyp, der mit dem Server verbunden ist

- *tapelibrary* Ist der von Ihnen definierte Bandbibliothek
- *tapetype* Ist der Tape-Typ, z. B. ultrium3

6. Fügen Sie dem Bestand der Bibliothek Bandvolumen hinzu.

   ```
   checkin libvolume tapelibrary
   ```

   tapelibrary Ist der von Ihnen definierte Bandbibliothek.

7. Erstellen Sie den primären Bandspeicherpool.

   ```
   define stgpool SGWSTapePool DeviceClassName description=description
   collocate=filespace maxscratch=XX
   ```

   - *SGWSTapePool* Ist der Name des Bandspeicherpools des Archiv-Nodes. Sie können einen beliebigen Namen für den Bandspeicher-Pool auswählen (sofern der Name die vom TSM-Server erwarteten Syntaxkonventionen verwendet).
   - *DeviceClassName* Ist der Name des Klassennamens für die Bandbibliothek.
   - *description* Ist eine Beschreibung des Speicherpools, der mithilfe des auf dem TSM-Server angezeigt werden kann `query stgpool` Befehl. Beispiel: „`Bandspeicher-Pool für den Archiv-Node`“
   - *collocate=filespace* Gibt an, dass der TSM-Server Objekte aus demselben Dateispeicher auf ein einzelnes Band schreiben soll.
   - `XX` Ist eine der folgenden Optionen:
     - Die Anzahl der leeren Bänder in der Bandbibliothek (falls der Archivknoten die einzige Anwendung ist, die die Bibliothek verwendet).
     - Die Anzahl der vom StorageGRID System zugewiesenen Tapes (in Fällen, in denen die Tape-Bibliothek gemeinsam genutzt wird).

8. Erstellen Sie auf einem TSM-Server einen Festplatten-Speicherpool. Geben Sie an der Administrationskonsole des TSM-Servers ein

   ```
   define stgpool SGWSDiskPool disk description=description
   maxsize=maximum_file_size nextstgpool=SGWSTapePool highmig=percent_high
   lowmig=percent_low
   ```

   - *SGWSDiskPool* Ist der Name des Festplatten-Pools des Archiv-Nodes. Sie können einen beliebigen Namen für den Festplatten-Speicherpool auswählen (sofern der Name die vom TSM erwarteten Syntaxkonventionen verwendet).
   - *description* Ist eine Beschreibung des Speicherpools, der mithilfe des auf dem TSM-Server angezeigt werden kann `query stgpool` Befehl. Beispiel: „`DFestplatten-Storage-Pool für den Archiv-Node`“
   - *maximum_file_size* Zwingt das Schreiben von Objekten, die größer sind als diese Größe, direkt auf Tape, statt im Festplatten-Pool gespeichert zu werden. Es wird empfohlen, die Einstellung festzulegen *maximum_file_size* Bis 10 GB.
   - *nextstgpool=SGWSTapePool* Bezeichnet den Festplatten-Speicherpool auf den für den Archiv-Node definierten Bandspeicher-Pool.
   - *percent_high* Legt den Wert fest, mit dem der Laufwerk-Pool seine Inhalte in den Bandpool migriert.

Es wird empfohlen, die Einstellung festzulegen *percent_high* Zu 0, sodass sofort die Datenmigration beginnt

- *percent_low* Legt den Wert fest, mit dem die Migration zum Bandpool angehalten wird. Es wird empfohlen, die Einstellung festzulegen *percent_low* Zu 0, um den Laufwerk-Pool zu löschen.

9. Erstellen Sie auf einem TSM-Server ein Festplatten-Volume (oder Volumes) und weisen Sie es dem Festplatten-Pool zu.

   `define volume SGWSDiskPool volume_name formatsize=size`

   - *SGWSDiskPool* Ist der Name des Disk-Pools.
   - *volume_name* Ist der vollständige Pfad zum Speicherort des Volumes (z. B. `/var/local/arc/stage6.dsm`) Auf dem TSM-Server, wo er den Inhalt des Laufwerk-Pools in Vorbereitung für die Übertragung auf Band schreibt.
   - *size* Ist die Größe des Datenträgers in MB.

