StorageGRID verwalten

StorageGRID software

NetApp
January 15, 2026

Inhalt

StorageGRID verwalten

StorageGRID verwalten

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

Informationen zu diesen Anweisungen

Mit den primären Aufgaben zum Konfigurieren und Verwalten von StorageGRID können Sie:

- Verwenden Sie den Grid Manager, um Gruppen und Benutzer einzurichten
- Erstellen von Mandantenkonten, die S3-Client-Applikationen das Speichern und Abrufen von Objekten erlauben
- Konfiguration und Management von StorageGRID-Netzwerken
- Konfigurieren Sie AutoSupport
- Managen der Knoteneinstellungen

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.

Erste Schritte mit Grid Manager

Anforderungen an einen Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	Unterstützte Mindestversion
Google Chrome	138
Microsoft Edge	138
Mozilla Firefox	140

Stellen Sie das Browserfenster auf eine empfohlene Breite ein.

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.

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. Einige Wartungsverfahren können jedoch nur über den primären Admin-Node durchgeführt werden.

Stellen Sie eine Verbindung mit der HA-Gruppe her

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. Siehe "Management von Hochverfügbarkeitsgruppen".

Verwenden Sie SSO

Die Anmeldeschritte sind etwas anders, wenn"Single Sign-On (SSO) wurde konfiguriert" .

Melden Sie sich beim Grid-Manager beim ersten Admin-Node an

Bevor Sie beginnen

- Sie haben Ihre Anmeldedaten.
- Sie verwenden einen "Unterstützter Webbrowser".
- Cookies sind in Ihrem Webbrowser aktiviert.
- Sie gehören einer Benutzergruppe an, die über mindestens eine Berechtigung verfügt.
- Sie haben die URL für den Grid-Manager:

  `https://FQDN_or_Admin_Node_IP/`

  Sie können den vollständig qualifizierten Domänennamen, die IP-Adresse eines Admin-Node oder die virtuelle IP-Adresse einer HA-Gruppe von Admin-Nodes verwenden.

  Um auf einen anderen Port als den Standardport für HTTPS (443) auf den Grid-Manager zuzugreifen, geben Sie die Portnummer in die URL ein:

  `https://FQDN_or_Admin_Node_IP:port/`

  > SSO ist auf dem eingeschränkten Grid Manager-Port nicht verfügbar. Sie müssen Port 443 verwenden.

Schritte

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

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

   Der angezeigte Anmeldebildschirm hängt davon ab, ob Single Sign-On (SSO) für StorageGRID konfiguriert wurde.

   SSO wird nicht verwendet

   a. Geben Sie Ihren Benutzernamen und Ihr Kennwort für den Grid Manager ein.
   b. Wählen Sie **Anmelden**.

   SSO wird verwendet

   - Wenn StorageGRID SSO verwendet und Sie zum ersten Mal auf die URL in diesem Browser zugreifen:
     i. Wählen Sie **Anmelden**. Sie können die 0 im Feld „Konto“ belassen.
     ii. Geben Sie Ihre Standard-SSO-Anmeldeinformationen auf der SSO-Anmeldeseite Ihrer Organisation ein.

     Wenn StorageGRID beispielsweise SSO verwendet und Sie zuvor auf den Grid Manager oder ein Mandantenkonto zugegriffen haben:

     A. Geben Sie **0** (die Konto-ID für den Grid-Manager) ein oder wählen Sie **Grid-Manager** aus, wenn er in der Liste der letzten Konten angezeigt wird.
     B. Wählen Sie **Anmelden**.
     C. Melden Sie sich mit Ihren Standard-SSO-Anmeldedaten auf der SSO-Anmeldeseite Ihres Unternehmens an.

Wenn Sie angemeldet sind, wird die Startseite des Grid-Managers angezeigt, die das Dashboard enthält. Informationen zu den bereitgestellten Informationen finden Sie unter "Das Dashboard anzeigen und verwalten".

Melden Sie sich bei einem anderen Admin-Node an

Führen Sie die folgenden Schritte aus, um sich bei einem anderen Admin-Node anzumelden.

SSO wird nicht verwendet

Schritte

1. 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.
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort für den Grid Manager ein.
3. Wählen Sie **Anmelden**.

SSO wird verwendet

Wenn StorageGRID SSO verwendet und Sie sich bei einem Admin-Knoten angemeldet haben, können Sie auf andere Admin-Knoten zugreifen, ohne sich erneut anmelden zu müssen.

Schritte

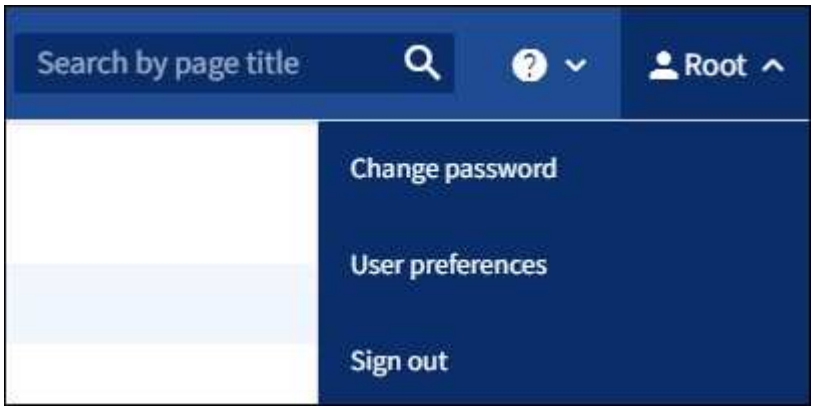
1. Geben Sie den vollständig qualifizierten Domänennamen oder die IP-Adresse des anderen Admin-Knotens in die Adressleiste des Browsers ein.
2. Wenn Ihre SSO-Sitzung abgelaufen ist, geben Sie Ihre Anmeldedaten erneut ein.

Melden Sie sich vom Grid Manager ab

Wenn Sie die Arbeit mit dem Grid-Manager abgeschlossen haben, müssen Sie sich abmelden, um sicherzustellen, dass nicht autorisierte Benutzer keinen Zugriff auf das StorageGRID-System haben. 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 Tenant Manager angemeldet sind, müssen Sie auch"melden Sie sich vom Mieterkonto ab" Zu"von SSO abmelden" .

Passwort ändern

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

Bevor Sie beginnen

Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".

Über diese Aufgabe

Wenn Sie sich bei StorageGRID als föderierter Benutzer anmelden oder Single Sign-On (SSO) aktiviert ist, können Sie Ihr Passwort 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**.

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.

Bevor Sie beginnen

Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".

Über diese Aufgabe

Wenn es ein Problem mit der Softwarelizenz für dieses StorageGRID-System gibt, enthält die Statuskarte für den Systemzustand auf dem Dashboard ein Lizenzstatus-Symbol und einen Link **Lizenz**. Die Zahl gibt die Anzahl der lizenzbezogenen Probleme an.

Schritte

1. Rufen Sie die Lizenzseite auf, indem Sie einen der folgenden Schritte ausführen:
   - Wählen Sie **Wartung** > **System** > **Lizenz**.
   - Wählen Sie auf der Statuskarte für den Systemzustand im Dashboard das Symbol Lizenzstatus oder den Link **Lizenz** aus.

     Dieser Link wird nur angezeigt, wenn ein Problem mit der Lizenz vorliegt.

2. Anzeigen der schreibgeschützten Details für die aktuelle Lizenz:
   - StorageGRID System-ID. Hierbei handelt es sich um die eindeutige Identifikationsnummer für diese StorageGRID Installation
   - Seriennummer der Lizenz
   - Lizenztyp, entweder **Perpetual** oder **Subscription**
   - Lizenzierte Storage-Kapazität des Grid
   - Unterstützte Storage-Kapazität
   - Enddatum der Lizenz. **N/A** erscheint für eine unbefristete Lizenz.
   - Enddatum des Supports

     Dieses Datum wird aus der aktuellen Lizenzdatei gelesen und ist möglicherweise veraltet, wenn Sie den Supportvertrag nach Erhalt der Lizenzdatei verlängert oder verlängert haben. Informationen zum Aktualisieren dieses Werts finden Sie unter "Aktualisieren Sie die StorageGRID-Lizenzinformationen". Sie können auch das tatsächliche Enddatum des Vertrags mithilfe von Active IQ anzeigen.

   - Inhalt der Lizenztext-Datei

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.

Bevor Sie beginnen

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

Schritte

1. Wählen Sie **Wartung** > **System** > **Lizenz**.
2. Wählen Sie im Abschnitt Lizenz aktualisieren die Option **Durchsuchen** aus.
3. Suchen und wählen Sie die neue Lizenzdatei (`.txt`).

   Die neue Lizenzdatei wird validiert und angezeigt.

4. Geben Sie die Provisionierungs-Passphrase ein.
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.

Bevor Sie beginnen

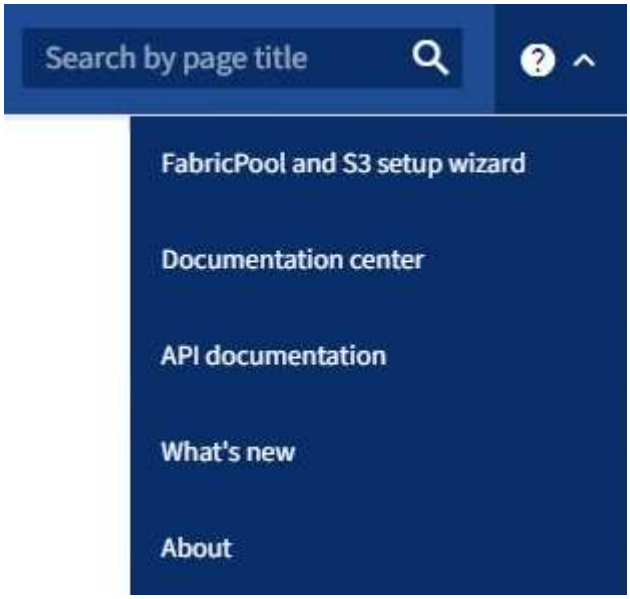
- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".

- Sie haben "Bestimmte Zugriffsberechtigungen".

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

Schritte

1. Wählen Sie im Grid Manager Header das Hilfesymbol aus und wählen Sie **API documentation**.



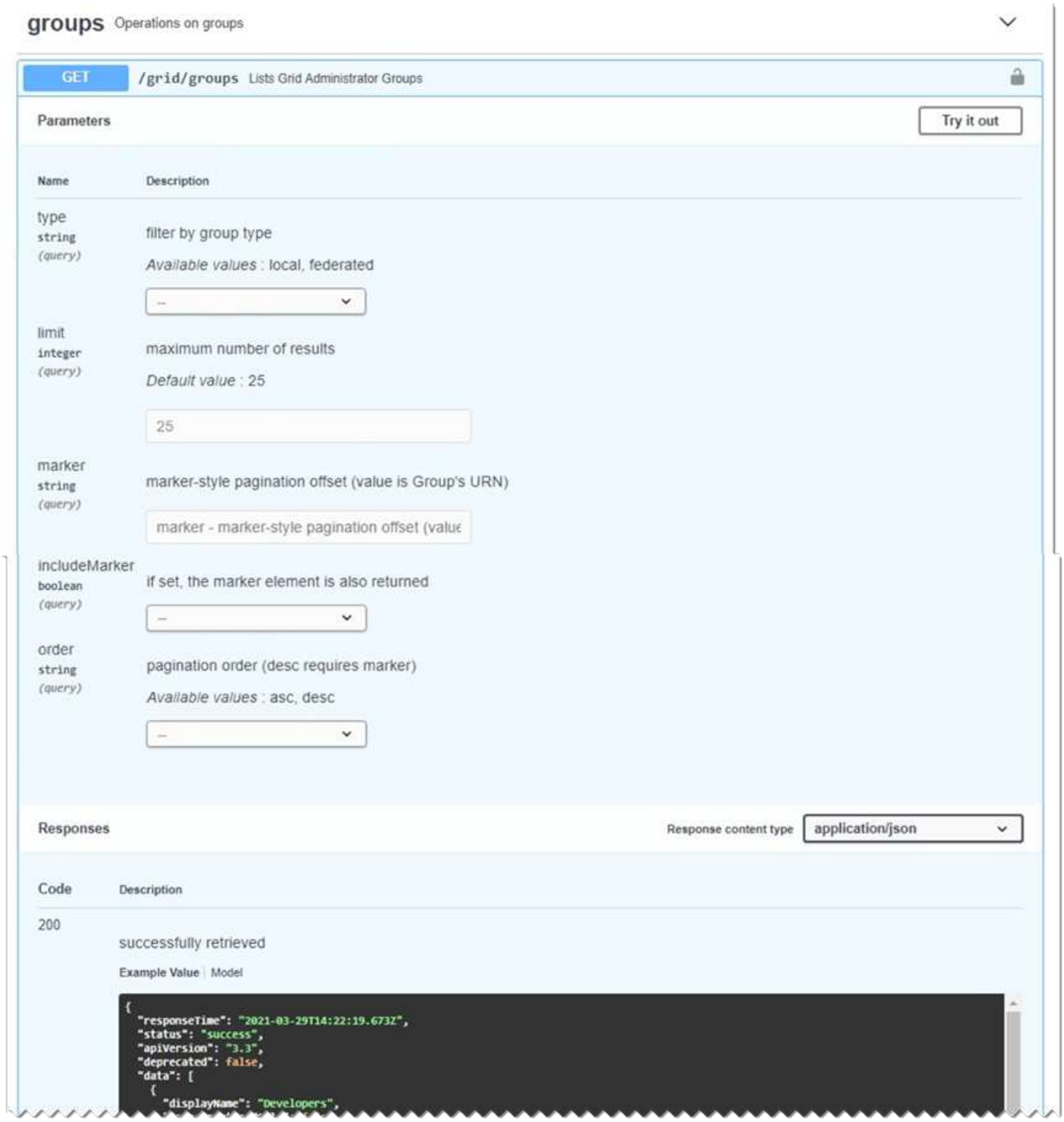
2. Um eine Operation mit der privaten API durchzuführen, wählen Sie auf der StorageGRID Management API-Seite **Gehe zur privaten API-Dokumentation** aus.

   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 zur Verwaltung von Storage-Mandanten-Konten, einschließlich der Erstellung neuer Konten und dem Abruf der Speichernutzung für ein bestimmtes Konto.
- **Alert-history**: Operationen bei aufgelösten Warnmeldungen.
- **Alert-Receivers**: Operationen auf Alert-Notification-Receivern (E-Mail).
- **Alert-rules**: Operationen auf Warnungsregeln.
- **Alert-Silences**: Operationen bei Alarmstummzuständen.
- **Alerts**: Operationen bei Alerts.
- **Audit**: Operationen zum Auflisten und Aktualisieren der Überwachungskonfiguration.
- **Auth**: Operationen zur Authentifizierung der Benutzersitzung.

  Die Grid Management API unterstützt das Authentifizierungsschema für das Inhabertoken. Um sich anzumelden, geben Sie einen Benutzernamen und ein Passwort im JSON-Textkörper der Authentifizierungsanfrage (d.h. `POST /api/v3/authorize`) an. 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. Das Token läuft nach 16 Stunden ab.

  Wenn Single Sign-On für das StorageGRID-System aktiviert ist, müssen Sie zur Authentifizierung verschiedene Schritte durchführen. Siehe „Authentifizierung an der API, wenn Single Sign-On aktiviert ist“.

  Informationen zur Verbesserung der Authentifizierungssicherheit finden Sie unter „Schutz gegen standortübergreifende Forgery“.

- **Client-Certificates**: Operationen zur Konfiguration von Client-Zertifikaten, damit StorageGRID sicher über externe Überwachungstools aufgerufen werden kann.
- **Config**: Operationen im Zusammenhang mit der Produktfreigabe und den 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.
- **Deactivated-Features**: Operationen zum Anzeigen von Features, die möglicherweise deaktiviert wurden.
- **dns-Server**: Operationen zum Auflisten und Ändern von konfigurierten externen DNS-Servern.
- **Drive-Details**: Betrieb von Laufwerken für bestimmte Storage Appliance-Modelle.
- **Endpunktdomänennamen**: Operationen zum Auflisten und Ändern von S3-Endpunktdomänennamen.
- **Erasure-Coding**: Operationen auf Erasure-Coding-Profilen.
- **Erweiterung**: Expansionsbetrieb (Verfahrensebene).
- **Expansion-Nodes**: Erweiterungsvorgänge (Node-Ebene).
- **Erweiterungsstandorte**: Expansionsbetrieb (Standort-Ebene).
- **Grid-Networks**: Operationen zum Auflisten und Ändern der Grid Network List.

- **Grid-passwords**: Operationen zur Grid-Passwortverwaltung.
- **Groups**: Operationen zur Verwaltung lokaler Grid-Administratorgruppen und zum Abrufen föderierter Grid-Administratorgruppen von einem externen LDAP-Server.
- **Identity-source**: Operationen zum Konfigurieren einer externen Identitätsquelle und zum manuellen Synchronisieren von föderierten Gruppen- und Benutzerinformationen.
- **ilm**: Operationen zum Information Lifecycle Management (ILM).
- **In-progress-procedures**: Ruft die derzeit laufenden Wartungsverfahren ab.
- **Lizenz**: Operationen zum Abrufen und Aktualisieren der StorageGRID-Lizenz.
- **Logs**: Operationen zum Sammeln und Herunterladen von Logfiles.V
- **Metrics**: Operationen auf StorageGRID-Metriken einschließlich sofortiger metrischer Abfragen an einem einzelnen Zeitpunkt und Range metrischer Abfragen 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 in ihren Namen enthalten *private*sind, sind nur für den internen Gebrauch bestimmt. Diese Kennzahlen können sich ohne Ankündigung zwischen StorageGRID Versionen ändern.

- **Node-Details**: Operationen für Node-Details.
- **Node-Health**: Operationen auf dem Node-Status.
- **Node-Storage-State**: Vorgänge im Speicherstatus der Knoten.
- **ntp-Server**: Operationen zum Auflisten oder Aktualisieren externer NTP-Server (Network Time Protocol).
- **Objekte**: Operationen an Objekten und Objektmetadaten.
- **Erholung**: Operationen für die Wiederherstellung.
- **recovery-package**: Vorgänge zum Herunterladen des Wiederherstellungspakets.
- **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**: Operationen auf der aktuellen SNMP-Konfiguration.
- **Storage-Wasserzeichen**: Storage-Knoten Wasserzeichen.
- **Traffic-Klassen**: Operationen für Verkehrsklassifizierungsrichtlinien.
- **Nicht vertrauenswürdig-Client-Network**: 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 die Version 4 der API an.

`https://hostname_or_ip_address/api/v4/authorize`

Die Hauptversion der API wird bei Änderungen, die *nicht kompatibel* mit älteren Versionen sind, angestoßen. Die Minor-Version der API wird bei Änderungen, die *kompatibel* mit älteren Versionen gemacht werden, angestoßen. 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, wird nur die neueste Version der 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 unterstützten Versionen konfigurieren. Weitere Informationen finden Sie im Abschnitt **config** der Dokumentation zur Swagger API"Grid Management API". Sie sollten die Unterstützung für die ältere Version deaktivieren, nachdem Sie alle 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 v2 API at POST "/api/v2/authorize"
```

Legen Sie fest, welche API-Versionen in der aktuellen Version unterstützt werden

Verwenden Sie die `GET /versions` API-Anforderung, um eine Liste der unterstützten API-Hauptversionen zurückzugeben. Diese Anfrage befindet sich im Abschnitt **config** der Swagger API-Dokumentation.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Geben Sie eine API-Version für eine Anforderung an

Sie können die API-Version mit einem PATH-Parameter (`Api-Version: 4`)(`/api/v4` oder einem Header) angeben. Wenn Sie beide Werte angeben, überschreibt der Kopfzeilenwert den Pfadwert.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" 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, setzen Sie den `csrfToken` Parameter während der Authentifizierung auf `true`. Der Standardwert ist `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, wird ein `GridCsrfToken` Cookie mit einem zufälligen Wert für die Anmeldung beim Grid Manager gesetzt, und das `AccountCsrfToken` Cookie wird mit einem zufälligen Wert für die Anmeldung beim 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:

- Die `X-Csrf-Token` Kopfzeile mit dem Wert der Kopfzeile auf den Wert des CSRF-Token-Cookies gesetzt.
- Für Endpunkte, die einen formularkodierten Körper akzeptieren: Einen `csrfToken` formularkodierten Anforderungskörper-Parameter.

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

> Anforderungen, die ein CSRF-Token-Cookie gesetzt haben, erzwingen auch den "Content-Type: Application/json"-Header für jede Anforderung, die einen JSON-Request-Body 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"Konfiguration und Aktivierung von Single Sign On (SSO)" und Sie Active Directory als SSO-Anbieter verwenden, müssen Sie eine Reihe von API-Anfragen stellen, um ein Authentifizierungstoken zu erhalten, das für die Grid Management API oder die Tenant Management 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.

Bevor Sie beginnen

- 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 StorageGRID

Installationsdateien befindet(`./rpms` für RHEL, `./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.

Wenn Sie ein Problem mit der URL-Kodierung 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 das `storagegrid-ssoauth.py` Python-Skript. Weiter mit Schritt 2.
   - Verwenden Sie Curl-Anforderungen. Weiter mit Schritt 3.
2. Wenn Sie das Skript verwenden möchten `storagegrid-ssoauth.py`, 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, stellen Sie eine POST-Anforderung an `/api/v3/authorize-saml`, aus und entfernen Sie die zusätzliche JSON-Codierung aus der Antwort.

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

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

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

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

c. Speichern Sie die `SAMLRequest` aus der Antwort für die 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 das `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 den `SAMLResponse` aus dem ausgeblendeten Feld:

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

j. Erstellen Sie mit dem gespeicherten `SAMLResponse` eine StorageGRID-`/api/saml-response`Anforderung, um ein StorageGRID-Authentifizierungstoken zu generieren.

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 Authentifizierungstoken in der Antwort als `MYTOKEN`.

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

Sie können jetzt `MYTOKEN` für andere Anfragen verwenden, ähnlich wie Sie die API verwenden würden, wenn SSO nicht verwendet würde.

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

Falls erforderlich, können Sie sich von der StorageGRID-API abmelden, indem Sie sich von der einzelnen Abmeldeseite Ihres Unternehmens abmelden. Alternativ können Sie einzelne Abmeldungen (SLO) von StorageGRID auslösen, was ein gültiges StorageGRID-Überträger-Token erfordert.

Schritte

1. Um eine Anforderung für eine signierte Abmeldung zu generieren, übergeben Sie `Cookie „sso=true“ an die 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“ nicht angegeben wird, wird der Benutzer ohne Beeinträchtigung des SSO-Status bei StorageGRID abgemeldet.

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

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

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

Verwenden Sie die API, wenn Single Sign-On aktiviert ist (Entra-ID).

Wenn Sie"Konfiguration und Aktivierung von Single Sign On (SSO)" und Sie Entra ID als SSO-Anbieter verwenden, können Sie zwei Beispielskripte verwenden, um ein Authentifizierungstoken zu erhalten, das für die Grid Management API oder die Tenant Management API gültig ist.

Sign in , wenn die einmalige Anmeldung bei Entra ID aktiviert ist.

Diese Anweisungen gelten, wenn Sie Entra ID als SSO-Identitätsanbieter verwenden

Bevor Sie beginnen

- 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:

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

Beide Skripte befinden sich im StorageGRID Installationsverzeichnis(`./rpms` für RHEL, `./debs` für Ubuntu oder Debian und `./vsphere` für VMware).

Informationen zum Schreiben Ihrer eigenen API-Integration mit Entra ID finden Sie im `storagegrid-ssoauth-azure.py` Skript. Das Python-Skript sendet zwei Anfragen direkt an StorageGRID (zuerst, um die SAML-Anforderung abzurufen, und später, um das Autorisierungstoken abzurufen) und ruft außerdem das Node.js-Skript auf, um mit der Entra-ID zu interagieren und die SSO-Vorgänge durchzuführen.

SSO-Vorgänge können mithilfe einer Reihe von API-Anfragen ausgeführt werden, dies ist jedoch nicht ganz einfach. Das Puppeteer Node.js-Modul wird zum Scrapen der Entra ID SSO-Schnittstelle verwendet.

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

Schritte

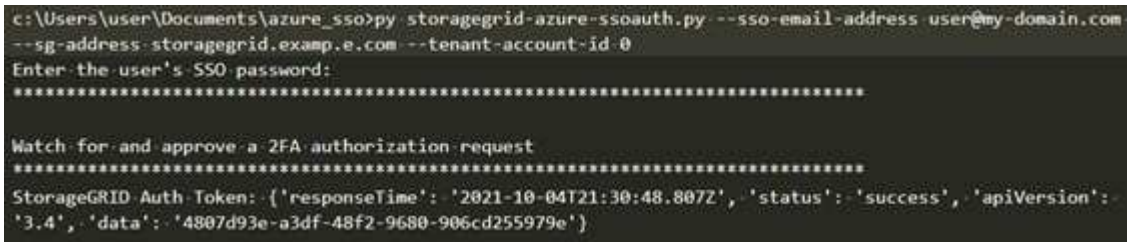
1. Installieren Sie die erforderlichen Abhängigkeiten:
   a. Installieren Sie Node.js (siehe "https://nodejs.org/en/download/").
   b. Installieren Sie die erforderlichen Node.js-Module (Puppenspieler und jsdom):

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

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

   Das Python-Skript ruft dann das entsprechende Node.js-Skript auf, um die Entra ID 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, die zur Anmeldung bei Entra ID verwendet wird
   - Die Adresse für StorageGRID
   - Die Mandantenkonto-ID, wenn Sie auf die Mandantenmanagement-API zugreifen möchten
4. Geben Sie bei der entsprechenden Aufforderung das Kennwort ein und seien Sie bereit, Entra ID auf Anfrage eine MFA-Autorisierung zu erteilen.



> 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. die Eingabe eines Codes, der in einer Textnachricht empfangen wird).

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"Konfiguration und Aktivierung von Single Sign On (SSO)" und Sie PingFederate als SSO-Anbieter verwenden, müssen Sie eine Reihe von API-Anfragen stellen, um ein Authentifizierungstoken zu erhalten, das für die Grid Management API oder die Tenant Management API gültig ist.

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

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

Bevor Sie beginnen

- 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 StorageGRID Installationsdateien befindet(`./rpms` für RHEL, `./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.

  Wenn Sie ein Problem mit der URL-Kodierung 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 das `storagegrid-ssoauth.py` Python-Skript. Weiter mit Schritt 2.
   - Verwenden Sie Curl-Anforderungen. Weiter mit Schritt 3.
2. Wenn Sie das Skript verwenden möchten `storagegrid-ssoauth.py`, 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" eingeben (PINGFEDERATE, PINGFEDERATE usw.).
   - 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, stellen Sie eine POST-Anforderung an `/api/v3/authorize-saml`, aus und entfernen Sie die zusätzliche JSON-Codierung 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 für die 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 den `SAMLResponse` aus dem ausgeblendeten Feld:

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

j. Erstellen Sie mit dem gespeicherten `SAMLResponse` eine StorageGRID-`/api/saml-response`Anforderung, um ein StorageGRID-Authentifizierungstoken zu generieren.

   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 Authentifizierungstoken in der Antwort als `MYTOKEN`.

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

Sie können jetzt `MYTOKEN` für andere Anfragen verwenden, ähnlich wie Sie die API verwenden würden, wenn SSO nicht verwendet würde.

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

Falls erforderlich, können Sie sich von der StorageGRID-API abmelden, indem Sie sich von der einzelnen Abmeldeseite Ihres Unternehmens abmelden. Alternativ können Sie einzelne Abmeldungen (SLO) von StorageGRID auslösen, was ein gültiges StorageGRID-Überträger-Token erfordert.

Schritte

1. Um eine Anforderung für eine signierte Abmeldung zu generieren, übergeben Sie `Cookie „sso=true“ an die 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“ nicht angegeben wird, wird der Benutzer ohne Beeinträchtigung des SSO-Status bei StorageGRID abgemeldet.

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

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

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

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 Funktion **Change Tenant root password** im Grid Manager (sowohl die Benutzeroberfläche als auch die API) stellt Unternehmen A sicher, dass Admin-Benutzer - einschließlich des Root-Benutzers und Benutzer, die zu Gruppen mit der Berechtigung **Root-Zugriff** gehören - das Passwort für den Root-Benutzer eines Mandantenkontos nicht ändern können.*

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 Verwaltungsberechtigung **Change Tenant root password** wird nicht mehr in der Benutzeroberfläche angezeigt, und jede API-Anforderung, die versucht, das Root-Passwort für einen Mandanten zu ändern, schlägt mit "403 Verboten" 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 Funktion **activateFeatures** 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. Wenn Sie beispielsweise die Funktion zum Ändern des Stammkennworts für den Mandanten erneut aktivieren und die Berechtigung zum Verwalten von storageAdmin deaktivieren möchten, senden Sie diese PUT-Anforderung:

```
{ "grid": {"storageAdmin": true} }
```

Kontrolle des Zugriffs auf StorageGRID

Kontrolle über den StorageGRID-Zugriff

Sie steuern, wer auf StorageGRID zugreifen kann und welche Aufgaben Benutzer ausführen können, indem Sie Gruppen und Benutzer erstellen oder importieren und jeder Gruppe Berechtigungen zuweisen. Optional können Sie Single Sign On (SSO) aktivieren, Client-Zertifikate erstellen und Grid-Passwörter ändern.

Den Zugriff auf den Grid Manager steuern

Sie bestimmen, wer auf den Grid Manager und die Grid Management API zugreifen kann, indem Sie Gruppen und Benutzer von einem Identitätsverbundservice aus importieren oder lokale Gruppen und lokale Benutzer einrichten.

Mit "Identitätsföderation" wird die Einrichtung "Gruppen"beschleunigt und "Benutzer"Benutzer können sich mit vertrauten Anmeldeinformationen bei StorageGRID anmelden. Sie können die Identitätsföderation konfigurieren, wenn Sie Active Directory, OpenLDAP oder Oracle Directory Server verwenden.

Wenden Sie sich an den technischen Support, wenn Sie einen anderen LDAP v3-Dienst verwenden möchten.

Sie legen fest, welche Aufgaben jeder Benutzer durchführen kann, indem Sie jeder Gruppe unterschiedliche Aufgaben zuweisen"Berechtigungen". Beispielsweise können Benutzer in einer Gruppe in der Lage sein, ILM-Regeln und Benutzer in einer anderen Gruppe zu verwalten, um Wartungsaufgaben durchzuführen. Ein Benutzer muss mindestens einer Gruppe angehören, um auf das System zuzugreifen.

Optional können Sie eine Gruppe als schreibgeschützt konfigurieren. Benutzer in einer schreibgeschützten Gruppe können nur Einstellungen und Funktionen anzeigen. Sie können keine Änderungen an der Grid Manager- oder Grid-Management-API vornehmen oder Vorgänge ausführen.

Aktivieren Sie Single Sign On

Das StorageGRID -System unterstützt Single Sign-On (SSO) mithilfe des Standards Security Assertion Markup Language 2.0 (SAML 2.0). Nach Ihnen"Konfigurieren und aktivieren Sie SSO" müssen alle Benutzer von einem externen Identitätsanbieter authentifiziert werden, bevor sie auf den Grid Manager, den Tenant Manager, die Grid Management API oder die Tenant Management API zugreifen können. Lokale Benutzer können sich nicht bei StorageGRID anmelden.

Provisionierungs-Passphrase ändern

Die Bereitstellungspassphrase wird für viele Installations- und Wartungsverfahren sowie zum Herunterladen des StorageGRID -Wiederherstellungspakets benötigt. Die Passphrase ist auch zum Herunterladen von Backups der Grid-Topologieinformationen und Verschlüsselungsschlüssel für das StorageGRID -System erforderlich. Du kannst"Ändern Sie die Passphrase" nach Bedarf.

Ändern der Passwörter für die Node-Konsole

Jeder Knoten in Ihrem Grid verfügt über ein Knotenkonsolenkennwort, das Sie benötigen, um sich per SSH als „Admin“ beim Knoten oder bei einer VM-/physischen Konsolenverbindung als Root-Benutzer anzumelden. Bei Bedarf können Sie"Ändern Sie das Passwort für die Node-Konsole" für jeden Knoten.

Ändern Sie die Provisionierungs-Passphrase

Verwenden Sie dieses Verfahren, um die Passphrase für die StorageGRID Bereitstellung zu ändern. Die Passphrase wird für Wiederherstellungs-, Erweiterungs- und Wartungsverfahren benötigt. Die Passphrase ist auch zum Herunterladen von Backups des Wiederherstellungspakets erforderlich, die Informationen zur Grid-Topologie, Passwörter für die Grid-Knotenkonsole und Verschlüsselungsschlüssel für das StorageGRID System enthalten.

Bevor Sie beginnen

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

Über diese Aufgabe

Die Bereitstellungspassphrase wird für viele Installations- und Wartungsverfahren benötigt, sowie für"Herunterladen des Wiederherstellungspakets" . Die Bereitstellungspassphrase ist nicht aufgeführt in der `Passwords.txt` Datei. Dokumentieren Sie die Bereitstellungspassphrase und bewahren Sie sie an einem sicheren Ort auf.

Schritte

1. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Grid-Passwörter**.
2. Wählen Sie unter **Change Provisioning Passphrase** die Option **make a change** aus
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.

Bewahren Sie die Bereitstellungspassphrase an einem sicheren Ort auf. Es wird für Installations-, Erweiterungs- und Wartungsverfahren benötigt.

5. 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.

6. Wählen Sie **Wiederherstellungspaket**.
7. Geben Sie die neue Bereitstellungspassphrase ein, um das neue Wiederherstellungspaket herunterzuladen.

Nach dem Ändern der Bereitstellungspassphrase müssen Sie sofort ein neues Wiederherstellungspaket herunterladen. Mit der Wiederherstellungspaketdatei können Sie das System wiederherstellen, wenn ein Fehler auftritt.

Ändern der Passwörter für die Node-Konsole

Jeder Knoten in Ihrem Grid verfügt über ein Knotenkonsolenkennwort, mit dem Sie sich beim Knoten anmelden. Standardmäßig hat jeder Knoten ein eindeutiges Passwort. Sie können jedes Kennwort in ein neues, eindeutiges Kennwort ändern oder das Kennwort für jeden Knoten ändern, um ein globales Kennwort zu verwenden. Die Passwörter werden im Wiederherstellungspaket gespeichert.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Berechtigung für Wartung oder Root-Zugriff".
- Sie haben die aktuelle Provisionierungs-Passphrase.

Über diese Aufgabe

Sie verwenden ein Knotenkonsolenkennwort, um sich per SSH als „Administrator“ bei einem Knoten oder als Root-Benutzer bei einer VM-/physischen Konsolenverbindung anzumelden. Sie können die Passwörter der Knotenkonsole mit einer der folgenden Optionen ändern:

- Wenden Sie automatisch zufällige Passwörter auf jeden Knoten an
- Ein globales Passwort für alle Knoten festlegen und anwenden
- Geben Sie ein eindeutiges Kennwort an und wenden Sie es auf einen oder mehrere Knoten an.

Die Passwörter werden in einer aktualisierten `Passwords.txt` Datei im Wiederherstellungspaket. Die Passwörter sind in der Spalte „Passwort“ der Datei aufgeführt.

Der"SSH-Zugriffspasswörter" denn die für die Kommunikation zwischen Knoten verwendeten SSH-Schlüssel sind von den Passwörtern der Knotenkonsole getrennt. Dieses Verfahren ändert die SSH-Zugriffskennwörter nicht.

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.

Laden Sie das aktuelle Wiederherstellungspaket herunter

Laden Sie das aktuelle Wiederherstellungspaket herunter, bevor Sie die Passwörter der Knotenkonsole ändern. Sie können die Passwörter in dieser Datei verwenden, wenn der Passwortänderungsprozess für einen beliebigen Knoten fehlschlägt.

Schritte

1. Geben Sie die Provisionierungs-Passphrase für Ihr Grid ein.
2. Wählen Sie **Wiederherstellungspaket herunterladen**.
3. Kopieren Sie die Wiederherstellungspaketdatei(`.zip`) an zwei sichere und getrennte Orte.

> Die Wiederherstellungspaketdatei muss gesichert werden, da sie Verschlüsselungsschlüssel und Passwörter enthält, mit denen Daten aus dem StorageGRID -System abgerufen werden können.

4. Wählen Sie **Weiter**.

Neue Passwörter bereitstellen

1. Wählen Sie die gewünschte Methode zum Ändern des Kennworts aus.
   - **Automatisch**: StorageGRID weist allen Knoten automatisch ein neues zufälliges Konsolenkennwort zu.
   - **Benutzerdefiniert**: Sie geben Konsolenkennwörter an.

Automatisch

1. Wählen Sie **Weiter**.

Individuell

1. Wählen Sie eine der folgenden Optionen:
   - **Globales Konsolenkennwort**: Wenden Sie auf allen Knoten dasselbe Konsolenkennwort an.
   - **Eindeutige Konsolenkennwörter**: Wenden Sie auf einem oder mehreren Knoten ein anderes Kennwort an.
2. Wenn Sie **Globales Konsolenkennwort** ausgewählt haben, geben Sie das Kennwort ein, das Sie für alle Knoten verwenden möchten.
3. Wenn Sie **Eindeutige Konsolenkennwörter** ausgewählt haben, geben Sie ein eindeutiges Kennwort für einen oder mehrere Knoten ein.
4. Wählen Sie **Weiter**.

Schließen Sie die Passwortänderung ab

1. Wenn das Bestätigungsdialogfeld angezeigt wird, wählen Sie **Ja**, wenn Sie bereit sind, dass StorageGRID mit der Änderung der Knotenkonsolenkennwörter beginnt.

   Sie können diesen Vorgang nach dem Start nicht abbrechen.

   StorageGRID generiert ein neues Wiederherstellungspaket, das das neue Passwort enthält.

2. Wenn das neue Wiederherstellungspaket fertig ist, wählen Sie **Neues Wiederherstellungspaket herunterladen** und speichern Sie das Wiederherstellungspaket.
3. Öffnen Sie die `.zip` Datei.
4. Vergewissern Sie sich, dass Sie auf den Inhalt zugreifen können, einschließlich der `Passwords.txt` Datei, die die neuen Kennwörter der Node-Konsole enthält.
5. Kopieren Sie die neue Wiederherstellungspaketdatei(`.zip`) an zwei sichere und getrennte Orte.

   Überschreiben Sie nicht das alte Wiederherstellungspaket.

   Sie müssen die Wiederherstellungsdatei sichern, da sie Verschlüsselungsschlüssel und Passwörter enthält, mit denen Daten aus dem StorageGRID -System abgerufen werden können.

6. Aktivieren Sie das Kontrollkästchen, um anzugeben, dass Sie das neue Wiederherstellungspaket heruntergeladen und den Inhalt überprüft haben.
7. Wählen Sie **Weiter**.

   StorageGRID aktualisiert das Passwort für jeden Knoten.

   Wenn während des Aktualisierungsvorgangs ein Fehler auftritt, wird in der Fortschrittsleiste die Anzahl der Knoten aufgeführt, deren Passwörter nicht geändert werden konnten. Das System wiederholt den Vorgang automatisch auf jedem Knoten, dessen Kennwort nicht geändert werden konnte. Wenn der Vorgang endet und einige Knoten immer noch kein geändertes Kennwort haben, wird die Schaltfläche **Wiederholen** angezeigt.

8. 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.

9. Wenn der Fortschrittsbalken anzeigt, dass keine Updates mehr verfügbar sind, wählen Sie **Fertig**.
10. Nachdem die Passwörter der Knotenkonsole für alle Knoten geändert wurden, löschen Sie diedas erste Wiederherstellungspaket, das Sie heruntergeladen haben .

Ändern Sie die SSH-Zugriffskennwörter für Admin-Nodes

Wenn Sie die SSH-Zugriffskennwörter für Admin-Nodes ändern, werden auch die eindeutigen Sätze interner SSH-Schlüssel für jeden Node im Grid aktualisiert. Der

primäre Admin-Node verwendet diese SSH-Schlüssel, um mit einer sicheren Authentifizierung ohne Kennwort auf Knoten zuzugreifen.

Verwenden Sie einen SSH-Schlüssel, um sich bei einem Node als `admin` oder beim Root-Benutzer auf einer VM- oder physischen Konsolenverbindung anzumelden.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Berechtigung für Wartung oder Root-Zugriff".
- Sie haben die aktuelle Provisionierungs-Passphrase.

Über diese Aufgabe

Die neuen Zugangspasswörter für Admin-Knoten und die neuen internen Schlüssel für jeden Knoten werden im `Passwords.txt` Datei im Wiederherstellungspaket. Die Schlüssel sind in der Spalte „Passwort“ dieser Datei aufgeführt.

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

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Grid-Passwörter**.
2. Wählen Sie unter **SSH-Schlüssel ändern Änderung vornehmen**.

Laden Sie das aktuelle Wiederherstellungspaket herunter

Laden Sie vor dem Ändern der SSH-Zugriffsschlüssel das aktuelle Wiederherstellungspaket herunter. Sie können die Schlüssel in dieser Datei verwenden, wenn der Schlüsseländerungsprozess für einen beliebigen Knoten fehlschlägt.

Schritte

1. Geben Sie die Provisionierungs-Passphrase für Ihr Grid ein.
2. Wählen Sie **Wiederherstellungspaket herunterladen**.
3. Kopieren Sie die Wiederherstellungspaketdatei(`.zip`) an zwei sichere und getrennte Orte.

> Die Wiederherstellungspaketdatei muss gesichert werden, da sie Verschlüsselungsschlüssel und Passwörter enthält, mit denen Daten aus dem StorageGRID -System abgerufen werden können.

4. Wählen Sie **Weiter**.
5. Wenn das Bestätigungsdialogfeld angezeigt wird, wählen Sie **Yes** aus, wenn Sie bereit sind, die SSH-Zugriffsschlüssel zu ändern.

> Sie können diesen Vorgang nach dem Start nicht abbrechen.

Ändern Sie die SSH-Zugriffsschlüssel

Wenn der Prozess zum Ändern der SSH-Zugriffsschlüssel beginnt, wird ein neues Wiederherstellungspaket generiert, das die neuen Schlüssel enthält. Anschließend werden die Schlüssel auf jedem Knoten aktualisiert.

Schritte

1. Warten Sie, bis das neue Wiederherstellungspaket generiert wurde. Dies kann einige Minuten dauern.
2. Wenn die Schaltfläche „Neues Wiederherstellungspaket herunterladen“ aktiviert ist, wählen Sie „Neues Wiederherstellungspaket herunterladen“ und speichern Sie die neue Wiederherstellungspaketdatei(`.zip`) an zwei sichere und getrennte Orte.
3. Wenn der Download abgeschlossen ist:

   a. Öffnen Sie die `.zip` Datei.

   b. Bestätigen Sie, dass Sie auf den Inhalt zugreifen können, einschließlich der `Passwords.txt` Datei, die die neuen SSH-Zugriffsschlüssel enthält.

   c. Kopieren Sie die neue Wiederherstellungspaketdatei(`.zip`) an zwei sichere und getrennte Orte.

   > ! Überschreiben Sie nicht das alte Wiederherstellungspaket.

   Die Wiederherstellungspaketdatei muss gesichert werden, da sie Verschlüsselungsschlüssel und Passwörter enthält, mit denen Daten aus dem StorageGRID -System abgerufen werden können.

4. Warten Sie, bis die Schlüssel auf jedem Node aktualisiert werden. Dies kann einige Minuten dauern.

   Wenn die Schlüssel für alle Nodes geändert werden, wird ein grünes Success-Banner angezeigt.

   Wenn während des Aktualisierungsvorgangs ein Fehler auftritt, wird in einer Banner-Meldung die Anzahl der Knoten aufgeführt, bei denen die Schlüssel nicht geändert wurden. Das System wiederholt den Prozess automatisch auf jedem Node, bei dem der Schlüssel nicht geändert wurde. Wenn der Prozess mit einigen Knoten endet, die noch keinen geänderten Schlüssel haben, wird die Schaltfläche **Wiederholen** angezeigt.

   Wenn das Schlüsselupdate für einen oder mehrere Nodes fehlgeschlagen ist:

   a. Überprüfen Sie die in der Tabelle aufgeführten Fehlermeldungen.

   b. Beheben Sie die Probleme.

   c. Wählen Sie **Wiederholen**.

      Durch die erneute Versuche werden nur die SSH-Zugriffsschlüssel auf den Nodes geändert, die bei vorherigen Versuchen mit Schlüsseländerungen fehlgeschlagen sind.

5. Nachdem die SSH-Zugriffsschlüssel für alle Knoten geändert wurden, löschen Sie diedas erste Wiederherstellungspaket, das Sie heruntergeladen haben .
6. Wählen Sie optional **Wartung** > **System** > **Wiederherstellungspaket**, um eine zusätzliche Kopie des neuen Wiederherstellungspakets herunterzuladen.

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

Konfigurieren Sie die Identitätsföderation für Grid Manager

Sie können die Identitätsföderation im Grid Manager konfigurieren, wenn Sie möchten, dass Administratorgruppen und Benutzer in einem anderen System wie Active Directory, Microsoft Entra ID, OpenLDAP oder Oracle Directory Server verwaltet werden.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"Unterstützter Webbrowser" .
- Du hast"Bestimmte Zugriffsberechtigungen" .
- Sie verwenden Active Directory, Microsoft Entra ID, OpenLDAP oder Oracle Directory Server als Identitätsanbieter.

> ⓘ Wenn Sie einen LDAP v3-Dienst verwenden möchten, der nicht aufgeführt ist, 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"Voraussetzungen und Überlegungen für 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

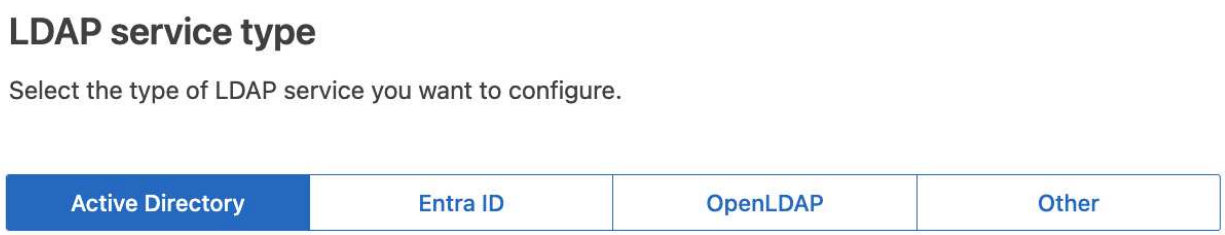
Sie können eine Identitätsquelle für den Grid Manager konfigurieren, wenn Sie Gruppen aus einem anderen System wie Active Directory, Microsoft Entra ID, OpenLDAP oder Oracle Directory Server importieren möchten. Sie können die folgenden Gruppentypen importieren:

- Admin-Gruppen. Die Benutzer in Admin-Gruppen können sich beim Grid Manager anmelden und anhand der Verwaltungsberechtigungen, die der Gruppe zugewiesen sind, Aufgaben ausführen.
- Mandantenbenutzergruppen für Mandanten, die keine eigene Identitätsquelle 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. Weitere Informationen finden Sie unter "Erstellen eines Mandantenkontos" und"Verwenden Sie ein Mandantenkonto".

Geben Sie die Konfiguration ein

Schritte

1. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Identitätsföderation**.
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 gleichbedeutend mit `sAMAccountName` für Active Directory und `uid` für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie `uid` .
   - **Benutzer-UUID**: Der Name des Attributs, das die permanente eindeutige Kennung eines LDAP-Benutzers enthält. Dieses Attribut ist gleichbedeutend mit `objectGUID` für Active Directory und `entryUUID` für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie `nsuniqueid` . Der Wert jedes Benutzers für das angegebene Attribut muss eine 32-stellige Hexadezimalzahl im 16-Byte- oder Zeichenfolgenformat sein, wobei Bindestriche ignoriert werden.
   - **Eindeutiger Gruppenname**: Der Name des Attributs, das die eindeutige Kennung einer LDAP-Gruppe enthält. Dieses Attribut ist gleichbedeutend mit `sAMAccountName` für Active Directory und `cn` für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie `cn` .
   - **Gruppen-UUID**: Der Name des Attributs, das die permanente eindeutige Kennung einer LDAP-Gruppe enthält. Dieses Attribut ist gleichbedeutend mit `objectGUID` für Active Directory und `entryUUID` für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie `nsuniqueid` . Der Wert jeder Gruppe für das angegebene Attribut muss eine 32-stellige Hexadezimalzahl im 16-Byte- oder Zeichenfolgenformat 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`
- **Eintritts-ID**: `accountEnabled` Und `userPrincipalName`

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

> Wenn Sie das Passwort in Zukunft ändern, müssen Sie es auf dieser Seite aktualisieren.

◦ **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-Muster (AD- und Entra-ID)**: `[USERNAME]@*example*.com`
- **Anmeldenamenmuster auf niedrigerer Ebene (AD- und Entra-ID)**: `*example*\[USERNAME]`
- **Distinguished Namensmuster**: `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.
   ◦ **STARTLS verwenden**: Verwenden Sie STARTTLS, um die Kommunikation mit dem LDAP-Server zu sichern. Dies ist die empfohlene Option für Active Directory, OpenLDAP oder Andere, aber diese Option wird für Microsoft Entra ID nicht unterstützt.
   ◦ **LDAPS verwenden**: Die Option LDAPS (LDAP über SSL) verwendet TLS, um eine Verbindung zum LDAP-Server herzustellen. Sie müssen diese Option für die Microsoft Entra ID auswählen.
   ◦ **TLS nicht verwenden**: Der Netzwerkverkehr zwischen dem StorageGRID -System und dem LDAP-Server wird nicht gesichert. Diese Option wird für die Microsoft Entra ID nicht unterstützt.

Die Verwendung der Option **TLS nicht verwenden** wird nicht unterstützt, wenn Ihr Active Directory-Server die LDAP-Signierung 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.

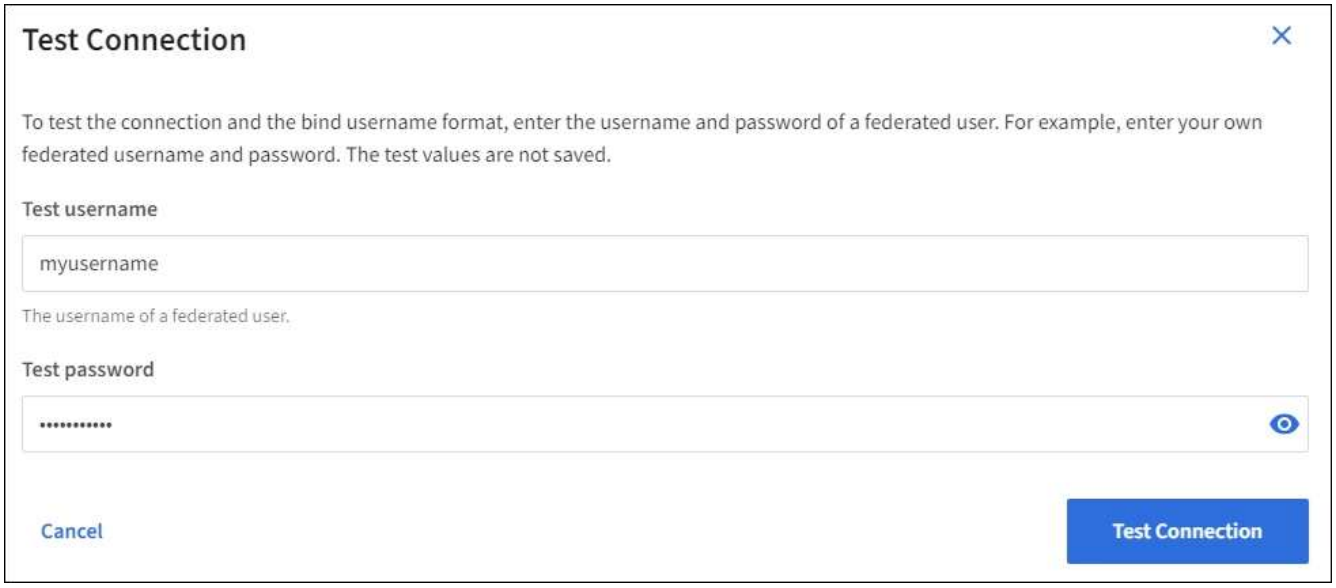
Testen Sie die Verbindung und speichern Sie die Konfiguration

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.

Schritte

1. Wählen Sie **Verbindung testen**.
2. Wenn Sie kein Bind-Benutzernamenformat angegeben haben:
   - Wenn die Verbindungseinstellungen gültig sind, wird die Meldung „Verbindung erfolgreich testen“ angezeigt. Wählen Sie **Speichern**, um die Konfiguration zu speichern.
   - Wenn die Verbindungseinstellungen ungültig sind, wird die Meldung „Testverbindung konnte nicht hergestellt werden“ 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 die 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 die Identitätsföderation für Gruppen und Benutzer vorübergehend oder dauerhaft deaktivieren. Wenn die Identitätsföderation deaktiviert ist, findet keine Kommunikation zwischen StorageGRID und der Identitätsquelle statt. Alle von Ihnen konfigurierten Einstellungen bleiben jedoch erhalten, sodass Sie die Identitätsföderation in Zukunft problemlos 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.
- Es findet keine Synchronisierung zwischen dem StorageGRID -System und der Identitätsquelle statt und es werden keine Warnungen für Konten ausgelöst, die nicht synchronisiert wurden.
- Das Kontrollkästchen **Identitätsföderation aktivieren** ist deaktiviert, wenn der Single Sign-On-Status (SSO) **Aktiviert** oder **Sandbox-Modus** ist. Der SSO-Status auf der Single Sign-On-Seite muss **Deaktiviert** sein, bevor Sie die Identitätsföderation deaktivieren können. Sehen "Deaktivieren Sie Single Sign-On" .

Schritte

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

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.

Bei Identitätsquellen, bei denen es sich nicht um Active Directory oder Microsoft Entra ID handelt, blockiert StorageGRID den S3-Zugriff für extern deaktivierte Benutzer nicht automatisch. Um den S3-Zugriff zu blockieren, löschen Sie alle S3-Schlüssel für den Benutzer oder 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 Pflege der umgekehrten Gruppenmitgliedschaft im "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 Pflege der umgekehrten Gruppenmitgliedschaft finden Sie im "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.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben "Bestimmte 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

Schritte

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

Schritte

1. Wählen Sie **Lokale Gruppe**.
2. Geben Sie einen Anzeigenamen für die Gruppe ein, den Sie bei Bedarf später aktualisieren können. Beispiel: „Maintenance Users“ oder „ILM Administrators“.
3. Geben Sie einen eindeutigen Namen für die Gruppe ein, den Sie später nicht mehr aktualisieren können.
4. Wählen Sie **Weiter**.

Föderierte Gruppe

Schritte

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 Microsoft Entra ID 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

Schritte

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 an der Grid Manager- oder Grid-Management-API vornehmen oder Vorgänge 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 "Berechtigungen für Administratorgruppen".

   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)

Schritte

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. Weitere Informationen finden Sie unter "Benutzer managen" .

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 Symbol Bearbeiten . 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 oder löschen Sie optional "Berechtigungen für Administratorgruppen". 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 oder löschen Sie optional "Berechtigungen für Administratorgruppen". d. Wählen Sie **Änderungen speichern**.

Duplizieren einer Gruppe

Schritte

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.

Schritte

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**.

Berechtigungen für Admin-Gruppen

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
- Dashboard anzeigen
- Zeigen Sie die Seiten Knoten an
- Anzeige aktueller und aufgelöster Warnmeldungen
- 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.

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.

ILM

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

- Regeln
- Richtlinien
- Richtlinien-Tags
- Storage-Pools
- Lagergüten
- Regionen
- Suche nach Objektmetadaten

> Benutzer müssen über die Berechtigung **Andere Rasterkonfiguration** verfügen, um Speicherklassen verwalten zu können.

Wartung

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

- **Konfiguration** > **Zugriffskontrolle**:
  - Grid-Passwörter
- **Konfiguration** > **Netzwerk**:
  - Domänennamen des S3-Endpunkts
- **Wartung** > **Aufgaben**:
  - Ausmustern
  - Erweiterung
  - Überprüfung der Objektexistenz
  - Recovery
- **Wartung** > **System**:
  - Recovery-Paket

    - Software-Update
- **Support** > **Tools**:
    - Protokolle

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

- **Wartung** > **Netzwerk**:
    - DNS-Server
    - Grid-Netzwerk
    - NTP-Server
- **Wartung** > **System**:
    - Lizenz
- **Konfiguration** > **Netzwerk**:
    - Domänennamen des S3-Endpunkts
- **Konfiguration** > **Sicherheit**:
    - Zertifikate
- **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

Diese Berechtigung bietet Zugriff auf:

- **Support** > **Tools** > **Metriken**-Seite
- Benutzerdefinierte Prometheus-Metrikabfragen mit dem Abschnitt **Metrics** der Grid Management API
- Dashboard-Karten von Grid Manager, die Metriken enthalten

Suche nach Objektmetadaten

Mit dieser Berechtigung erhalten Sie Zugriff auf die Seite **ILM** > **Objekt-Metadaten-Lookup**.

Andere Grid-Konfiguration

Diese Berechtigung bietet Zugriff auf diese zusätzlichen Rasterkonfigurationsoptionen:

- **ILM**:
    - Lagergüten
- **Konfiguration** > **System**:
- **Support** > **Sonstiges**:

- Verbindungskosten

Storage Appliance-Administrator

Diese Berechtigung bietet:

- Zugriff auf den E-Series SANtricity System Manager auf Storage Appliances über den Grid Manager
- Die Möglichkeit zur Durchführung von Fehlerbehebungs- und Wartungsaufgaben auf der Registerkarte Laufwerke managen für Appliances, die diese Vorgänge unterstützen.

Mandantenkonten

Mit dieser Berechtigung können Sie:

- Öffnen Sie die Seite Tenants, auf der Sie Mandantenkonten erstellen, bearbeiten und entfernen können
- Zeigen Sie vorhandene Richtlinien zur Verkehrsklassifizierung an
- Dashboard-Karten von Grid Manager anzeigen, die Mandantendetails enthalten

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.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben "Bestimmte 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

Schritte

1. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Admin-Benutzer**.
2. Wählen Sie **Benutzer erstellen**.

Geben Sie die Anmeldedaten des Benutzers ein

Schritte

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

Schritte

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. Weitere Informationen finden Sie unter "Managen von Admin-Gruppen" .

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 über die Option **Passwort ändern** im Grid Manager Banner 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.

Aufgabe	Menü „Aktionen“	Detailseite
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 Symbol Bearbeiten . 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**.
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**.

Aufgabe	Menü „Aktionen“	Detailseite
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**.

Importieren von Verbundbenutzern

Sie können einen oder mehrere Verbundbenutzer (bis zu maximal 100 Benutzer) direkt in die Seite „Benutzer“ importieren.

Schritte

1. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Admin-Benutzer**.
2. Wählen Sie **Verbundbenutzer importieren**.
3. Geben Sie die UUID oder den Benutzernamen für einen oder mehrere Verbundbenutzer ein.

   Fügen Sie bei mehreren Einträgen jede UUID oder jeden Benutzernamen in einer neuen Zeile hinzu.

4. Wählen Sie **Importieren**.

   Wenn der Import in das Feld „Benutzer“ für einen oder mehrere Benutzer fehlschlägt, führen Sie die folgenden Schritte aus:

   a. Erweitern Sie **Nicht importierte Benutzer** und wählen Sie **Benutzer kopieren**.
   b. Versuchen Sie den Import erneut, indem Sie **Zurück** auswählen und die kopierten Benutzer in das Dialogfeld **Verbundbenutzer importieren** einfügen.

   Nachdem Sie das Dialogfeld **Verbundbenutzer importieren** geschlossen haben, werden die Verbundbenutzerinformationen für die erfolgreich importierten Benutzer auf der Seite „Benutzer“ angezeigt.

Duplizieren eines Benutzers

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

Schritte

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.

Schritte

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

So funktioniert SSO

Wenn Single Sign-On (SSO) aktiviert ist, können Benutzer nur dann auf den Grid Manager, den Tenant Manager, die Grid Management API oder die Tenant Management API zugreifen, wenn ihre Anmeldeinformationen mithilfe des von Ihrer Organisation implementierten SSO-Anmeldevorgangs autorisiert sind. Lokale Benutzer können sich nicht bei StorageGRID anmelden.

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 die URL zum ersten Mal in diesem Browser aufrufen, werden Sie zur Eingabe einer Konto-ID aufgefordert.
   - 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 StorageGRID-Anmeldeseite wird nicht angezeigt, wenn Sie die vollständige URL für ein Mandantenkonto eingeben (d. h. einen vollständig qualifizierten Domänennamen oder eine IP-Adresse gefolgt von `/?accountId=20-digit-account-id`). Stattdessen werden Sie sofort zur SSO-Anmeldeseite Ihres Unternehmens weitergeleitet, auf der Sie die Möglichkeit habenmelden 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. Suchen Sie den Link **Abmelden** in der oberen rechten Ecke der Benutzeroberfläche.
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.

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.

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 die Entra-ID für SSO verwenden, kann es einige Minuten dauern, bis Sie von allen Admin-Knoten abgemeldet sind.
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.

Anforderungen und Überlegungen für SSO

Bevor Sie Single Sign-On (SSO) für ein StorageGRID-System aktivieren, lesen Sie die Anforderungen und Überlegungen.

Anforderungen an Identitätsanbieter

StorageGRID unterstützt die folgenden SSO-Identitätsanbieter (IdP):

- Active Directory Federation Service (AD FS)
- Microsoft Entra ID
- 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 • Entra-ID • PingFederate
Entra-ID	Entra-ID

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 , oder höher verwenden "KB3201845-Update".

Zusätzlichen Anforderungen

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

Überlegungen zur Entra-ID

Wenn Sie Entra ID als SSO-Typ verwenden und Benutzer über Benutzerprinzipalnamen verfügen, die nicht sAMAccountName als Präfix verwenden, können Anmeldeprobleme auftreten, wenn StorageGRID die Verbindung zum LDAP-Server verliert. Um Benutzern die Anmeldung zu ermöglichen, müssen Sie die Verbindung zum LDAP-Server wiederherstellen.

Serverzertifikate-Anforderungen

Standardmäßig verwendet StorageGRID auf jedem Admin-Knoten ein Verwaltungsschnittstellenzertifikat, um den Zugriff auf den Grid Manager, den Tenant Manager, die Grid Management API und die Tenant Management API zu sichern. Wenn Sie Vertrauensstellungen der vertrauenden Seite (AD FS), Unternehmensanwendungen (Entra ID) oder Dienstanbieterverbindungen (PingFederate) für StorageGRID konfigurieren, verwenden Sie das Serverzertifikat als Signaturzertifikat für StorageGRID Anfragen.

Wenn Sie noch nicht"Ein benutzerdefiniertes Zertifikat für die Managementoberfläche konfiguriert", sollten Sie dies 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 Befehlsshell des Knotens anmelden und zum Verzeichnis wechseln `/var/local/mgmt-api`. Ein benutzerdefiniertes Serverzertifikat wird benannt `custom-server.crt`. Das Standardserverzertifikat des Knotens lautet `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 über externe Firewall".

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.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben "Bestimmte 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 **Zugriffsverwaltung** > **Identitätsföderation**.
   c. Bestätigen Sie, dass das Kontrollkästchen **Enable Identity Federation** nicht aktiviert ist.
   d. Wenn dies der Fall ist, bestätigen Sie, dass keine föderierten Gruppen mehr für dieses Mandantenkonto benötigt werden, 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** > **Admingruppen**.
   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 **Mandanten** 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** aus.

      Die Seite Mandant wird angezeigt.

   e. Wählen Sie das Mandantenkonto aus, wählen Sie **Anmelden** und melden Sie sich als lokaler Root-Benutzer beim Mandantenkonto an.
   f. Wählen Sie im Mandanten-Manager **Zugriffsverwaltung** > **Gruppen**.

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

h. Abmelden.

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

Verwandte Informationen

- "Voraussetzungen und Überlegungen für Single Sign-On"
- "Managen von Admin-Gruppen"
- "Verwenden Sie ein Mandantenkonto"

SSO konfigurieren

Sie können dem Assistenten „SSO konfigurieren“ folgen und in den Sandbox-Modus wechseln, um Single Sign-On (SSO) zu konfigurieren und zu testen, bevor Sie es für alle StorageGRID Benutzer aktivieren. Nachdem SSO aktiviert wurde, können Sie bei Bedarf in den Sandbox-Modus zurückkehren, um die Konfiguration zu ändern oder erneut zu testen.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Root-Zugriffsberechtigung".
- Sie haben eine Identitätsföderation für Ihr StorageGRID System konfiguriert.
- Für den Identitätsverbund **LDAP-Diensttyp** haben Sie je nach dem SSO-Identitätsanbieter, den Sie verwenden möchten, entweder Active Directory oder Entra ID ausgewählt.

Konfigurierter LDAP-Servicetyp	Optionen für SSO-Identitätsanbieter
Active Directory Federation Service (AD FS)	• Active Directory • Entra-ID • PingFederate
Entra-ID	Entra-ID

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 Entra ID enthält einen User Principal Name (UPN).

Damit StorageGRID (der Dienstanbieter) und der SSO-Identitätsanbieter sicher über Benutzerauthentifizierungsanforderungen kommunizieren können, führen Sie die folgenden Aufgaben aus:

1. Konfigurieren Sie die Einstellungen in StorageGRID.
2. Verwenden Sie die Software des SSO-Identitätsanbieters, um für jeden Admin-Knoten eine Vertrauensstellung der vertrauenden Partei (AD FS), eine Unternehmensanwendung (Entra ID) oder einen Dienstanbieter (PingFederate) zu erstellen.
3. Kehren Sie zu StorageGRID zurück, um SSO zu aktivieren.

Der Sandbox-Modus erleichtert die Durchführung dieser Hin- und Her-Konfiguration und das Testen aller Ihrer Einstellungen, bevor Sie SSO aktivieren. Wenn Sie den Sandbox-Modus verwenden, können sich Benutzer nicht per SSO anmelden.

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Einmaliges Anmelden**. Die Seite „Single Sign-On“ wird angezeigt.

   Wenn die Schaltfläche „SSO-Einstellungen konfigurieren“ deaktiviert ist, bestätigen Sie, dass Sie den Identitätsanbieter als Verbundidentitätsquelle konfiguriert haben. Weitere Informationen finden Sie unter "Voraussetzungen und Überlegungen für Single Sign-On" .

2. Wählen Sie **SSO-Einstellungen konfigurieren**. Die Seite „Identitätsanbieterdetails angeben“ wird angezeigt.

Geben Sie die Details des Identitätsanbieters an

Schritte

1. Wählen Sie aus der Dropdown-Liste den **SSO-Typ** aus.
2. Wenn Sie Active Directory als SSO-Typ ausgewählt haben, geben Sie den **Verbunddienstnamen** für den Identitätsanbieter genau so ein, 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**. Wählen Sie im Menü Aktion die Option **Eigenschaften des Föderationsdienstes bearbeiten** aus. Der Name des Föderationsdienstes wird im zweiten Feld angezeigt.

3. 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.

     Wenn Sie das Zertifizierungsstellenzertifikat ändern, führen Sie sofort "Starten Sie den Management-API-Service auf den Admin-Nodes neu"eine erfolgreiche SSO-Prüfung im Grid Manager durch.

4. Wählen Sie **Weiter**. Die Seite „Relying Party Identifier angeben“ wird angezeigt.

Geben Sie die Kennung der vertrauenden Partei an

1. Füllen Sie die Felder auf der Seite „Identifikator der vertrauenden Seite angeben“ basierend auf dem von Ihnen ausgewählten SSO-Typ aus.

Active Directory

a. Geben Sie die **Relying Party Identifier** für StorageGRID an. Dieser Wert steuert den Namen, den Sie für jede Vertrauensstellung der vertrauenden Seite in AD FS verwenden.

   - Wenn Ihr Grid beispielsweise nur über einen Admin-Knoten verfügt und Sie in Zukunft nicht mehr Admin-Knoten hinzufügen möchten, geben Sie `SG` oder `StorageGRID`ein.
   - Wenn Ihr Raster mehr als einen Admin-Knoten enthält, fügen Sie die Zeichenfolge ein `[HOSTNAME]` im Bezeichner. Beispiel: `SG-[HOSTNAME]` . Durch Einfügen dieser Zeichenfolge wird eine Tabelle erstellt, die die Kennung der vertrauenden Partei für jeden Admin-Knoten im Raster basierend auf dem 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.

b. Wählen Sie **Speichern und Sandbox-Modus aufrufen**.

Entra-ID

a. Geben Sie im Abschnitt „Unternehmensanwendung“ den **Namen der Unternehmensanwendung** für StorageGRID an. Dieser Wert steuert den Namen, den Sie für jede Unternehmensanwendung in Entra ID verwenden.

   - Wenn Ihr Grid beispielsweise nur über einen Admin-Knoten verfügt und Sie in Zukunft nicht mehr Admin-Knoten hinzufügen möchten, geben Sie `SG` oder `StorageGRID`ein.
   - Wenn Ihr Raster mehr als einen Admin-Knoten enthält, fügen Sie die Zeichenfolge ein `[HOSTNAME]` im Bezeichner. Beispiel: `SG-[HOSTNAME]` . Durch Einfügen dieser Zeichenfolge wird eine Tabelle erstellt, die basierend auf dem Hostnamen des Knotens einen Unternehmensanwendungsnamen für jeden Admin-Knoten in Ihrem System anzeigt.

   > 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.

b. Befolgen Sie die Schritte in"Erstellen Sie Unternehmensanwendungen in Entra ID" um für jeden in der Tabelle aufgeführten Admin-Knoten eine Unternehmensanwendung zu erstellen.

c. Kopieren Sie aus der Entra-ID die URL der Verbundmetadaten für jede Unternehmensanwendung. Fügen Sie diese URL dann in das entsprechende Feld **Federation metadata URL** in StorageGRID ein.

d. Nachdem Sie eine Föderationsmetadaten-URL für alle Admin-Knoten kopiert und eingefügt haben, wählen Sie **Speichern und in den Sandbox-Modus wechseln**.

PingFederate

a. 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 über einen Admin-Knoten verfügt und Sie in Zukunft nicht mehr Admin-Knoten hinzufügen möchten, geben Sie `SG` oder `StorageGRID`ein.
   - Wenn Ihr Raster mehr als einen Admin-Knoten enthält, fügen Sie die Zeichenfolge ein `[HOSTNAME]` im Bezeichner. Beispiel: `SG-[HOSTNAME]` . Durch Einfügen dieser

Zeichenfolge wird eine Tabelle erstellt, die die SP Verbindungs-ID für jeden Admin-Knoten in Ihrem System basierend auf dem Hostnamen des Knotens anzeigt.

> 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.

b. 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>
   ```

c. Wählen Sie **Speichern und Sandbox-Modus aufrufen**.

Konfigurieren Sie Vertrauensstellungen von Drittanbietern, Unternehmensanwendungen oder SP-Verbindungen

Nachdem Sie die Konfiguration gespeichert und in den Sandbox-Modus gewechselt haben, können Sie die Konfiguration für den ausgewählten SSO-Typ abschließen und testen.

StorageGRID kann so lange wie nötig im Sandbox-Modus bleiben. Allerdings können sich nur Verbundbenutzer und lokale Benutzer anmelden.

Active Directory

Schritte

1. Wechseln Sie zu Active Directory Federation Services (AD FS).
2. Erstellen Sie eine oder mehrere Vertrauensstellungen der vertrauenden Seite für StorageGRID und verwenden Sie dabei die einzelnen Kennungen der vertrauenden Seite, die in der Tabelle auf der Seite „SSO konfigurieren“ angezeigt werden.

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

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

Entra-ID

Schritte

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** > **Zugriffskontrolle** > **Einmaliges Anmelden**.
   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 in"Erstellen Sie Unternehmensanwendungen in Entra ID" um die SAML-Metadatendatei für jeden Admin-Knoten in die entsprechende Entra ID-Unternehmensanwendung hochzuladen.

PingFederate

Schritte

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** > **Zugriffskontrolle** > **Einmaliges Anmelden**.
   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-Knoten (angezeigt in der Tabelle auf der Seite „SSO konfigurieren“) und die SAML-Metadaten, die Sie für diesen Admin-Knoten heruntergeladen haben.

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

Testkonfiguration

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

Active Directory

Schritte

1. Suchen Sie auf der Seite „SSO konfigurieren“ den Link zum Schritt „Konfiguration testen“ des Assistenten.

   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.

Entra-ID

Schritte

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.
   - 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

Schritte

1. Wählen Sie auf der Seite „SSO konfigurieren“ den ersten Link in der Sandbox-Modus-Nachricht 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.
   - 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.

Schritte

1. Wählen Sie im Schritt „Testkonfiguration“ des SSO-Konfigurationsassistenten die Option „SSO aktivieren“ aus.
2. Überprüfen Sie die Warnmeldung und wählen Sie **SSO aktivieren**.

   Single Sign-On ist jetzt aktiviert. Die Seite „Single Sign-On“ wird angezeigt und enthält jetzt die Details für das gerade konfigurierte SSO.

3. Um die Konfiguration zu bearbeiten, wählen Sie **Bearbeiten**.
4. Um die einmalige Anmeldung zu deaktivieren, wählen Sie **SSO deaktivieren**.

Wenn Sie das Azure-Portal verwenden und von demselben Computer aus auf StorageGRID zugreifen, den Sie für den Zugriff auf Entra ID verwenden, stellen Sie sicher, dass der Azure-Portalbenutzer auch ein autorisierter StorageGRID Benutzer ist (ein Benutzer in einer Verbundgruppe, der in StorageGRID importiert wurde, oder melden Sie sich vom Azure-Portal ab, bevor Sie versuchen, sich bei StorageGRID anzumelden.

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.

Bevor Sie beginnen

- Sie haben Single Sign-On für StorageGRID konfiguriert und als SSO-Typ **AD FS** ausgewählt.
- Du hast"Sandbox-Modus aufgerufen" im Grid Manager.
- Sie kennen den vollqualifizierten Domänennamen (oder die IP-Adresse) und die Kennung der vertrauenden Partei für jeden Admin-Knoten in Ihrem System. Sie finden diese Werte in der Detailtabelle „Admin-Knoten“ auf der StorageGRID -Seite „SSO konfigurieren“.

  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"
   ```

   - Geben Sie für *`Admin_Node_Identifier`* die ID der aussetzenden Partei für den Admin-Knoten genau so ein, wie sie auf der Seite Single Sign-On angezeigt wird. `SG-DC1-ADM1`Beispiel: .
   - Geben Sie für *`Admin_Node_FQDN`* 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** > **vertraut auf Partei**.

   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 zu Name ID** oder **UPN zu Name ID**.

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

g. Geben Sie in der Spalte LDAP Attribute der Zuordnungstabelle **objectGUID** ein oder wählen Sie **User-Principal-Name** aus.

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, überprüfen Sie, ob die Metadatenadresse der Föderation korrekt ist, oder geben Sie 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 Vertrauensstellungen der vertrauenden Parteien" um zu bestätigen, dass sie richtig konfiguriert sind.

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`

   Geben Sie für *`Admin_Node_FQDN`* 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. `SG-DC1-ADM1`Beispiel: .

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 zu Name ID** oder **UPN zu Name ID**.

   e. Wählen Sie im Attributspeicher die Option **Active Directory** aus.
   f. Geben Sie in der Spalte LDAP Attribute der Zuordnungstabelle **objectGUID** ein oder wählen Sie **User-Principal-Name** aus.
   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, überprüfen Sie, ob die Metadatenadresse der Föderation korrekt ist, oder geben Sie 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 Vertrauensstellungen der vertrauenden Parteien" um zu bestätigen, dass sie richtig konfiguriert sind.

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. `SG-DC1-ADM1`Beispiel: .

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`

   Geben Sie für *`Admin_Node_FQDN`* 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`

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

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 zu Name ID** oder **UPN zu Name ID**.

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

   d. Geben Sie in der Spalte LDAP Attribute der Zuordnungstabelle **objectGUID** ein oder wählen Sie **User-Principal-Name** aus.

   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
```

Geben Sie für *`Admin_Node_FQDN`* 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 in das `/var/local/mgmt-api` Verzeichnis des Admin-Knotens, und fügen Sie die Zertifikatdatei hinzu `custom-server.crt`.

> Die Verwendung des Standardzertifikats des Admin-Knotens (`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 Vertrauensstellungen der vertrauenden Parteien" um zu bestätigen, dass sie richtig konfiguriert sind.

Erstellen Sie Unternehmensanwendungen in Entra ID

Sie verwenden die Entra-ID, um für jeden Admin-Knoten in Ihrem System eine Unternehmensanwendung zu erstellen.

Bevor Sie beginnen

- Sie haben mit der Konfiguration der einmaligen Anmeldung für StorageGRID begonnen und **Entra ID** als SSO-Typ ausgewählt.
- Du hast"Sandbox-Modus aufgerufen" im Grid Manager.
- Sie haben den **Namen der Unternehmensanwendung** für jeden Admin-Knoten in Ihrem System. Sie können diese Werte aus der Detailtabelle des Admin-Knotens auf der Seite „SSO konfigurieren“ 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 mit der Erstellung von Unternehmensanwendungen in Entra ID.
- Sie haben ein Entra-ID-Konto mit einem aktiven Abonnement.
- Sie haben eine der folgenden Rollen im Entra ID-Konto: Globaler Administrator, Cloud-Anwendungsadministrator, Anwendungsadministrator oder Besitzer des Dienstprinzipals.

Zugang zur Entra-ID

Schritte

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

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

Um die SSO-Konfiguration für Entra ID in StorageGRID zu speichern, müssen Sie Entra ID verwenden, um für jeden Admin-Knoten eine Unternehmensanwendung zu erstellen. Sie kopieren die URLs der Föderationsmetadaten von Entra ID und fügen sie in die entsprechenden Felder **Föderationsmetadaten-URL** auf der Seite „SSO konfigurieren“ ein.

Schritte

1. Wiederholen Sie die folgenden Schritte für jeden Admin-Node.
   a. Wählen Sie im Bereich „Entra ID Enterprise-Anwendungen“ **Neue Anwendung** aus.
   b. Wählen Sie **Erstellen Sie Ihre eigene Anwendung**.
   c. Geben Sie als Namen den **Namen der Unternehmensanwendung** ein, den Sie aus der Tabelle mit den Admin-Knotendetails auf der Seite „SSO konfigurieren“ 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 zur Seite „SSO konfigurieren“ und fügen Sie die URL in das Feld „URL der Verbundmetadaten“ ein, die dem von Ihnen verwendeten „Namen der Unternehmensanwendung“ entspricht.
2. Nachdem Sie für jeden Admin-Knoten eine URL mit Verbundmetadaten eingefügt und alle anderen erforderlichen Änderungen an der SSO-Konfiguration vorgenommen haben, wählen Sie auf der Seite „SSO konfigurieren“ **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.

Schritte

1. Wiederholen Sie diese Schritte für jeden Admin-Node.
   a. Melden Sie sich über den Admin-Node bei StorageGRID an.
   b. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Einmaliges Anmelden**.
   c. Wählen Sie die Schaltfläche, um die SAML-Metadaten für diesen Admin-Node herunterzuladen.
   d. Speichern Sie die Datei, die Sie in Entra ID hochladen.

Hochladen von SAML-Metadaten in jede Enterprise-Applikation

Nachdem Sie für jeden StorageGRID Admin-Knoten eine SAML-Metadatendatei heruntergeladen haben, führen Sie in Entra ID die folgenden Schritte aus:

Schritte

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. "Testen Sie jede Anwendung" .

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.

Bevor Sie beginnen

- Sie haben Single Sign-On für StorageGRID konfiguriert und als SSO-Typ * Ping föderate* ausgewählt.
- Du hast"Sandbox-Modus aufgerufen" im Grid Manager.
- Sie haben die * SP Verbindungs-ID* für jeden Admin-Knoten in Ihrem System. Sie finden diese Werte in der Detailtabelle „Admin-Knoten“ auf der Seite „SSO konfigurieren“.
- 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 den "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 in StorageGRID verwendet "Identitätsföderation wird konfiguriert"haben.

- **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.

Schritte

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 dieGültigkeitsprüfung für Kennwortausweise Sie erstellt haben.
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.

Schritte

1. Gehen Sie zu **Sicherheit** > **Signieren & Entschlüsseln Schlüssel & Zertifikate**.
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. Gehen Sie dann zu, um zusätzliche Verbindungen zu Erstellen Sie zusätzliche SP-Verbindungenerstellen, die Sie benötigen.

Wählen Sie den SP-Verbindungstyp

Schritte

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

Schritte

1. Wählen Sie auf der Registerkarte Metadaten importieren die Option **Datei**.
2. Wählen Sie die SAML-Metadatendatei aus, die Sie von der Seite „SSO konfigurieren“ für den Admin-Knoten heruntergeladen haben.
3. Überprüfen Sie die Metadatenübersicht 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

Schritte

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. Wählen Sie unter Vertrag verlängern die Option **Löschen**, um das nicht verwendete , zu entfernen `urn:oid`.

Adapterinstanz zuordnen

Schritte

1. Wählen Sie auf der Registerkarte Authentication Source Mapping die Option **Map New Adapter Instance**.
2. Wählen Sie auf der Registerkarte Adapterinstanz die erstellte ausAdapterinstanz.
3. Wählen Sie auf der Registerkarte Zuordnungsmethode die Option **Weitere Attribute aus einem Datenspeicher abrufen** aus.
4. Wählen Sie auf der Registerkarte Attributquelle und Benutzersuche die Option **Attributquelle hinzufügen** aus.
5. Geben Sie auf der Registerkarte Datenspeicher eine Beschreibung ein, und wählen Sie die hinzugefügte ausDatastore.
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 und fügen Sie für die Root-Objektklasse eines der folgenden Attribute hinzu: **ObjectGUID** oder **userPrincipalName**.
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 Contract Fulfillment die Option **LDAP (Attribut)** aus der Dropdown-Liste Source aus und wählen Sie entweder **objectGUID** oder **userPrincipalName** aus der Dropdown-Liste Value 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

Schritte

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 (**POST** für Bindung und für Endpunkt-URL) importiert wurden

`/api/saml-response`.

3. Akzeptieren Sie auf der Registerkarte SLO Service URLs die Standardwerte, die aus den StorageGRID SAML-Metadaten (**REDIRECT** für Bindung und für Endpunkt-URL importiert wurden `/api/saml-logout`.
4. Deaktivieren Sie auf der Registerkarte Allowable SAML Bindings **ARTIFACT** und **SOAP**. Es sind nur **POST** und **REDIRECT** erforderlich.
5. Lassen Sie auf der Registerkarte Signature Policy die Kontrollkästchen **require AUTHN Requests to be signed** und **always Sign Assertion** ausgewählt.
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

Schritte

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 dieSignieren 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.

Schritte

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-Erstellung konfigurieren > Attributvertrag** aus.

c. Löschen Sie den Eintrag für **Urne:oid**.

d. Wählen Sie **Speichern**.

SSO deaktivieren

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.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben "Bestimmte Zugriffsberechtigungen".

Schritte

1. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Einmaliges Anmelden**.

   Die Seite Single Sign-On wird angezeigt.

2. Wählen Sie **SSO deaktivieren**.
3. Wählen Sie **Ja**.

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

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.

SSO für einen Admin-Knoten vorübergehend deaktivieren und wieder aktivieren

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.

Bevor Sie beginnen

- Sie haben "Bestimmte 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 werden beibehalten, sofern 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 in der Datei aufgeführte Passwort ein `Passwords.txt`.
   c. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
   d. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.

   Wenn Sie als root angemeldet sind, wechselt die Eingabeaufforderung von `$` zu `#`.

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** > **Zugriffskontrolle** > **Einmaliges Anmelden**.
   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.

- Grid-Node neu booten: `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.

Grid-Verbund verwenden

Was ist Grid Federation?