     Wenn Sie beispielsweise ein einzelnes Laufwerk-Volume so erstellen möchten, dass der Inhalt eines Festplattenpools ein einzelnes Band enthält, setzen Sie den Wert der Größe auf 200000, wenn das Bandvolumen 200 GB hat.

     Es könnte jedoch wünschenswert sein, mehrere Festplatten-Volumes einer kleineren Größe zu erstellen, da der TSM-Server auf jedes Volume im Festplatten-Pool schreiben kann. Wenn die Bandgröße beispielsweise 250 GB beträgt, erstellen Sie 25 Festplatten-Volumes mit jeweils 10 GB (10000).

   Der TSM-Server weist im Verzeichnis für das Festplatten-Volume vorab Speicherplatz zu. Dies kann einige Zeit in Anspruch nehmen (mehr als drei Stunden für ein 200-GB-Laufwerk).

Definieren Sie eine Domänenrichtlinie und registrieren Sie einen Knoten

Sie müssen eine Domänenrichtlinie definieren, die die TSM-Managementklasse für die Daten verwendet, die vom Archiv-Node gespeichert wurden, und dann einen Knoten registrieren, um diese Domänenrichtlinie zu verwenden.

> Archive Node-Prozesse können Speicher auslaufen, wenn das Clientpasswort für den Archive Node im Tivoli Storage Manager (TSM) abläuft. Stellen Sie sicher, dass der TSM-Server so konfiguriert ist, dass der Client-Benutzername/das Passwort für den Archiv-Node nie abläuft.

Wenn Sie einen Knoten auf dem TSM-Server für die Verwendung des Archiv-Knotens registrieren (oder einen vorhandenen Knoten aktualisieren), müssen Sie die Anzahl der Mount-Punkte angeben, die der Knoten für Schreibvorgänge verwenden kann, indem Sie den MAXNUMMP-Parameter für den BEFEHL REGISTER NODE angeben. Die Anzahl der Bereitstellungspunkte entspricht in der Regel der Anzahl der Bandlaufwerksköpfe, die dem Archiv-Node zugewiesen sind. Die für MAXNUMMP auf dem TSM-Server angegebene Nummer muss mindestens so groß sein wie der Wert für die **ARC Target Configuration Main Maximum Store Sessions** für den Archiv-Node, Der auf den Wert 0 oder 1 gesetzt ist, da gleichzeitige Speichersitzungen vom Archiv-Node nicht unterstützt werden.

Der Wert des MAXSESSIONS-Satzes für den TSM-Server steuert die maximale Anzahl von Sitzungen, die für den TSM-Server von allen Client-Anwendungen geöffnet werden können. Der auf dem TSM angegebene MAXSESSIONS-Wert muss mindestens genauso groß sein wie der für **ARC Target Configuration Main Anzahl der Sitzungen** im Grid Manager für den Archiv-Node angegebene Wert. Der Archivknoten erstellt gleichzeitig höchstens eine Sitzung pro Bereitstellungspunkt plus eine kleine Zahl (5) zusätzlicher Sitzungen.

Der dem Archiv-Node zugewiesene TSM-Node verwendet eine benutzerdefinierte Domänenrichtlinie `tsm-domain`. Der `tsm-domain` Die Domänenrichtlinie ist eine geänderte Version der Domänenrichtlinie „`standard`“, die auf Band geschrieben und als Speicherpool des StorageGRID Systems das Archivziel festgelegt wurde (*`SGWSDiskPool`*).

> Sie müssen sich am TSM-Server mit Administratorrechten anmelden und das dsmadmc-Tool verwenden, um die Domänenrichtlinie zu erstellen und zu aktivieren.