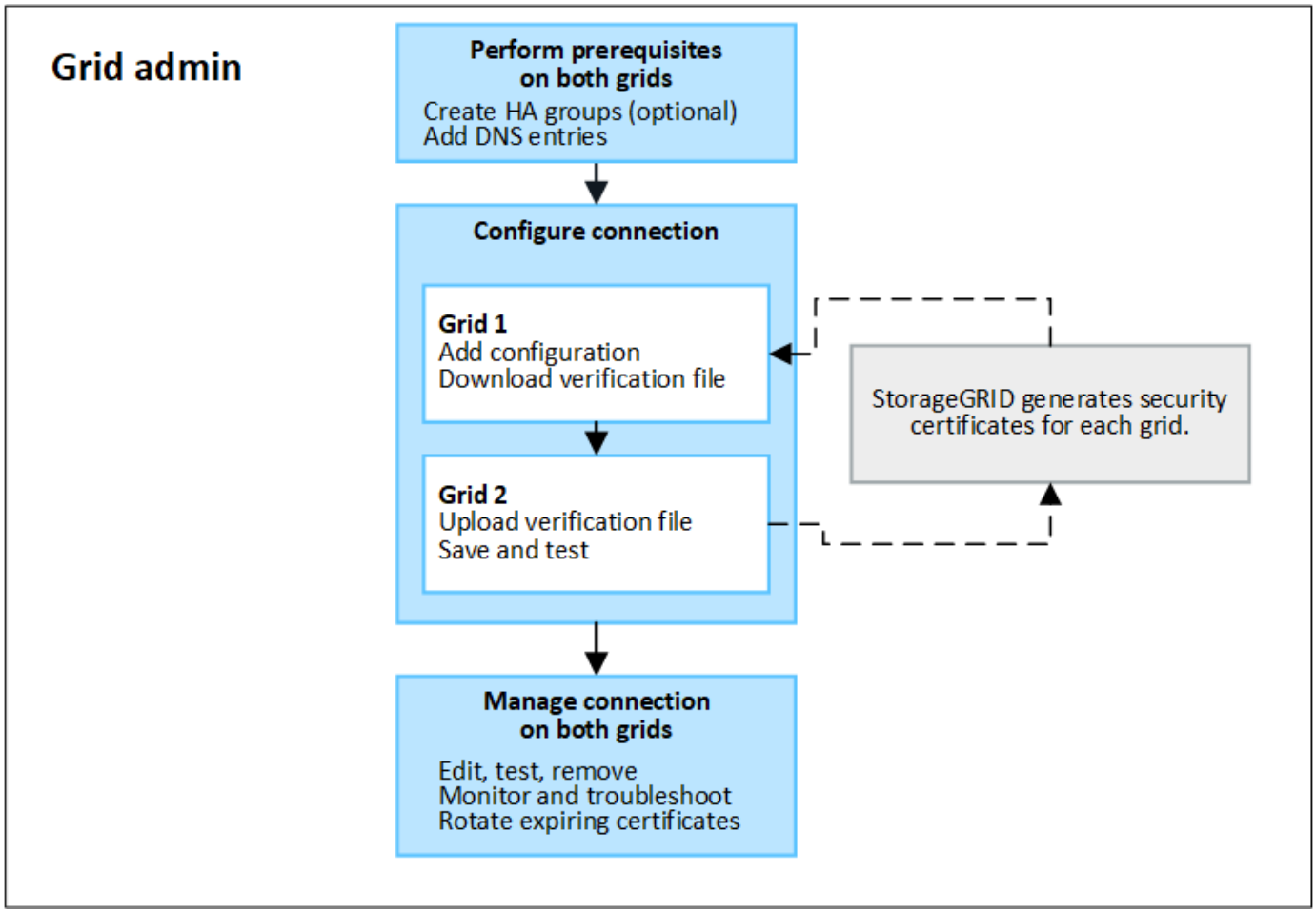
Mithilfe des Grid-Verbunds können Mandanten geklont und ihre Objekte zwischen zwei StorageGRID Systemen für das Disaster Recovery repliziert werden.

Was ist eine Netzverbundverbindung?

Eine Grid-Verbundverbindung ist eine bidirektionale, zuverlässige und sichere Verbindung zwischen dem Administrator und den Gateway Nodes in zwei StorageGRID Systemen.

Workflow für Grid-Verbund

Das Workflow-Diagramm fasst die Schritte zur Konfiguration einer Grid Federation-Verbindung zwischen zwei Grids zusammen.



Überlegungen und Anforderungen für Netzverbundverbindungen

- Auf den Grids, die für den Grid-Verbund verwendet werden, müssen StorageGRID-Versionen ausgeführt werden, die entweder identisch sind oder nicht mehr als einen Hauptversionsunterschied aufweisen.

  Weitere Informationen zu Versionsanforderungen finden Sie im "Versionshinweise".

- Ein Grid kann eine oder mehrere Netzverbundverbindungen zu anderen Grids haben. Jede Netzverbundverbindung ist unabhängig von allen anderen Verbindungen. Wenn beispielsweise Grid 1 eine Verbindung mit Grid 2 und eine zweite Verbindung mit Grid 3 hat, besteht keine implizierte Verbindung zwischen Grid 2 und Grid 3.
- Netzverbundverbindungen sind bidirektional. Nachdem die Verbindung hergestellt wurde, können Sie die Verbindung von beiden Grids aus überwachen und verwalten.
- Mindestens eine Netzverbundverbindung muss vorhanden sein, bevor Sie oder verwenden können"Konto-Klon""Grid-übergreifende Replizierung".

Netzwerkanforderungen und IP-Adresse

- Grid-Verbindungen können im Grid-Netzwerk, im Admin-Netzwerk oder im Client-Netzwerk auftreten.
- Eine Netzverbundverbindung verbindet ein Grid mit einem anderen Grid. Die Konfiguration für jedes Grid gibt einen Grid-Verbundendpunkt auf dem anderen Grid an, der aus Admin-Nodes, Gateway-Nodes oder beidem besteht.
- Die Best Practice besteht darin, die Gateway- und Admin-Nodes in jedem Grid zu verbinden"Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen". Durch die Verwendung von HA-Gruppen wird sichergestellt, dass die Verbindungen mit dem Grid-Verbund online bleiben, wenn die Nodes nicht mehr verfügbar sind. Wenn die aktive Schnittstelle in einer der HA-Gruppen ausfällt, kann die Verbindung eine Backup-Schnittstelle verwenden.
- Das Erstellen einer Grid-Federation-Verbindung, die die IP-Adresse eines einzelnen Admin-Node oder Gateway-Node verwendet, wird nicht empfohlen. Wenn der Node nicht mehr verfügbar ist, ist auch die Verbindung zum Grid-Verbund nicht mehr verfügbar.
- "Grid-übergreifende Replizierung" Der Objekte erfordert, dass die Storage Nodes in jedem Grid auf die konfigurierten Admin- und Gateway-Nodes im anderen Grid zugreifen können. Vergewissern Sie sich für jedes Grid, dass alle Storage-Nodes eine Route mit hoher Bandbreite als Admin-Nodes oder Gateway-Nodes haben, die für die Verbindung verwendet werden.

Verwenden Sie FQDNs, um die Verbindung auszugleichen

Verwenden Sie für eine Produktionsumgebung vollständig qualifizierte Domänennamen (FQDNs), um jedes Raster in der Verbindung zu identifizieren. Erstellen Sie dann die entsprechenden DNS-Einträge wie folgt:

- Der FQDN für Grid 1, der einer oder mehreren virtuellen IP-Adressen (VIP) für HA-Gruppen in Grid 1 oder der IP-Adresse eines oder mehrerer Admin- oder Gateway-Nodes in Grid 1 zugeordnet ist.
- Der FQDN für Grid 2, der einer oder mehreren VIP-Adressen für Grid 2 oder der IP-Adresse eines oder mehrerer Administrator- oder Gateway-Knoten in Grid 2 zugeordnet ist.

Wenn Sie mehrere DNS-Einträge verwenden, werden Anforderungen zur Verwendung der Verbindung wie folgt ausgeglichen:

- DNS-Einträge, die den VIP-Adressen mehrerer HA-Gruppen zugeordnet sind, werden für den Lastausgleich zwischen den aktiven Nodes in den HA-Gruppen eingesetzt.
- DNS-Einträge, die den IP-Adressen mehrerer Admin-Nodes oder Gateway-Nodes zugeordnet sind,

werden zwischen den zugeordneten Nodes gleichmäßig verteilt.

Port-Anforderungen

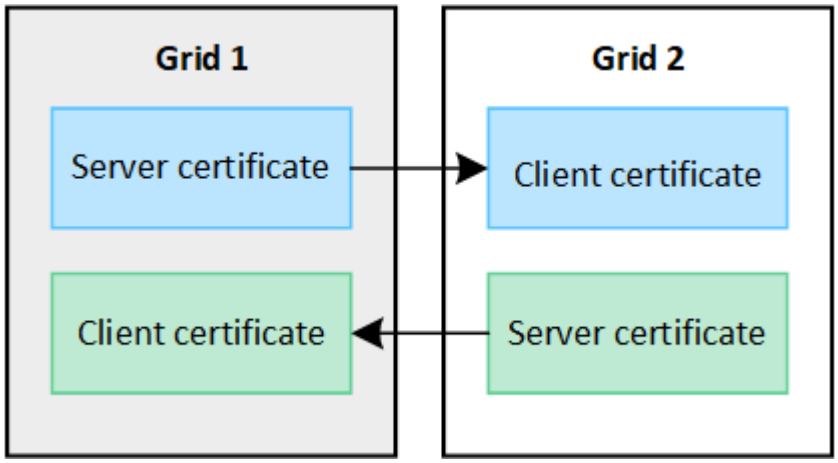
Beim Erstellen einer Grid-Federation-Verbindung können Sie alle nicht verwendeten Portnummern zwischen 23000 und 23999 angeben. Beide Grids in dieser Verbindung verwenden den gleichen Port.

Sie müssen sicherstellen, dass kein Node in einem Grid diesen Port für andere Verbindungen verwendet.

Zertifikatanforderungen

Wenn Sie eine Grid-Federation-Verbindung konfigurieren, generiert StorageGRID automatisch vier SSL-Zertifikate:

- Server- und Client-Zertifikate zur Authentifizierung und Verschlüsselung von Informationen, die von Grid 1 an Grid 2 gesendet werden
- Server- und Client-Zertifikate zur Authentifizierung und Verschlüsselung von Informationen, die von Grid 2 an Grid 1 gesendet werden



Standardmäßig sind die Zertifikate 730 Tage (2 Jahre) gültig. Wenn diese Zertifikate in der Nähe ihres Ablaufdatums liegen, erinnert die Warnung **Ablauf des Grid Federation Certificate** Sie daran, die Zertifikate zu drehen, was Sie mit dem Grid Manager tun können.

> Wenn die Zertifikate an einem Ende der Verbindung ablaufen, funktioniert die Verbindung nicht mehr. Die Datenreplikation steht aus, bis die Zertifikate aktualisiert werden.

Weitere Informationen .

- "Erstellen von Grid Federation-Verbindungen"
- "Grid-Verbindungen verwalten"
- "Fehler beim Grid-Verbund beheben"

Was ist Account-Klon?

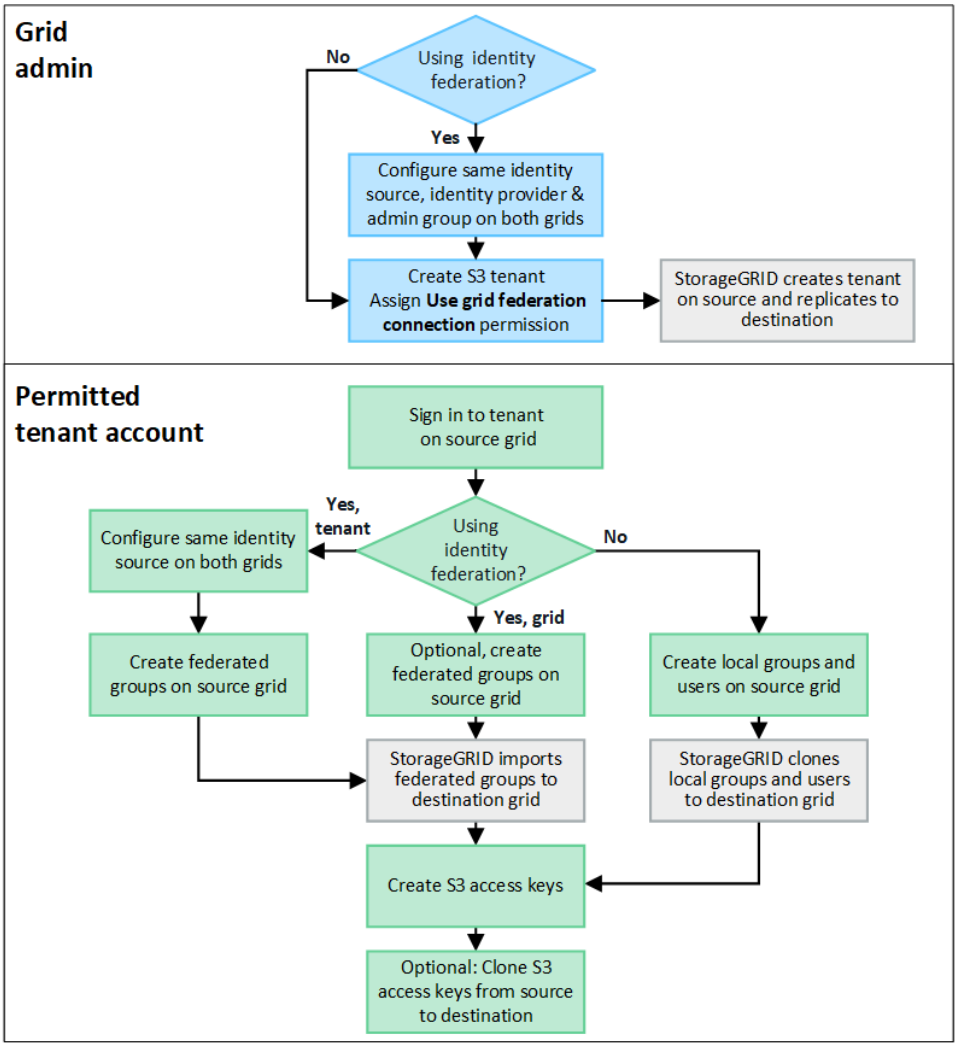
Account-Klon ist die automatische Replizierung eines Mandantenkontos, von Mandantengruppen, von Mandantenbenutzern und optional von S3-Zugriffsschlüsseln zwischen den StorageGRID-Systemen in einem "Netzverbundverbindung".

Kontoklone ist für erforderlich"Grid-übergreifende Replizierung". Durch das Klonen von Kontoinformationen

aus einem Quell-StorageGRID-System auf ein Ziel-StorageGRID-System wird sichergestellt, dass Mandantenbenutzer und -Gruppen auf die entsprechenden Buckets und Objekte in beiden Grids zugreifen können.

Workflow für Konto-Klon

Das Workflow-Diagramm zeigt die Schritte, die Grid-Administratoren und berechtigte Mandanten zum Einrichten des Kontoklons durchführen. Diese Schritte werden nach dem durchgeführt"Die Grid-Federation-Verbindung ist konfiguriert".



Grid-Administrator-Workflow

Die Schritte, die Grid-Administratoren durchführen, hängen davon ab, ob die StorageGRID-Systeme in der "Netzverbundverbindung"Single Sign-On (SSO) oder Identity Federation verwenden.

SSO für Kontoklone konfigurieren (optional)

Wenn eines der StorageGRID-Systeme in der Grid-Federation-Verbindung SSO verwendet, müssen beide Grids SSO verwenden. Vor dem Erstellen der Mandantenkonten für den Grid-Verbund müssen die Grid-Administratoren der Quell- und Zielraster des Mandanten die folgenden Schritte durchführen.

Schritte

1. Konfigurieren Sie dieselbe Identitätsquelle für beide Raster. Siehe "Verwenden Sie den Identitätsverbund".

2. Konfigurieren Sie für beide Grids denselben SSO-Identitätsanbieter (IdP). Sehen "Konfigurieren Sie Single Sign-On" .
3. "Erstellen Sie dieselbe Administratorgruppe" Auf beiden Rastern durch Importieren derselben Verbundgruppe.

   Wenn Sie den Mandanten erstellen, wählen Sie diese Gruppe aus, um die anfängliche Root-Zugriffsberechtigung für die Quell- und Zielmandantenkonten zu erhalten.

   > Wenn diese Administratorgruppe vor dem Erstellen des Mandanten nicht auf beiden Grids vorhanden ist, wird der Mandant nicht am Ziel repliziert.

Konfigurieren der Identity Federation auf Grid-Ebene für Kontoklone (optional)

Wenn eines der StorageGRID-Systeme Identitätsföderation ohne SSO verwendet, müssen beide Grids Identitätsföderation verwenden. Vor dem Erstellen der Mandantenkonten für den Grid-Verbund müssen die Grid-Administratoren der Quell- und Zielraster des Mandanten die folgenden Schritte durchführen.

Schritte

1. Konfigurieren Sie dieselbe Identitätsquelle für beide Raster. Siehe "Verwenden Sie den Identitätsverbund".
2. Optional, wenn eine föderierte Gruppe erste Root-Zugriffsberechtigungen für die Quell- und Zielmandanten-Konten hat, "Erstellen Sie dieselbe Administratorgruppe" auf beiden Grids durch Importieren derselben föderierten Gruppe.

   > Wenn Sie einer föderierten Gruppe Root-Zugriffsberechtigungen zuweisen, die nicht in beiden Grids vorhanden ist, wird der Mandant nicht in das Zielraster repliziert.

3. Wenn Sie nicht möchten, dass eine föderierte Gruppe erste Root-Zugriffsberechtigungen für beide Konten hat, geben Sie ein Passwort für den lokalen Root-Benutzer an.

Zulässiges S3-Mandantenkonto erstellen

Nach der optionalen Konfiguration von SSO oder Identity Federation führt ein Grid-Administrator diese Schritte aus, um zu ermitteln, welche Mandanten Bucket-Objekte auf andere StorageGRID-Systeme replizieren können.

Schritte

1. Legen Sie fest, welches Raster das Quell-Grid des Mandanten für Account-Klonvorgänge sein soll.

   Das Grid, in dem der Tenant ursprünglich erstellt wurde, wird als *source Grid* des Tenants bezeichnet. Das Grid, in dem der Mandant repliziert wird, wird als *Destination Grid* des Mandanten bezeichnet.

2. Erstellen Sie in diesem Raster ein neues S3-Mandantenkonto, oder bearbeiten Sie ein vorhandenes Konto.
3. Weisen Sie die Berechtigung **Grid Federation connection** zu.
4. Wenn das Mandantenkonto seine eigenen föderierten Benutzer verwalten wird, weisen Sie die Berechtigung **eigene Identitätsquelle verwenden** zu.

   Wenn diese Berechtigung zugewiesen ist, müssen sowohl die Quell- als auch die Zielmandanten-Konten dieselbe Identitätsquelle konfigurieren, bevor verbundene Gruppen erstellt werden. Verbundene Gruppen, die dem Quellmandanten hinzugefügt werden, können nicht auf den Zielmandanten geklont werden, wenn nicht beide Grids dieselbe Identitätsquelle verwenden.

5. Wählen Sie eine bestimmte Netzverbundverbindung aus.
6. Speichern Sie die neue oder geänderte Serviceeinheit.

   Wenn ein neuer Mandant mit der Berechtigung **use Grid Federation connection** gespeichert wird, erstellt StorageGRID automatisch ein Replikat dieses Mandanten auf dem anderen Grid, wie folgt:

   - Beide Mandantenkonten haben die gleiche Konto-ID, den gleichen Namen, das gleiche Speicherkontingent und die gleichen Berechtigungen.
   - Wenn Sie eine föderierte Gruppe ausgewählt haben, die über Root-Zugriffsberechtigungen für den Mandanten verfügt, wird diese Gruppe auf den Zielmandanten geklont.
   - Wenn Sie einen lokalen Benutzer mit Root-Zugriffsberechtigungen für den Mandanten ausgewählt haben, wird dieser Benutzer auf den Zielmandanten geklont. Das Passwort für diesen Benutzer ist jedoch nicht geklont.

Weitere Informationen finden Sie unter "Management zulässiger Mandanten für Grid-Verbund".

Zulässiger Mandantenkonto-Workflow

Nachdem ein Mandant mit der Berechtigung **use Grid Federation connection** in das Zielraster repliziert wurde, können zugelassene Mandantenkonten diese Schritte durchführen, um Mandantengruppen, Benutzer und S3-Zugriffsschlüssel zu klonen.

Schritte

1. Melden Sie sich beim Mandantenkonto im Quellraster des Mandanten an.
2. Falls zulässig, konfigurieren Sie den Verbund auf den Quell- und Ziel-Mandantenkonten.
3. Erstellen Sie Gruppen und Benutzer auf dem Quellmandanten.

   Wenn neue Gruppen oder Benutzer auf dem Quellmandanten erstellt werden, klont StorageGRID sie automatisch auf dem Zielmandanten, es wird jedoch kein Klonen vom Ziel zurück zur Quelle erstellt.

4. Erstellen von S3 Zugriffsschlüsseln
5. Optional können Sie S3-Zugriffsschlüssel vom Quell-Mandanten zum Ziel-Mandanten klonen.

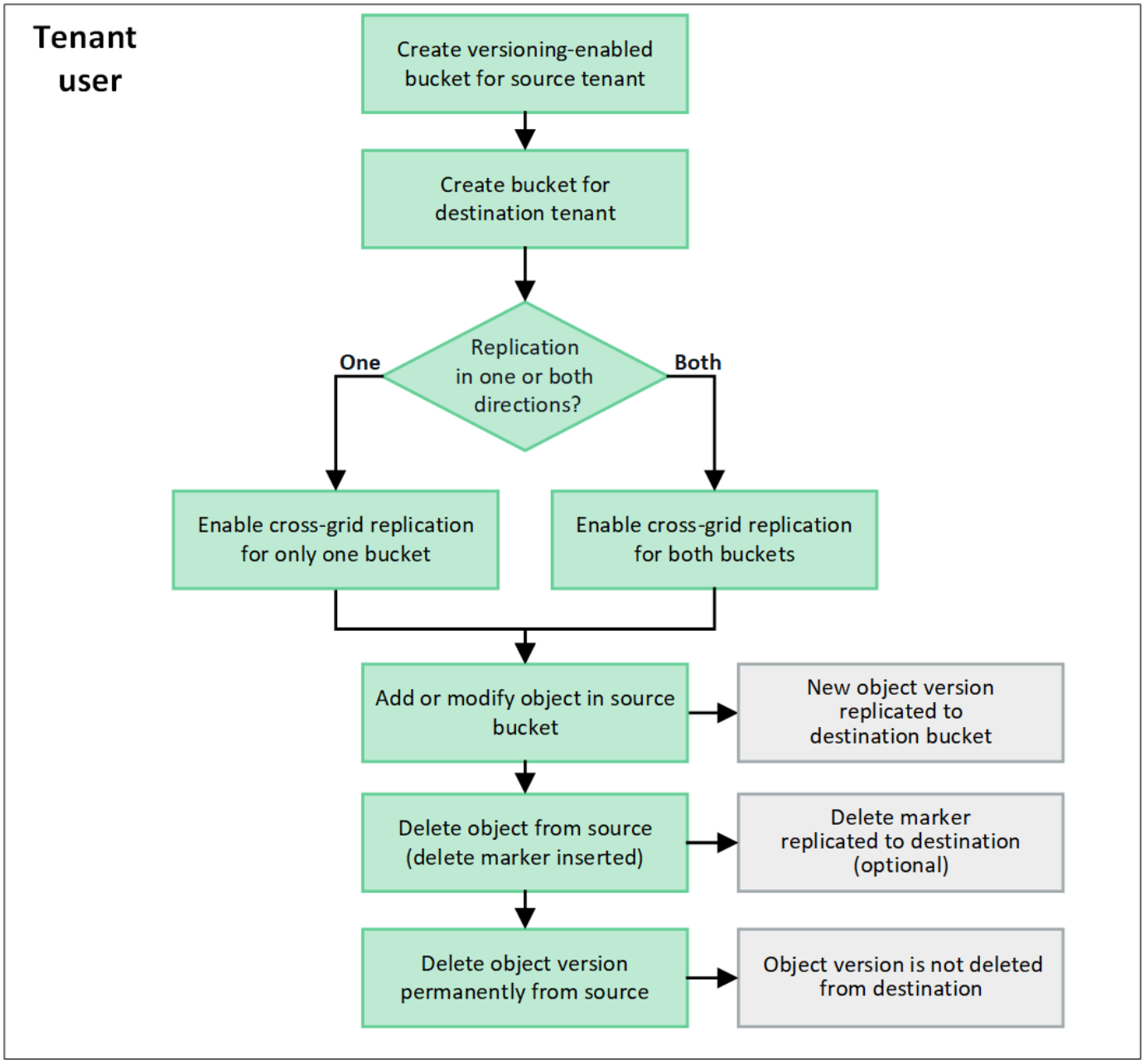
Details zum Workflow zulässiger Mandantenkonten und Informationen darüber, wie Gruppen, Benutzer und S3-Zugriffsschlüssel geklont werden, finden Sie unter "Klonen von Mandantengruppen und Benutzern" und "Klonen von S3-Zugriffsschlüsseln mithilfe der API".

Was ist Grid-übergreifende Replizierung?

Grid-übergreifende Replizierung ist die automatische Replizierung von Objekten zwischen ausgewählten S3 Buckets in zwei StorageGRID-Systemen, die in einem verbunden sind"Netzverbundverbindung". "Konto-Klon" Ist für die Grid-übergreifende Replizierung erforderlich.

Workflow für Grid-übergreifende Replizierung

Das Workflow-Diagramm fasst die Schritte zum Konfigurieren der Cross-Grid-Replikation zwischen Buckets auf zwei Grids zusammen.



Anforderungen für die Grid-übergreifende Replizierung

Wenn ein Mandantenkonto die Berechtigung **Grid-Föderationsverbindung verwenden** hat, um eine oder mehrere"Netzverbundverbindungen" , ein Mandantenbenutzer mit Root-Zugriffsberechtigung kann Buckets in den entsprechenden Mandantenkonten auf jedem Raster erstellen. Diese Eimer:

- Können unterschiedliche Namen haben
- Kann verschiedene Regionen haben
- Versionierung muss aktiviert sein
- Muss leer sein

Nachdem beide Buckets erstellt wurden, kann die Grid-übergreifende Replizierung für einen oder beide Buckets konfiguriert werden.

Weitere Informationen .

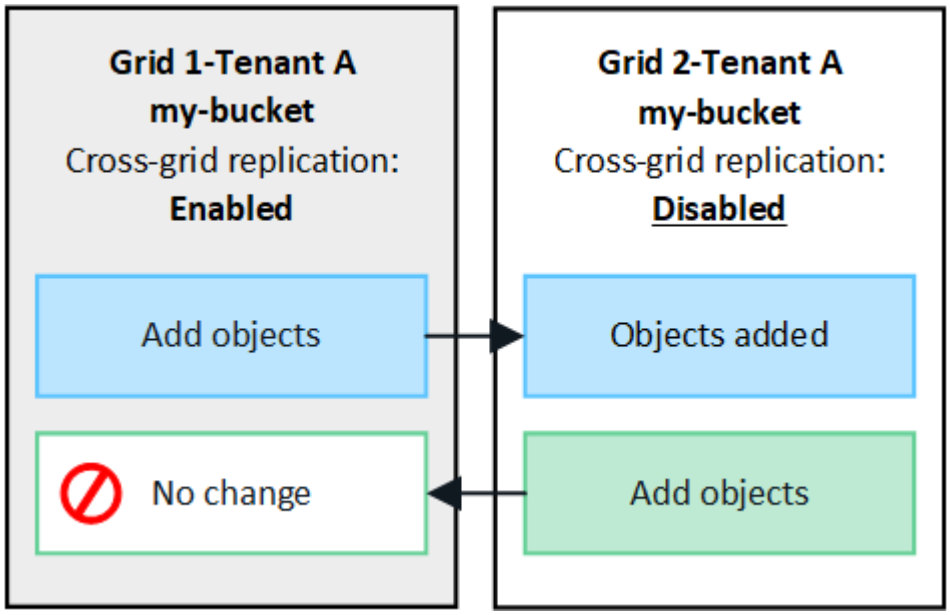
"Grid-übergreifende Replizierung managen"

Funktionsweise der Grid-übergreifenden Replizierung

Sie können die Cross-Grid-Replikation so konfigurieren, dass sie in eine oder in beide Richtungen erfolgt.

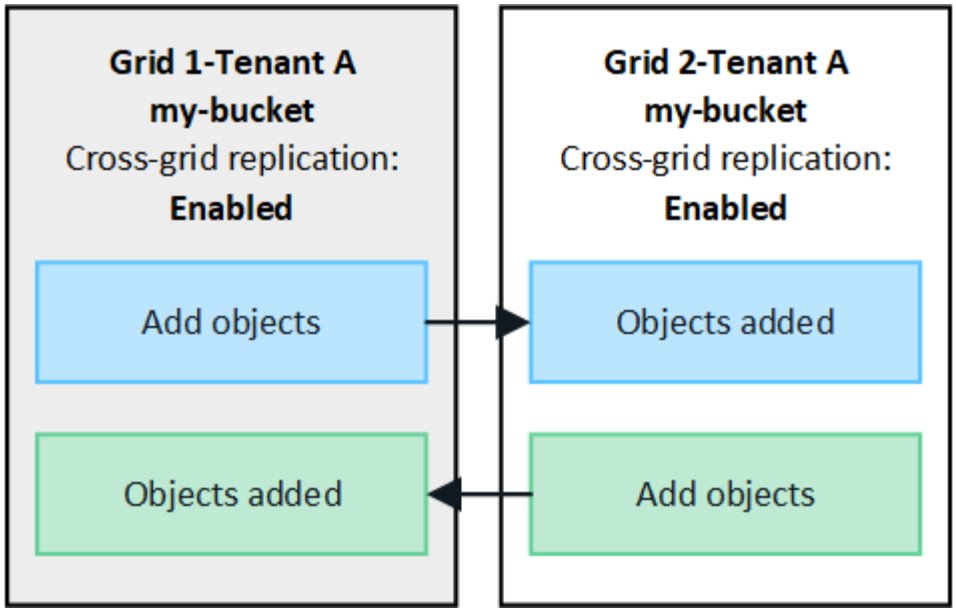
Replikation in eine Richtung

Wenn Sie die Cross-Grid-Replikation für einen Bucket nur auf einem Grid aktivieren, werden die diesem Bucket (dem Quell-Bucket) hinzugefügten Objekte in den entsprechenden Bucket auf dem anderen Grid (dem Ziel-Bucket) repliziert. Dem Ziel-Bucket hinzugefügte Objekte werden jedoch nicht zurück zur Quelle repliziert. In der Abbildung ist die Cross-Grid-Replikation aktiviert für `my-bucket` von Raster 1 zu Raster 2, aber in die andere Richtung ist es nicht aktiviert.



Replikation in beide Richtungen

Wenn Sie auf beiden Grids die Grid-übergreifende Replizierung für denselben Bucket aktivieren, werden die zu einem Bucket hinzugefügten Objekte in das andere Grid repliziert. In der Abbildung ist die Grid-übergreifende Replizierung für in beide Richtungen aktiviert `my-bucket`.



Was passiert, wenn Objekte aufgenommen werden?

Wenn ein S3-Client einem Bucket ein Objekt hinzufügt, für das die Grid-übergreifende Replizierung aktiviert ist, geschieht Folgendes:

1. StorageGRID repliziert das Objekt automatisch aus dem Quell-Bucket in den Ziel-Bucket. Die Dauer dieses Hintergrundreplizierungsvorgangs hängt von verschiedenen Faktoren ab, darunter von der Anzahl der weiteren ausstehenden Replikationsvorgänge.

   Der S3-Client kann den Replikationsstatus eines Objekts überprüfen, indem er eine GetObject- oder HeadObject-Anforderung ausgibt. Die Antwort enthält eine StorageGRID-spezifische `x-ntap-sg-cgr-replication-status` Antwortheader, der einen der folgenden Werte hat:

Raster	Replikationsstatus
Quelle	• **ABGESCHLOSSEN**: Die Replikation war für alle Grid-Verbindungen erfolgreich. • **AUSSTEHEND**: Das Objekt wurde nicht auf mindestens eine Grid-Verbindung repliziert. • **FEHLER**: Für keine Netzverbindung steht eine Replikation aus und mindestens eine ist mit einem dauerhaften Fehler fehlgeschlagen. Der Fehler muss von einem Benutzer behoben werden.
Ziel	**REPLIKAT**: Das Objekt wurde aus dem Quellraster repliziert.

   StorageGRID unterstützt nicht die `x-amz-replication-status` Kopfzeile.

2. StorageGRID verwendet die aktiven ILM-Richtlinien der einzelnen Grids für die Objektverwaltung, wie bei jedem anderen Objekt. Objekt A in Tabelle 1 kann beispielsweise als zwei replizierte Kopien gespeichert und für immer aufbewahrt werden, während die Kopie von Objekt A, das in Tabelle 2 repliziert wurde, unter Verwendung von 2+1 Erasure Coding gespeichert und nach drei Jahren gelöscht werden kann.

Was passiert, wenn Objekte gelöscht werden?

Wie in beschrieben"Löschen des Datenflusses", kann StorageGRID ein Objekt aus einem der folgenden Gründe löschen:

- Der S3-Client stellt eine Löschanfrage aus.
- Ein Tenant Manager-Benutzer wählt die "Löschen von Objekten in Bucket" Option zum Entfernen aller Objekte aus einem Bucket aus.
- Der Bucket verfügt über eine Lebenszykluskonfiguration, die abläuft.
- Der letzte Zeitraum in der ILM-Regel für das Objekt endet, und es sind keine weiteren Platzierungen angegeben.

Wenn StorageGRID ein Objekt aufgrund von Löschobjekten im Bucket-Betrieb, bis zum Ablauf des Bucket-Lebenszyklus oder bis zum Ablauf der ILM-Platzierung löscht, wird das replizierte Objekt niemals aus dem anderen Grid in einer Grid-Federation-Verbindung gelöscht. Löschmarkierungen, die durch S3-Client-Löschungen zum Quell-Bucket hinzugefügt wurden, können jedoch optional in den Ziel-Bucket repliziert werden.

Um nachzuvollziehen, was passiert, wenn ein S3-Client Objekte aus einem Bucket löscht, für den die Grid-übergreifende Replizierung aktiviert ist, überprüfen Sie wie S3-Clients Objekte aus Buckets löschen, für die Versionierung aktiviert ist:

- Wenn ein S3-Client eine Löschanfrage mit einer Versions-ID ausstellt, wird diese Version des Objekts dauerhaft entfernt. Dem Bucket wurde keine Löschmarkierung hinzugefügt.
- Wenn ein S3-Client eine Löschanforderung ausgibt, die keine Versions-ID enthält, löscht StorageGRID keine Objektversionen. Stattdessen wird dem Bucket eine Löschmarkierung hinzugefügt. Die Löschmarkierung bewirkt, dass StorageGRID so reagiert, als ob das Objekt gelöscht worden wäre:
  - Eine GetObject-Anforderung ohne Versions-ID schlägt fehl mit `404 No Object Found`
  - Eine GetObject-Anforderung mit einer gültigen Versions-ID ist erfolgreich und gibt die angeforderte Objektversion zurück.

Wenn ein S3-Client ein Objekt aus einem Bucket löscht, für den die Grid-übergreifende Replizierung aktiviert ist, bestimmt StorageGRID, ob die Löschanforderung wie folgt auf das Ziel repliziert werden soll:

- Wenn die Löschanforderung eine Versions-ID enthält, wird diese Objektversion dauerhaft aus dem Quellraster entfernt. StorageGRID repliziert jedoch keine Löschanforderungen, die eine Versions-ID enthalten, sodass dieselbe Objektversion nicht vom Ziel gelöscht wird.
- Wenn die Löschanforderung keine Versions-ID enthält, kann StorageGRID die Löschmarkierung optional replizieren, je nachdem, wie die Cross-Grid-Replikation für den Bucket konfiguriert ist:
  - Wenn Sie Löschmarkierungen replizieren (Standard), wird dem Quell-Bucket eine Löschmarkierung hinzugefügt und zum Ziel-Bucket repliziert. In der Tat scheint das Objekt auf beiden Rastern gelöscht zu sein.
  - Wenn Sie sich gegen die Replikation von Löschmarkierungen entscheiden, wird dem Quell-Bucket eine Löschmarkierung hinzugefügt, diese wird jedoch nicht in den Ziel-Bucket repliziert. Tatsächlich werden Objekte, die im Quellraster gelöscht werden, nicht im Zielraster gelöscht.

In der Abbildung wurde **Löschmarkierungen replizieren** auf **Ja** gesetzt, als"Die Grid-übergreifende Replizierung wurde aktiviert" . Löschanforderungen für den Quell-Bucket, die eine Versions-ID enthalten, löschen keine Objekte aus dem Ziel-Bucket. Löschanforderungen für den Quell-Bucket, die keine Versions-ID enthalten, scheinen Objekte im Ziel-Bucket zu löschen.

Wenn Sie die Objektlöschungen zwischen den Rastern synchronisieren möchten, erstellen Sie für die Planungsperioden auf beiden Rastern entsprechende Objekte"S3 Lifecycle-Konfigurationen".

Wie verschlüsselte Objekte repliziert werden

Wenn Sie Objekte zwischen Grids mithilfe von Grid-übergreifender Replizierung verschlüsseln, können Sie einzelne Objekte verschlüsseln, die standardmäßige Bucket-Verschlüsselung verwenden oder die Grid-weite Verschlüsselung konfigurieren. Sie können Standard-Bucket- oder Grid-Verschlüsselungseinstellungen vor oder nach der Grid-übergreifenden Replizierung für einen Bucket hinzufügen, ändern oder entfernen.

Um einzelne Objekte zu verschlüsseln, können Sie beim Hinzufügen der Objekte zum Quell-Bucket SSE (Server-seitige Verschlüsselung mit von StorageGRID gemanagten Schlüsseln) verwenden. Verwenden Sie den `x-amz-server-side-encryption` Anforderungskopf und geben Sie an `AES256`. Siehe "Serverseitige Verschlüsselung".

Die Verwendung von SSE-C (serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln) wird für die Cross-Grid-Replikation nicht unterstützt. Der Aufnahmevorgang schlägt fehl.

Um die Standardverschlüsselung für einen Bucket zu verwenden, verwenden Sie eine Anforderung von PutBucketEncryption und setzen Sie den `SSEAlgorithm` Parameter auf `AES256`. Die Verschlüsselung auf Bucket-Ebene gilt für alle Objekte, die ohne den Request-Header aufgenommen `x-amz-server-side-encryption` wurden. Siehe "Operationen auf Buckets".

Um die Verschlüsselung auf Grid-Ebene zu verwenden, setzen Sie die Option **gespeicherte Objektverschlüsselung** auf **AES-256**. Die Verschlüsselung auf Grid-Ebene gilt für alle Objekte, die nicht auf Bucket-Ebene verschlüsselt oder ohne Anforderungsheader aufgenommen `x-amz-server-side-encryption` werden. Siehe "Konfigurieren Sie Netzwerk- und Objektoptionen".

SSE unterstützt AES-128 nicht. Wenn die Option **Gespeicherte Objektverschlüsselung** für das Quellraster mit der Option **AES-128** aktiviert ist, wird die Verwendung des AES-128-Algorithmus nicht auf das replizierte Objekt übertragen. Stattdessen verwendet das replizierte Objekt die Standard-Bucket- oder Grid-Level-Verschlüsselungseinstellung des Ziels, sofern verfügbar.

Bei der Festlegung, wie Quellobjekte verschlüsselt werden, wendet StorageGRID folgende Regeln an:

1. Verwenden Sie ggf. den `x-amz-server-side-encryption` Ingest Header.
2. Wenn kein Ingest-Header vorhanden ist, verwenden Sie die Bucket-Standardverschlüsselungseinstellung, sofern konfiguriert.
3. Wenn keine Bucket-Einstellung konfiguriert ist, verwenden Sie die gitterweite Verschlüsselungseinstellung, sofern konfiguriert.
4. Wenn keine rasterweite Einstellung vorhanden ist, verschlüsseln Sie das Quellobjekt nicht.

Beim Bestimmen, wie replizierte Objekte verschlüsselt werden, wendet StorageGRID die folgenden Regeln in der folgenden Reihenfolge an:

1. Verwenden Sie dieselbe Verschlüsselung wie das Quellobjekt, es sei denn, dieses Objekt verwendet AES-128-Verschlüsselung.
2. Wenn das Quellobjekt nicht verschlüsselt ist oder AES-128 verwendet, verwenden Sie die

Standardverschlüsselungseinstellung des Ziel-Buckets, sofern konfiguriert.

3. Wenn der Ziel-Bucket keine Verschlüsselungseinstellung hat, verwenden Sie die gridweite Verschlüsselungseinstellung des Ziels, sofern konfiguriert.
4. Wenn keine rasterweite Einstellung vorhanden ist, verschlüsseln Sie das Zielobjekt nicht.

Cross-Grid-Replikation mit S3 Object Lock

Sie können die Cross-Grid-Replikation zwischen StorageGRID Buckets mit aktivierter S3-Objektsperre unter den folgenden Umständen konfigurieren.

Wenn die S3-Objektsperre für den Quell-Bucket … ist.	Und die S3-Objektsperre im Ziel-Bucket ist …
Ermöglicht	Ermöglicht
Deaktiviert	Ermöglicht

Wenn die S3-Objektsperre im Quell-Bucket aktiviert ist:

- Die Objekte werden mit Aufbewahrungseinstellungen am Ziel in dieser Reihenfolge gesperrt:
  a. Die Aufbewahrungsheaderwerte des Quellobjekts für:

     `x-amz-object-lock-mode`

     `x-amz-object-lock-retain-until-date`

  b. Die Standardaufbewahrung des Quell-Buckets, falls festgelegt.
  c. Die Standardaufbewahrung des Ziel-Buckets, falls festgelegt.

  Die Standardaufbewahrung des Ziel-Buckets überschreibt nicht die vom Quellobjekt replizierten Aufbewahrungseinstellungen.
- Sie können den Legal Hold-Status für das Zielobjekt festlegen, indem Sie `x-amz-object-lock-legal-hold` beim Hochladen des Objekts.
- Ein Fehler tritt auf, wenn der Zielmandant oder -Bucket die S3-Objektsperreinstellungen des Quellobjekts nicht unterstützt. Siehe "Warnungen und Fehler bei der Cross-Grid-Replikation."

Wenn die S3-Objektsperre im Quell-Bucket deaktiviert ist:

- Sie können die Standardaufbewahrung im Ziel-Bucket konfigurieren, um die S3 Object Lock-Aufbewahrungseinstellungen auf das Zielobjekt anzuwenden.
- Das Zielobjekt kann keinen Legal Hold-Status festlegen.

PutObjectTagging und DeleteObjectTagging werden nicht unterstützt

PutObjectTagging- und DeleteObjectTagging-Anforderungen werden nicht für Objekte in Buckets unterstützt, für die die Grid-übergreifende Replikation aktiviert ist.

Wenn ein S3-Client eine PutObjectTagging- oder DeleteObjectTagging-Anforderung ausgibt, `501 Not Implemented` wird zurückgegeben. Die Botschaft ist `Put(Delete) ObjectTagging isn't available for buckets that have cross-grid replication configured.`

PutObjectRetention und PutObjectLegalHold werden nicht unterstützt

PutObjectRetention- und PutObjectLegalHold-Anfragen werden für Objekte in Buckets, für die die Cross-Grid-Replikation aktiviert ist, nicht vollständig unterstützt.

Wenn ein S3-Client eine PutObjectRetention- oder PutObjectLegalHold-Anforderung ausgibt, werden die Einstellungen des Quellobjekts geändert, die Änderungen werden jedoch nicht auf das Ziel angewendet.

Wie segmentierte Objekte repliziert werden

Die maximale Segmentgröße des Quellrasters gilt für Objekte, die in das Zielraster repliziert werden. Wenn Objekte in ein anderes Raster repliziert werden, wird die Einstellung **Maximale Segmentgröße** (**Konfiguration** > **System** > **Speicheroptionen**) des Quellrasters auf beiden Rastern verwendet. Angenommen, die maximale Segmentgröße für das Quellraster beträgt 1 GB, während die maximale Segmentgröße des Zielrasters 50 MB beträgt. Wenn Sie ein 2-GB-Objekt in das Quellraster aufnehmen, wird dieses Objekt als zwei 1-GB-Segmente gespeichert. Es wird auch als zwei 1-GB-Segmente in das Zielraster repliziert, obwohl die maximale Segmentgröße dieses Rasters 50 MB beträgt.

Vergleichen Sie Grid-Replizierung und CloudMirror Replizierung

Wenn Sie mit Grid Federation beginnen, überprüfen Sie die Ähnlichkeiten und Unterschiede zwischen "Grid-übergreifende Replizierung" und "StorageGRID CloudMirror Replikationsservice".

> ⓘ Sie können CloudMirror nicht auf einem Bucket verwenden, der durch Cross-Grid-Replikation repliziert wurde, und umgekehrt.

	Grid-übergreifende Replizierung	CloudMirror Replikationsservice
Was ist der primäre Zweck?	Ein StorageGRID System fungiert als Disaster Recovery-System. Objekte in einem Bucket können zwischen den Grids in eine oder beide Richtungen repliziert werden.	Ermöglicht einem Mandanten, automatisch Objekte aus einem Bucket in StorageGRID (Quelle) in einen externen S3-Bucket (Ziel) zu replizieren Die CloudMirror-Replikation erstellt eine unabhängige Kopie eines Objekts in einer unabhängigen S3-Infrastruktur. Diese unabhängige Kopie dient nicht als Backup, sondern wird häufig in der Cloud weiterverarbeitet.

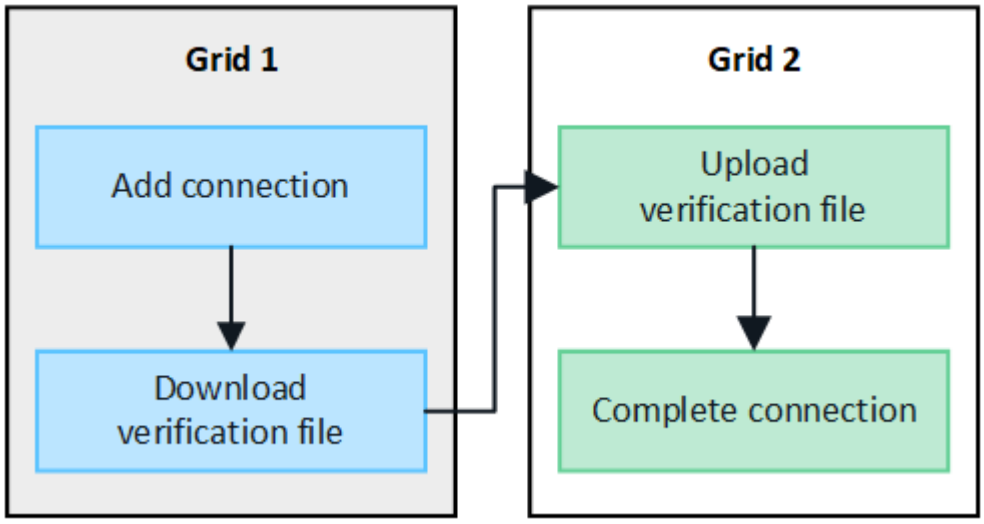
	Grid-übergreifende Replizierung	CloudMirror Replikationsservice
Wie ist es eingerichtet?	1. Konfigurieren Sie eine Grid Federation-Verbindung zwischen zwei Grids. 2. Fügen Sie neue Mandantenkonten hinzu, die automatisch in der anderen Tabelle geklont werden. 3. Fügen Sie neue Mandantengruppen und -Benutzer hinzu, die ebenfalls geklont werden. 4. Erstellen Sie entsprechende Buckets in jedem Grid und ermöglichen Sie die Grid-übergreifende Replizierung in eine oder beide Richtungen.	1. Ein Mandantenbenutzer konfiguriert die CloudMirror-Replizierung mithilfe des Tenant Manager oder der S3-API durch Definition eines CloudMirror-Endpunkts (IP-Adresse, Anmeldeinformationen usw.). 2. Jeder Bucket dieses Mandantenkontos kann so konfiguriert werden, dass er auf den CloudMirror-Endpunkt verweisen kann.
Wer ist für die Einrichtung zuständig?	• Ein Grid-Administrator konfiguriert die Verbindung und die Mandanten. • Mandantenbenutzer konfigurieren die Gruppen, Benutzer, Schlüssel und Buckets.	Normalerweise wird ein Mandantenbenutzer verwendet.
Was ist das Ziel?	Ein entsprechender und identischer S3-Bucket auf dem anderen StorageGRID-System in der Grid-Federation-Verbindung.	• Kompatible S3-Infrastruktur (einschließlich Amazon S3) • Google Cloud Platform (GCP)
Ist eine Objektversionierung erforderlich?	Ja, sowohl in den Quell- als auch in den Ziel-Buckets muss die Objektversionierung aktiviert sein.	Nein, die CloudMirror Replizierung unterstützt beliebige Kombinationen aus unversionierten und versionierten Buckets sowohl am Quell- als auch am Zielsystem.
Was bewirkt, dass Objekte zum Ziel verschoben werden?	Objekte werden automatisch repliziert, wenn sie zu einem Bucket hinzugefügt werden, für den die Grid-übergreifende Replizierung aktiviert ist.	Objekte werden automatisch repliziert, wenn sie zu einem Bucket hinzugefügt werden, der mit einem CloudMirror-Endpunkt konfiguriert wurde. Objekte, die sich im Quell-Bucket befanden, bevor der Bucket mit dem CloudMirror-Endpunkt konfiguriert wurde, werden nur repliziert, wenn sie geändert wurden.
Wie werden Objekte repliziert?	Grid-übergreifende Replizierung erstellt versionierte Objekte und repliziert die Versions-ID vom Quell-Bucket auf den Ziel-Bucket. Dadurch kann die Versionsreihenfolge über beide Raster hinweg beibehalten werden.	Bei der CloudMirror Replizierung sind keine Buckets mit Versionierung erforderlich – CloudMirror kann also nur die Bestellung für einen Schlüssel innerhalb eines Standorts aufrechterhalten. Es gibt keine Garantie, dass die Bestellung für Anfragen an ein Objekt an einem anderen Standort aufrechterhalten wird.

	Grid-übergreifende Replizierung	CloudMirror Replikationsservice
Was ist, wenn ein Objekt nicht repliziert werden kann?	Das Objekt befindet sich in der Warteschlange zur Replizierung, vorbehaltlich der Speichergrenzen für Metadaten.	Das Objekt wird zur Replikation in die Warteschlange eingereiht "Empfehlungen für die Nutzung von Plattform-Services"und unterliegt den Einschränkungen der Plattformdienste (siehe).
Werden die System-Metadaten des Objekts repliziert?	Ja, wenn ein Objekt in das andere Grid repliziert wird, werden auch die Systemmetadaten repliziert. Die Metadaten sind auf beiden Grids identisch.	Nein, wenn ein Objekt in den externen Bucket repliziert wird, werden die Systemmetadaten aktualisiert. Die Metadaten unterscheiden sich je nach Zeitpunkt der Aufnahme und dem Verhalten der unabhängigen S3-Infrastruktur zwischen den Standorten.
Wie werden Objekte abgerufen?	Applikationen können Objekte abrufen oder lesen, indem sie an den Bucket auf beiden Grid eine Anfrage stellen.	Applikationen können Objekte abrufen oder lesen, indem sie eine Anfrage entweder an StorageGRID oder am S3-Ziel stellen. Angenommen, Sie verwenden CloudMirror Replizierung, um Objekte auf eine Partnerorganisation zu spiegeln. Der Partner kann mithilfe eigener Applikationen Objekte direkt vom S3-Ziel lesen oder aktualisieren. Die Verwendung von StorageGRID ist nicht erforderlich.
Was passiert, wenn ein Objekt gelöscht wird?	• Löschanforderungen, die eine Versions-ID enthalten, werden nie in das Zielraster repliziert. • Löschanforderungen, die keine Versions-ID enthalten, fügen dem Quell-Bucket eine Löschmarkierung hinzu, die optional in das Zielraster repliziert werden kann. • Wenn die Grid-übergreifende Replizierung nur für eine Richtung konfiguriert ist, können Objekte im Ziel-Bucket gelöscht werden, ohne die Quelle zu beeinträchtigen.	Die Ergebnisse variieren je nach Versionsstatus der Quell- und Ziel-Buckets (die nicht identisch sein müssen): • Wenn beide Buckets versioniert sind, wird bei einer Löschanforderung an beiden Standorten eine Löschmarkierung hinzugefügt. • Wenn nur der Quell-Bucket versioniert ist, fügt eine Löschanforderung der Quelle eine Löschmarkierung hinzu, nicht jedoch dem Ziel. • Wenn kein Bucket versioniert ist, wird das Objekt durch eine Löschanforderung aus der Quelle, aber nicht aus dem Ziel gelöscht. Ebenso können Objekte im Ziel-Bucket gelöscht werden, ohne dass die Quelle beeinträchtigt wird.

Erstellen von Grid Federation-Verbindungen

Sie können eine Grid-Verbundverbindung zwischen zwei StorageGRID Systemen erstellen, wenn Sie Mandantendetails klonen und Objektdaten replizieren möchten.

Wie in der Abbildung gezeigt, umfasst das Erstellen einer Netzverbundverbindung Schritte auf beiden Grids. Sie fügen die Verbindung auf einem Raster hinzu und schließen sie auf dem anderen Raster ab. Sie können von beiden Rastergitten aus starten.



Bevor Sie beginnen

- Sie haben das für die Konfiguration von Grid Federation-Verbindungen überprüft"Überlegungen und Anforderungen".
- Wenn Sie für jedes Raster statt für IP- oder VIP-Adressen vollständig qualifizierte Domänennamen (FQDNs) verwenden möchten, wissen Sie, welche Namen verwendet werden sollen, und Sie haben bestätigt, dass der DNS-Server für jedes Raster die entsprechenden Einträge enthält.
- Sie verwenden einen "Unterstützter Webbrowser".
- Sie verfügen über Root-Zugriffsberechtigungen und die Provisionierungs-Passphrase für beide Grids.

Verbindung hinzufügen

Führen Sie diese Schritte auf einem der beiden StorageGRID-Systeme aus.

Schritte

1. Melden Sie sich über den primären Admin-Node auf beiden Grids beim Grid-Manager an.
2. Wählen Sie **Konfiguration** > **System** > **Grid-Föderation**.
3. Wählen Sie **Verbindung hinzufügen**.
4. Geben Sie Details für die Verbindung ein.

Feld	Beschreibung
Verbindungsname	Ein eindeutiger Name, der Ihnen hilft, diese Verbindung zu erkennen, z. B. „Raster 1-Raster 2“.

Feld	Beschreibung
FQDN oder IP für dieses Raster	Eine der folgenden Optionen: • Der FQDN des Rasters, bei dem Sie derzeit angemeldet sind • Eine VIP-Adresse einer HA-Gruppe in diesem Raster • Eine IP-Adresse eines Admin-Knotens oder Gateway-Knotens in diesem Grid. Die IP kann sich auf jedem Netzwerk befinden, das das Zielraster erreichen kann.
Port	Der Port, den Sie für diese Verbindung verwenden möchten. Sie können eine beliebige nicht verwendete Portnummer zwischen 23000 und 23999 eingeben. Beide Grids in dieser Verbindung verwenden den gleichen Port. Sie müssen sicherstellen, dass kein Node in einem Grid diesen Port für andere Verbindungen verwendet.
Zertifikat gültige Tage für dieses Raster	Die Anzahl der Tage, an denen die Sicherheitszertifikate für dieses Raster in der Verbindung gültig sein sollen. Der Standardwert ist 730 Tage (2 Jahre), Sie können jedoch einen beliebigen Wert zwischen 1 und 762 Tagen eingeben. StorageGRID generiert automatisch Client- und Serverzertifikate für jedes Grid, wenn Sie die Verbindung speichern.
Provisionierungs-Passphrase für dieses Grid	Die Provisionierungs-Passphrase für das Grid, bei dem Sie angemeldet sind.
FQDN oder IP für das andere Raster	Eine der folgenden Optionen: • Der FQDN des Rasters, mit dem Sie eine Verbindung herstellen möchten • Eine VIP-Adresse einer HA-Gruppe im anderen Raster • Eine IP-Adresse eines Admin-Knotens oder Gateway-Knotens im anderen Grid. Die IP kann sich auf jedem Netzwerk befinden, das das Quellraster erreichen kann.

5. Wählen Sie **Speichern und fortfahren**.
6. Wählen Sie für den Schritt zum Download der Überprüfungsdatei **Download der Überprüfungsdatei** aus.

   Nachdem die Verbindung auf dem anderen Raster abgeschlossen ist, können Sie die Überprüfungsdatei nicht mehr von beiden Rastergitten herunterladen.

7. Suchen Sie die heruntergeladene Datei (*`connection-name`*`.grid-federation`), und speichern Sie sie an einem sicheren Ort.

   Diese Datei enthält Geheimnisse (maskiert als *****) und andere sensible Details und muss sicher gespeichert und übertragen werden.

8. Wählen Sie **Schließen**, um zur Seite Grid Federation zurückzukehren.
9. Bestätigen Sie, dass die neue Verbindung angezeigt wird und ihr **Verbindungsstatus Waiting to connect** ist.
10. Geben Sie die Datei dem Grid-Administrator für das andere Grid an `connection-name.grid-federation`.

Vollständige Verbindung

Führen Sie diese Schritte auf dem StorageGRID-System durch, mit dem Sie eine Verbindung herstellen (das andere Raster).

Schritte

1. Melden Sie sich über den primären Admin-Knoten beim Grid-Manager an.
2. Wählen Sie **Konfiguration** > **System** > **Grid-Föderation**.
3. Wählen Sie **Upload Verification file**, um auf die Seite Upload zuzugreifen.
4. Wählen Sie **Überprüfungsdatei hochladen**. Navigieren Sie dann zu der Datei, die aus dem ersten Raster heruntergeladen wurde (`connection-name.grid-federation`).

   Die Details für die Verbindung werden angezeigt.

5. Geben Sie optional eine andere Anzahl von gültigen Tagen für die Sicherheitszertifikate für dieses Raster ein. Der Eintrag **Certificate valid days** entspricht standardmäßig dem Wert, den Sie in der ersten Tabelle eingegeben haben, aber jedes Raster kann unterschiedliche Ablaufdaten verwenden.

   Verwenden Sie im Allgemeinen die gleiche Anzahl von Tagen für die Zertifikate auf beiden Seiten der Verbindung.

   > Wenn die Zertifikate an einem der beiden Enden der Verbindung ablaufen, wird die Verbindung unterbrochen und Replikationen stehen aus, bis die Zertifikate aktualisiert werden.

6. Geben Sie die Provisionierungs-Passphrase für das Raster ein, bei dem Sie derzeit angemeldet sind.
7. Wählen Sie **Speichern und testen**.

   Die Zertifikate werden generiert und die Verbindung wird getestet. Wenn die Verbindung gültig ist, wird eine Erfolgsmeldung angezeigt, und die neue Verbindung wird auf der Seite Grid Federation aufgeführt. Der **Verbindungsstatus** wird **verbunden**.

   Wenn eine Fehlermeldung angezeigt wird, beheben Sie alle Probleme. Siehe "Fehler beim Grid-Verbund beheben".

8. Rufen Sie die Seite Grid Federation im ersten Raster auf, und aktualisieren Sie den Browser. Bestätigen Sie, dass der **Verbindungsstatus** jetzt **verbunden** ist.
9. Löschen Sie nach dem Verbindungsaufbau alle Kopien der Überprüfungsdatei sicher.

   Wenn Sie diese Verbindung bearbeiten, wird eine neue Überprüfungsdatei erstellt. Die Originaldatei kann nicht wiederverwendet werden.

Nachdem Sie fertig sind

- Überprüfen Sie die Überlegungen für "Management zulässiger Mandanten".

- "Erstellen Sie ein oder mehrere neue Mandantenkonten", Weisen Sie die Berechtigung **use Grid Federation connection** zu und wählen Sie die neue Verbindung aus.
- "Verwalten Sie die Verbindung" Nach Bedarf. Sie können Verbindungswerte bearbeiten, eine Verbindung testen, Verbindungszertifikate drehen oder eine Verbindung entfernen.
- "Überwachen Sie die Verbindung" Im Rahmen Ihrer normalen StorageGRID-Monitoring-Aktivitäten.
- "Beheben Sie die Verbindungsherstellung", Einschließlich der Behebung von Warnungen und Fehlern im Zusammenhang mit Account-Clone und Grid-Replikation.

Grid-Verbindungen verwalten

Das Management von Grid-Verbindungen zwischen StorageGRID Systemen umfasst das Bearbeiten von Verbindungsdetails, das Drehen der Zertifikate, das Entfernen von Mandantenberechtigungen und das Entfernen nicht verwendeter Verbindungen.

Bevor Sie beginnen

- Sie sind auf beiden Rastergitten mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Root-Zugriffsberechtigung" für das Raster, bei dem Sie angemeldet sind.

Bearbeiten einer Verbindung zum Grid Federation

Sie können eine Grid Federation-Verbindung bearbeiten, indem Sie sich beim primären Admin-Node auf einem der beiden Raster der Verbindung anmelden. Nachdem Sie Änderungen am ersten Raster vorgenommen haben, müssen Sie eine neue Überprüfungsdatei herunterladen und in das andere Raster hochladen.

> Während die Verbindung bearbeitet wird, werden Kontoklone- oder Grid-übergreifende Replikationsanforderungen weiterhin die vorhandenen Verbindungseinstellungen verwenden. Alle Änderungen, die Sie am ersten Raster vornehmen, werden lokal gespeichert, aber erst dann verwendet, wenn sie in das zweite Raster hochgeladen, gespeichert und getestet wurden.

Beginnen Sie mit der Bearbeitung der Verbindung

Schritte

1. Melden Sie sich über den primären Admin-Node auf beiden Grids beim Grid-Manager an.
2. Wählen Sie **Knoten** und bestätigen Sie, dass alle anderen Admin-Knoten in Ihrem System online sind.

> Wenn Sie eine Grid-Federation-Verbindung bearbeiten, versucht StorageGRID, eine Datei mit der Kandidatenkonfiguration auf allen Admin-Knoten im ersten Grid zu speichern. Wenn diese Datei nicht in allen Admin-Knoten gespeichert werden kann, wird eine Warnmeldung angezeigt, wenn Sie **Speichern und Testen** auswählen.

3. Wählen Sie **Konfiguration** > **System** > **Grid-Föderation**.
4. Bearbeiten Sie die Verbindungsdetails über das Menü **actions** auf der Seite Grid Federation oder über die Detailseite für eine bestimmte Verbindung. Siehe "Erstellen von Grid Federation-Verbindungen" für das, was Sie teilnehmen.

Menü „Aktionen“

a. Wählen Sie das Optionsfeld für die Verbindung aus.
b. Wählen Sie **Actions** > **Edit**.
c. Geben Sie die neuen Informationen ein.

Detailseite

a. Wählen Sie einen Verbindungsnamen aus, um dessen Details anzuzeigen.
b. Wählen Sie **Bearbeiten**.
c. Geben Sie die neuen Informationen ein.

5. Geben Sie die Provisionierungs-Passphrase für das Raster ein, bei dem Sie angemeldet sind.
6. Wählen Sie **Speichern und fortfahren**.

   Die neuen Werte werden gespeichert, werden aber erst dann auf die Verbindung angewendet, wenn Sie die neue Überprüfungsdatei auf das andere Raster hochgeladen haben.

7. Wählen Sie **Überprüfungsdatei herunterladen**.

   Um diese Datei zu einem späteren Zeitpunkt herunterzuladen, gehen Sie zur Detailseite für die Verbindung.

8. Suchen Sie die heruntergeladene Datei (*`connection-name`*`.grid-federation`), und speichern Sie sie an einem sicheren Ort.

   Die Überprüfungsdatei enthält Geheimnisse und muss sicher gespeichert und übertragen werden.

9. Wählen Sie **Schließen**, um zur Seite Grid Federation zurückzukehren.
10. Bestätigen Sie, dass der **Verbindungsstatus ausstehende Bearbeitung** ist.

    Wenn der Verbindungsstatus etwas anderes als **Verbunden** war, als Sie mit der Bearbeitung der Verbindung begonnen haben, ändert er sich nicht in **Ausstehende Bearbeitung**.

11. Geben Sie die Datei dem Grid-Administrator für das andere Grid an *`connection-name`*`.grid-federation`.

Schließen Sie die Bearbeitung der Verbindung ab

Schließen Sie die Bearbeitung der Verbindung ab, indem Sie die Überprüfungsdatei auf das andere Raster hochladen.

Schritte

1. Melden Sie sich über den primären Admin-Knoten beim Grid-Manager an.
2. Wählen Sie **Konfiguration** > **System** > **Grid-Föderation**.
3. Wählen Sie **Upload Verification file**, um auf die Upload-Seite zuzugreifen.
4. Wählen Sie **Überprüfungsdatei hochladen**. Navigieren Sie dann zu der Datei, die aus dem ersten Raster

heruntergeladen wurde, und wählen Sie sie aus.

5. Geben Sie die Provisionierungs-Passphrase für das Raster ein, bei dem Sie derzeit angemeldet sind.
6. Wählen Sie **Speichern und testen**.

   Wenn die Verbindung über die bearbeiteten Werte hergestellt werden kann, wird eine Erfolgsmeldung angezeigt. Andernfalls wird eine Fehlermeldung angezeigt. Überprüfen Sie die Nachricht und beheben Sie alle Probleme.

7. Schließen Sie den Assistenten, um zur Seite „Grid Federation“ zurückzukehren.
8. Bestätigen Sie, dass der **Verbindungsstatus verbunden** ist.
9. Rufen Sie die Seite Grid Federation im ersten Raster auf, und aktualisieren Sie den Browser. Bestätigen Sie, dass der **Verbindungsstatus** jetzt **verbunden** ist.
10. Löschen Sie nach dem Verbindungsaufbau alle Kopien der Überprüfungsdatei sicher.

Testen einer Netzverbundverbindung

Schritte

1. Melden Sie sich über den primären Admin-Knoten beim Grid-Manager an.
2. Wählen Sie **Konfiguration** > **System** > **Grid-Föderation**.
3. Testen Sie die Verbindung mit dem Menü **actions** auf der Seite Grid Federation oder der Detailseite für eine bestimmte Verbindung.

   Menü „Aktionen“

   a. Wählen Sie das Optionsfeld für die Verbindung aus.

   b. Wählen Sie **Actions** > **Test**.

   Detailseite

   a. Wählen Sie einen Verbindungsnamen aus, um dessen Details anzuzeigen.

   b. Wählen Sie **Verbindung testen**.

4. Überprüfen Sie den Verbindungsstatus:

Verbindungsstatus	Beschreibung
Verbunden	Beide Netze sind angeschlossen und kommunizieren normal.
Fehler	Die Verbindung befindet sich in einem Fehlerzustand. Beispielsweise ist ein Zertifikat abgelaufen oder ein Konfigurationswert ist nicht mehr gültig.
Bearbeitung ausstehend	Sie haben die Verbindung in diesem Raster bearbeitet, aber die Verbindung verwendet weiterhin die vorhandene Konfiguration. Um die Bearbeitung abzuschließen, laden Sie die neue Überprüfungsdatei in das andere Raster hoch.

Verbindungsstatus	Beschreibung
Warten auf Verbindung	Sie haben die Verbindung in diesem Raster konfiguriert, aber die Verbindung wurde auf dem anderen Raster nicht abgeschlossen. Laden Sie die Überprüfungsdatei von diesem Raster herunter, und laden Sie sie in das andere Raster hoch.
Unbekannt	Die Verbindung befindet sich in einem unbekannten Zustand, möglicherweise aufgrund eines Netzwerkproblems oder eines Offline-Knotens.

5. Wenn der Verbindungsstatus **Error** lautet, beheben Sie alle Probleme. Wählen Sie dann erneut **Verbindung testen** aus, um zu bestätigen, dass das Problem behoben wurde.

Verbindungszertifikate drehen

Jede Grid Federation-Verbindung verwendet vier automatisch generierte SSL-Zertifikate, um die Verbindung zu sichern. Wenn die beiden Zertifikate für jedes Raster in der Nähe ihres Ablaufdatums liegen, erinnert die Warnung **Ablauf des Grid Federation Certificate** Sie daran, die Zertifikate zu drehen.

> Wenn die Zertifikate an einem der beiden Enden der Verbindung ablaufen, wird die Verbindung unterbrochen und Replikationen stehen aus, bis die Zertifikate aktualisiert werden.

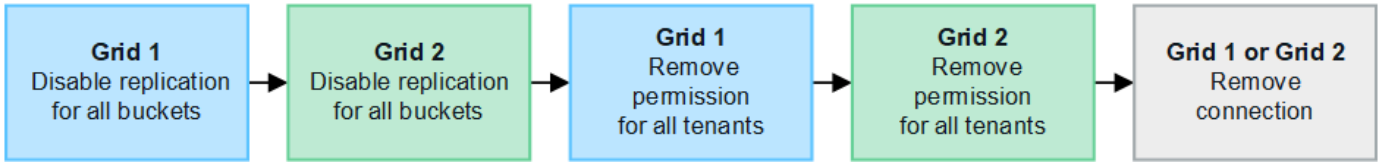
Schritte

1. Melden Sie sich über den primären Admin-Node auf beiden Grids beim Grid-Manager an.
2. Wählen Sie **Konfiguration** > **System** > **Grid-Föderation**.
3. Wählen Sie auf einer der Registerkarten auf der Seite Grid Federation den Verbindungsnamen aus, um die zugehörigen Details anzuzeigen.
4. Wählen Sie die Registerkarte **Zertifikate** aus.
5. Wählen Sie **Zertifikate drehen**.
6. Geben Sie an, wie viele Tage die neuen Zertifikate gültig sein sollen.
7. Geben Sie die Provisionierungs-Passphrase für das Raster ein, bei dem Sie angemeldet sind.
8. Wählen Sie **Zertifikate drehen**.
9. Wiederholen Sie diese Schritte bei Bedarf auf dem anderen Raster der Verbindung.

   Verwenden Sie im Allgemeinen die gleiche Anzahl von Tagen für die Zertifikate auf beiden Seiten der Verbindung.

Entfernen Sie eine Netzverbundverbindung

Sie können eine Netzverbundverbindung aus jedem Raster der Verbindung entfernen. Wie in der Abbildung gezeigt, müssen Sie auf beiden Rastern erforderliche Schritte ausführen, um zu bestätigen, dass die Verbindung nicht von einem Mandanten in einem der beiden Raster verwendet wird.



Beachten Sie vor dem Entfernen einer Verbindung Folgendes:

- Durch das Entfernen einer Verbindung werden keine Elemente gelöscht, die bereits zwischen den Rastern kopiert wurden. So werden beispielsweise Mandantenbenutzer, -Gruppen und -Objekte, die auf beiden Grids vorhanden sind, nicht aus beiden Grids gelöscht, wenn die Berechtigung des Mandanten entfernt wird. Wenn Sie diese Elemente löschen möchten, müssen Sie sie manuell aus beiden Rastern löschen.
- Wenn Sie eine Verbindung entfernen, wird die Replikation aller Objekte, die noch nicht repliziert werden (aufgenommen, aber noch nicht in das andere Grid repliziert), dauerhaft fehlgeschlagen.

Deaktivieren Sie die Replizierung für alle Mandanten-Buckets

Schritte

1. Melden Sie sich vom primären Admin-Node aus an einem der beiden Raster beim Grid Manager an.
2. Wählen Sie **Konfiguration** > **System** > **Grid-Föderation**.
3. Wählen Sie den Verbindungsnamen aus, um die zugehörigen Details anzuzeigen.
4. Bestimmen Sie auf der Registerkarte **zulässige Mieter**, ob die Verbindung von einem Mieter verwendet wird.
5. Wenn Mandanten aufgeführt sind, weisen Sie alle Mandanten an"Deaktivieren Sie die Grid-übergreifende Replizierung", für alle ihre Buckets auf beiden Rastern in der Verbindung zu verwenden.

> Sie können die Berechtigung **use Grid Federation connection** nicht entfernen, wenn in einem Mandanten-Buckets die Grid-übergreifende Replikation aktiviert ist. Jedes Mandantenkonto muss die Grid-übergreifende Replizierung für seine Buckets auf beiden Grids deaktivieren.

Berechtigung für jeden Mandanten entfernen

Nachdem die Grid-übergreifende Replikation für alle Mandanten-Buckets deaktiviert wurde, entfernen Sie die **use Grid Federation permission** von allen Mandanten auf beiden Grids.

Schritte

1. Wählen Sie **Konfiguration** > **System** > **Grid-Föderation**.
2. Wählen Sie den Verbindungsnamen aus, um die zugehörigen Details anzuzeigen.
3. Entfernen Sie für jeden Mandanten auf der Registerkarte **zulässige Mieter** die Berechtigung **Grid Federation connection** von jedem Mandanten. Siehe "Management zulässiger Mandanten".
4. Wiederholen Sie diese Schritte für die zulässigen Mandanten im anderen Raster.

Verbindung entfernen

Schritte

1. Wenn keine Mieter in einem der beiden Raster die Verbindung verwenden, wählen Sie **Entfernen**.
2. Überprüfen Sie die Bestätigungsmeldung, und wählen Sie **Entfernen**.
   - Wenn die Verbindung entfernt werden kann, wird eine Erfolgsmeldung angezeigt. Die Netzverbundverbindung wird nun aus beiden Grids entfernt.
   - Wenn die Verbindung nicht entfernt werden kann (z. B. wird sie noch verwendet oder es liegt ein Verbindungsfehler vor), wird eine Fehlermeldung angezeigt. Sie können eine der folgenden Aktionen ausführen:

- Beheben Sie den Fehler (empfohlen). Siehe "Fehler beim Grid-Verbund beheben".
- Entfernen Sie die Verbindung mit Gewalt. Siehe nächster Abschnitt.

Entfernen Sie eine Verbindung zum Grid-Verbund mit Gewalt

Bei Bedarf können Sie das Entfernen einer Verbindung erzwingen, die nicht den Status **Verbunden** hat.

Das Entfernen erzwingen löscht nur die Verbindung aus dem lokalen Grid. Um die Verbindung vollständig zu entfernen, führen Sie die gleichen Schritte auf beiden Rastern aus.

Schritte

1. Wählen Sie im Bestätigungsdialogfeld **Entfernen erzwingen** aus.

   Eine Erfolgsmeldung wird angezeigt. Diese Netzverbundverbindung kann nicht mehr verwendet werden. Allerdings ist für Mandanten-Buckets möglicherweise weiterhin die Grid-übergreifende Replizierung aktiviert, und einige Objektkopien wurden möglicherweise bereits zwischen den Grids in der Verbindung repliziert.

2. Melden Sie sich vom anderen Raster der Verbindung aus über den primären Admin-Node beim Grid Manager an.
3. Wählen Sie **Konfiguration** > **System** > **Grid-Föderation**.
4. Wählen Sie den Verbindungsnamen aus, um die zugehörigen Details anzuzeigen.
5. Wählen Sie **Entfernen** und **Ja**.
6. Wählen Sie **Entfernen erzwingen**, um die Verbindung aus diesem Raster zu entfernen.

Verwalten Sie die zulässigen Mandanten für den Grid-Verbund

Sie können S3-Mandantenkonten die Verwendung einer Grid-Federation-Verbindung zwischen zwei StorageGRID-Systemen erlauben. Wenn Mandanten eine Verbindung verwenden dürfen, sind spezielle Schritte erforderlich, um die Mandantendetails zu bearbeiten oder die Berechtigung eines Mandanten zur Verwendung der Verbindung dauerhaft zu entfernen.

Bevor Sie beginnen

- Sie sind auf beiden Rastergitten mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Root-Zugriffsberechtigung" für das Raster, bei dem Sie angemeldet sind.
- Sie haben "Grid Federation-Verbindung erstellt" zwischen zwei Rastern.
- Sie haben die Workflows für und überprüft"Konto-Klon""Grid-übergreifende Replizierung".
- Bei Bedarf haben Sie bereits Single Sign-On (SSO) oder Identify Federation für beide Grids in der Verbindung konfiguriert. Siehe "Was ist Account-Klon".

Erstellen Sie eine zulässige Serviceeinheit

Wenn Sie einem neuen oder vorhandenen Mandantenkonto die Verwendung einer Grid-Federation-Verbindung für Account-Klonen und Grid-Replizierung erlauben möchten, befolgen Sie die allgemeinen Anweisungen zu "Erstellen Sie einen neuen S3-Mandanten" bzw. "Bearbeiten Sie ein Mandantenkonto" und beachten Sie Folgendes:

- Sie können die Serviceeinheit aus jedem Raster der Verbindung erstellen. Das Raster, in dem ein Mandant erstellt wird, ist das Quellraster des *Mandanten*.
- Der Status der Verbindung muss **connected** sein.
- Wenn der Mandant erstellt oder bearbeitet wird, um die Berechtigung **use Grid Federation connection** zu aktivieren und dann im ersten Grid zu speichern, wird automatisch ein identischer Mandant in das andere Grid repliziert. Das Grid, in dem der Mandant repliziert wird, ist das Zielraster des *Mandanten*.
- Die Mandanten in beiden Grids haben die gleiche 20-stellige Konto-ID, den gleichen Namen, die gleiche Beschreibung, das gleiche Kontingent und die gleichen Berechtigungen. Optional können Sie das Feld **Beschreibung** verwenden, um zu ermitteln, welcher Quellmandant und welcher Zielmandant ist. Beispielsweise wird diese Beschreibung für einen Mandanten, der in Grid 1 erstellt wurde, auch für den Mandanten angezeigt, der in Grid 2 repliziert wurde: „Dieser Mandant wurde in Grid 1 erstellt.“
- Aus Sicherheitsgründen wird das Kennwort für einen lokalen Root-Benutzer nicht in das Zielraster kopiert.

> Bevor ein lokaler Root-Benutzer sich beim replizierten Mandanten im Zielraster anmelden kann, muss ein Grid-Administrator für dieses Grid angemeldet "Ändern Sie das Passwort für den lokalen Root-Benutzer"sein.

- Nachdem der neue oder bearbeitete Mandant auf beiden Grids verfügbar ist, können Mandantenbenutzer die folgenden Vorgänge ausführen:
  - Erstellen Sie im Quellraster des Mandanten Gruppen und lokale Benutzer, die automatisch im Zielraster des Mandanten geklont werden. Siehe "Klonen von Mandantengruppen und Benutzern".
  - Erstellen neuer S3-Zugriffsschlüssel, die optional im Zielraster des Mandanten geklont werden können Siehe "Klonen von S3-Zugriffsschlüsseln mithilfe der API".
  - Erstellen Sie auf beiden Grids in der Verbindung identische Buckets und ermöglichen Sie die Grid-übergreifende Replizierung in eine oder beide Richtungen. Siehe "Grid-übergreifende Replizierung managen".

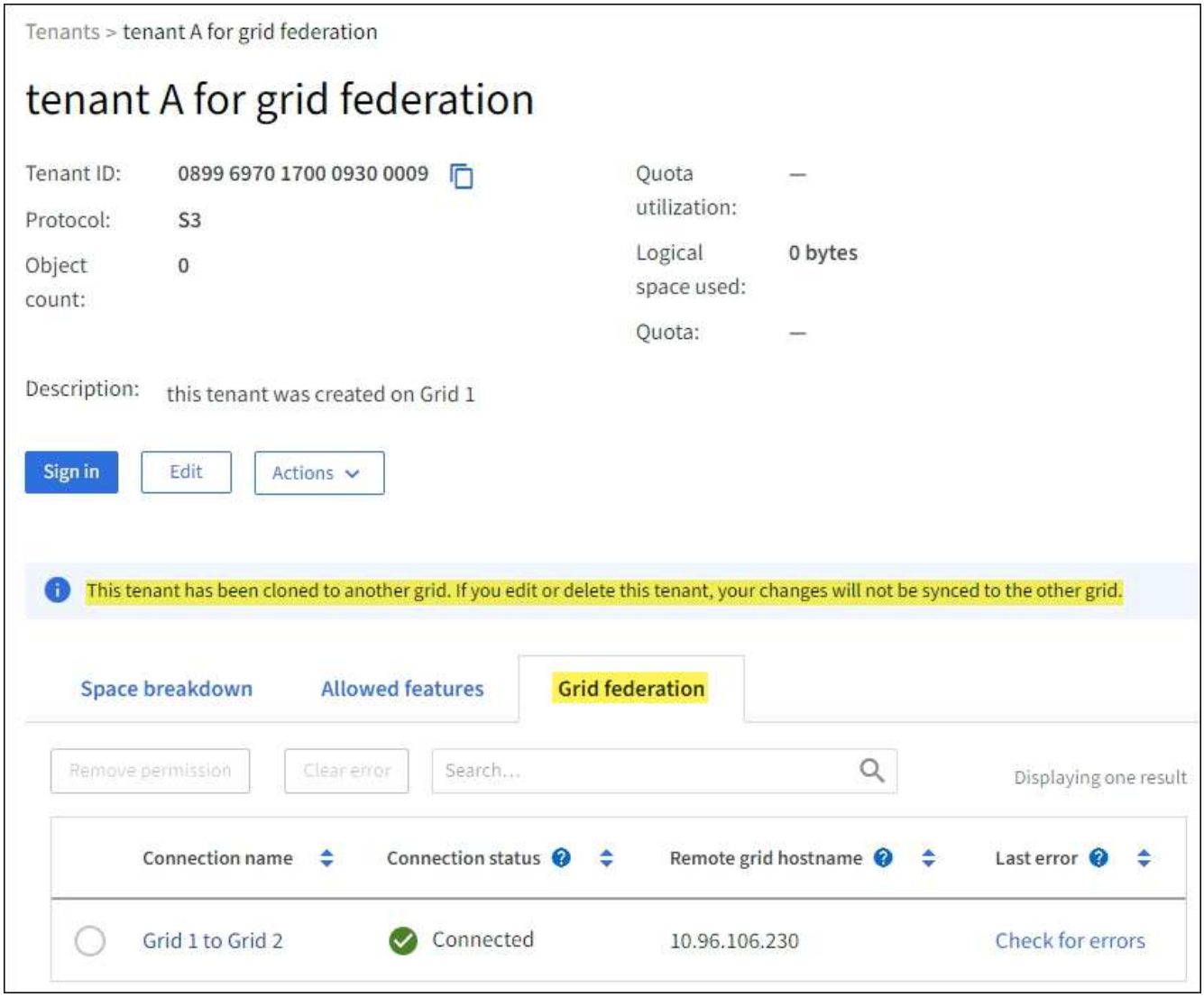
Zeigen Sie eine zulässige Serviceeinheit an

Sie können Details zu einem Mandanten anzeigen, der eine Verbindung mit dem Grid Federation verwenden darf.

Schritte

1. Wählen Sie **Mandanten** aus.
2. Wählen Sie auf der Seite Tenants den Namen der Serviceeinheit aus, um die Seite mit den Details der Serviceeinheit anzuzeigen.

   Wenn es sich hierbei um das Quellraster für den Mandanten handelt (d. h. wenn der Mandant in diesem Raster erstellt wurde), wird ein Banner angezeigt, das Sie daran erinnert, dass der Mandant in einem anderen Raster geklont wurde. Wenn Sie diesen Mandanten bearbeiten oder löschen, werden Ihre Änderungen nicht mit dem anderen Raster synchronisiert.



3. Wählen Sie optional die Registerkarte **Grid Federation** auf "Überwachen der Netzverbundverbindung".

Bearbeiten Sie eine zulässige Serviceeinheit

Wenn Sie einen Mandanten bearbeiten müssen, der über die Berechtigung **Grid Federation connection** verfügt, befolgen Sie die allgemeinen Anweisungen für "Bearbeiten eines Mandantenkontos" und beachten Sie Folgendes:

- Wenn ein Mandant über die Berechtigung **Grid Federation connection** verwenden verfügt, können Sie die Mandantendetails von beiden Rastergittern in der Verbindung bearbeiten. Alle Änderungen, die Sie vornehmen, werden jedoch nicht in das andere Raster kopiert. Wenn Sie die Details der Serviceeinheit zwischen den Rastern synchronisieren möchten, müssen Sie die gleichen Änderungen an beiden Rastern vornehmen.
- Sie können die Berechtigung **Grid Federation connection** verwenden* nicht löschen, wenn Sie einen Mandanten bearbeiten.
- Sie können keine andere Grid Federation-Verbindung auswählen, wenn Sie eine Serviceeinheit bearbeiten.

Löschen Sie eine zulässige Serviceeinheit

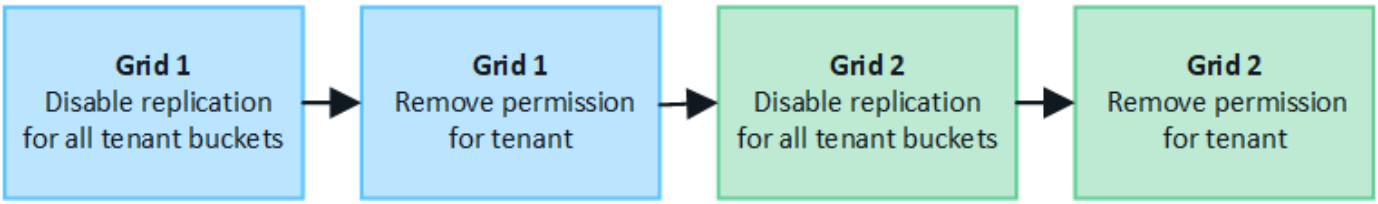
Wenn Sie einen Mandanten entfernen müssen, der über die Berechtigung **Grid Federation connection** verfügt, befolgen Sie die allgemeinen Anweisungen für "Löschen eines Mandantenkontos" und beachten Sie Folgendes:

- Bevor Sie den ursprünglichen Mandanten im Quellraster entfernen können, müssen Sie alle Buckets für das Konto im Quellraster entfernen.
- Bevor Sie den geklonten Mandanten im Zielraster entfernen können, müssen Sie alle Buckets für das Konto im Zielraster entfernen.
- Wenn Sie den ursprünglichen oder den geklonten Mandanten entfernen, kann das Konto nicht mehr für die Grid-übergreifende Replizierung verwendet werden.
- Wenn Sie den ursprünglichen Mandanten im Quellraster entfernen, werden alle Mandantengruppen, Benutzer oder Schlüssel, die im Zielraster geklont wurden, nicht beeinträchtigt. Sie können den geklonten Mandanten entweder löschen oder seiner eigenen Gruppe, Benutzern, Zugriffsschlüsseln und Buckets verwalten.
- Wenn Sie den geklonten Mandanten im Zielraster entfernen, treten Klonfehler auf, wenn dem ursprünglichen Mandanten neue Gruppen oder Benutzer hinzugefügt werden.

  Um diese Fehler zu vermeiden, entfernen Sie die Berechtigung des Mandanten zur Verwendung der Grid Federation-Verbindung, bevor Sie den Mandanten aus diesem Raster löschen.

Remove Use Grid Federation connection permission

Um zu verhindern, dass ein Mandant eine Netzverbundverbindung verwendet, müssen Sie die Berechtigung **Grid Federation Connection** verwenden entfernen.