Erstellen und aktivieren Sie die Domänenrichtlinie

Sie müssen eine Domänenrichtlinie erstellen und diese dann aktivieren, um den TSM-Server so zu konfigurieren, dass die vom Archiv-Node gesendeten Daten gespeichert werden.

Schritte

1. Eine Domänenrichtlinie erstellen.

   ```
   copy domain standard tsm-domain
   ```

2. Wenn Sie keine vorhandene Managementklasse verwenden, geben Sie eine der folgenden Werte ein:

   ```
   define policyset tsm-domain standard
   ```

   ```
   define mgmtclass tsm-domain standard default
   ```

   `default` Ist die Standard-Managementklasse für die Bereitstellung.

3. Erstellen Sie eine Copygroup in den entsprechenden Speicherpool. Geben Sie (in einer Zeile) ein:

   ```
   define copygroup tsm-domain standard default type=archive
   destination=SGWSDiskPool retinit=event retmin=0 retver=0
   ```

   `default` Ist die Standard-Managementklasse für den Archivknoten. Die Werte von `retinit`, `retmin`, und `retver` Wurden ausgewählt, um das Aufbewahrungsverhalten wiederzugeben, das derzeit vom Archiv-Knoten verwendet wird

   > Nicht einstellen `retinit` Bis `retinit=create`. Einstellung `retinit=create` Blockiert den Archiv-Knoten vom Löschen von Inhalten, da Aufbewahrungsereignisse verwendet werden, um Inhalte vom TSM-Server zu entfernen.

4. Weisen Sie die Managementklasse als Standard zu.

   ```
   assign defmgmtclass tsm-domain standard default
   ```

5. Legen Sie den neuen Richtliniensatz als aktiv fest.

   ```
   activate policyset tsm-domain standard
   ```

   Ignorieren Sie die Warnung „`no Backup copy Group`“, die beim Eingeben des Befehls activate angezeigt wird.

6. Registrieren Sie einen Knoten, um den neuen Richtliniensatz auf dem TSM-Server zu verwenden. Geben Sie auf dem TSM-Server (in einer Zeile) Folgendes ein:

   ```
   register node arc-user arc-password passexp=0 domain=tsm-domain
   MAXNUMMP=number-of-sessions
   ```

   Arc-user und Arc-password sind der Name und das Kennwort des Client-Knotens, den Sie auf dem Archiv-Node definieren, und der Wert von MAXNUMMP ist auf die Anzahl der Bandlaufwerke festgelegt, die für Archive Node Store-Sessions reserviert sind.

   > Durch die Registrierung eines Knotens wird standardmäßig eine Administrator-Benutzer-ID mit der Berechtigung des Clienteigentümers erstellt, wobei das für den Knoten definierte Passwort angegeben ist.

Datenmigration zu StorageGRID

Sie können große Datenmengen bei gleichzeitigem Einsatz des StorageGRID Systems auf das StorageGRID System migrieren.

Der folgende Abschnitt enthält einen Leitfaden zu verstehen und zu planen, eine Migration großer Datenmengen in das StorageGRID System durchzuführen. Sie ist kein allgemeiner Leitfaden für die Datenmigration und enthält keine detaillierten Schritte zur Durchführung einer Migration. Befolgen Sie die Richtlinien und Anweisungen in diesem Abschnitt, um sicherzustellen, dass Daten effizient in das StorageGRID System migriert werden, ohne den täglichen Betrieb zu beeinträchtigen und dass die migrierten Daten vom StorageGRID System entsprechend gehandhabt werden.

Bestätigen Sie die Kapazität des StorageGRID Systems

Bevor Sie große Datenmengen in das StorageGRID System migrieren, vergewissern Sie sich, dass das StorageGRID System über die Festplattenkapazität verfügt, um das erwartete Volume zu verwalten.