Beachten Sie Folgendes, bevor Sie die Berechtigung eines Mandanten zur Verwendung einer Grid-Federation-Verbindung entfernen:

- Sie können die Berechtigung **use Grid Federation connection** nicht entfernen, wenn eine der Buckets des Mandanten Grid-übergreifende Replikation aktiviert hat. Das Mandantenkonto muss zunächst die Grid-übergreifende Replizierung für alle Buckets deaktivieren.
- Wenn Sie die Berechtigung **Grid Federation connection** verwenden entfernen, werden keine Elemente gelöscht, die bereits zwischen den Rastern repliziert wurden. So werden beispielsweise alle Mandantenbenutzer, -Gruppen und -Objekte, die auf beiden Grids vorhanden sind, nicht aus beiden Grids gelöscht, wenn die Berechtigung des Mandanten entfernt wird. Wenn Sie diese Elemente löschen möchten, müssen Sie sie manuell aus beiden Rastern löschen.
- Wenn Sie diese Berechtigung mit derselben Grid Federation-Verbindung erneut aktivieren möchten, löschen Sie diesen Mandanten zuerst im Zielraster. Andernfalls führt die erneute Aktivierung dieser Berechtigung zu einem Fehler.

Durch die erneute Aktivierung der Berechtigung **use Grid Federation connection** wird das lokale Grid zum Quellraster und löst das Klonen auf das Remote Grid aus, das von der ausgewählten Grid Federation-Verbindung angegeben wird. Wenn das Mandantenkonto bereits im Remote-Grid vorhanden ist, führt das Klonen zu einem Konfliktfehler.

Bevor Sie beginnen

- Sie verwenden einen "Unterstützter Webbrowser".
- Sie haben die "Root-Zugriffsberechtigung" für beide Raster.

Deaktivieren Sie die Replizierung für Mandanten-Buckets

Deaktivieren Sie als ersten Schritt die Grid-übergreifende Replizierung für alle Mandanten-Buckets.

Schritte

1. Melden Sie sich vom primären Admin-Node aus an einem der beiden Raster beim Grid Manager an.
2. Wählen Sie **Konfiguration** > **System** > **Grid-Föderation**.
3. Wählen Sie den Verbindungsnamen aus, um die zugehörigen Details anzuzeigen.
4. Bestimmen Sie auf der Registerkarte **zulässige Mieter**, ob der Mieter die Verbindung nutzt.
5. Wenn der Mieter aufgeführt ist, weisen Sie ihn an"Deaktivieren Sie die Grid-übergreifende Replizierung", alle seine Eimer auf beiden Rastern in der Verbindung zu besetzen.

Sie können die Berechtigung **use Grid Federation connection** nicht entfernen, wenn in einem Mandanten-Buckets die Grid-übergreifende Replikation aktiviert ist. Der Mandant muss die Grid-übergreifende Replizierung für seine Buckets auf beiden Grids deaktivieren.

Berechtigung für Serviceeinheit entfernen

Nachdem die Grid-übergreifende Replizierung für Mandanten-Buckets deaktiviert ist, können Sie die Berechtigung des Mandanten zur Verwendung der Grid-Verbundverbindung entfernen.

Schritte

1. Melden Sie sich über den primären Admin-Knoten beim Grid-Manager an.
2. Entfernen Sie die Berechtigung von der Seite „Grid Federation“ oder der Seite „Tenants“.

Seite „Grid Federation“

a. Wählen Sie **Konfiguration** > **System** > **Grid-Föderation**.
b. Wählen Sie den Verbindungsnamen aus, um die Detailseite anzuzeigen.
c. Wählen Sie auf der Registerkarte **zulässige Mieter** die Optionsschaltfläche für den Mieter aus.
d. Wählen Sie **Berechtigung entfernen**.

Mandanten werden gestartet

a. Wählen Sie **Mandanten** aus.
b. Wählen Sie den Namen des Mandanten aus, um die Detailseite anzuzeigen.
c. Wählen Sie auf der Registerkarte **Grid Federation** das Optionsfeld für die Verbindung aus.
d. Wählen Sie **Berechtigung entfernen**.

3. Überprüfen Sie die Warnungen im Bestätigungsdialogfeld, und wählen Sie **Entfernen**.
   - Wenn die Berechtigung entfernt werden kann, kehren Sie zur Detailseite zurück, und eine Erfolgsmeldung wird angezeigt. Dieser Mandant kann die Grid Federation-Verbindung nicht mehr verwenden.
   - Wenn für einen oder mehrere Mandanten-Buckets die Grid-übergreifende Replizierung weiterhin aktiviert ist, wird ein Fehler angezeigt.

     Sie können eine der folgenden Aktionen ausführen:

     - (Empfohlen.) Melden Sie sich beim Tenant Manager an und deaktivieren Sie die Replikation für jeden Buckets des Mandanten. Siehe "Grid-übergreifende Replizierung managen". Wiederholen Sie dann die Schritte, um die Berechtigung **Grid-Verbindung verwenden** zu entfernen.
     - Entfernen Sie die Berechtigung mit Gewalt. Siehe nächster Abschnitt.
4. Gehen Sie zum anderen Raster, und wiederholen Sie diese Schritte, um die Berechtigung für denselben Mandanten auf dem anderen Raster zu entfernen.

Entfernen Sie die Berechtigung mit Gewalt

Bei Bedarf können Sie das Entfernen der Berechtigung eines Mandanten zur Verwendung einer Grid-Verbundverbindung erzwingen, selbst wenn für Mandanten-Buckets die Grid-übergreifende Replizierung aktiviert ist.

Bevor Sie die Erlaubnis eines Mandanten gewaltsam entfernen, notieren Sie sich die allgemeinen Überlegungen sowie die Entfernen der Berechtigungfolgenden zusätzlichen Überlegungen:

- Wenn Sie die Berechtigung **use Grid Federation connection** per Force entfernen, werden alle Objekte, die eine Replikation auf das andere Grid ausstehen (aufgenommen, aber noch nicht repliziert), weiterhin repliziert. Um zu verhindern, dass diese in-Process-Objekte den Ziel-Bucket erreichen, müssen Sie auch die Berechtigung des Mandanten für das andere Raster entfernen.
- Alle Objekte, die in den Quell-Bucket aufgenommen wurden, nachdem Sie die Berechtigung **Grid Federation Connection** verwenden entfernt haben, werden niemals in den Ziel-Bucket repliziert.

Schritte

1. Melden Sie sich über den primären Admin-Knoten beim Grid-Manager an.
2. Wählen Sie **Konfiguration** > **System** > **Grid-Föderation**.
3. Wählen Sie den Verbindungsnamen aus, um die Detailseite anzuzeigen.
4. Wählen Sie auf der Registerkarte **zulässige Mieter** die Optionsschaltfläche für den Mieter aus.
5. Wählen Sie **Berechtigung entfernen**.
6. Überprüfen Sie die Warnungen im Bestätigungsdialogfeld, und wählen Sie **Entfernen erzwingen**.

   Eine Erfolgsmeldung wird angezeigt. Dieser Mandant kann die Grid Federation-Verbindung nicht mehr verwenden.
7. Gehen Sie bei Bedarf zum anderen Raster, und wiederholen Sie diese Schritte, um die Berechtigung für das gleiche Mandantenkonto im anderen Raster zu erzwingen. Sie sollten diese Schritte beispielsweise auf dem anderen Raster wiederholen, um zu verhindern, dass in-Process-Objekte den Ziel-Bucket erreichen.

Fehler beim Grid-Verbund beheben

Unter Umständen müssen Sie Warnmeldungen und Fehler in Bezug auf Grid-Verbindungen, Account-Klone und Grid-Replizierung beheben.

Warnungen und Fehler der Grid Federation-Verbindung

Möglicherweise erhalten Sie Warnmeldungen oder Fehler bei den Verbindungen des Grid-Verbunds.

Nachdem Sie Änderungen vorgenommen haben, um ein Verbindungsproblem zu beheben, testen Sie die Verbindung, um sicherzustellen, dass der Verbindungsstatus wieder auf **Connected** zurückkehrt. Anweisungen hierzu finden Sie unter "Grid-Verbindungen verwalten".

Warnmeldung bei Ausfall der Grid-Verbindung

Problem

Die Warnung **Grid Federation Connection failure** wurde ausgelöst.

Details

Diese Warnung zeigt an, dass die Verbindung zwischen den Rastern nicht funktioniert.

Empfohlene Maßnahmen

1. Überprüfen Sie die Einstellungen auf der Seite „Grid Federation“ für beide Raster. Vergewissern Sie sich, dass alle Werte korrekt sind. Siehe "Grid-Verbindungen verwalten".
2. Überprüfen Sie die für die Verbindung verwendeten Zertifikate. Stellen Sie sicher, dass keine Warnungen für abgelaufene Grid Federation-Zertifikate vorhanden sind und dass die Details für jedes Zertifikat gültig sind. Siehe die Anleitung für rotierende Verbindungszertifikate in "Grid-Verbindungen verwalten".
3. Vergewissern Sie sich, dass alle Admin- und Gateway-Nodes in beiden Grids online und verfügbar sind. Beheben Sie alle Warnmeldungen, die sich auf diese Knoten auswirken könnten, und versuchen Sie es erneut.
4. Wenn Sie einen vollständig qualifizierten Domänennamen (FQDN) für das lokale oder Remote-Grid angegeben haben, vergewissern Sie sich, dass der DNS-Server online und verfügbar ist. Informationen zu Netzwerk-, IP-Adresse- und DNS-Anforderungen finden Sie unter"Was ist Grid Federation?".

Ablauf der Warnmeldung für das Grid-Verbundzertifikat

Problem

Die Warnung **Ablauf des Grid Federation Certificate** wurde ausgelöst.

Details

Diese Warnmeldung gibt an, dass ein oder mehrere Grid-Verbundzertifikate bald ablaufen.

Empfohlene Maßnahmen

Siehe die Anleitung für rotierende Verbindungszertifikate in "Grid-Verbindungen verwalten".

Fehler beim Bearbeiten einer Verbindung zum Grid Federation

Problem

Beim Bearbeiten einer Grid Federation-Verbindung wird die folgende Warnmeldung angezeigt, wenn Sie **Speichern und Testen** auswählen: "Es konnte keine Kandidatenkonfigurationsdatei auf einem oder mehreren Knoten erstellt werden."

Details

Wenn Sie eine Grid-Federation-Verbindung bearbeiten, versucht StorageGRID, eine Datei mit der Kandidatenkonfiguration auf allen Admin-Knoten im ersten Grid zu speichern. Eine Warnmeldung wird angezeigt, wenn diese Datei nicht in allen Admin-Knoten gespeichert werden kann, z. B. weil ein Admin-Knoten offline ist.

Empfohlene Maßnahmen

1. Wählen Sie im Raster, das Sie zum Bearbeiten der Verbindung verwenden, **Knoten** aus.
2. Vergewissern Sie sich, dass alle Admin-Nodes für dieses Grid online sind.
3. Wenn Knoten offline sind, schalten Sie sie wieder online und versuchen Sie erneut, die Verbindung zu bearbeiten.

Fehler beim Klonen des Kontos

Keine Anmeldung bei einem geklonten Mandantenkonto möglich

Problem

Sie können sich nicht bei einem geklonten Mandantenkonto anmelden. Die Fehlermeldung auf der Anmeldeseite des Tenant Manager lautet „Ihre Anmeldedaten für dieses Konto waren ungültig. Bitte versuchen Sie es erneut.“

Details

Wenn ein Mandantenkonto aus dem Quellraster des Mandanten im Zielraster des Mandanten geklont wird, wird aus Sicherheitsgründen das Passwort, das Sie für den lokalen Stammbenutzer des Mandanten festgelegt haben, nicht geklont. Wenn ein Mandant lokale Benutzer in seinem Quellraster erstellt, werden die lokalen Benutzerpasswörter nicht im Zielraster geklont.

Empfohlene Maßnahmen

Bevor sich der Root-Benutzer im Zielraster des Mandanten anmelden kann, muss zunächst ein Grid-Administrator "Ändern Sie das Passwort für den lokalen Root-Benutzer"im Zielraster angemeldet werden.

Bevor sich ein geklonter lokaler Benutzer beim Zielraster des Mandanten anmelden kann, muss der Root-Benutzer des geklonten Mandanten ein Kennwort für den Benutzer im Zielraster hinzufügen. Anweisungen hierzu finden Sie unter"Benutzer managen" in der Anleitung zur Nutzung des Tenant Managers.

Mandant wird ohne Klon erstellt

Problem

Sie sehen die Meldung "Tenant created without a Clone", nachdem Sie einen neuen Tenant mit der Berechtigung **use Grid Federation connection** erstellt haben.

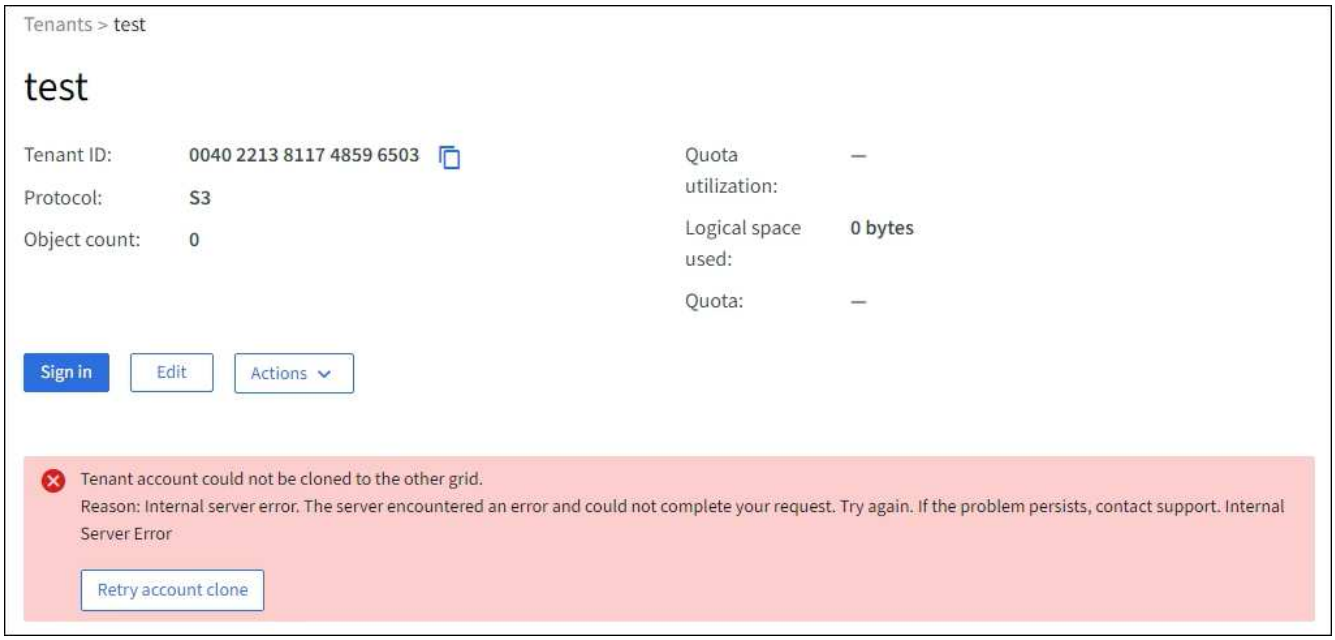
Details

Dieses Problem kann auftreten, wenn Aktualisierungen des Verbindungsstatus verzögert werden, was dazu führen kann, dass eine fehlerhafte Verbindung als **verbunden** aufgeführt wird.

Empfohlene Maßnahmen

1. Überprüfen Sie den in der Fehlermeldung aufgeführten Grund, und beheben Sie alle Netzwerk- oder anderen Probleme, die möglicherweise die Funktion der Verbindung verhindern. Siehe Warnmeldungen und Fehler bei der Grid-Verbundverbindung.
2. Befolgen Sie die Anweisungen zum Testen einer Netzverbundverbindung in"Grid-Verbindungen verwalten", um zu bestätigen, dass das Problem behoben wurde.

3. Wählen Sie im Quellraster des Mandanten **Mandanten** aus.
4. Suchen Sie das Mandantenkonto, das nicht geklont werden konnte.
5. Wählen Sie den Namen der Serviceeinheit aus, um die Detailseite anzuzeigen.
6. Wählen Sie **Kontoklone wiederholen**.



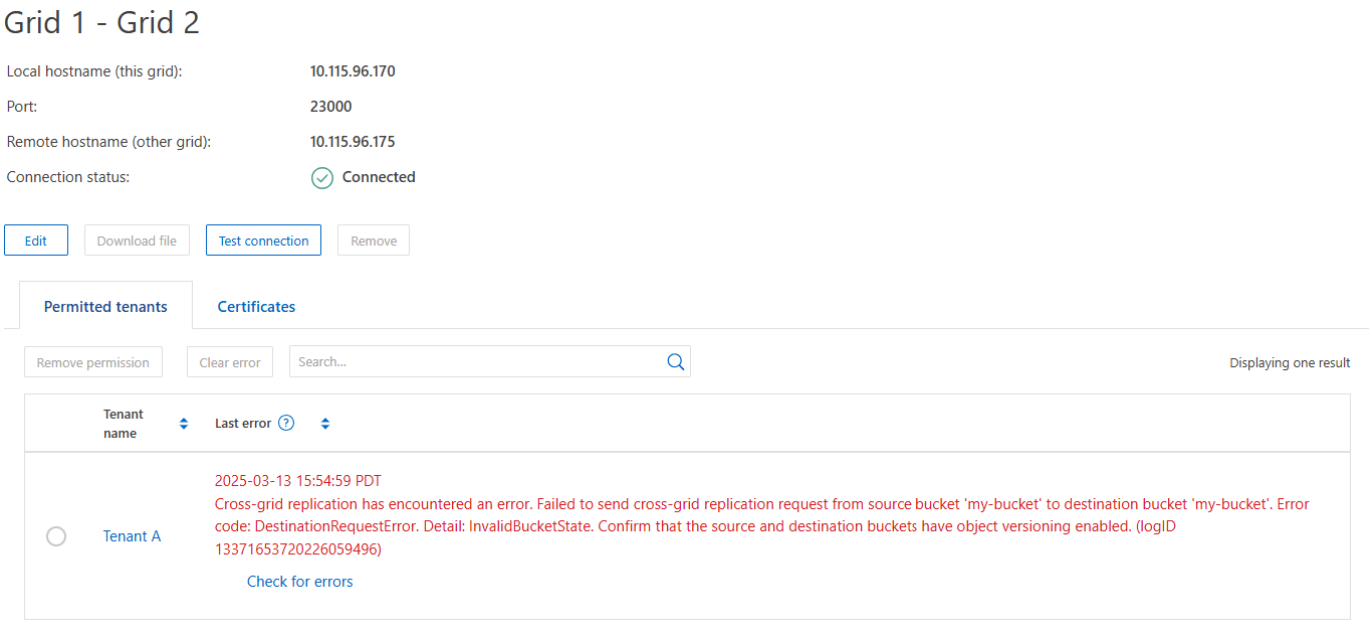
Wenn der Fehler behoben wurde, wird das Mandantenkonto jetzt in das andere Raster geklont.

Grid-übergreifende Replizierungswarnungen und Fehler

Letzter Fehler für Verbindung oder Mandant

Problem

Wenn "Anzeigen einer Netzverbundverbindung" (oder wann "Verwalten der zulässigen Mandanten" für eine Verbindung) Sie einen Fehler in der Spalte **Last error** auf der Seite mit den Verbindungsdetails bemerken. Beispiel:



Details

Für jede Grid-Föderationsverbindung zeigt die Spalte **Letzter Fehler** den letzten Fehler an, der ggf. beim Replizieren der Daten eines Mandanten in das andere Grid aufgetreten ist. In dieser Spalte wird nur der letzte aufgetretene Fehler bei der Cross-Grid-Replikation angezeigt. Eventuell zuvor aufgetretene Fehler werden nicht angezeigt. Ein Fehler in dieser Spalte kann aus einem der folgenden Gründe auftreten:

- Die Quellobjektversion wurde nicht gefunden.
- Der Quell-Bucket wurde nicht gefunden.
- Der Ziel-Bucket wurde gelöscht.
- Der Ziel-Bucket wurde von einem anderen Konto neu erstellt.
- Im Ziel-Bucket ist die Versionierung angehalten.
- Der Ziel-Bucket wurde vom selben Konto neu erstellt, ist aber jetzt nicht mehr versioniert.
- Das Quellobjekt verfügt über S3-Objektsperreinstellungen, die nicht mit den Aufbewahrungseinstellungen auf Mandantenebene des Zielrasters übereinstimmen.
- Das Quellobjekt verfügt über S3 Object Lock-Einstellungen und S3 Object Lock ist im Ziel-Bucket deaktiviert.

Empfohlene Maßnahmen

Wenn in der Spalte **Last error** eine Fehlermeldung angezeigt wird, gehen Sie wie folgt vor:

1. Überprüfen Sie den Nachrichtentext.
2. Führen Sie alle empfohlenen Aktionen aus. Wenn beispielsweise die Versionierung auf dem Ziel-Bucket für die Grid-übergreifende Replizierung angehalten wurde, aktivieren Sie die Versionierung für diesen Bucket neu.
3. Wählen Sie das Verbindungs- oder Mandantenkonto aus der Tabelle aus.
4. Wählen Sie **Fehler löschen**.
5. Wählen Sie **Ja**, um die Meldung zu löschen und den Systemstatus zu aktualisieren.
6. Warten Sie 5-6 Minuten, und nehmen Sie dann ein neues Objekt in den Bucket auf. Bestätigen Sie, dass die Fehlermeldung nicht erneut angezeigt wird.

Um sicherzustellen, dass die Fehlermeldung gelöscht wird, warten Sie mindestens 5 Minuten nach dem Zeitstempel in der Nachricht, bevor Sie ein neues Objekt aufnehmen.

Nachdem Sie den Fehler gelöscht haben, kann ein neuer **Last error** auftreten, wenn Objekte in einem anderen Bucket aufgenommen werden, der ebenfalls einen Fehler hat.

7. Informationen darüber, ob Objekte aufgrund des Bucket-Fehlers nicht repliziert werden konnten, finden Sie unter "Identifizieren Sie fehlgeschlagene Replikationsvorgänge und versuchen Sie es erneut".

Grid-übergreifende Replizierung mit permanenter Fehlerwarnung

Problem

Die Warnung **Cross-Grid Replikation Permanent Failure** wurde ausgelöst.

Details

Diese Warnmeldung weist darauf hin, dass Tenant-Objekte aus einem Grund, der vom Benutzer behoben werden muss, nicht zwischen den Buckets auf zwei Grids repliziert werden können. Diese Warnmeldung wird in der Regel durch eine Änderung an der Quelle oder dem Ziel-Bucket verursacht.

Empfohlene Maßnahmen

1. Melden Sie sich am Raster an, in dem die Warnmeldung ausgelöst wurde.
2. Gehen Sie zu **Konfiguration** > **System** > **Grid-Föderation** und suchen Sie den in der Warnung aufgeführten Verbindungsnamen.
3. Sehen Sie auf der Registerkarte zulässige Mieter in der Spalte **Letzter Fehler** nach, um zu bestimmen, welche Mandantenkonten Fehler aufweisen.
4. Weitere Informationen über den Fehler finden Sie in den Anweisungen unter"Überwachen von Netzverbundverbindungen", um die Grid-übergreifenden Replikationskennzahlen zu überprüfen.
5. Für jedes betroffene Mandantenkonto:
   a. Lesen Sie die Anweisungen in"Überwachen Sie die Mandantenaktivität", um zu bestätigen, dass der Mandant sein Kontingent im Zielraster für die Grid-übergreifende Replikation nicht überschritten hat.
   b. Erhöhen Sie bei Bedarf das Kontingent des Mandanten im Zielraster, damit neue Objekte gespeichert werden können.
6. Melden Sie sich für jeden betroffenen Mandanten in beiden Grids bei Tenant Manager an, damit Sie die Liste der Buckets vergleichen können.
7. Bestätigen Sie für jeden Bucket, für den die Grid-übergreifende Replizierung aktiviert ist:
   - Es gibt einen entsprechenden Bucket für denselben Mandanten auf dem anderen Grid (muss den genauen Namen verwenden).
   - Beide Buckets haben die Objektversionierung aktiviert (die Versionierung kann in keinem Grid ausgesetzt werden).
   - Keiner der Buckets befindet sich im Status **delete objects: Read-only**.
8. Um zu bestätigen, dass das Problem behoben wurde, lesen Sie die Anweisungen unter"Überwachen von Netzverbundverbindungen", um die Grid-übergreifenden Replikationsmetriken zu überprüfen, oder führen Sie die folgenden Schritte aus:
   a. Kehren Sie zur Seite „Grid Federation“ zurück.
   b. Wählen Sie den betroffenen Mandanten aus, und wählen Sie in der Spalte **Letzter Fehler** die Option **Fehler löschen** aus.

c. Wählen Sie **Ja**, um die Meldung zu löschen und den Systemstatus zu aktualisieren.

d. Warten Sie 5-6 Minuten, und nehmen Sie dann ein neues Objekt in den Bucket auf. Bestätigen Sie, dass die Fehlermeldung nicht erneut angezeigt wird.

> Um sicherzustellen, dass die Fehlermeldung gelöscht wird, warten Sie mindestens 5 Minuten nach dem Zeitstempel in der Nachricht, bevor Sie ein neues Objekt aufnehmen.

> Es kann bis zu einem Tag dauern, bis die Warnmeldung gelöscht wird, nachdem sie behoben wurde.

a. Gehen Sie zu, um Objekte zu identifizieren oder Marker zu "Identifizieren Sie fehlgeschlagene Replikationsvorgänge und versuchen Sie es erneut"löschen, die nicht in das andere Grid repliziert wurden, und wiederholen Sie die Replikation bei Bedarf.

Warnung: Grid-übergreifende Replikationsressource nicht verfügbar

Problem

Die Warnung **Grid-übergreifende Replikationsressource nicht verfügbar** wurde ausgelöst.

Details

Diese Warnmeldung weist darauf hin, dass Grid-übergreifende Replikationsanforderungen ausstehen, da eine Ressource nicht verfügbar ist. Es kann beispielsweise ein Netzwerkfehler auftreten.

Empfohlene Maßnahmen

1. Überwachen Sie die Warnmeldung, um zu prüfen, ob das Problem eigenständig gelöst wird.
2. Wenn das Problem weiterhin besteht, prüfen Sie, ob eines der Grid-Netze eine Warnmeldung für die Verbindung **Grid Federation Connection failure** für die gleiche Verbindung oder eine Warnung für einen Knoten **Unable to communicate with Node** hat. Diese Warnmeldung wird möglicherweise behoben, wenn Sie diese Warnungen beheben.
3. Weitere Informationen über den Fehler finden Sie in den Anweisungen unter"Überwachen von Netzverbundverbindungen", um die Grid-übergreifenden Replikationskennzahlen zu überprüfen.
4. Wenn Sie die Warnmeldung nicht beheben können, wenden Sie sich an den technischen Support.

Die Grid-übergreifende Replizierung wird wie gewohnt ausgeführt, nachdem das Problem behoben wurde.

Identifizieren Sie fehlgeschlagene Replikationsvorgänge und versuchen Sie es erneut

Nach dem Beheben der Warnung * Cross-Grid Replikation Permanent Failure* sollten Sie feststellen, ob Objekte oder Löschmarkierungen nicht in das andere Raster repliziert werden konnten. Sie können diese Objekte dann wieder aufnehmen oder die Grid Management API verwenden, um die Replikation erneut zu versuchen.

Die Warnung **Grid-übergreifende Replikation Permanent Failure** weist darauf hin, dass Tenant Objects nicht zwischen den Buckets auf zwei Grids repliziert werden können, aus einem Grund, der vom Benutzer behoben werden muss. Diese Warnmeldung wird in der Regel durch eine Änderung an der Quelle oder dem Ziel-Bucket verursacht. Weitere Informationen finden Sie unter "Fehler beim Grid-Verbund beheben".

Ermitteln Sie, ob Objekte nicht repliziert werden konnten

Um festzustellen, ob Objekte oder Löschmarkierungen nicht in das andere Raster repliziert wurden, können Sie das Überwachungsprotokoll nach Meldungen durchsuchen"CGRR (Grid-übergreifende Replikationsanforderung)". Diese Meldung wird dem Protokoll hinzugefügt, wenn StorageGRID ein Objekt, ein mehrteiliges Objekt oder eine Löschmarkierung nicht in den Ziel-Bucket repliziert.

Sie können die verwenden"Audit-Explain-Tool", um die Ergebnisse in ein übersichtliches Format zu übersetzen.

Bevor Sie beginnen

- Sie haben Root-Zugriffsberechtigung.
- Sie haben die `Passwords.txt` Datei.
- Sie kennen die IP-Adresse des primären Admin-Knotens.

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

   Wenn Sie als root angemeldet sind, wechselt die Eingabeaufforderung von `$` zu `#`.

2. Durchsuchen Sie audit.log nach CGRR-Meldungen, und formatieren Sie die Ergebnisse mit dem Audit-Explain-Tool.

   Dieser Befehl gibt beispielsweise für alle CGRR-Meldungen in den letzten 30 Minuten eine abgrüßungsfunktion ein und verwendet das Audit-Explain-Tool.

   ```
   # awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date { print }' audit.log | grep CGRR | audit-explain
   ```

   Die Ergebnisse des Befehls sehen wie in diesem Beispiel aus, das Einträge für sechs CGRR-Meldungen enthält. In diesem Beispiel gaben alle Grid-übergreifenden Replikationsanforderungen einen allgemeinen Fehler zurück, da das Objekt nicht repliziert werden konnte. Die ersten drei Fehler gelten für die Vorgänge „Objekt replizieren“, und die letzten drei Fehler gelten für die Vorgänge „Markierung zum Löschen von Replikationen“.

```
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-0"
version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-3"
version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-1"
version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-5"
version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
error
```

Jeder Eintrag enthält folgende Informationen:

Feld	Beschreibung
CGRR-Anforderung für Grid-übergreifende Replikation	Der Name der Anforderung
Mandant	Die Konto-ID des Mandanten
Verbindung	Die ID der Netzverbundverbindung
Betrieb	Der Typ des zu versuchenden Replikationsvorgangs: • Objekt replizieren • Löschmarkierung replizieren • Mehrteiliges Objekt replizieren
Eimer	Der Bucket-Name
Objekt	Der Objektname
Version	Die Versions-ID für das Objekt

Feld	Beschreibung
Fehler	Der Fehlertyp. Wenn die Grid-übergreifende Replikation fehlgeschlagen ist, lautet der Fehler „Allgemeiner Fehler“.

Wiederholen Sie fehlgeschlagene Replikationen

Nach dem Generieren einer Liste von Objekten und Löschen von Markierungen, die nicht in den Ziel-Bucket repliziert wurden, und dem Beheben der zugrunde liegenden Probleme können Sie die Replikation auf zwei Arten wiederholen:

- Nehmen Sie jedes Objekt erneut in den Quell-Bucket auf.
- Verwenden Sie die private Grid Management-API, wie beschrieben.

Schritte

1. Wählen Sie oben im Grid Manager das Hilfesymbol aus und wählen Sie **API-Dokumentation**.
2. Wählen Sie **Gehe zu privater API-Dokumentation**.

   Die mit „Privat“ gekennzeichneten StorageGRID-API-Endpunkte können sich ohne Ankündigung ändern. Private StorageGRID-Endpunkte ignorieren auch die API-Version der Anforderung.

3. Wählen Sie im Abschnitt **Cross-Grid-Replication-Advanced** den folgenden Endpunkt aus:

   ```
   POST /private/cross-grid-replication-retry-failed
   ```

4. Wählen Sie **Probieren Sie es aus**.
5. Ersetzen Sie im Textfeld **body** den Beispieleintrag für **versionID** durch eine Versions-ID aus der audit.log, die einer fehlgeschlagenen Cross-Grid-Replikations-Anforderung entspricht.

   Achten Sie darauf, dass die doppelten Anführungszeichen um die Zeichenfolge herum beibehalten werden.

6. Wählen Sie **Ausführen**.
7. Bestätigen Sie, dass der Server-Antwortcode **204** lautet. Dies bedeutet, dass das Objekt oder die Löschmarkierung als ausstehend für die Grid-übergreifende Replikation auf das andere Raster markiert wurde.

   Ausstehend bedeutet, dass die Grid-übergreifende Replikationsanforderung zur Verarbeitung der internen Warteschlange hinzugefügt wurde.

Überwachen Sie Wiederholungen der Replikation

Sie sollten die Wiederholungen der Replikation überwachen, um sicherzustellen, dass sie abgeschlossen sind.

Es kann mehrere Stunden oder länger dauern, bis ein Objekt oder eine Löschmarkierung in das andere Raster repliziert wird.

Sie haben zwei Möglichkeiten, Wiederholungsoperationen zu überwachen:

- Verwenden Sie eine S3- "HeadObject" oder "GetObject" Anforderung. Die Antwort enthält den StorageGRID-spezifischen `x-ntap-sg-cgr-replication-status` Antwortheader, der einen der folgenden Werte enthält:

Raster	Replikationsstatus
Quelle	• **ABGESCHLOSSEN**: Die Replikation war erfolgreich. • **AUSSTEHEND**: Das Objekt wurde noch nicht repliziert. • **FAILURE**: Die Replikation ist mit einem permanenten Fehler fehlgeschlagen. Ein Benutzer muss den Fehler beheben.
Ziel	**REPLIKAT**: Das Objekt wurde aus dem Quellraster repliziert.

- Verwenden Sie die private Grid Management-API, wie beschrieben.

Schritte

1. Wählen Sie im Abschnitt **Cross-Grid-Replication-Advanced** der privaten API-Dokumentation den folgenden Endpunkt aus:

   `GET /private/cross-grid-replication-object-status/{id}`

2. Wählen Sie **Probieren Sie es aus**.
3. Geben Sie im Abschnitt Parameter die Versions-ID ein, die Sie in der Anforderung verwendet `cross-grid-replication-retry-failed` haben.
4. Wählen Sie **Ausführen**.
5. Bestätigen Sie, dass der Server-Antwortcode **200** lautet.
6. Überprüfen Sie den Replikationsstatus. Dieser wird folgendermaßen lauten:
   - **AUSSTEHEND**: Das Objekt wurde noch nicht repliziert.
   - **ABGESCHLOSSEN**: Die Replikation war erfolgreich.
   - **FAILED**: Die Replikation ist mit einem permanenten Fehler fehlgeschlagen. Ein Benutzer muss den Fehler beheben.

Sicherheitsmanagement

Sicherheitsmanagement

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

Verschlüsselung managen

StorageGRID bietet verschiedene Optionen zur Datenverschlüsselung. Sie sollten "Überprüfen Sie die verfügbaren Verschlüsselungsmethoden"herausfinden, welche davon Ihre Datensicherungsanforderungen erfüllen.

Verwalten von Zertifikaten

Sie können "Konfigurieren und verwalten Sie die Serverzertifikate"für HTTP-Verbindungen oder die Clientzertifikate verwendet werden, mit denen eine Client- oder Benutzeridentität beim Server authentifiziert wird.

Konfigurieren von Verschlüsselungsmanagement-Servern

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

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

Proxy-Einstellungen verwalten

Wenn Sie S3-Plattformservices oder Cloud Storage-Pools verwenden, können Sie ein zwischen Storage-Nodes und den externen S3-Endpunkten konfigurieren"Storage-Proxyserver". Wenn Sie AutoSupport-Pakete über HTTPS oder HTTP senden, können Sie ein zwischen Admin-Knoten und technischem Support konfigurieren"Admin-Proxyserver".

Kontrollieren Sie Firewalls

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

Prüfen Sie die StorageGRID Verschlüsselungsmethoden

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

Die Tabelle bietet eine allgemeine Zusammenfassung der in StorageGRID verfügbaren Verschlüsselungsmethoden.

Verschlüsselungsoption	So funktioniert es	Gilt für
Verschlüsselungsmanagement-Server (KMS) in Grid Manager	Sie "Konfigurieren eines Verschlüsselungsmanagement-Servers" für die StorageGRID-Website und "Aktivieren Sie die Node-Verschlüsselung für die Appliance". Anschließend stellt ein Appliance-Node eine Verbindung mit dem KMS her, um einen Schlüsselverschlüsselungsschlüssel (KEK) anzufordern. Dieser Schlüssel verschlüsselt und entschlüsselt den Datenverschlüsselungsschlüssel (DEK) auf jedem Volume.	Appliance-Knoten, deren **Node Encryption** während der Installation aktiviert ist. Alle Daten auf der Appliance sind gegen physischen Verlust oder aus dem Datacenter geschützt. **Hinweis**: Die Verwaltung von Verschlüsselungsschlüsseln mit einem KMS wird nur für Storage Nodes und Service Appliances unterstützt.
Seite „Laufwerkverschlüsselung“ im Installationsprogramm von StorageGRID Appliance	Wenn die Appliance Laufwerke enthält, die Hardwareverschlüsselung unterstützen, können Sie während der Installation eine Passphrase für das Laufwerk festlegen. Wenn Sie eine Passphrase für ein Laufwerk festlegen, kann niemand gültige Daten von Laufwerken wiederherstellen, die aus dem System entfernt wurden, es sei denn, sie kennen die Passphrase. Bevor Sie mit der Installation beginnen, wechseln Sie zu **Hardware konfigurieren** > **Festplattenverschlüsselung**, um eine Passphrase für Laufwerke festzulegen, die für alle von StorageGRID gemanagten Self-Encrypting Drives in einem Node gilt.	Appliances mit Self-Encrypting Drives Alle Daten auf den gesicherten Laufwerken sind vor physischem Verlust oder Entfernung aus dem Datacenter geschützt. Die Festplattenverschlüsselung ist nicht bei von SANtricity gemanagten Laufwerken möglich. Bei einer Storage Appliance mit Self-Encrypting Drives und SANtricity Controllern können Sie die Laufwerksicherheit in SANtricity aktivieren.
Laufwerkssicherheit in SANtricity System Manager	Wenn die Laufwerkssicherheitsfunktion für Ihre StorageGRID-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-Appliances mit Full Disk Encryption-Laufwerken (FDE) oder Self-Encrypting Drives Alle Daten auf den gesicherten Laufwerken sind vor physischem Verlust oder Entfernung aus dem Datacenter geschützt. Kann nicht mit einigen Storage Appliances oder Service-Appliances verwendet werden.

Verschlüsselungsoption	So funktioniert es	Gilt für
Verschlüsselung gespeicherter Objekte	Sie aktivieren die "Verschlüsselung gespeicherter Objekte" Option im Grid-Manager. Wenn diese Option aktiviert ist, werden alle neuen Objekte, die nicht auf Bucket-Ebene oder Objektebene verschlüsselt sind, bei der Aufnahme verschlüsselt.	Neu aufgenommene S3-Objektdaten Vorhandene gespeicherte Objekte werden nicht verschlüsselt. Objektmetadaten und andere sensible Daten werden nicht verschlüsselt.
S3-Bucket-Verschlüsselung	Sie stellen eine PutBucketEncryption-Anforderung aus, um die Verschlüsselung für den Bucket zu aktivieren. Alle neuen Objekte, die nicht auf Objektebene verschlüsselt werden, werden bei der Aufnahme verschlüsselt.	Nur neu aufgenommene S3-Objektdaten Für den Bucket muss eine Verschlüsselung angegeben werden. Vorhandene Bucket-Objekte werden nicht verschlüsselt. Objektmetadaten und andere sensible Daten werden nicht verschlüsselt. "Operationen auf Buckets"
S3-Objektserverseitige Verschlüsselung (SSE)	Sie stellen eine S3-Anforderung zum Speichern eines Objekts aus und schließen den `x-amz-server-side-encryption` Anforderungsheader ein.	Nur neu aufgenommene S3-Objektdaten Für das Objekt muss eine Verschlüsselung angegeben werden. Objektmetadaten und andere sensible Daten werden nicht verschlüsselt. StorageGRID verwaltet die Schlüssel. "Serverseitige Verschlüsselung"
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. Objektmetadaten und andere sensible Daten werden nicht verschlüsselt. Schlüssel werden außerhalb von StorageGRID gemanagt. "Serverseitige Verschlüsselung"

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 - Benutzerhandbuch: Schutz von Daten durch Client-seitige Verschlüsselung"

Verwendung mehrerer Verschlüsselungsmethoden

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

- Sie können einen KMS zum Schutz von Appliance-Nodes verwenden und die Laufwerkssicherheitsfunktion in SANtricity System Manager zum „Doppelverschlüsseln“ von Daten auf den Self-Encrypting Drives in denselben Appliances verwenden.
- Sie können ein KMS verwenden, um Daten auf Appliance-Nodes zu sichern, und die Option gespeicherte Objektverschlüsselung verwenden, um alle Objekte bei der Aufnahme zu verschlüsseln.

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

Verwandte Informationen

"Erfahren Sie mehr über die FIPS-zertifizierten Verschlüsselungsoptionen"

Verwalten von Zertifikaten

Verwalten von Sicherheitszertifikaten

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

StorageGRID verwendet zwei Arten von Sicherheitszertifikaten:

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

Wenn ein Client über HTTPS eine Verbindung zum Server herstellt, antwortet der Server mit dem Serverzertifikat, das einen öffentlichen Schlüssel enthält. Der Client vergleicht die Serversignatur mit der Signatur auf seiner Kopie des Zertifikats. Wenn die Signaturen übereinstimmen, startet der Client eine Sitzung mit dem Server unter Verwendung desselben öffentlichen Schlüssels.

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

Standard Grid CA-Zertifikat

StorageGRID verfügt über eine integrierte Zertifizierungsstelle (CA), die während der Systeminstallation ein internes Grid-CA-Zertifikat generiert. Das Grid-CA-Zertifikat wird standardmäßig verwendet, um den internen StorageGRID -Verkehr zu sichern. Eine externe Zertifizierungsstelle (CA) kann benutzerdefinierte Zertifikate ausstellen, die vollständig mit den Informationssicherheitsrichtlinien Ihres Unternehmens konform sind.

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

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

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

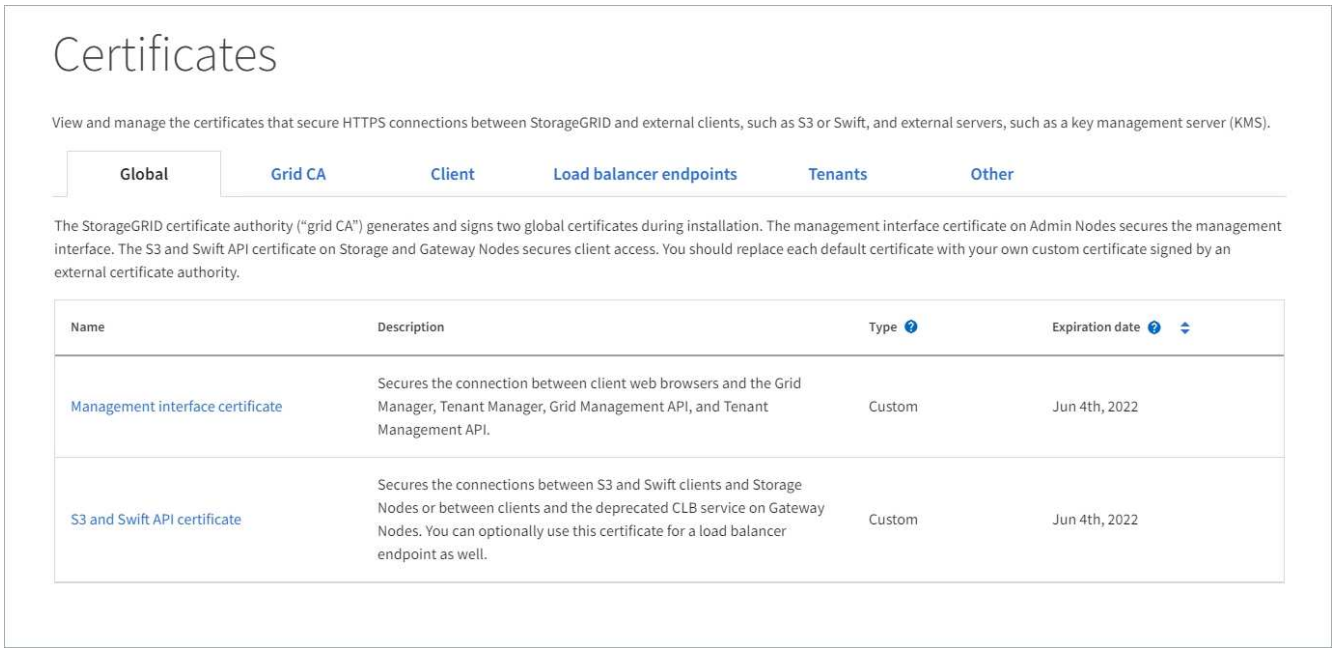
Varianten der Server- und Client-Zertifikatstypen werden auf verschiedene Weise implementiert. Vor der Konfiguration des Systems sollten Sie alle erforderlichen Zertifikate für Ihre spezifische StorageGRID-Konfiguration bereithaben.

Greifen Sie auf Sicherheitszertifikate zu

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

Schritte

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



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 auf eine Registerkarte zugreifen, wenn Sie über die verfügen"Entsprechende Berechtigung".

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

     Jede Registerkarte wird unten mit Links zu weiteren Zertifikatdetails beschrieben.

Weltweit

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

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

Informationen zu den installierten globalen Zertifikaten umfassen:

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

Ihre Vorteile:

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

Grid CA

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

Zertifikatsinformationen umfassen das Ablaufdatum des Zertifikats und den Zertifikatinhalt.

Sie können "Kopieren oder laden Sie das Zertifikat der Grid-Zertifizierungsstelle herunter", aber Sie können es nicht ändern.

Client

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

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

Ihre Vorteile:

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

Load Balancer-Endpunkte

Load Balancer-Endpunktzertifikate Sichern der Verbindungen zwischen S3-Clients und dem StorageGRID Load Balancer-Service auf Gateway-Nodes und Admin-Nodes

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

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

Ihre Vorteile:

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

Mandanten

Mandanten können ihre Verbindungen zu StorageGRID nutzen Identity Federation Server-Zertifikate oder Endpoint-Zertifikate für Plattformservicesichern.

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

Ihre Vorteile:

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

anzuzeigen"

- "Festlegen eines Endpunktzertifikats für den Plattformservice während der Endpunkterstellung"

Sonstiges

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

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

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

> Sie können Informationen für andere Zertifikate nur anzeigen und darauf zugreifen, wenn Sie über die verfügen"Entsprechende Berechtigung".

Ihre Vorteile:

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

Details zum Sicherheitszertifikat

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

Zertifikat für die Managementoberfläche

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	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 dann **Management-Schnittstellenzertifikat**	"Konfigurieren Sie Zertifikate für die Managementoberfläche"

S3-API-Zertifikat

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

Grid-CA-Zertifikat

Siehe Beschreibung des Standard Grid CA-Zertifikats.

Administrator-Client-Zertifikat

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Client	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 wählen Sie dann die Registerkarte **Client**	"Konfigurieren Sie Client-Zertifikate"

Endpunkt-Zertifikat für Load Balancer

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	Authentifiziert die Verbindung zwischen S3 Clients und dem StorageGRID Load Balancer auf Gateway-Nodes und Admin-Nodes. Sie können ein Load Balancer-Zertifikat hochladen oder generieren, wenn Sie einen Load Balancer-Endpunkt konfigurieren. Client-Applikationen verwenden das Load Balancer-Zertifikat, wenn Sie eine Verbindung zu StorageGRID herstellen, um Objektdaten zu speichern und abzurufen. Sie können auch eine benutzerdefinierte Version des globalen Zertifikats verwendenS3-API-Zertifikat, um Verbindungen zum Load Balancer-Dienst zu authentifizieren. Wenn das globale Zertifikat zur Authentifizierung von Load Balancer-Verbindungen verwendet wird, müssen Sie kein separates Zertifikat für jeden Load Balancer-Endpunkt hochladen oder generieren. **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"

Endpunkt-Zertifikat für Cloud Storage Pool

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

Zertifikat für eine E-Mail-Benachrichtigung

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server und Client	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.	**Benachrichtigungen** > **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**	"Verwenden Sie einen externen Syslog-Server"

Verbindungszertifikat für Grid Federation

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server und Client	Authentifizieren und verschlüsseln Sie Informationen, die zwischen dem aktuellen StorageGRID-System und einem anderen Grid in einer Grid-Verbundverbindung gesendet werden.	**Konfiguration** > **System** > **Grid-Föderation**	• "Erstellen von Grid Federation-Verbindungen" • "Verbindungszertifikate drehen"

Zertifikat für Identitätsföderation

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

KMS-Zertifikat (Key Management Server)

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

Endpoint-Zertifikat für Plattform-Services

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

SSO-Zertifikat (Single Sign On)

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

Beispiele für Zertifikate

Beispiel 1: Load Balancer Service

In diesem Beispiel fungiert StorageGRID als Server.

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

Beispiel 2: Externer KMS (Key Management Server)

In diesem Beispiel fungiert StorageGRID als Client.

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

Unterstützte Serverzertifikatstypen

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

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

Weitere Informationen darüber, wie StorageGRID Clientverbindungen sichert, finden Sie unter "Sicherheit für S3-Clients".

Konfigurieren Sie Zertifikate für die Managementoberfläche

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

Über diese Aufgabe

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

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

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

> Um sicherzustellen, dass der Betrieb nicht durch ein fehlerhaftes Serverzertifikat unterbrochen wird, wird die Warnung **Ablauf des Serverzertifikats für die Verwaltungsschnittstelle** ausgelöst, wenn dieses Serverzertifikat bald abläuft. Bei Bedarf können Sie das Ablaufdatum des aktuellen Zertifikats anzeigen, indem Sie **Konfiguration** > **Sicherheit** > **Zertifikate** auswählen und auf der Registerkarte „Global“ das Ablaufdatum für das Management-Schnittstellenzertifikat prüfen.

> Wenn Sie mit einem 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.
> - Sie Zurücksetzen von einem Zertifikat der benutzerdefinierten Managementoberfläche auf das Standard-Serverzertifikat.

Fügen Sie ein Zertifikat für eine benutzerdefinierte Managementoberfläche hinzu

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

Schritte

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

Zertifikat hochladen

Laden Sie die erforderlichen Serverzertifikatdateien hoch.

a. Wählen Sie **Zertifikat hochladen**.

b. Laden Sie die erforderlichen Serverzertifikatdateien hoch:

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

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

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

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

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

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

  Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Zertifikat kopieren PEM** oder **CA-Paket kopieren PEM** aus, um den 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:

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

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

c. Wählen Sie **Erzeugen**.

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

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

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

     Beispiel: `storagegrid_certificate.pem`

   - Wählen Sie **Zertifikat kopieren PEM** aus, um den 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 der Verwaltungsschnittstelle wiederherstellen, werden die von Ihnen konfigurierten benutzerdefinierten Serverzertifikatdateien gelöscht und können nicht vom System wiederhergestellt werden. Das Standardzertifikat für die Verwaltungsschnittstelle wird für alle nachfolgenden neuen Clientverbindungen verwendet.

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

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

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

Bevor Sie beginnen

- Sie haben "Bestimmte Zugriffsberechtigungen".
- Sie haben die `Passwords.txt` Datei.

Über diese Aufgabe

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

Schritte

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

   Wenn Sie als root angemeldet sind, wechselt die Eingabeaufforderung von `$` zu `#`.

3. Konfigurieren Sie StorageGRID mit einem neuen selbstsignierten Zertifikat.

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

   - Für `--domains` verwenden Sie Platzhalter, um die vollständig qualifizierten Domänennamen aller Admin-Knoten darzustellen. Zum Beispiel `*.ui.storagegrid.example.com` verwendet den Platzhalter * für `admin1.ui.storagegrid.example.com` und `admin2.ui.storagegrid.example.com`.
   - Legen Sie fest `--type management`, um das Zertifikat für die Managementoberfläche zu

konfigurieren, das von Grid Manager und Tenant Manager verwendet wird.

- Die erstellten Zertifikate sind standardmäßig für ein Jahr (365 Tage) gültig und müssen vor Ablauf neu erstellt werden. Sie können das Argument verwenden `--days`, um die Standardgültigkeitsdauer zu überschreiben.

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

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

Die resultierende Ausgabe enthält das öffentliche Zertifikat, das vom Management-API-Client benötigt wird.

4. Wählen Sie das Zertifikat aus, und kopieren Sie es.

   Geben Sie DIE START- und DAS ENDE-Tags in Ihre Auswahl ein.

5. Melden Sie sich von der Befehls-Shell ab. `$ exit`
6. Bestätigen Sie, dass das Zertifikat konfiguriert wurde:
   a. Greifen Sie auf den Grid Manager zu.
   b. Wählen Sie **Konfiguration** > **Sicherheit** > **Zertifikate**
   c. Wählen Sie auf der Registerkarte **Global** die Option **Management Interface Certificate** aus.
7. Konfigurieren Sie den Management-Client so, dass er das öffentliche Zertifikat verwendet, das Sie kopiert haben. Geben Sie DIE START- und END-Tags an.

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

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

Schritte

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

Laden Sie die Zertifikatdatei oder das CA-Paket herunter

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

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

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

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

   Beispiel: `storagegrid_certificate.pem`

Zertifikat oder CA-Bundle-PEM kopieren

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

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

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

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

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

   Beispiel: `storagegrid_certificate.pem`

Konfigurieren Sie S3-API-Zertifikate

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

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

Über diese Aufgabe

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

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

Nach Abschluss der Konfiguration auf dem Server müssen Sie möglicherweise auch das Grid-CA-Zertifikat in

dem S3-API-Client installieren, den Sie für den Zugriff auf das System verwenden, je nachdem, welche Root-Zertifizierungsstelle Sie verwenden.

> Um sicherzustellen, dass der Betrieb nicht durch ein fehlerhaftes Serverzertifikat unterbrochen wird, wird die Warnung **Ablauf des globalen Serverzertifikats für S3-API** ausgelöst, wenn das Stammserverzertifikat bald abläuft. Bei Bedarf können Sie das Ablaufdatum des aktuellen Zertifikats anzeigen, indem Sie **Konfiguration** > **Sicherheit** > **Zertifikate** auswählen und auf der Registerkarte „Global“ das Ablaufdatum für das S3-API-Zertifikat anzeigen.

Sie können ein benutzerdefiniertes S3-API-Zertifikat hochladen oder generieren.

Fügen Sie ein benutzerdefiniertes S3-API-Zertifikat hinzu

Schritte

1. Wählen Sie **Konfiguration** > **Sicherheit** > **Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global S3 API-Zertifikat** aus.
3. Wählen Sie **Benutzerdefiniertes Zertifikat verwenden**.
4. Hochladen oder Generieren des Zertifikats

Zertifikat hochladen

Laden Sie die erforderlichen Serverzertifikatdateien hoch.

a. Wählen Sie **Zertifikat hochladen**.

b. Laden Sie die erforderlichen Serverzertifikatdateien hoch:

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

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

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

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

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

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

  Beispiel: `storagegrid_certificate.pem`

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

d. Wählen Sie **Speichern**.

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

Zertifikat wird generiert

Erstellen Sie die Serverzertifikatdateien.

a. Wählen Sie **Zertifikat erstellen**.

b. Geben Sie die Zertifikatsinformationen an:

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

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

c. Wählen Sie **Erzeugen**.

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

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

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

   Beispiel: `storagegrid_certificate.pem`

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

e. Wählen Sie **Speichern**.

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

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

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

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

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

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

Stellen Sie das standardmäßige S3-API-Zertifikat wieder her

Sie können auf die Verwendung des standardmäßigen S3-API-Zertifikats für S3-Client-Verbindungen zu Storage-Nodes zurücksetzen. Sie können jedoch das S3-API-Standardzertifikat nicht für einen Load Balancer-Endpunkt verwenden.

Schritte

1. Wählen Sie **Konfiguration** > **Sicherheit** > **Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global S3 API-Zertifikat** aus.
3. Wählen Sie **Standard-Zertifikat verwenden**.

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

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

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

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

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

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

Schritte

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

Laden Sie die Zertifikatdatei oder das CA-Paket herunter

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

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

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

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

   Beispiel: `storagegrid_certificate.pem`

Zertifikat oder CA-Bundle-PEM kopieren

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

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

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

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

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

   Beispiel: `storagegrid_certificate.pem`

Verwandte Informationen

- "S3-REST-API VERWENDEN"
- "Konfigurieren Sie die Domänennamen des S3-Endpunkts"

Kopieren Sie das Grid-CA-Zertifikat

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

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben "Bestimmte Zugriffsberechtigungen".

Über diese Aufgabe

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

Schritte

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

Laden Sie die Zertifikatdatei herunter

Laden Sie die Zertifikatdatei herunter `.pem`.

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

   Beispiel: `storagegrid_certificate.pem`

Zertifikat PEM kopieren

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

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

   Beispiel: `storagegrid_certificate.pem`

Konfigurieren Sie StorageGRID-Zertifikate für FabricPool

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

Bevor Sie beginnen

- Sie haben "Bestimmte Zugriffsberechtigungen".
- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".

Über diese Aufgabe

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

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

Schritte

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

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

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

   Geben Sie den Endpunkt-Port des Load Balancer und den vollständig qualifizierten 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.

Siehe "Verwalten von Sicherheitszertifikaten" und "Konfigurieren Sie benutzerdefinierte Serverzertifikate".

> Um sicherzustellen, dass der Betrieb nicht durch ein fehlerhaftes Serverzertifikat unterbrochen wird, wird die Warnung **Ablauf der auf der Seite „Zertifikate“ konfigurierten Clientzertifikate** ausgelöst, wenn dieses Serverzertifikat bald abläuft. Bei Bedarf können Sie das Ablaufdatum des aktuellen Zertifikats anzeigen, indem Sie **Konfiguration** > **Sicherheit** > **Zertifikate** auswählen und auf der Registerkarte „Client“ das Ablaufdatum für das Client-Zertifikat anzeigen.

> Wenn Sie einen Schlüsselverwaltungsserver (KMS) zum Schutz der Daten auf speziell konfigurierten Geräteknoten verwenden, lesen Sie die spezifischen Informationen zu "Hochladen eines KMS-Clientzertifikats".

Bevor Sie beginnen

- Sie haben Root-Zugriffsberechtigung.
- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- So konfigurieren Sie ein Clientzertifikat:
  - Sie haben die IP-Adresse oder den 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 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

Gehen Sie wie folgt vor, um das Clientzertifikat hinzuzufügen:

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

Das Zertifikat der Managementoberfläche ist bereits konfiguriert

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

Schritte

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

      Das neue Zertifikat wird auf der Registerkarte Client angezeigt.
7. Konfiguration eines externen Überwachungstools, Wie Grafana.

KANN Client-Zertifikat AUSGESTELLT haben

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

Schritte

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

Zertifikat vom Grid Manager generiert

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

Schritte

1. Wählen Sie im Grid Manager **Konfiguration** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Client**.
2. Wählen Sie **Hinzufügen**.
3. Geben Sie einen Zertifikatnamen ein.
4. Um über Ihr externes Monitoring-Tool auf Prometheus-Kennzahlen zuzugreifen, wählen Sie **prometheus zulassen**.
5. Wählen Sie **Weiter**.
6. Wählen Sie für den Schritt **Zertifikate anhängen Zertifikat generieren** aus.
7. Geben Sie die Zertifikatsinformationen an:
   - **Subject** (optional): X.509 Subject oder Distinguished Name (DN) des Zertifikateigentümers.
   - **Tage gültig**: Die Anzahl der Tage, an denen das generierte Zertifikat gültig ist, beginnend mit dem Zeitpunkt, an dem es generiert wird.
   - **Key-Usage-Erweiterungen hinzufügen**: Wenn ausgewählt (Standard und empfohlen), werden Key-Usage und erweiterte Key-Usage-Erweiterungen zum generierten Zertifikat hinzugefügt.

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

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

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

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

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

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

     Beispiel: `storagegrid_certificate.pem`

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

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

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

    Das neue Zertifikat wird auf der Registerkarte Client angezeigt.

11. Wählen Sie im Grid Manager **Konfiguration** > **Sicherheit** > **Zertifikate** und wählen Sie dann die Registerkarte **Global**.
12. Wählen Sie **Management Interface Certificate** aus.
13. Wählen Sie **Benutzerdefiniertes Zertifikat verwenden**.
14. Laden Sie die Dateien Certificate.pem und private_key.pem aus dem Schritt hochDetails zum Clientzertifikat. 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 **Speichern**, um das Zertifikat im Grid Manager zu speichern.

       Das neue Zertifikat wird auf der Zertifikatsseite der Verwaltungsschnittstelle angezeigt.

15. Konfiguration eines externen Überwachungstools, Wie Grafana.

Konfigurieren Sie ein externes Monitoring-Tool

Schritte

1. Konfigurieren Sie die folgenden Einstellungen für Ihr externes Monitoring-Tool, z. B. Grafana.
   a. **Name**: Geben Sie einen Namen für die Verbindung ein.

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

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

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

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

d. Kopieren Sie unter TLS/SSL Auth Details und fügen Sie: + ein
   - Das Management-Interface-CA-Zertifikat nach **CA-Zertifikat**
   - Das Client-Zertifikat an **Client-Zertifikat**
   - Der private Schlüssel zu **Client Key**

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

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

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

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

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

Client-Zertifikate bearbeiten

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

Schritte

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

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

2. Wählen Sie das Zertifikat aus, das Sie bearbeiten möchten.
3. Wählen Sie **Bearbeiten** und dann **Name und Berechtigung bearbeiten** aus
4. Geben Sie einen Zertifikatnamen ein.
5. Um über Ihr externes Monitoring-Tool auf Prometheus-Kennzahlen zuzugreifen, wählen Sie **prometheus zulassen**.
6. Wählen Sie **Weiter**, um das Zertifikat im Grid Manager zu speichern.

   Das aktualisierte Zertifikat wird auf der Registerkarte Client angezeigt.

Verbinden Sie das neue Clientzertifikat

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

Schritte

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

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

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

Zertifikat hochladen

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

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

b. Laden Sie den Namen des Client-Zertifikats hoch (`.pem`).

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

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

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

   Beispiel: `storagegrid_certificate.pem`

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

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

   Das aktualisierte Zertifikat wird auf der Registerkarte Client angezeigt.

Zertifikat wird generiert

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

a. Wählen Sie **Zertifikat erstellen**.

b. Geben Sie die Zertifikatsinformationen an:

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

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

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

c. Wählen Sie **Erzeugen**.

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

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

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

andere Stelle zu kopieren.

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

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

  Beispiel: `storagegrid_certificate.pem`

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

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

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

Das neue Zertifikat wird auf der Registerkarte Client angezeigt.

Herunterladen oder Kopieren von Clientzertifikaten

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

Schritte

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

Laden Sie die Zertifikatdatei herunter

Laden Sie die Zertifikatdatei herunter `.pem`.

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

   Beispiel: `storagegrid_certificate.pem`

Zertifikat kopieren

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

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

   Beispiel: `storagegrid_certificate.pem`

Entfernen Sie Client-Zertifikate

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

Schritte

1. Wählen Sie **Konfiguration** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Client**.
2. Wählen Sie das Zertifikat aus, das Sie entfernen möchten.
3. Wählen Sie **Löschen** und bestätigen Sie dann.

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

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

Konfigurieren Sie die Sicherheitseinstellungen

Verwalten Sie die TLS- und SSH-Richtlinie

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

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

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

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Root-Zugriffsberechtigung".

Wählen Sie eine Sicherheitsrichtlinie aus

Schritte

1. Wählen Sie **Konfiguration** > **Sicherheit** > **Sicherheitseinstellungen**.

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

2. Sehen Sie sich die Registerkarten an, um mehr über die verfügbaren Richtlinien zu erfahren.

Moderne Kompatibilität (Standard)

Verwenden Sie die Standardrichtlinie, wenn Sie eine starke Verschlüsselung benötigen und keine besonderen Anforderungen haben. Diese Richtlinie ist mit den meisten TLS- und SSH-Clients kompatibel.

Kompatibilität mit älteren Systemen

Verwenden Sie die Legacy-Kompatibilitätsrichtlinie, wenn Sie zusätzliche Kompatibilitätsoptionen für ältere Clients benötigen. Die zusätzlichen Optionen in dieser Richtlinie machen sie möglicherweise weniger sicher als die moderne Kompatibilitätsrichtlinie.

Gemeinsame Kriterien

Verwenden Sie die Common Criteria-Richtlinie, wenn Sie eine Common Criteria-Zertifizierung benötigen.

FIPS-strikt

Verwenden Sie die strikte FIPS-Richtlinie, wenn Sie eine Common Criteria-Zertifizierung benötigen und das NetApp Cryptographic Security Module (NCSM) 3.0.8 oder das NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64-Modul für externe Clientverbindungen zu Load Balancer-Endpunkten, Tenant Manager und Grid Manager verwenden müssen. Die Verwendung dieser Richtlinie kann die Leistung beeinträchtigen.

Das NCSM 3.0.8- und NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64-Modul wird in den folgenden Vorgängen verwendet:

- NCSM
  - TLS-Verbindungen zwischen den folgenden Diensten: ADC, AMS, CMN, DDS, LDR, SSM, NMS, mgmt-api, nginx, nginx-gw und cache-svc
  - TLS-Verbindungen zwischen Clients und dem nginx-gw-Dienst (Load Balancer-Endpunkte)
  - TLS-Verbindungen zwischen Clients und dem LDR-Dienst
  - Objektinhaltsverschlüsselung für SSE-S3, SSE-C und die Einstellung „Gespeicherte Objektverschlüsselung“
  - SSH-Verbindungen

  Weitere Informationen finden Sie im NIST Cryptographic Algorithm Validation Program."Zertifikat Nr. 4838" .

- NetApp StorageGRID Kernel Crypto API-Modul

  Das NetApp StorageGRID Kernel Crypto API-Modul ist nur auf VM- und StorageGRID Appliance-Plattformen vorhanden.

  - Entropie-Sammlung
  - Knotenverschlüsselung

  Weitere Informationen finden Sie im NIST Cryptographic Algorithm Validation Program."Zertifikate Nr. A6242 bis Nr. A6257" Und"Entropie-Zertifikat Nr. E223" .

Hinweis: Nachdem Sie diese Richtlinie ausgewählt haben,"Führen Sie einen Rolling Reboot durch" für alle Knoten, um das NCSM zu aktivieren. Verwenden Sie **Wartung** > **Rollierender Neustart**, um Neustarts zu initiieren und zu überwachen.

Individuell

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

Wenn Ihr StorageGRID FIPS 140-Kryptografieanforderungen hat, aktivieren Sie optional die FIPS-Modusfunktion, um das NCSM 3.0.8- und NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64-Modul zu verwenden:

a. Legen Sie die `fipsMode` Parameter auf `true` .

b. Wenn Sie dazu aufgefordert werden,"Führen Sie einen Rolling Reboot durch" für alle Knoten, um die Kryptografiemodule zu aktivieren. Verwenden Sie **Wartung** > **Rollierender Neustart**, um Neustarts zu initiieren und zu überwachen.

c. Wählen Sie **Support** > **Diagnose**, um die aktiven FIPS-Modulversionen anzuzeigen.

3. Um Details zu den Chiffren, Protokollen und Algorithmen der einzelnen Richtlinien anzuzeigen, wählen Sie **Details anzeigen**.
4. Um die aktuelle Richtlinie zu ändern, wählen Sie **Richtlinie verwenden**.

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

Erstellen Sie eine benutzerdefinierte Sicherheitsrichtlinie

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

Schritte

1. Wählen Sie auf der Kachel der Richtlinie, die der benutzerdefinierten Richtlinie, die Sie erstellen möchten, am ähnlichsten ist, **Details anzeigen** aus.
2. Wählen Sie **in Zwischenablage kopieren**, und wählen Sie dann **Abbrechen**.

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

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

angezeigt.

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

Vorübergehendes Zurücksetzen auf die Standard-Sicherheitsrichtlinie

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

Sie können vorübergehend auf die Standard-Sicherheitsrichtlinie zurücksetzen.

Schritte

1. Melden Sie sich bei einem Admin-Knoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@Admin_Node_IP`
   b. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.
   c. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
   d. Geben Sie das in der Datei aufgeführte Passwort ein `Passwords.txt`.

   Wenn Sie als root angemeldet sind, wechselt die Eingabeaufforderung von `$` zu `#`.

2. Führen Sie den folgenden Befehl aus:

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

3. Greifen Sie über einen Webbrowser auf den Grid Manager auf demselben Admin-Node zu.
4. Befolgen Sie die Schritte unterWählen Sie eine Sicherheitsrichtlinie aus, um die Richtlinie erneut zu konfigurieren.

Konfigurieren Sie die Netzwerk- und Objektsicherheit

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

Verschlüsselung gespeicherter Objekte

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

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

Weitere Informationen zu Verschlüsselungsmethoden von StorageGRID finden Sie unter "Prüfen Sie die StorageGRID Verschlüsselungsmethoden".

Client-Änderung verhindern

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

S3-REST-API

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

Aktivieren Sie HTTP für Storage Node-Verbindungen

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

Verwenden Sie HTTP nur für Storage-Node-Verbindungen, wenn S3-Clients HTTP-Verbindungen direkt zu Storage-Nodes herstellen müssen. Sie müssen diese Option nicht für Clients verwenden, die nur HTTPS-Verbindungen verwenden, oder für Clients, die eine Verbindung zum Load Balancer-Dienst herstellen (da Sie entweder HTTP oder HTTPS verwenden können"Konfigurieren Sie jeden Endpunkt der Lastverteilung").

Unter "Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen"erfahren Sie, welche Ports S3-Clients bei der Verbindung mit Storage-Nodes über HTTP oder HTTPS verwenden.

Wählen Sie Optionen aus

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben Root-Zugriffsberechtigung.

Schritte

1. Wählen Sie **Konfiguration** > **Sicherheit** > **Sicherheitseinstellungen**.
2. Wählen Sie die Registerkarte **Netzwerk und Objekte**.
3. Verwenden Sie für die Verschlüsselung gespeicherter Objekte die Einstellung **None** (Standard), wenn Sie keine Verschlüsselung gespeicherter Objekte wünschen, oder wählen Sie **AES-128** oder **AES-256**, um gespeicherte Objekte zu verschlüsseln.
4. Wählen Sie optional **Client-Änderung verhindern** aus, wenn Sie S3-Clients daran hindern möchten, bestimmte Anfragen zu stellen.

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

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

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

6. Wählen Sie **Speichern**.

Ändern Sie die Sicherheitseinstellungen der Schnittstelle

Mit den Sicherheitseinstellungen der Schnittstelle können Sie festlegen, ob Benutzer abgemeldet werden, wenn sie länger als die angegebene Zeit inaktiv sind und ob ein Stack Trace in API-Fehlermeldungen enthalten ist.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben "Root-Zugriffsberechtigung".

Über diese Aufgabe

Die Seite **Sicherheitseinstellungen** enthält die Einstellungen **Browser Inaktivität Timeout** und **Management API Stack Trace**.

Zeitlimit für Inaktivität des Browsers

Gibt an, wie lange der Browser eines Benutzers inaktiv sein kann, bevor der Benutzer abgemeldet wird. Die Standardeinstellung ist 15 Minuten.

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

- Ein separater, nicht konfigurierbarer StorageGRID-Timer, der für die Systemsicherheit enthalten ist. Das Authentifizierungstoken jedes Benutzers läuft 16 Stunden nach der Anmeldung des Benutzers ab. Wenn die Authentifizierung eines Benutzers abläuft, wird dieser Benutzer automatisch abgemeldet, auch wenn das Zeitlimit für die Inaktivität des Browsers deaktiviert ist oder der Wert für das Browsertimeout nicht erreicht wurde. Um das Token zu erneuern, muss sich der Benutzer erneut anmelden.
- Timeout-Einstellungen für den Identitäts-Provider, vorausgesetzt, Single Sign-On (SSO) ist für StorageGRID aktiviert.

  Wenn SSO aktiviert ist und es beim Browser eines Benutzers zu einer Zeitüberschreitung kommt, muss der Benutzer seine SSO-Anmeldeinformationen erneut eingeben, um wieder auf StorageGRID zugreifen zu können. Sehen "So funktioniert SSO" .

Management-API-Stack-Trace

Steuert, ob ein Stack-Trace in den Fehlerantworten von Grid Manager und Tenant Manager API zurückgegeben wird.

Diese Option ist standardmäßig deaktiviert, aber Sie möchten diese Funktion möglicherweise für eine Testumgebung aktivieren. Im Allgemeinen sollten Sie Stack Trace in Produktionsumgebungen deaktiviert lassen, um zu vermeiden, dass interne Softwaredetails bei Auftreten von API-Fehlern offengelegt werden.

Schritte

1. Wählen Sie **Konfiguration** > **Sicherheit** > **Sicherheitseinstellungen**.
2. Wählen Sie die Registerkarte **Interface**.
3. So ändern Sie die Einstellung für das Zeitlimit für die Inaktivität des Browsers:
   a. Erweitern Sie die Ziehharmonika.
   b. Um die Sperrzeit zu ändern, geben Sie einen Wert zwischen 60 Sekunden und 7 Tagen an. Die standardmäßige Zeitüberschreitung beträgt 15 Minuten.
   c. Um diese Funktion zu deaktivieren, deaktivieren Sie das Kontrollkästchen.

d. Wählen Sie **Speichern**.

   Die neue Einstellung wirkt sich nicht auf Benutzer aus, die gerade angemeldet sind. Benutzer müssen sich erneut anmelden oder ihren Browser aktualisieren, damit die neue Timeout-Einstellung wirksam wird.

4. So ändern Sie die Einstellung für Management-API-Stapelverfolgung:
   a. Erweitern Sie die Ziehharmonika.
   b. Aktivieren Sie das Kontrollkästchen, um eine Stapelverfolgung in den Fehlerantworten von Grid Manager und Tenant Manager API zurückzugeben.

      Lassen Sie Stack Trace in Produktionsumgebungen deaktiviert, um zu vermeiden, dass interne Softwaredetails bei API-Fehlern offengelegt werden.

   c. Wählen Sie **Speichern**.

Externen SSH-Zugriff verwalten

Verwalten Sie den SSH-Zugriff für eingehenden Datenverkehr in das Grid, indem Sie den externen Zugriff blockieren oder zulassen. Die Verwaltung des externen SSH-Zugriffs hat keine Auswirkungen auf den Datenverkehr zwischen Knoten im Grid.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben "Root-Zugriffsberechtigung".

Über diese Aufgabe

Um die Systemsicherheit zu erhöhen, wird der externe SSH-Zugriff standardmäßig blockiert. Wenn Sie Aufgaben ausführen müssen, die eingehenden SSH-Zugriff erfordern, wie etwa die Fehlerbehebung, lassen Sie vorübergehend den externen Zugriff zu. Wenn Sie die Aufgabe abgeschlossen haben, blockieren Sie den externen Zugriff.

Schritte

1. Wählen Sie **Konfiguration** > **Sicherheit** > **Sicherheitseinstellungen**.
2. Wählen Sie die Registerkarte **SSH blockieren**.
3. Verwenden Sie die Option **Eingehenden SSH-Zugriff blockieren**, um den externen SSH-Zugriff zu verwalten:
   a. Aktivieren Sie das Kontrollkästchen, um den Zugriff zu blockieren (Standard).
   b. Deaktivieren Sie das Kontrollkästchen, um den Zugriff zuzulassen.

      Erfordert Zugriff auf Port 22 zwischen dem Service-Laptop und allen anderen Grid-Knoten. Entfernen Sie den Zugriff auf Port 22, sobald Sie die Wartungsarbeiten abgeschlossen haben.

4. Wählen Sie **Speichern**.

Konfigurieren von Verschlüsselungsmanagement-Servern

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.

StorageGRID unterstützt nur bestimmte Verschlüsselungsmanagement-Server. Eine Liste der unterstützten Produkte und Versionen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool (IMT)".

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

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

KMS und Appliance-Konfiguration

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

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

Das Flussdiagramm zeigt die parallele Einrichtung von KMS und die Einrichtung der Appliance. Sie können jedoch die Verschlüsselungsmanagement-Server je nach Ihren Anforderungen vor oder nach Aktivierung der Node-Verschlüsselung für neue Appliance-Nodes einrichten.

Einrichten des Verschlüsselungsmanagement-Servers (KMS)

Die Einrichtung eines Schlüsselverwaltungsservers umfasst die folgenden grundlegenden Schritte.

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

Richten Sie das Gerät ein

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

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

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

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

Weitere Informationen finden Sie unter "Aktivieren Sie die Node-Verschlüsselung".

Verschlüsselungsmanagementprozess (wird automatisch durchgeführt)

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

1. Wenn Sie eine Appliance installieren, bei der die Node-Verschlüsselung im Grid aktiviert ist, bestimmt StorageGRID, ob für den Standort, der den neuen Node enthält, eine KMS-Konfiguration vorhanden ist.
   - Wenn bereits ein KMS für den Standort konfiguriert wurde, erhält die Appliance die KMS-Konfiguration.
   - Wenn ein KMS für den Standort noch nicht konfiguriert wurde, werden die Daten auf der Appliance weiterhin durch die temporäre KEK verschlüsselt, bis Sie einen KMS für den Standort konfigurieren

und die Appliance die KMS-Konfiguration erhält.

2. Die Appliance verwendet die KMS-Konfiguration, um eine Verbindung zum KMS herzustellen und einen Verschlüsselungsschlüssel anzufordern.
3. Der KMS sendet einen Verschlüsselungsschlüssel an die Appliance. Der neue Schlüssel des KMS ersetzt die temporäre KEK und wird nun zur Verschlüsselung und Entschlüsselung der DEKs für die Appliance-Volumes verwendet.

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

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

Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers

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

Welche Version von KMIP wird unterstützt?

StorageGRID unterstützt KMIP Version 1.4.

"Spezifikation Des Key Management Interoperability Protocol Version 1.4"

Was sind die Netzwerküberlegungen?

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.

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

Welche Versionen von TLS werden unterstützt?

Für die Kommunikation zwischen den Appliance-Nodes und dem konfigurierten KMS werden sichere TLS-Verbindungen verwendet. StorageGRID unterstützt entweder das TLS 1.2- oder TLS 1.3-Protokoll, wenn KMIP-Verbindungen zu einem KMS- oder KMS-Cluster hergestellt werden, basierend auf den von KMS unterstützten und von "TLS- und SSH-Richtlinie" Ihnen verwendeten Komponenten.

StorageGRID handelt beim Herstellen der Verbindung das Protokoll und die Verschlüsselung (TLS 1.2) oder die Verschlüsselungssuite (TLS 1.3) mit dem KMS aus. Um zu sehen, welche Protokollversionen und Chiffren/Chiffrensammlungen verfügbar sind, lesen Sie die `tlsOutbound` Abschnitt der aktiven TLS- und SSH-Richtlinie des Grids (**Konfiguration** > **Sicherheit Sicherheitseinstellungen**).

Welche Appliances werden unterstützt?

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

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

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

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

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

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

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

Wann sollte ich wichtige Management-Server konfigurieren?

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

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

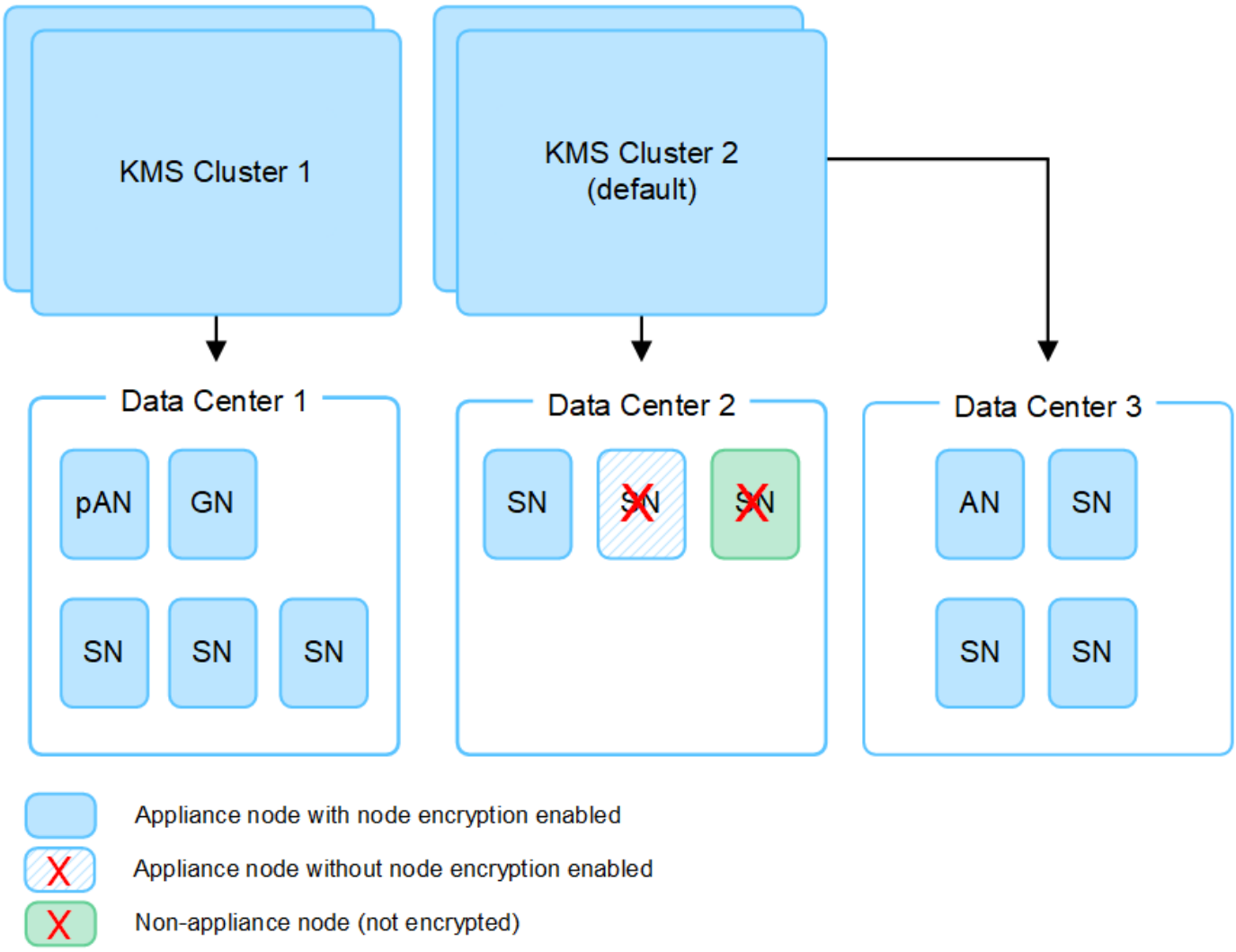
Wie viele wichtige Management Server brauche ich?

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

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

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

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



Was passiert, wenn eine Taste gedreht wird?

Als bewährte Sicherheitsverfahren sollten Sie regelmäßig "Drehen Sie den Verschlüsselungsschlüssel"von jedem konfigurierten KMS verwendet werden.

Wenn die neue Schlüsselversion verfügbar ist:

- Die Appliance wird automatisch auf die verschlüsselten Appliance-Nodes am Standort oder an den dem KMS zugeordneten Standorten verteilt. Die Verteilung sollte innerhalb einer Stunde erfolgen, wenn der Schlüssel gedreht wird.
- Wenn der Node der verschlüsselten Appliance offline ist, wenn die neue Schlüsselversion verteilt ist, erhält der Node den neuen Schlüssel, sobald er neu gebootet wird.
- Wenn die neue Schlüsselversion aus irgendeinem Grund nicht zur Verschlüsselung von Appliance-Volumes verwendet werden kann, wird der Alarm **KMS-Schlüsselrotation fehlgeschlagen** für den Appliance-Knoten ausgelöst. Möglicherweise müssen Sie sich an den technischen Support wenden, um Hilfe bei der Lösung dieses Alarms zu erhalten.

Kann ich einen Appliance-Knoten nach der Verschlüsselung wiederverwenden?

Wenn Sie eine verschlüsselte Appliance in einem anderen StorageGRID System installieren müssen, müssen Sie zuerst den Grid-Node außer Betrieb nehmen, um Objektdaten auf einen anderen Node zu verschieben.

Anschließend können Sie das Installationsprogramm der StorageGRID-Appliance für verwenden "Löschen Sie die KMS-Konfiguration". Durch das Löschen der KMS-Konfiguration wird die **Node Encryption**-Einstellung deaktiviert und die Zuordnung zwischen dem Appliance-Knoten und der KMS-Konfiguration für den StorageGRID-Standort wird aufgehoben.