Wenn das StorageGRID-System einen Archivknoten umfasst und eine Kopie migriertes Objekt in Nearline-Speicher (z. B. Band) gespeichert wurde, stellen Sie sicher, dass der Speicher des Archivknotens über ausreichende Kapazität für das erwartete Volumen migriertes Datenvolumen verfügt.

Sehen Sie sich als Teil der Kapazitätsbewertung das Datenprofil der zu migrierenden Objekte an und berechnen Sie die erforderliche Festplattenkapazität. Weitere Informationen zum Monitoring der Festplattenkapazität Ihres StorageGRID Systems finden Sie unter Managen Sie Storage-Nodes Und Monitoring und Fehlerbehebung.

ILM-Richtlinie für migrierte Daten bestimmen

Die ILM-Richtlinie von StorageGRID bestimmt, wie viele Kopien erstellt werden, an welchen Standorten Kopien gespeichert werden und wie lange diese Kopien aufbewahrt werden. Eine ILM-Richtlinie besteht aus mehreren ILM-Regeln, die die Filterung von Objekten und das Managen von Objektdaten über einen längeren Zeitraum beschreiben.

Je nachdem, wie migrierte Daten verwendet werden und Ihre Anforderungen für migrierte Daten erfüllt werden, können Sie eindeutige ILM-Regeln für migrierte Daten definieren, die sich von den ILM-Regeln unterscheiden,

die für tägliche Betriebsabläufe verwendet werden. Wenn z. B. für das tägliche Datenmanagement unterschiedliche gesetzliche Anforderungen gelten als für die in der Migration enthaltenen Daten, möchten Sie möglicherweise eine andere Anzahl von Kopien der zu migrierenden Daten in einer anderen Storage-Klasse nutzen.

Sie können Regeln konfigurieren, die ausschließlich für migrierte Daten gelten, wenn es möglich ist, zwischen migrierten Daten und Objektdaten, die von den täglichen Abläufen gespeichert werden, eindeutig zu unterscheiden.

Wenn Sie mit einem der Metadatenkriterien zuverlässig zwischen den Datentypen unterscheiden können, können Sie anhand dieser Kriterien eine ILM-Regel definieren, die nur für migrierte Daten gilt.

Bevor Sie mit der Datenmigration beginnen, sollten Sie sich mit der ILM-Richtlinie des StorageGRID Systems und der Anwendung auf die migrierten Daten vertraut machen und alle Änderungen an der ILM-Richtlinie vorgenommen und getestet haben. Siehe Objektmanagement mit ILM.

Eine falsch angegebene ILM-Richtlinie kann zu nicht wiederherstellbaren Datenverlusten führen. Überprüfen Sie alle Änderungen an einer ILM-Richtlinie sorgfältig, bevor Sie sie aktivieren, um sicherzustellen, dass die Richtlinie wie vorgesehen funktioniert.

Auswirkungen der Migration auf den Betrieb

Ein StorageGRID System wurde entwickelt, um einen effizienten Objekt-Storage- und -Abruf-Service zu ermöglichen. Durch die nahtlose Erstellung redundanter Kopien von Objektdaten und Metadaten ist ein hervorragender Schutz vor Datenverlust gewährleistet.

Die Datenmigration muss jedoch gemäß den Anweisungen in diesem Kapitel sorgfältig gemanagt werden, um die alltäglichen Systemvorgänge zu vermeiden oder im Extremfall das Risiko eines Datenverlusts bei einem Ausfall im StorageGRID System zu gefährden.

Die Migration großer Datenmengen belastet das System zusätzlich. Bei starker Beladung des StorageGRID Systems reagiert das System langsamer auf Anfragen zum Speichern und Abrufen von Objekten. Dies beeinträchtigt das Speichern und Abrufen von Anfragen, die von wesentlicher Bedeutung für die täglichen Betriebsabläufe sind. Die Migration kann auch andere betriebliche Probleme verursachen. Wenn sich beispielsweise ein Storage-Node der Kapazität nähert, kann die hohe intermittierende Last aufgrund der Batch-Aufnahme dazu führen, dass der Storage Node zwischen Lese- und Schreibvorgängen wechseln und Meldungen generieren kann.