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

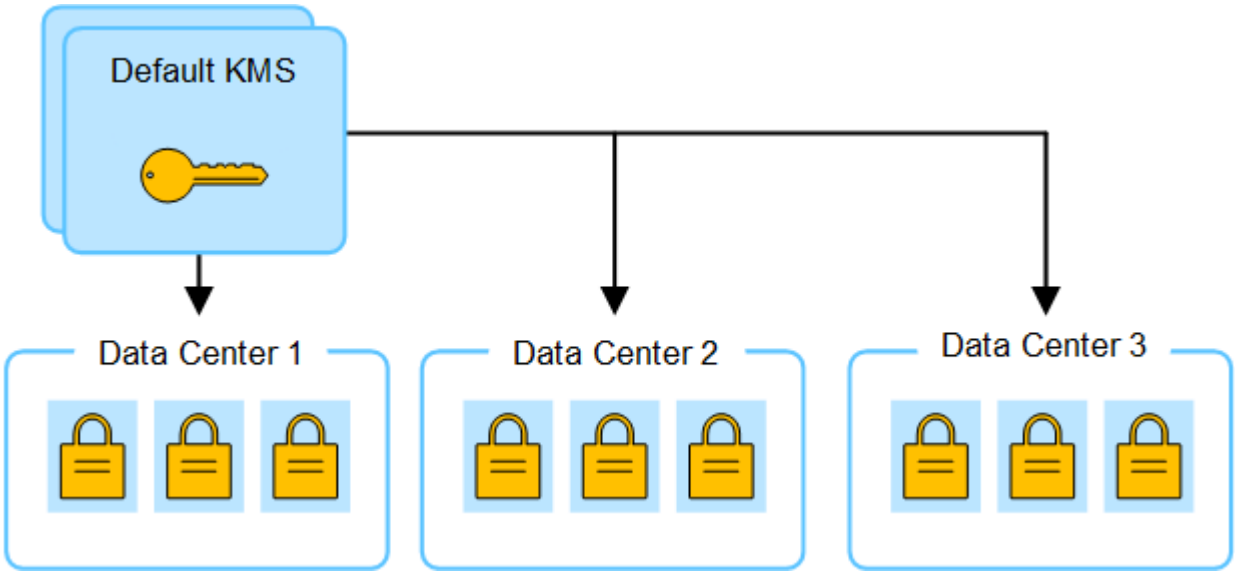
Überlegungen für das Ändern des KMS für einen Standort

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

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

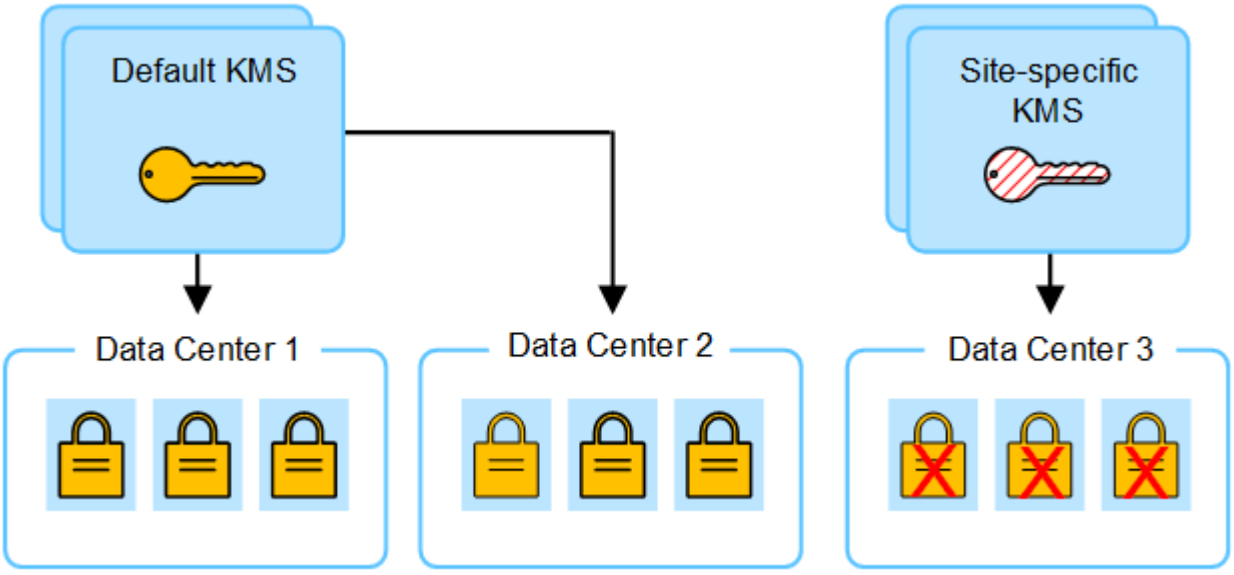
Beispiel:

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

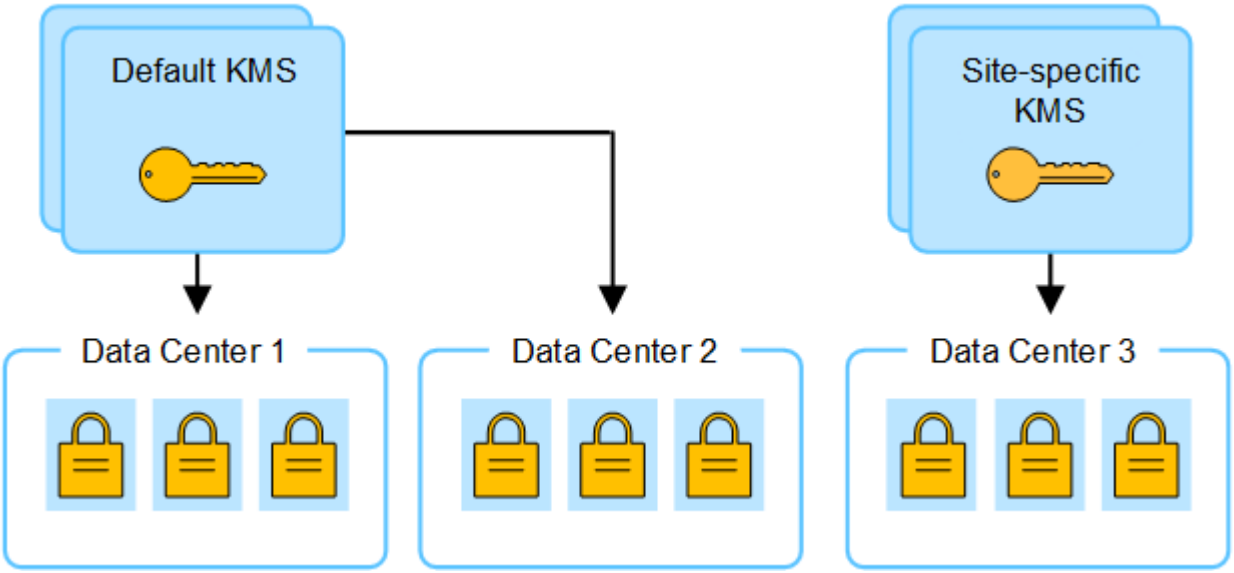


3. Sie entscheiden, einen standortspezifischen KMS für einen Standort hinzuzufügen (Datacenter 3 in der Abbildung). Da die Appliance-Nodes jedoch bereits verschlüsselt sind, tritt ein Validierungsfehler auf, wenn Sie versuchen, die Konfiguration für den standortspezifischen KMS zu speichern. Der Fehler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

Standort zu entschlüsseln.



4. Um das Problem zu beheben, kopieren Sie die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS auf den neuen KMS. (Technisch kopieren Sie den Originalschlüssel in einen neuen Schlüssel mit dem gleichen Alias. Der ursprüngliche Schlüssel wird zu einer früheren Version des neuen Schlüssels.) Der standortspezifische KMS verfügt nun über den richtigen Schlüssel zur Entschlüsselung der Appliance-Nodes in Rechenzentrum 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. Sie gilt für alle Standorte, die kein dediziertes KMS haben. "Bearbeiten eines Verschlüsselungsmanagement-Servers (KMS)"
Sie haben einen Standard-KMS, und Sie fügen eine neue Site in einer Erweiterung hinzu. Sie möchten nicht das Standard-KMS für den neuen Standort verwenden.	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)"
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.

Diese Anweisungen gelten für Thales CipherTrust Manager und Hashicorp Vault. Eine Liste der unterstützten Produkte und Versionen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool (IMT)".

Schritte

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

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

2. Erstellen Sie einen Schlüssel mit einer der folgenden beiden Methoden:
   - Verwenden Sie die Schlüsselverwaltungsseite Ihres KMS-Produkts. Erstellen Sie für jeden KMS- oder KMS-Cluster einen AES-Verschlüsselungsschlüssel.

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

- Lassen Sie StorageGRID den Schlüssel erstellen. Sie werden beim Testen und Speichern nach aufgefordert"Client-Zertifikate werden hochgeladen".

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

   Diese Informationen benötigen Sie, wenn Sie den KMS zu StorageGRID hinzufügen:

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

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.

Bevor Sie beginnen

- Sie haben die überprüft"Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers".
- Sie haben "StorageGRID wurde als Client im KMS konfiguriert", und Sie haben die erforderlichen Informationen für jeden KMS oder KMS Cluster.
- Sie sind im Grid Manager mit einem 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. Weitere Informationen finden Sie unter "Überlegungen für das Ändern des KMS für einen Standort" .

Schritt 1: KM Details

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

Schritte

1. Wählen Sie **Konfiguration** > **Sicherheit** > **Schlüsselverwaltungsserver**.

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

2. Wählen Sie **Erstellen**.

   Schritt 1 (KMS-Details) 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-Name	Einen beschreibenden Namen, der Ihnen bei der Identifizierung dieses KMS hilft. Muss zwischen 1 und 64 Zeichen lang sein.
Schlüsselname	Der exakte Schlüssel-Alias für den StorageGRID-Client im KMS. Muss zwischen 1 und 255 Zeichen lang sein. **Hinweis**: Wenn Sie keinen Schlüssel mit Ihrem KMS-Produkt erstellt haben, werden Sie aufgefordert, StorageGRID den Schlüssel erstellen zu lassen.

Feld	Beschreibung
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 Not Managed by another KMS (default KMS)** aus, um ein Standard-KMS zu konfigurieren, das für alle Sites gilt, die kein dediziertes KMS haben, und für alle Sites, die Sie in nachfolgenden Erweiterungen hinzufügen. **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 Feld Subject Alternative Name (SAN) des Serverzertifikats muss den FQDN oder die IP-Adresse enthalten, die Sie hier eingeben. Andernfalls kann StorageGRID keine Verbindung zum KMS oder zu allen Servern eines KMS-Clusters herstellen.

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

Schritt 2: Serverzertifikat hochladen

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

Schritte

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

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

Schritte

1. Navigieren Sie unter **Schritt 3 (Client-Zertifikate hochladen)** zum Speicherort des Client-Zertifikats.
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.
5. Wählen Sie **Test und Speichern**.

   Wenn kein Schlüssel vorhanden ist, werden Sie aufgefordert, einen Schlüssel von StorageGRID zu erstellen.

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

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

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

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

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

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

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 verwalten

Zum Verwalten eines Schlüsselverwaltungsservers (KMS) gehören das Anzeigen oder Bearbeiten von Details, das Verwalten von Zertifikaten, das Anzeigen verschlüsselter Knoten und das Entfernen eines KMS, wenn er nicht mehr benötigt wird.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Erforderliche Zugriffsberechtigung".

KMS-Details anzeigen

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

Schritte

1. Wählen Sie **Konfiguration** > **Sicherheit** > **Schlüsselverwaltungsserver**.

   Die Seite Key Management Server wird angezeigt und zeigt die folgenden Informationen an:

   - Auf der Registerkarte Konfigurationsdetails werden alle konfigurierten Schlüsselverwaltungsserver aufgeführt.
   - Auf der Registerkarte Verschlüsselte Knoten werden alle Knoten aufgelistet, für die die Knotenverschlüsselung aktiviert ist.

2. Um die Details für ein bestimmtes KMS anzuzeigen und Vorgänge für dieses KMS auszuführen, wählen Sie den Namen des KMS aus. Auf der Detailseite des KMS sind folgende Informationen aufgeführt:

Feld	Beschreibung
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. Zum 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 **Bearbeiten** oder **Aktionen** > **Bearbeiten**.

3. Wählen Sie auf der KMS-Detailseite eine Registerkarte aus, um die folgenden Informationen anzuzeigen:

Registerkarte	Feld	Beschreibung
Wichtige Details	Schlüsselname	Der Schlüsselalias für den StorageGRID-Client im KMS.
Schlüssel-UID	Die eindeutige Kennung der neuesten Version des Schlüssels.	Zuletzt geändert
Datum und Uhrzeit der neuesten Version des Schlüssels.	Serverzertifikat	Metadaten
Die Metadaten für das Zertifikat, z. B. Seriennummer, Ablaufdatum und -Uhrzeit sowie das Zertifikat-PEM.	Zertifikat-PEM	Der Inhalt der PEM-Datei (Privacy Enhanced Mail) für das Zertifikat.
Client-Zertifikat	Metadaten	Die Metadaten für das Zertifikat, z. B. Seriennummer, Ablaufdatum und -Uhrzeit sowie das Zertifikat-PEM.

4. Wählen Sie **Schlüssel drehen** aus, oder verwenden Sie die KMS-Software, um eine neue Version des Schlüssels zu erstellen.

   Wenn die Schlüsselrotation erfolgreich ist, werden die Felder Schlüssel-UID und Letzte Änderung aktualisiert.

> Wenn Sie den Verschlüsselungsschlüssel mit der KMS-Software drehen, drehen Sie ihn von der zuletzt verwendeten Version des Schlüssels in eine neue Version desselben Schlüssels. Drehen Sie nicht zu einer ganz anderen Taste.
>
> Versuchen Sie niemals, einen Schlüssel zu drehen, indem Sie den Schlüsselnamen (Alias) für den KMS ändern. 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.

Verwalten von Zertifikaten

Beheben Sie umgehend alle Probleme mit dem Server- oder Client-Zertifikat. Ersetzen Sie nach Möglichkeit Zertifikate, bevor sie ablaufen.

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

Schritte

1. Wählen Sie **Konfiguration** > **Sicherheit** > **Schlüsselverwaltungsserver**.

2. Sehen Sie sich in der Tabelle den Wert für den Ablauf des Zertifikats für jeden KMS an.
3. Wenn der Zertifikatablauf für ein KMS unbekannt ist, warten Sie bis zu 30 Minuten, und aktualisieren Sie dann Ihren Webbrowser.
4. Wenn in der Spalte Zertifikatablauf angezeigt wird, dass ein Zertifikat abgelaufen ist oder kurz vor dem Ablaufdatum steht, wählen Sie das KMS aus, um zur Seite KMS-Details zu gelangen.
   a. Wählen Sie **Server Certificate** aus, und überprüfen Sie den Wert für das Feld „expires on“.
   b. Um das Zertifikat zu ersetzen, wählen Sie **Zertifikat bearbeiten**, um ein neues Zertifikat hochzuladen.
   c. Wiederholen Sie diese Unterschritte und wählen Sie **Clientzertifikat** anstelle des Serverzertifikats aus.
5. Wenn die Warnungen **KMS CA Certificate Expiration**, **KMS Client Certificate Expiration** und **KMS Server Certificate Expiration** ausgelöst werden, notieren Sie sich die Beschreibung der einzelnen Warnungen und führen Sie die empfohlenen Aktionen durch.

   Es kann bis zu 30 Minuten dauern, bis StorageGRID Updates für den Ablauf des Zertifikats erhält. Aktualisieren Sie Ihren Webbrowser, um die aktuellen Werte anzuzeigen.

> Wenn Sie den Status **Server Certificate Status is unknown** erhalten, stellen Sie sicher, dass Ihr KMS den Erhalt eines Serverzertifikats ohne ein Client-Zertifikat zulässt.

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, für die die Einstellung **Knotenverschlüsselung** aktiviert ist.

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

Spalte	Beschreibung
Node-Name	Der Name des Appliance-Node.
Node-Typ	Der Node-Typ: Storage, Admin oder Gateway.
Standort	Der Name der StorageGRID-Site, auf der der Node installiert ist.

Spalte	Beschreibung
Kms-Name	Der beschreibende Name des für den Knoten verwendeten KMS. Wenn kein KMS aufgeführt ist, wählen Sie die Registerkarte Konfigurationsdetails aus, um ein 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. Um eine gesamte Schlüssel-UID anzuzeigen, wählen Sie den Text aus. 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:** Aktualisieren Sie Ihren Webbrowser, 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

   Führen Sie die empfohlenen Aktionen für diese Warnmeldungen aus.

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

KMS bearbeiten

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

Bevor Sie beginnen

- Wenn Sie planen, den für einen KMS ausgewählten Standort zu aktualisieren, haben Sie die überprüft"Überlegungen für das Ändern des KMS für einen Standort".
- Sie sind im Grid Manager mit einem 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 Key Management Server an.

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

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

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

Feld	Beschreibung
Kms-Name	Einen beschreibenden Namen, der Ihnen bei der Identifizierung dieses KMS hilft. Muss zwischen 1 und 64 Zeichen lang sein.
Schlüsselname	Der exakte Schlüssel-Alias für den StorageGRID-Client im KMS. Muss zwischen 1 und 255 Zeichen lang sein. 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.
Verwaltet Schlüssel für	Wenn Sie ein standortspezifisches KMS bearbeiten und noch kein Standard-KMS haben, wählen Sie optional **Sites Not Managed by another KMS (default KMS)** aus. Diese Auswahl konvertiert ein standortspezifisches KMS in das Standard-KMS, das für alle Standorte gilt, die kein dediziertes KMS haben, und für alle Sites, die in einer Erweiterung hinzugefügt wurden. **Hinweis:** Wenn Sie eine Site-spezifische KMS bearbeiten, können Sie keine andere Site auswählen. Wenn Sie das Standard-KMS bearbeiten, können Sie keine bestimmte Site auswählen.
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.

Feld	Beschreibung
Hostname	Der vollständig qualifizierte Domänenname oder die IP-Adresse für den KMS. **Hinweis:** das Feld Subject Alternative Name (SAN) des Serverzertifikats muss den FQDN oder die IP-Adresse enthalten, die Sie hier eingeben. Andernfalls kann StorageGRID keine Verbindung zum KMS oder zu allen Servern eines KMS-Clusters herstellen.

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

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

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

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

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

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

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

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

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

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

    Die KMS-Konfiguration wird gespeichert.

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

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

Entfernen eines Verschlüsselungsmanagement-Servers (KMS)

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

Bevor Sie beginnen

- Sie haben die überprüft"Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers".
- Sie sind im Grid Manager mit einem 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 Key Management Server an.

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

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

3. Bestätigen Sie, dass Folgendes zutrifft:
   - Sie entfernen ein standortspezifisches KMS für einen Standort, der keinen Appliance-Knoten mit aktivierter Knotenverschlüsselung hat.
   - Sie entfernen den Standard-KMS, aber für jeden Standort mit Knotenverschlüsselung ist bereits ein standortspezifisches KMS vorhanden.
4. Wählen Sie **Ja**.

   Die KMS-Konfiguration wurde entfernt.

Proxy-Einstellungen verwalten

Konfigurieren Sie den Speicher-Proxy

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.

Konfigurierte Speicher-Proxy-Einstellungen gelten nicht für Kafka-Plattformdienste-Endpunkte.

Bevor Sie beginnen

- Sie haben "Bestimmte Zugriffsberechtigungen".
- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".

Über diese Aufgabe

Sie können die Einstellungen für einen einzelnen Speicher-Proxy konfigurieren.

Schritte

1. Wählen Sie **Konfiguration** > **Sicherheit** > **Proxy-Einstellungen**.
2. Aktivieren Sie auf der Registerkarte **Storage** das Kontrollkästchen **Speicher-Proxy aktivieren**.
3. Wählen Sie das Protokoll für den 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.

   Lassen Sie dieses Feld leer, um den Standardport für das Protokoll zu verwenden: 80 für HTTP oder 1080 für SOCKS5.

6. Wählen Sie **Speichern**.

   Nachdem der Storage-Proxy gespeichert wurde, 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.
8. Wenn Sie einen Speicher-Proxy deaktivieren müssen, deaktivieren Sie das Kontrollkästchen und wählen Sie **Speichern**.

Konfigurieren Sie die Administrator-Proxy-Einstellungen

Wenn Sie AutoSupport-Pakete über HTTP oder HTTPS senden, können Sie einen nicht transparenten Proxyserver zwischen Admin-Knoten und technischem Support (AutoSupport) konfigurieren.

Weitere Informationen über AutoSupport finden Sie unter "Konfigurieren Sie AutoSupport".

Bevor Sie beginnen

- Sie haben "Bestimmte Zugriffsberechtigungen".
- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".

Über diese Aufgabe

Sie können die Einstellungen für einen einzelnen Administrator-Proxy konfigurieren.

Schritte

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

   Die Seite Proxy-Einstellungen wird angezeigt. Standardmäßig ist Speicher im Registerkartenmenü ausgewählt.

2. Wählen Sie die Registerkarte **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 einen Benutzernamen und ein Kennwort für den Proxyserver ein.

   Lassen Sie diese Felder leer, wenn Ihr Proxyserver keinen Benutzernamen oder kein Passwort benötigt.

7. Wählen Sie eine der folgenden Optionen:

   - Wenn Sie die Verbindung zum Admin-Proxy sichern möchten, wählen Sie **Proxy-Zertifikat überprüfen** aus. Laden Sie ein CA-Bundle hoch, um die Authentizität der SSL-Zertifikate zu überprüfen, die vom Administrator-Proxy-Server präsentiert werden.

     AutoSupport On-Demand, E-Series AutoSupport über StorageGRID und die Ermittlung des Aktualisierungspfads auf der StorageGRID Upgrade-Seite funktionieren nicht, wenn ein Proxy-Zertifikat verifiziert wurde.

   Nach dem Hochladen des CA-Bündels werden die zugehörigen Metadaten angezeigt.

   - Wenn Sie Zertifikate bei der Kommunikation mit dem Admin-Proxyserver nicht überprüfen möchten, wählen Sie **Proxy-Zertifikat nicht verifizieren**.

8. Wählen Sie **Speichern**.

   Nachdem der Admin-Proxy gespeichert wurde, wird der Proxy-Server zwischen Admin-Knoten und technischem Support konfiguriert.

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

9. Wenn Sie den Admin-Proxy deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Admin-Proxy aktivieren** und wählen Sie dann **Speichern**.

Kontrollieren Sie Firewalls

Kontrolle des Zugriffs über externe Firewall

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

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

Informationen zum Konfigurieren der internen Firewall von StorageGRID finden Sie unter "Konfigurieren Sie die interne Firewall".

Port	Beschreibung	Port offen…
443	Standard-HTTPS-Port für Admin-Nodes	Webbrowser und Management-API-Clients können auf den Grid Manager, die Grid Management API, den Mandanten-Manager und die Mandanten-Management-API zugreifen. **Hinweis:** Port 443 wird auch für einen internen Verkehr genutzt.
8443	Eingeschränkter Grid Manager-Port an Admin-Nodes	• Webbrowser und Management-API-Clients können mithilfe von HTTPS auf den Grid Manager und die Grid Management API zugreifen. • Webbrowser und Management-API-Clients können nicht auf den Tenant Manager oder die Mandanten-Management-API zugreifen. • Anfragen nach internen Inhalten werden abgelehnt.
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"

Interne Firewall-Kontrollen verwalten

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

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

Zugriff anzupassen.

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

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

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

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

Informationen zum Konfigurieren der internen Firewall-Steuerelemente finden Sie unter "Konfigurieren Sie die Firewall-Steuerelemente".

Weitere Informationen zu externen Firewalls und Netzwerksicherheit finden Sie unter "Kontrolle des Zugriffs über externe Firewall".

Liste privilegierter Adressen und Verwaltung externer Zugriffsregisterkarten

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

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

Beispiel 1: Verwenden Sie einen Jump-Host für Wartungsaufgaben

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

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

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

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

Beispiel 2: Sperren sensibler Ports

Angenommen, Sie möchten sensible Ports und den Dienst auf diesem Port sperren. Sie können die folgenden allgemeinen Schritte ausführen:

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

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

Nachdem Sie Ihre Konfiguration gespeichert haben, stehen der sensible Port und der Dienst auf diesem Port den Hosts auf der Liste privilegierter Adressen zur Verfügung. Allen anderen Hosts wird der Zugriff auf den Dienst verweigert, unabhängig davon, von welcher Schnittstelle die Anforderung kommt.

Beispiel 3: Deaktivieren Sie den Zugriff auf nicht verwendete Dienste

Auf Netzwerkebene können Sie einige Dienste deaktivieren, die Sie nicht verwenden möchten. Um beispielsweise den HTTP S3-Clientverkehr zu blockieren, verwenden Sie den Umschalter auf der Registerkarte „externen Zugriff verwalten“, um Port 18084 zu blockieren.

Registerkarte nicht vertrauenswürdige Client-Netzwerke

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, standardmäßig vertraut StorageGRID eingehende Verbindungen zu jedem Grid-Knoten auf allen "Verfügbare externe Ports".

Sie können die Bedrohung durch feindliche Angriffe auf Ihrem StorageGRID-System verringern, indem Sie angeben, dass das Client-Netzwerk auf jedem Knoten *unvertrauenswürdig* ist. Wenn das Client-Netzwerk eines 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" und "Konfigurieren Sie die Firewall-Steuerelemente".

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

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

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

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

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

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

Beispiel 3: Zugriff auf Grid Manager auf ein Subnetz beschränken

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

1. Verbinden Sie das Client-Netzwerk Ihrer Admin-Knoten mit dem Subnetz.
2. Verwenden Sie die Registerkarte nicht vertrauenswürdiges Clientnetzwerk, um das Clientnetzwerk als nicht vertrauenswürdig zu konfigurieren.
3. Wenn Sie einen Load Balancer-Endpunkt der Managementoberfläche erstellen, geben Sie den Port ein und wählen Sie die Managementoberfläche aus, auf die der Port zugreifen soll.
4. Wählen Sie **Ja** für nicht vertrauenswürdiges Client-Netzwerk aus.
5. Verwenden Sie die Registerkarte externen Zugriff verwalten, um alle externen Ports zu blockieren (mit oder ohne privilegierte IP-Adressen für Hosts außerhalb dieses Subnetzes).

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

Konfigurieren Sie die interne Firewall

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

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben "Bestimmte Zugriffsberechtigungen".
- Sie haben die Informationen in und überprüft"Management der Firewall-Kontrollen""Netzwerkrichtlinien".
- Wenn ein Admin-Node oder Gateway-Node nur eingehenden Datenverkehr auf explizit konfigurierten Endpunkten annehmen soll, haben Sie die Load Balancer-Endpunkte definiert.

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

Über diese Aufgabe

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

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

Weitere Informationen zur Verwendung von Firewall-Kontrollen, einschließlich Beispiele, finden Sie unter "Management der Firewall-Kontrollen".

Weitere Informationen zu externen Firewalls und Netzwerksicherheit finden Sie unter "Kontrolle des Zugriffs über externe Firewall".

Firewall-Kontrollen für den Zugriff

Schritte

1. Wählen Sie **Konfiguration** > **Sicherheit** > **Firewall-Steuerung**.

   Die drei Registerkarten auf dieser Seite werden in beschrieben"Management der Firewall-Kontrollen".

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

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

Liste privilegierter Adressen

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

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

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

Schritte

1. Geben Sie auf der Registerkarte Liste der privilegierten Adressen die Adresse oder das IP-Subnetz ein, die

Sie Zugriff auf geschlossene Ports gewähren möchten.

2. Wählen Sie optional **Add another IP address or subnet in CIDR Notation** aus, um weitere privilegierte Clients hinzuzufügen.

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

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

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

4. Wählen Sie **Speichern**.

Management des externen Zugriffs

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

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

Schritte

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

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

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

3. Wählen Sie **Speichern**

Nicht Vertrauenswürdiges Client-Netzwerk

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

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

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

Schritte

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

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

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

3. Verwenden Sie die folgenden Optionen, um die Knoten auszuwählen, die Clientverbindungen nur an explizit konfigurierten Endpunkten des Lastausgleichs oder zusätzlichen ausgewählten Ports zulassen sollen:
   - Wählen Sie **Untrust on displayed Nodes** aus, um alle in der Tabelle angezeigten Knoten zur Liste UnTrusted Client Network hinzuzufügen.
   - Wählen Sie **Trust on displayed Nodes** aus, um alle in der Tabelle angezeigten Knoten aus der Liste UnTrusted Client Network zu entfernen.
   - Verwenden Sie den Umschalter neben den einzelnen Knoten, um das Client-Netzwerk für den ausgewählten Knoten als vertrauenswürdig oder nicht vertrauenswürdig festzulegen.

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

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

4. Wählen Sie **Speichern**.

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

Verwalten von Mandanten

Was sind Mandantenkonten?

Ein Mandantenkonto ermöglicht Ihnen die Verwendung der S3-REST-API (Simple Storage Service) zum Speichern und Abrufen von Objekten in einem StorageGRID System.

Swift-Details wurden aus dieser Version der doc-Site entfernt. Siehe "StorageGRID 11.8: Mandanten verwalten".

Als Grid-Administrator erstellen und managen Sie die Mandantenkonten, die S3-Clients zum Speichern und Abrufen von Objekten verwenden.

Jedes Mandantenkonto hat föderierte oder lokale Gruppen, Benutzer, S3 Buckets und Objekte.

Mandantenkonten können verwendet werden, um gespeicherte Objekte durch verschiedene Einheiten zu trennen. Beispielsweise können für einen der folgenden Anwendungsfälle mehrere Mandantenkonten verwendet werden:

- **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-Clientprotokoll verwenden, können Sie S3-Buckets und Bucket-Richtlinien verwenden, um Objekte zwischen den Abteilungen in einem Unternehmen zu trennen. Sie müssen keine Mieterkonten verwenden. Siehe Anweisungen zur Implementierung"S3-Buckets und Bucket-Richtlinien" für weitere Informationen.

- **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.

Weitere Informationen finden Sie unter "Verwenden Sie ein Mandantenkonto".

Wie erstelle ich ein Mandantenkonto?

Verwenden Sie den Grid-Manager, um ein Mandantenkonto zu erstellen. Wenn Sie ein Mandantenkonto erstellen, geben Sie die folgenden Informationen an:

- Grundlegende Informationen, einschließlich Mandantenname, Client-Typ (S3) und optionalem Storage-Kontingent.
- Berechtigungen für das Mandantenkonto, z. B. ob das Mandantenkonto S3-Plattformservices verwenden, seine eigene Identitätsquelle konfigurieren, S3 Select verwenden oder eine Grid-Verbundverbindung verwenden kann.
- Der erste Root-Zugriff für den Mandanten basiert darauf, ob das StorageGRID System lokale Gruppen und

Benutzer, Identitätsföderation oder Single Sign On (SSO) verwendet.

Darüber hinaus können Sie die S3-Objektsperrung für das StorageGRID-System aktivieren, wenn S3-Mandantenkonten gesetzliche Vorgaben erfüllen müssen. Wenn S3 Object Lock aktiviert ist, können alle S3-Mandantenkonten konforme Buckets erstellen und managen.

Wofür wird Tenant Manager verwendet?

Nachdem Sie das Mandantenkonto erstellt haben, können sich Mandantenbenutzer beim Tenant Manager anmelden, um Aufgaben wie die folgenden auszuführen:

- Identitätsföderation einrichten (es sei denn, die Identitätsquelle wird mit dem Grid gemeinsam genutzt)
- Verwalten von Gruppen und Benutzern
- Grid-Verbund für Account-Klone und Grid-übergreifende Replizierung verwenden
- Managen von S3-Zugriffsschlüsseln
- S3 Buckets erstellen und managen
- Verwenden Sie S3-Plattformservices
- Verwenden Sie S3 Select
- Monitoring der Storage-Auslastung

Benutzer von S3-Mandanten können mit dem Tenant Manager S3-Zugriffsschlüssel und -Buckets erstellen und managen, müssen jedoch Objekte mit einer S3-Client-Applikation aufnehmen und managen. Weitere Informationen finden Sie unter "S3-REST-API VERWENDEN" .

Erstellen Sie ein Mandantenkonto

Sie müssen mindestens ein Mandantenkonto erstellen, um den Zugriff auf den Storage in Ihrem StorageGRID-System zu kontrollieren.

Die Schritte zum Erstellen eines Mandantenkontos variieren je nachdem, ob"Identitätsföderation" Und"Single Sign On" konfiguriert sind und ob das Grid Manager-Konto, das Sie zum Erstellen des Mandantenkontos verwenden, zu einer Administratorgruppe mit Root-Zugriffsberechtigung gehört.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Berechtigung für Root-Zugriff oder Mandantenkonten".
- 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 Administratorgruppe keine Grid Manager-Berechtigungen zuweisen. Siehe "Managen von Admin-Gruppen".
- Wenn Sie einem S3-Mandanten das Klonen von Kontodaten und das Replizieren von Bucket-Objekten in einem anderen Grid über eine Grid-Federation-Verbindung ermöglichen möchten:
  - Sie haben "Grid Federation-Verbindung konfiguriert".
  - Der Status der Verbindung lautet **connected**.
  - Sie haben Root-Zugriffsberechtigung.

- Sie haben die Überlegungen für geprüft"Verwalten der zulässigen Mandanten für den Grid-Verbund".
- Wenn das Mandantenkonto die Identitätsquelle verwendet, die für Grid Manager konfiguriert wurde, haben Sie dieselbe Verbundgruppe in Grid Manager auf beiden Grids importiert.

  Wenn Sie den Mandanten erstellen, wählen Sie diese Gruppe aus, um die anfängliche Root-Zugriffsberechtigung für die Quell- und Zielmandantenkonten zu erhalten.

> Wenn diese Administratorgruppe vor dem Erstellen des Mandanten nicht auf beiden Grids vorhanden ist, wird der Mandant nicht am Ziel repliziert.

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **Mandanten** aus.
2. Wählen Sie **Erstellen**.

Geben Sie Details ein

Schritte

1. Geben Sie Details für die Serviceeinheit ein.

Feld	Beschreibung
Name	Ein Name für das Mandantenkonto. Mandantennamen müssen nicht eindeutig sein. Wenn das Mandantenkonto erstellt wird, erhält es eine eindeutige, 20-stellige Konto-ID.
Beschreibung (optional)	Eine Beschreibung zur Identifizierung des Mandanten. Wenn Sie einen Mandanten erstellen, der eine Grid-Federation-Verbindung verwendet, können Sie optional mithilfe dieses Felds ermitteln, welcher der Quell-Tenant ist und welcher der Zielmandant ist. Beispielsweise wird diese Beschreibung für einen Mandanten, der in Grid 1 erstellt wurde, auch für den Mandanten angezeigt, der in Grid 2 repliziert wurde: „Dieser Mandant wurde in Grid 1 erstellt.“
Client-Typ	Muss **S3** sein.
Storage-Kontingent (optional)	Wenn Sie möchten, dass dieser Mandant über ein Speicherkontingent, einen numerischen Wert für das Kontingent und die Einheiten verfügt.

2. Wählen Sie **Weiter**.

Wählen Sie Berechtigungen aus

Schritte

1. Wählen Sie optional die grundlegenden Berechtigungen aus, die dieser Mandant besitzen soll.

Einige dieser Berechtigungen haben zusätzliche Anforderungen. Für Details wählen Sie das Hilfesymbol für jede Berechtigung aus.

Berechtigung	Wenn ausgewählt…
Unterstützung von Plattform-Services	Der Mandant kann S3-Plattformservices wie CloudMirror verwenden. Siehe "Management von Plattform-Services für S3-Mandantenkonten".
Eigene Identitätsquelle verwenden	Der Mandant kann seine eigene Identitätsquelle für föderierte Gruppen und Benutzer konfigurieren und verwalten. Diese Option ist deaktiviert, wenn Sie"SSO konfiguriert" für Ihr StorageGRID System.
S3 Select zulassen	Der Mandant kann S3 SelectObjectContent API-Anforderungen ausgeben, um Objektdaten zu filtern und abzurufen. Siehe "Management von S3 Select für Mandantenkonten". **Wichtig**: SelectObjectContent Requests können die Load Balancer Performance für alle S3 Clients und alle Tenants verringern. Aktivieren Sie diese Funktion nur bei Bedarf und nur für vertrauenswürdige Mandanten.

2. Wählen Sie optional die erweiterten Berechtigungen aus, über die dieser Mandant verfügen soll.

Berechtigung	Wenn ausgewählt…
Netzverbundverbindung	Der Mandant kann eine Grid Federation-Verbindung verwenden, die: • Bewirkt, dass dieser Mandant und alle dem Konto hinzugefügten Mandantengruppen und Benutzer aus diesem Raster (das *source Grid*) in das andere Raster der ausgewählten Verbindung (das *Destination Grid*) geklont werden. • Ermöglicht diesem Mandanten, die Grid-übergreifende Replizierung zwischen entsprechenden Buckets in jedem Grid zu konfigurieren. Siehe "Verwalten Sie die zulässigen Mandanten für den Grid-Verbund".
S3-Objektsperre	Dem Mandanten erlauben, bestimmte Funktionen von S3 Object Lock zu verwenden: • **Maximale Aufbewahrungsfrist festlegen** definiert, wie lange neue Objekte, die zu diesem Bucket hinzugefügt werden, beibehalten werden sollen, beginnend mit dem Zeitpunkt, zu dem sie aufgenommen werden. • **Compliance-Modus zulassen** verhindert das Überschreiben oder Löschen geschützter Objektversionen während der Aufbewahrungsfrist.

3. Wählen Sie **Weiter**.

Root-Zugriff definieren und Mandanten erstellen

Schritte

1. Definieren Sie den Root-Zugriff für das Mandantenkonto, je nachdem, ob Ihr StorageGRID-System

Identitätsföderation, Single Sign-On (SSO) oder beides verwendet.

Option	Tun Sie das
Wenn die Identitätsföderation nicht aktiviert ist	Geben Sie das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.
Wenn die Identitätsföderation aktiviert ist	a. Wählen Sie eine vorhandene Verbundgruppe aus, um Root-Zugriffsberechtigungen für den Mandanten zu erhalten. b. Geben Sie optional das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.
Wenn sowohl Identitätsföderation als auch Single Sign-On (SSO) aktiviert sind	Wählen Sie eine vorhandene Verbundgruppe aus, um Root-Zugriffsberechtigungen für den Mandanten zu erhalten. Keine lokalen Benutzer können sich anmelden.

2. Wählen Sie **Create Tenant**.

   Eine Erfolgsmeldung wird angezeigt, und die neue Serviceeinheit wird auf der Seite „Serviceeinheiten“ aufgeführt. Informationen zum Anzeigen von Mandantendetails und zum Überwachen der Mandantenaktivität finden Sie unter "Überwachen Sie die Mandantenaktivität".

   Das Anwenden von Mandanteneinstellungen für das Grid kann je nach Netzwerkkonnektivität, Node-Status und Cassandra-Vorgängen 15 Minuten oder länger dauern.

3. Wenn Sie die Berechtigung **Grid Federation connection** für den Mieter verwenden ausgewählt haben:
   a. Vergewissern Sie sich, dass ein identischer Mandant auf das andere Grid in der Verbindung repliziert wurde. Die Mandanten in beiden Grids haben die gleiche 20-stellige Konto-ID, den gleichen Namen, die gleiche Beschreibung, das gleiche Kontingent und die gleichen Berechtigungen.

      Wenn die Fehlermeldung „Tenant created without a Clone“ angezeigt wird, lesen Sie die Anweisungen in "Fehler beim Grid-Verbund beheben".

   b. Wenn Sie beim Definieren des Root-Zugriffs ein lokales Root-Benutzerpasswort für den replizierten Mandanten angegeben "Ändern Sie das Passwort für den lokalen Root-Benutzer"haben.

      Ein lokaler Root-Benutzer kann sich erst bei Tenant Manager im Zielraster anmelden, wenn das Passwort geändert wurde.

Beim Mandanten anmelden (optional)

Sie können sich nach Bedarf jetzt beim neuen Mandanten anmelden, um die Konfiguration abzuschließen, oder sich später beim Mandanten anmelden. Die Schritte zur Anmeldung hängen davon ab, ob Sie über den Standardport (443) oder einen eingeschränkten Port beim Grid Manager angemeldet sind. Siehe "Kontrolle des Zugriffs über externe Firewall".

Jetzt anmelden

Sie verwenden…	Tun Sie das…
Port 443 und Sie legen ein Passwort für den lokalen Root-Benutzer fest	1. Wählen Sie **als root anmelden**. Wenn Sie sich anmelden, werden Links zum Konfigurieren von Buckets, Identitätsverbünden, Gruppen und Benutzern angezeigt. 2. 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".
Port 443 und Sie haben kein Passwort für den lokalen Root-Benutzer festgelegt	Wählen Sie **Anmelden**, und geben Sie die Anmeldeinformationen für einen Benutzer in der Gruppe Root Access Federated ein.
Ein eingeschränkter Port	1. Wählen Sie **Fertig Stellen** 2. Wählen Sie **eingeschränkt** in der Tabelle Tenant 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 Domänenname oder die IP-Adresse eines Admin-Knotens ◦ *port* Ist der nur-Mandanten-Port ◦ *20-digit-account-id* Ist die eindeutige Konto-ID des Mandanten

Melden Sie sich später an

Sie verwenden…	Führen Sie eine dieser…
Anschluss 443	• Wählen Sie im Grid Manager **Mandanten** und rechts neben dem Mandantennamen * Sign in* 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 Domänenname oder die IP-Adresse eines Admin-Knotens ◦ *20-digit-account-id* Ist die eindeutige Konto-ID des Mandanten

Sie verwenden…	Führen Sie eine dieser…
Ein eingeschränkter Port	• Wählen Sie im Grid Manager **Mandanten** und dann **Eingeschränkt** aus. • 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 Domänenname oder die IP-Adresse eines Admin-Knotens ◦ *port* Ist der nur für Mandanten beschränkte Port ◦ *20-digit-account-id* Ist die eindeutige Konto-ID des Mandanten

Konfigurieren Sie den Mandanten

Folgen Sie den Anweisungen in"Verwenden Sie ein Mandantenkonto", um Mandantengruppen und -Benutzer, S3-Zugriffsschlüssel, Buckets, Plattformservices sowie Account-Klone und Grid-übergreifende Replizierung zu managen.

Mandantenkonto bearbeiten

Sie können ein Mandantenkonto bearbeiten, um den Anzeigenamen, das Speicherkontingent oder die Berechtigungen für Mandanten zu ändern.

Wenn ein Mandant über die Berechtigung **Grid Federation connection** verwenden verfügt, können Sie die Mandantendetails von beiden Rastergittern in der Verbindung bearbeiten. Änderungen, die Sie an einem Raster in der Verbindung vornehmen, werden jedoch nicht in das andere Raster kopiert. Wenn Sie die Details der Serviceeinheit zwischen den Rastern exakt synchronisieren möchten, nehmen Sie die gleichen Änderungen an beiden Rastern vor. Siehe "Verwalten Sie die zulässigen Mandanten für die Grid Federation-Verbindung".