Bei hoher Auslastung können sich Warteschlangen für verschiedene Vorgänge entwickeln, die das StorageGRID System durchführen muss, um vollständige Redundanz von Objektdaten und -Metadaten sicherzustellen.

Die Datenmigration muss entsprechend den Richtlinien in diesem Dokument sorgfältig gemanagt werden, um einen sicheren und effizienten Betrieb des StorageGRID Systems während der Migration sicherzustellen. Nehmen Sie bei der Datenmigration Objekte in Batches auf oder drosseln Sie kontinuierlich die Aufnahme. Anschließend überwacht das StorageGRID System fortlaufend, um sicherzustellen, dass verschiedene Attributwerte nicht überschritten werden.

Planung und Überwachung der Datenmigration

Die Datenmigration muss bei Bedarf geplant und überwacht werden, um sicherzustellen, dass die Daten gemäß der ILM-Richtlinie innerhalb der erforderlichen Frist abgelegt

werden.

Planen Sie die Datenmigration

Vermeiden Sie die Datenmigration während der wichtigsten Geschäftszeiten. Begrenzen Sie die Datenmigration auf Abende, Wochenenden und andere Zeiten, in denen die Systemauslastung knapp ist.

Planen Sie die Datenmigration nach Möglichkeit nicht für Zeiten mit hoher Aktivität ein. Wenn es jedoch nicht sinnvoll ist, den hohen Aktivitätszeitraum vollständig zu vermeiden, ist es sicher, so lange vorzugehen, wie Sie die relevanten Attribute genau überwachen und Maßnahmen ergreifen, wenn sie akzeptable Werte überschreiten.

Monitoring der Datenmigration

In dieser Tabelle sind die Attribute aufgeführt, die während der Datenmigration überwacht werden müssen, und die jeweiligen Probleme aufgeführt.

Wenn Sie Traffic-Klassifizierungsrichtlinien mit Geschwindigkeitsbegrenzungen zur Drosselung verwenden, können Sie die beobachtete Rate in Verbindung mit den in der folgenden Tabelle beschriebenen Statistiken überwachen und die Grenzwerte bei Bedarf reduzieren.

Überwachen	Beschreibung
Anzahl an Objekten, die auf die ILM-Bewertung warten	1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus. 2. Wählen Sie ***Deployment* Übersicht Main**. 3. Überwachen Sie im Abschnitt ILM-Aktivität die Anzahl der für die folgenden Attribute angezeigten Objekte: ◦ **Ausstehend - alles (XQUZ)**: Die Gesamtzahl der Objekte, die auf die ILM-Bewertung warten. ◦ **Ausstehend - Client (XCQZ)**: Die Gesamtzahl der Objekte, die auf eine ILM-Bewertung aus Client-Operationen warten (zum Beispiel Aufnahme). 4. Wenn die Anzahl der für eines dieser Attribute angezeigten Objekte 100,000 überschreitet, drosseln Sie die Aufnahmegeschwindigkeit von Objekten, um die Last auf dem StorageGRID-System zu verringern.
Storage-Kapazität eines Targeted Archivsystems	Wenn durch die ILM-Richtlinie eine Kopie der migrierten Daten auf ein zielgerichtetes Storage-System (Band oder Cloud) gespeichert wird, überwachen Sie die Kapazität des Zielspeichersystems, um sicherzustellen, dass genügend Kapazität für die migrierten Daten vorhanden ist.
Archiv-Knoten ARC Store	Wenn ein Alarm für das Attribut **Store Failures (ARVF)** ausgelöst wird, hat das zielgerichtete Archivspeichersystem möglicherweise die Kapazität erreicht. Überprüfen Sie das ausgewählte Archivspeichersystem, und beheben Sie alle Probleme, die einen Alarm ausgelöst haben.