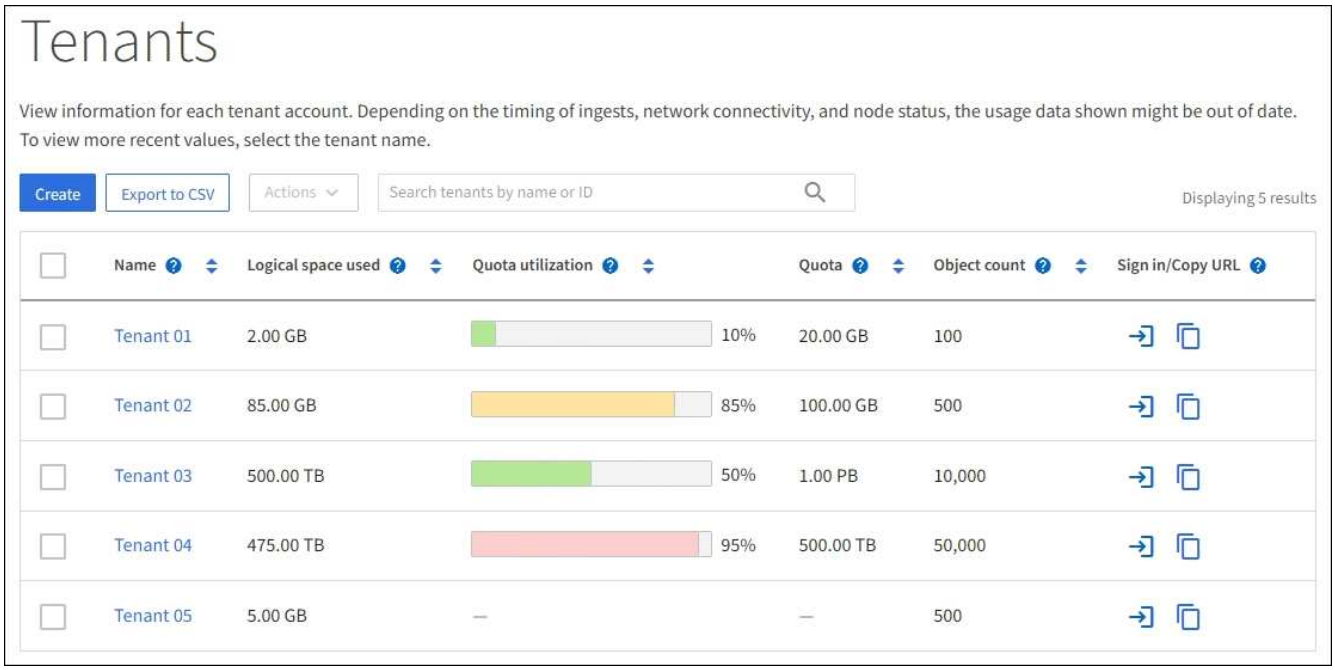
Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Berechtigung für Root-Zugriff oder Mandantenkonten".

Das Anwenden von Mandanteneinstellungen für das Grid kann je nach Netzwerkkonnektivität, Node-Status und Cassandra-Vorgängen 15 Minuten oder länger dauern.

Schritte

1. Wählen Sie **Mandanten** aus.



2. Suchen Sie das Mandantenkonto, das Sie bearbeiten möchten.

   Verwenden Sie das Suchfeld, um nach einem Mandanten anhand des Namens oder der Mandanten-ID zu suchen.

3. Wählen Sie den Mandanten aus. Sie können eine der folgenden Aktionen ausführen:
   - Aktivieren Sie das Kontrollkästchen für den Mandanten und wählen Sie **actions** > **Edit**.
   - Wählen Sie den Namen des Mandanten aus, um die Detailseite anzuzeigen, und wählen Sie **Bearbeiten**.
4. Ändern Sie optional die Werte für diese Felder:
   - **Name**
   - **Beschreibung**
   - **Speicherquote**
5. Wählen Sie **Weiter**.
6. Wählen oder deaktivieren Sie die Berechtigungen für das Mandantenkonto.
   - 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. Siehe "Management von Plattform-Services für S3-Mandantenkonten".
   - Ändern Sie die Einstellung **eigene Identitätsquelle verwenden**, um zu bestimmen, ob das Mandantenkonto seine eigene Identitätsquelle oder die für den Grid Manager konfigurierte Identitätsquelle verwendet.

     Wenn **eigene Identitätsquelle verwenden** ist:

     - Deaktiviert und ausgewählt, 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 nicht ausgewählt, SSO ist für das StorageGRID-System aktiviert. Der Mandant muss die Identitätsquelle verwenden, die für den Grid Manager konfiguriert wurde.

◦ Wählen oder deaktivieren Sie die Berechtigung **allow S3 Select** nach Bedarf. Siehe "Management von S3 Select für Mandantenkonten".

◦ So entfernen Sie die Berechtigung **Grid Federation connection**:

i. Wählen Sie die Registerkarte **Grid Federation** aus.

ii. Wählen Sie **Berechtigung entfernen**.

◦ So fügen Sie die Berechtigung **Grid Federation connection** ein:

i. Wählen Sie die Registerkarte **Grid Federation** aus.

ii. Aktivieren Sie das Kontrollkästchen **Grid Federation connection** verwenden.

iii. Wählen Sie optional **vorhandene lokale Benutzer und Gruppen klonen** aus, um sie in das Remote Grid zu klonen. Wenn Sie möchten, können Sie den Klonvorgang anhalten oder das Klonen erneut versuchen, wenn einige lokale Benutzer oder Gruppen nach Abschluss des letzten Klonvorgangs nicht geklont wurden.

◦ So legen Sie eine maximale Aufbewahrungsfrist fest oder erlauben Sie den Compliance-Modus:

> Die S3-Objektsperre muss im Raster aktiviert sein, bevor Sie diese Einstellungen verwenden können.

i. Wählen Sie die Registerkarte **S3 Object Lock**.

ii. Geben Sie für **Set Maximum Retention Period** einen Wert ein und wählen Sie den Zeitraum aus dem Pulldown-Menü aus.

iii. Aktivieren Sie für **allow Compliance Mode** das Kontrollkästchen.

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.

Bevor Sie beginnen

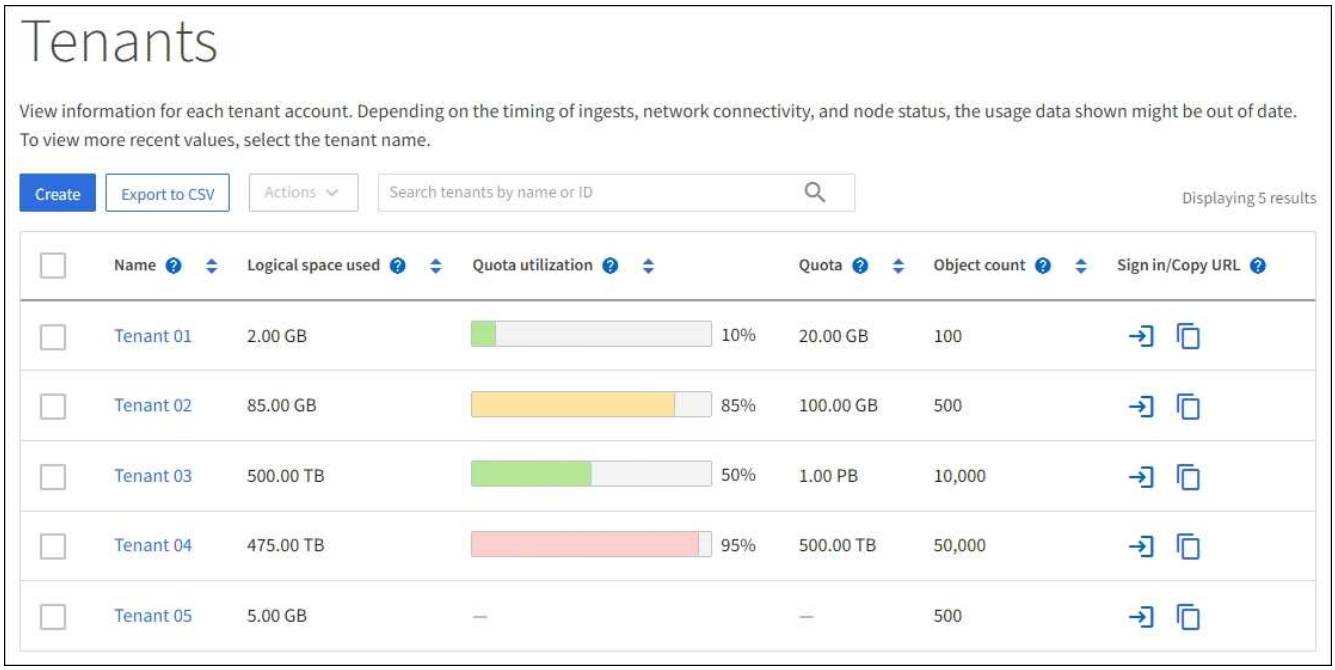
- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben "Bestimmte Zugriffsberechtigungen".

Über diese Aufgabe

Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, kann sich der lokale Root-Benutzer nicht beim Mandanten-Konto anmelden. Um Root-Benutzeraufgaben auszuführen, müssen Benutzer einer föderierten Gruppe angehören, die über die Root-Zugriffsberechtigung für den Mandanten verfügt.

Schritte

1. Wählen Sie **Mandanten** aus.



2. Wählen Sie das Mandantenkonto aus. Sie können eine der folgenden Aktionen ausführen:
   - Aktivieren Sie das Kontrollkästchen für den Mandanten, und wählen Sie **actions** > **root-Passwort ändern**.
   - Wählen Sie den Namen des Mandanten aus, um die Detailseite anzuzeigen, und wählen Sie **actions** > **root password ändern**.
3. Geben Sie das neue Kennwort für das Mandantenkonto ein.
4. Wählen Sie **Speichern**.

Mandantenkonto löschen

Sie können ein Mandantenkonto löschen, wenn Sie den Zugriff des Mandanten auf das System dauerhaft entfernen möchten.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben "Bestimmte Zugriffsberechtigungen".
- Sie haben alle S3-Buckets und Objekte entfernt, die mit dem Mandantenkonto verknüpft sind.
- Wenn der Mandant eine Grid Federation-Verbindung verwenden darf, haben Sie die Überlegungen für geprüft"Löschen eines Mandanten mit der Berechtigung Grid Federation verwenden".

Schritte

1. Wählen Sie **Mandanten** aus.
2. Suchen Sie das oder die Konten, die Sie löschen möchten.

   Verwenden Sie das Suchfeld, um nach einem Mandanten anhand des Namens oder der Mandanten-ID zu suchen.

3. Um mehrere Mandanten zu löschen, aktivieren Sie die Kontrollkästchen und wählen **Aktionen** > **Löschen**.
4. Führen Sie einen der folgenden Schritte aus, um eine einzelne Serviceeinheit zu löschen:

- Aktivieren Sie das Kontrollkästchen, und wählen Sie **Aktionen** > **Löschen**.
- Wählen Sie den Namen des Mandanten aus, um die Detailseite anzuzeigen, und wählen Sie dann **actions** > **Delete** aus.

5. Wählen Sie **Ja**.

Management von Plattform-Services

Was sind Plattform-Services?

Zu den Plattform-Services zählen die CloudMirror-Replizierung, Ereignisbenachrichtigungen und der Such-Integrationsservice.

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.

Plattformdienste werden nicht unterstützt für"Zweigeimer" .

Replizierung von CloudMirror

Der StorageGRID CloudMirror Replizierungsservice wird verwendet, um bestimmte Objekte aus einem StorageGRID Bucket auf ein angegebenes 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 weist einige wichtige Ähnlichkeiten und Unterschiede zur Grid-übergreifenden Replizierungsfunktion auf. Weitere Informationen finden Sie unter "Vergleichen Sie Grid-Replizierung und CloudMirror Replizierung".

> Die CloudMirror-Replikation wird nicht unterstützt, wenn im Quell-Bucket die S3-Objektsperre aktiviert ist.

Benachrichtigungen

Bucket-spezifische Ereignisbenachrichtigungen werden verwendet, um Benachrichtigungen über bestimmte an Objekten ausgeführte Aktionen an einen angegebenen externen Kafka-Cluster, Webhook-Endpunkt oder Amazon Simple Notification Service 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.

Suchintegrations-Service

Über den Suchintegrationsservice werden S3-Objektmetadaten an einen bestimmten Elasticsearch-Index gesendet, wo die Metadaten über den externen Service 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.
- Anforderungen an einen Endpunkt, die nicht abgeschlossen werden können, werden in die Warteschlange für maximal 500,000 Anfragen gestellt. Dieses Limit wird gleich von aktiven Mandanten gemeinsam genutzt. Neue Mandanten dürfen dieses Limit von 500,000 vorübergehend überschreiten, sodass neu erstellte Mandanten nicht unfair bestraft werden.

Verwandte Informationen

- "Management von Plattform-Services"
- "Konfigurieren Sie Speicher-Proxy-Einstellungen"
- "Monitoring von StorageGRID"

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 Amazon Simple Notification Service-Nachrichten unterstützt
- Ein lokal gehosteter Kafka-Cluster
- Ein externer oder lokal gehosteter Webhook-Endpunkt, der HTTP-POST-Benachrichtigungsanforderungen unterstützt.

  Dieser Endpunkt kann auf verschiedenen Webservern, Frameworks oder Datenverarbeitungstools wie Fluentd gehostet werden.

- 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 (die meisten Endpunkte)
- **443**: Für Endpunkt-URIs, die mit https beginnen (die meisten Endpunkte)
- **9092**: Für Endpunkt-URIs, die mit http oder https beginnen (nur Kafka-Endpunkte)

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"zulassen, dass Nachrichten an externe Endpunkte wie z. B. einen Endpunkt im Internet gesendet werden.

Verwandte Informationen

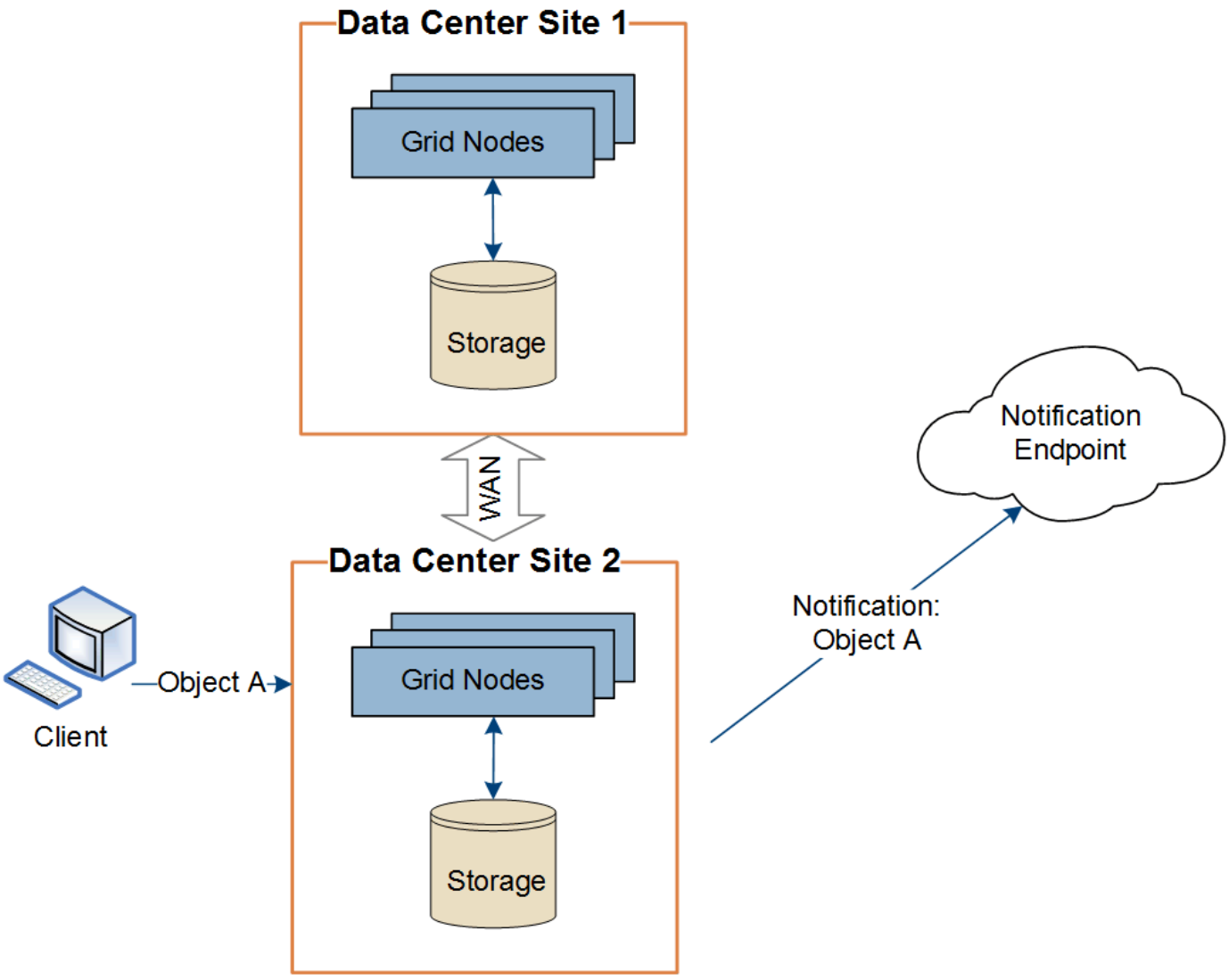
"Verwenden Sie ein Mandantenkonto"

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 ist ein externes Ziel für einen Plattformservice, z. B. einen StorageGRID S3-Bucket, einen Amazon Web Services-Bucket, ein Thema „Amazon Simple Notification Service“, ein Kafka-Thema oder ein Elasticsearch-Cluster, das 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

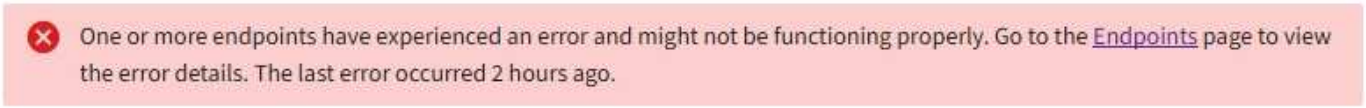
von einem Node an jedem Standort validiert.

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.

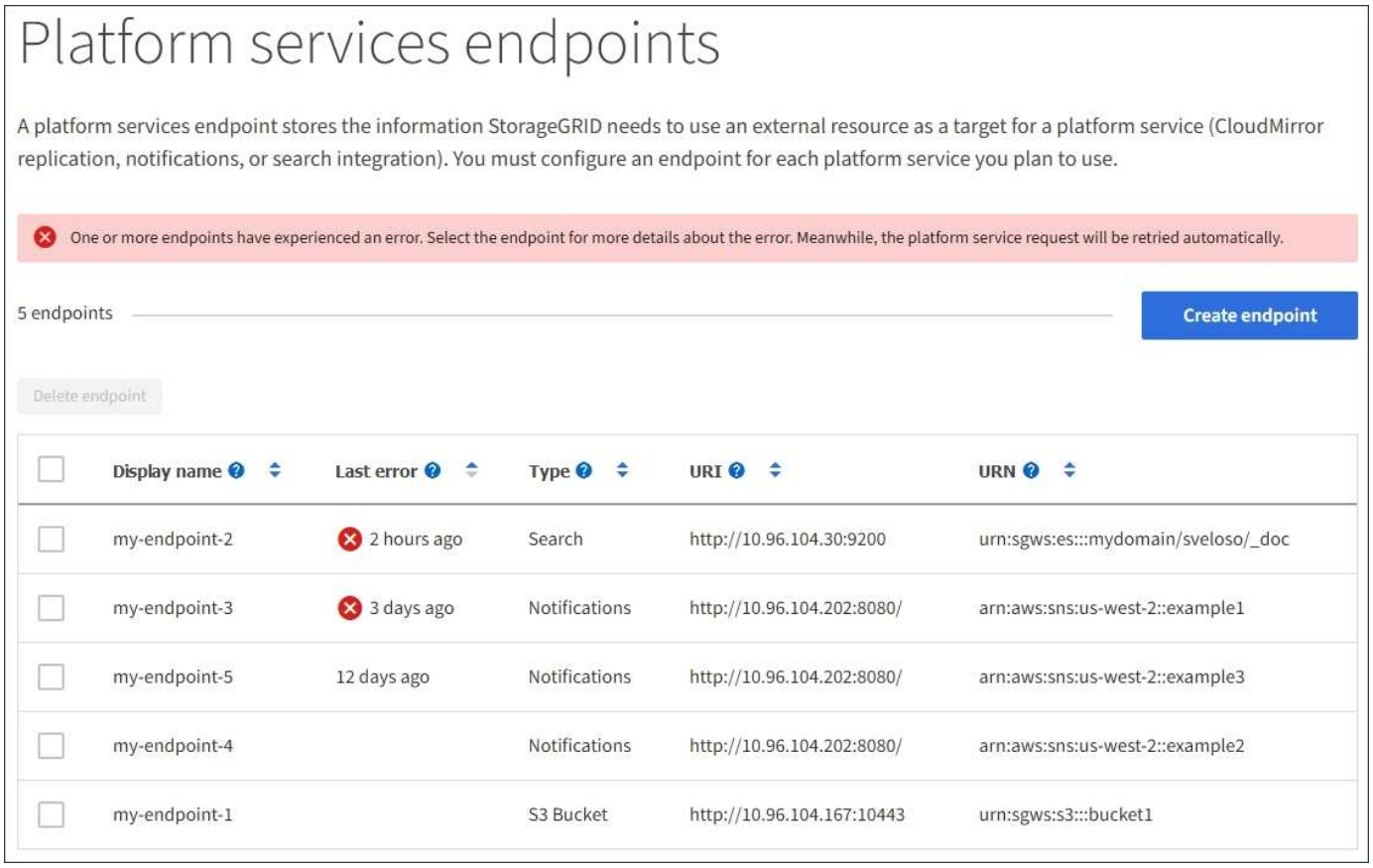
Die Erstellung von Endpunkten schlägt fehl, wenn Plattformdienste für das Mandantenkonto nicht aktiviert sind.

Probleme mit vorhandenen Endpunkten

Wenn ein Fehler auftritt, wenn StorageGRID versucht, einen vorhandenen Endpunkt zu erreichen, wird im Mandantenmanager eine Meldung auf dem Dashboard 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 Symbol enthalten, traten 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 eine"Storage-Proxy" zwischen Speicherknoten und Plattformdienst-Endpunkten können Fehler auftreten, wenn Ihr Proxydienst keine Nachrichten von StorageGRID zulässt. Um diese Probleme zu beheben, überprüfen Sie die Einstellungen Ihres Proxyservers, um sicherzustellen, dass plattformdienstbezogene Nachrichten nicht blockiert werden.

Ermitteln Sie, ob ein Fehler aufgetreten ist

Wenn in den letzten 7 Tagen Endpunktfehler aufgetreten sind, zeigt das Dashboard im Tenant Manager eine Warnmeldung an. 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 **Knoten** > ***Site*** > ***Speicherknoten*** > **Übersicht**.
2. Suchen Sie in der Warnungstabelle nach aktiven Warnungen.
3. Lösen Sie alle aktiven Warnungen. Wenden Sie sich bei Bedarf an den technischen Support.

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 existiert nicht.
- 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 sind nicht behebbar. Nicht behebbare Fehler können beispielsweise aus folgenden Gründen auftreten:

- Der Endpunkt wird gelöscht.
- Ein Webhook-Endpunktziel antwortet auf eine Benachrichtigungsanforderung mit einem `400 Bad Request` Fehler.

Wenn bei StorageGRID ein nicht behebbarer Endpunktfehler auftritt:

- Rufen Sie im Grid Manager **Support** > **Tools** > **Metrics** > **Grafana** > **Platform Services Overview** auf, um Fehlerdetails anzuzeigen.
- Gehen Sie im Tenant Manager zu **STORAGE (S3)** > **Platform Services Endpoints**, um die Fehlerdetails anzuzeigen.
- Prüfen Sie die `/var/local/log/bycast-err.log` auf zugehörige Fehler. Storage-Nodes mit dem ADC-Dienst enthalten diese Protokolldatei.

Nachrichten zu Plattform-Services können nicht bereitgestellt werden

Wenn beim Ziel ein Problem auftritt, das die Annahme von Plattformdienstnachrichten verhindert, ist der Clientvorgang für den Bucket zwar erfolgreich, die Plattformdienstnachricht wird jedoch nicht zugestellt. Dieser Fehler kann beispielsweise auftreten, wenn die Anmeldeinformationen am Ziel aktualisiert werden, sodass StorageGRID sich nicht mehr beim Zieldienst authentifizieren kann.

Prüfen Sie, ob entsprechende Warnmeldungen vorhanden sind.

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.

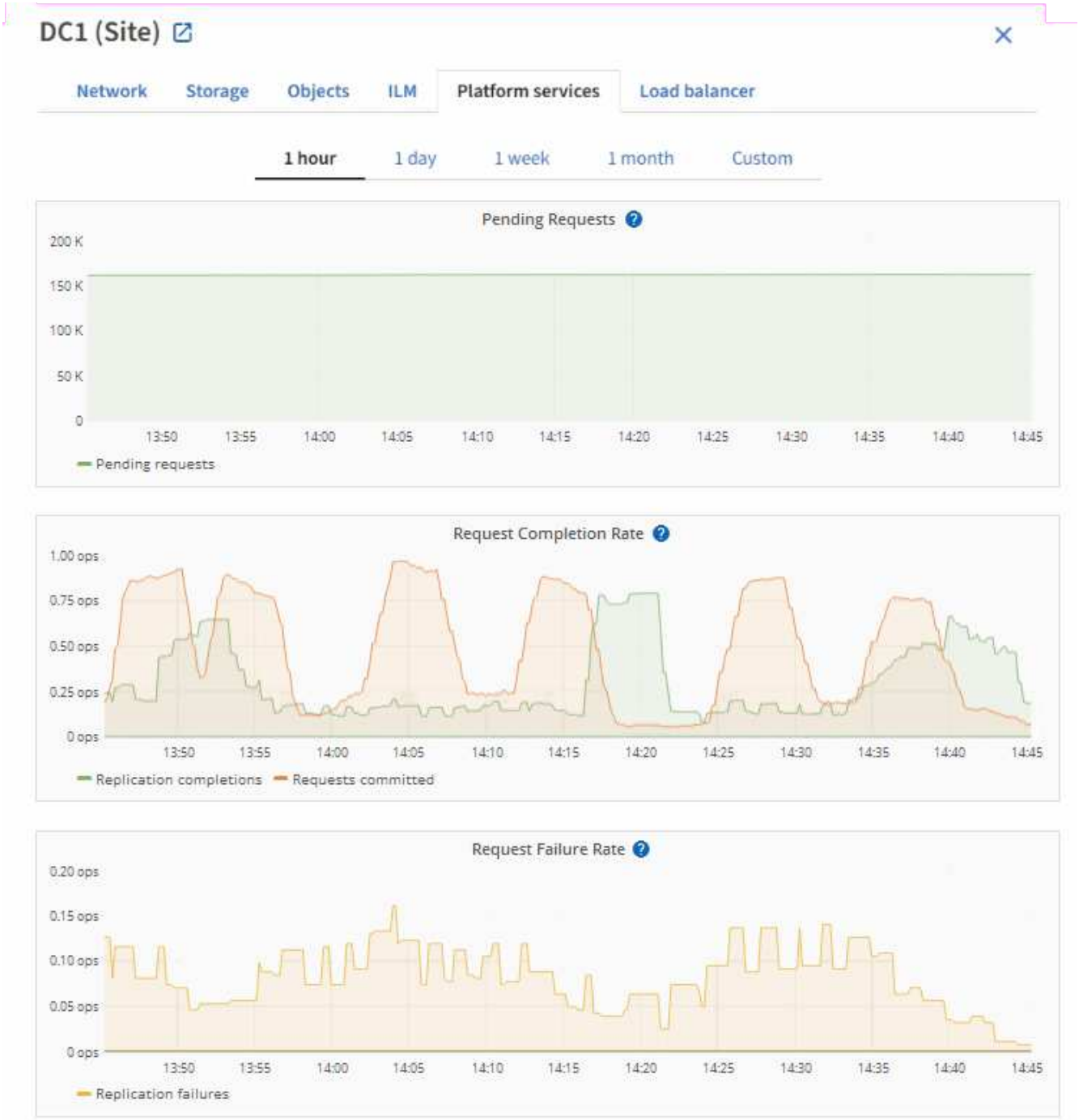
Der einzige sichtbare Effekt besteht darin, dass die eingehenden S3-Anforderungen länger in Anspruch nehmen. Wenn Sie die Performance deutlich schlechter erkennen, sollten Sie die Aufnahmerate reduzieren oder einen Endpunkt mit höherer Kapazität verwenden. Falls der Rückstand von Anforderungen weiterhin 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** aus.
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-Dienst ist auf Storage Nodes vorhanden, die auch den ADC-Dienst enthalten.) Stellen Sie dann sicher, dass eine einfache Mehrheit dieser Storage-Nodes 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 finden Sie unter **Verwenden Sie ein Mandantenkonto › Troubleshooting der Endpunkte für Plattformservices**.

Verwandte Informationen

"Fehlerbehebung für das StorageGRID-System"

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

Grid-Administrationsanforderungen

Der Grid-Administrator muss Mandanten die Möglichkeit S3 Select erteilen. Wählen Sie **S3 Select zulassen** Wann "Erstellen eines Mandanten" oder "Bearbeiten eines Mandanten".

Anforderungen an das Objektformat

Das Objekt, das Sie abfragen möchten, muss eines der folgenden Formate aufweisen:

- **CSV**. Kann wie ist verwendet oder in GZIP- oder BZIP2-Archiven komprimiert werden.
- **Parkett**. Zusätzliche Anforderungen an Parkett-Objekte:
  - S3 Select unterstützt nur Spaltenkomprimierung mit GZIP oder Snappy. S3 Select unterstützt keine Komprimierung ganzer Objekte für Parkett-Objekte.
  - S3 Select unterstützt keine Parkett-Ausgabe. Sie müssen das Ausgabeformat als CSV oder JSON angeben.
  - Die maximale Größe der nicht komprimierten Zeilengruppe beträgt 512 MB.
  - Sie müssen die im Objektschema angegebenen Datentypen verwenden.
  - Sie können KEINE logischen TYPEN VON INTERVALL, JSON, LISTE, ZEIT oder UUID verwenden.

Anforderungen an Endpunkte

Die SelectObjectContent-Anforderung muss an A gesendet werden"Endpunkt des StorageGRID-Load-

Balancer".

Die vom Endpunkt verwendeten Admin- und Gateway-Nodes müssen einen der folgenden sein:

- Ein Knoten der Service-Appliance
- Ein auf VMware basierender Software-Node
- Ein Bare-Metal-Knoten, auf dem ein Kernel mit aktivierter cgroup v2 ausgeführt wird

Allgemeine Überlegungen

Abfragen können nicht direkt an Storage-Nodes gesendet werden.

> 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".

Zum Ansehen"Grafana-Diagramme" Wählen Sie für S3 Select-Vorgänge im Zeitverlauf **Support** > **Tools** > **Metriken** im Grid Manager.

Client-Verbindungen konfigurieren

S3-Client-Verbindungen konfigurieren

Als Grid-Administrator managen Sie die Konfigurationsoptionen, die steuern, wie S3-Client-Applikationen zum Speichern und Abrufen von Daten mit Ihrem StorageGRID System verbunden sind.

> Swift-Details wurden aus dieser Version der doc-Site entfernt. Siehe "StorageGRID 11.8: Konfigurieren Sie S3- und Swift-Client-Verbindungen".

Konfigurationsaufgaben

1. Führen Sie erforderliche Aufgaben in StorageGRID aus, je nachdem, wie die Clientanwendung eine Verbindung zu StorageGRID herstellt.

Erforderliche Aufgaben

Sie müssen Folgendes erhalten:

- IP-Adressen
- Domain-Namen
- SSL-Zertifikat

Optionale Aufgaben

Optional konfigurieren:

- Identitätsföderation
- SSO

1. Verwenden Sie StorageGRID, um die Werte abzurufen, die die Anwendung für die Verbindung mit dem Grid benötigt. Sie können entweder den S3-Einrichtungsassistenten verwenden oder jede StorageGRID-Einheit manuell konfigurieren.

Verwenden Sie den S3-Einrichtungsassistenten

Befolgen Sie die Schritte im S3-Einrichtungsassistenten.

Manuell konfigurieren

1. Erstellen Sie eine Hochverfügbarkeitsgruppe
2. Lastausgleichsendpunkt erstellen
3. Erstellen eines Mandantenkontos
4. Erstellen von Buckets und Zugriffsschlüsseln
5. Konfigurieren Sie die ILM-Regel und -Richtlinie

1. Verwenden Sie die S3-Anwendung, um die Verbindung zu StorageGRID abzuschließen. Erstellen Sie DNS-Einträge, um IP-Adressen mit beliebigen Domänennamen zu verknüpfen, die Sie verwenden möchten.

   Führen Sie bei Bedarf zusätzliche Anwendungseinstellungen durch.

2. Laufende Aufgaben in der Applikation und in StorageGRID werden durchgeführt, um Objekt-Storage über einen längeren Zeitraum zu managen und zu überwachen.

Informationen, die zum Anhängen von StorageGRID an eine Client-Applikation erforderlich sind

Bevor Sie StorageGRID an eine S3-Client-Anwendung anhängen können, müssen Sie die Konfigurationsschritte in StorageGRID ausführen und einen bestimmten Wert erhalten.

Welche Werte brauche ich?

In der folgenden Tabelle sind die Werte aufgeführt, die Sie in StorageGRID konfigurieren müssen und bei denen diese Werte von der S3-Anwendung und dem DNS-Server verwendet werden.

Wert	Wobei der Wert konfiguriert ist	Wo Wert verwendet wird
Virtuelle IP-Adressen (VIP)	StorageGRID > HA-Gruppe	DNS-Eintrag
Port	StorageGRID > Endpunkt des Load Balancer	Client-Anwendung
SSL-Zertifikat	StorageGRID > Endpunkt des Load Balancer	Client-Anwendung
Servername (FQDN)	StorageGRID > Endpunkt des Load Balancer	• Client-Anwendung • DNS-Eintrag
S3 Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel	StorageGRID > Mandant und Bucket	Client-Anwendung
Bucket/Container-Name	StorageGRID > Mandant und Bucket	Client-Anwendung

Wie erhalte ich diese Werte?

Je nach Ihren Anforderungen können Sie eine der folgenden Möglichkeiten nutzen, um die benötigten Informationen zu erhalten:

- **Verwenden Sie die "S3-Einrichtungsassistent"**. Der S3-Einrichtungsassistent unterstützt Sie beim schnellen Konfigurieren der erforderlichen Werte in StorageGRID und gibt eine oder zwei Dateien aus, die Sie bei der Konfiguration der S3-Anwendung verwenden können. Der Assistent führt Sie durch die erforderlichen Schritte und stellt sicher, dass Ihre Einstellungen den StorageGRID Best Practices entsprechen.

  Wenn Sie eine S3-Applikation konfigurieren, wird die Verwendung des S3-Setup-Assistenten von empfohlen, es sei denn, Sie verfügen über besondere Anforderungen oder Ihre Implementierung erfordert eine umfangreiche Anpassung.

- **Verwenden Sie die "FabricPool Setup-Assistent"**. Ähnlich wie der S3-Einrichtungsassistent unterstützt Sie der FabricPool-Einrichtungsassistent bei der schnellen Konfiguration der erforderlichen Werte und gibt eine Datei aus, die Sie bei der Konfiguration eines FabricPool-Cloud-Tiers in ONTAP verwenden können.

  Wenn Sie StorageGRID als Objekt-Storage-System für eine FabricPool Cloud-Tier nutzen möchten, empfiehlt sich die Verwendung des FabricPool Setup-Assistenten, es sei denn, Sie haben besondere Anforderungen oder Ihre Implementierung erfordert erhebliche Anpassungen.

- **Elemente manuell konfigurieren**. Wenn Sie eine Verbindung zu einer S3-Anwendung herstellen und den S3-Einrichtungsassistenten nicht verwenden möchten, können Sie die erforderlichen Werte abrufen, indem Sie die Konfiguration manuell durchführen. Führen Sie hierzu folgende Schritte aus:

  a. Konfigurieren Sie die HA-Gruppe (High Availability, Hochverfügbarkeit), die Sie für die S3-Applikation verwenden möchten. Siehe "Konfigurieren Sie Hochverfügbarkeitsgruppen".

  b. Erstellen Sie den Load Balancer-Endpunkt, den die S3-Applikation verwenden wird. Siehe

"Konfigurieren von Load Balancer-Endpunkten".

c. Erstellen Sie das Mandantenkonto, das die S3-Anwendung verwenden wird. Siehe "Erstellen Sie ein Mandantenkonto".

d. Melden Sie sich für einen S3-Mandanten beim Mandantenkonto an und generieren Sie für jeden Benutzer, der auf die Applikation zugreift, eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel. Siehe "Erstellen Sie Ihre eigenen Zugriffsschlüssel".

e. Erstellen Sie einen oder mehrere S3-Buckets innerhalb des Mandantenkontos. Für S3 siehe "S3-Bucket erstellen".

f. Um Anweisungen zur Platzierung von Objekten, die zu dem neuen Mandanten oder Bucket/Container gehören, hinzuzufügen, erstellen Sie eine neue ILM-Regel und aktivieren Sie zur Verwendung dieser Regel eine neue ILM-Richtlinie. Siehe "ILM-Regel erstellen" und "ILM-Richtlinie erstellen".

Sicherheit für S3-Clients

StorageGRID-Mandantenkonten verwenden S3-Client-Applikationen, um Objektdaten in StorageGRID zu speichern. Überprüfen Sie die Sicherheitsmaßnahmen, die für Client-Anwendungen implementiert wurden.

Zusammenfassung

In der folgenden Liste wird zusammengefasst, wie Sicherheit für die S3-REST-API implementiert wird:

Verbindungssicherheit
: TLS

Serverauthentifizierung
: X.509-Serverzertifikat, das von der System-CA oder vom Administrator zur Verfügung gestellten benutzerdefinierten Serverzertifikat unterzeichnet wurde

Client-Authentifizierung
: Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel für das S3-Konto

Client-Autorisierung
: Eigentümerschaft von Buckets und alle anwendbaren Zugriffssteuerungsrichtlinien

Wie StorageGRID Sicherheit für Client-Anwendungen bietet

S3-Client-Applikationen können sich mit dem Load Balancer-Service auf Gateway-Nodes oder Admin-Nodes oder direkt mit Storage-Nodes verbinden.

- Clients, die sich mit dem Load Balancer-Dienst verbinden, können HTTPS oder HTTP verwenden, je nachdem, wie Sie "Konfigurieren Sie den Endpunkt des Load Balancer".

  HTTPS bietet eine sichere, TLS-verschlüsselte Kommunikation und wird empfohlen. Sie müssen dem Endpunkt ein Sicherheitszertifikat hinzufügen.

  HTTP bietet eine weniger sichere, unverschlüsselte Kommunikation und sollte nur für nicht-Produktions- oder Testraster verwendet werden.

- Clients, die eine Verbindung zu Storage Nodes herstellen, können auch HTTPS oder HTTP verwenden.

HTTPS ist der Standardwert und wird empfohlen.

HTTP bietet eine weniger sichere, unverschlüsselte Kommunikation, kann aber optional "Aktiviert" für nicht-Produktions- oder Testraster eingesetzt werden.

- Die Kommunikation zwischen StorageGRID und dem Client wird über TLS verschlüsselt.
- Die Kommunikation zwischen dem Load Balancer-Service und den Speicherknoten innerhalb des Grid wird verschlüsselt, ob der Load Balancer-Endpunkt für die Annahme von HTTP- oder HTTPS-Verbindungen konfiguriert ist.
- Clients müssen an StorageGRID bereitstellen"HTTP-Authentifizierungsheader", um REST-API-Operationen durchführen zu können.

Sicherheitszertifikate und Clientanwendungen

Clientanwendungen können in jedem Fall TLS-Verbindungen herstellen, indem sie entweder ein vom Grid-Administrator hochgeladenes benutzerdefiniertes Serverzertifikat oder ein vom StorageGRID-System generiertes Zertifikat verwenden:

- Wenn Clientanwendungen eine Verbindung zum Load Balancer-Dienst herstellen, verwenden sie das Zertifikat, das für den Load Balancer-Endpunkt konfiguriert wurde. Jeder Load Balancer-Endpunkt hat sein eigenes Zertifikat—entweder ein vom Grid-Administrator hochgeladenes benutzerdefiniertes Serverzertifikat oder ein Zertifikat, das der Grid-Administrator beim Konfigurieren des Endpunkts in StorageGRID generiert hat.

  Siehe "Überlegungen zum Lastausgleich".

- Wenn Client-Anwendungen eine direkte Verbindung zu einem Speicher-Node herstellen, verwenden sie entweder die vom System generierten Serverzertifikate, die bei der Installation des StorageGRID-Systems für Speicher-Nodes generiert wurden (die von der Systemzertifikatbehörde signiert werden). Oder ein einzelnes benutzerdefiniertes Serverzertifikat, das von einem Grid-Administrator für das Grid bereitgestellt wird. Siehe "Fügen Sie ein benutzerdefiniertes S3-API-Zertifikat hinzu".

Die Clients sollten so konfiguriert werden, dass sie der Zertifizierungsstelle vertrauen, die unabhängig davon, welches Zertifikat sie zum Erstellen von TLS-Verbindungen verwenden, unterzeichnet hat.

Unterstützte Hashing- und Verschlüsselungsalgorithmen für TLS-Bibliotheken

Das StorageGRID -System unterstützt eine Reihe von Verschlüsselungssammlungen, die Clientanwendungen beim Herstellen einer TLS-Sitzung verwenden können. Um Verschlüsselungen zu konfigurieren, gehen Sie zu **Konfiguration** > **Sicherheit** > **Sicherheitseinstellungen** und wählen Sie **TLS- und SSH-Richtlinien**.

Unterstützte Versionen von TLS

StorageGRID unterstützt TLS 1.2 und TLS 1.3.

SSLv3 und TLS 1.1 (oder frühere Versionen) werden nicht mehr unterstützt.

Verwenden Sie den S3-Einrichtungsassistenten

Überlegungen und Anforderungen im S3-Setup-Assistenten

Sie können mit dem S3-Einrichtungsassistenten StorageGRID als Objekt-Storage-System für eine S3-Applikation konfigurieren.

Wann der S3-Einrichtungsassistent verwendet werden soll

Der S3-Einrichtungsassistent führt Sie durch jeden Schritt bei der Konfiguration von StorageGRID für die Verwendung mit einer S3-Applikation. Im Rahmen der Ausführung des Assistenten laden Sie Dateien herunter, mit denen Sie Werte in die S3-Anwendung eingeben können. Mit dem Assistenten konfigurieren Sie Ihr System schneller und stellen sicher, dass Ihre Einstellungen den StorageGRID Best Practices entsprechen.

Wenn Sie über den verfügen"Root-Zugriffsberechtigung", können Sie den S3-Einrichtungsassistenten abschließen, wenn Sie den StorageGRID-Grid-Manager verwenden, oder Sie können den Assistenten zu einem späteren Zeitpunkt aufrufen und abschließen. Je nach Ihren Anforderungen können Sie auch einige oder alle erforderlichen Elemente manuell konfigurieren und dann mithilfe des Assistenten die Werte zusammenstellen, die eine S3-Anwendung benötigt.

Bevor Sie den Assistenten verwenden

Vergewissern Sie sich vor der Verwendung des Assistenten, dass Sie diese Voraussetzungen erfüllt haben.

Beziehen Sie IP-Adressen, und richten Sie VLAN-Schnittstellen ein

Wenn Sie eine HA-Gruppe (High Availability, Hochverfügbarkeit) konfigurieren, wissen Sie, mit welchen Nodes die S3-Applikation eine Verbindung herstellen und welches StorageGRID-Netzwerk verwendet wird. Sie wissen auch, welche Werte für das Subnetz CIDR, die Gateway-IP-Adresse und die virtuelle IP (VIP)-Adresse eingegeben werden sollen.

Wenn Sie planen, einen virtuellen LAN zur Trennung des Datenverkehrs von der S3-Anwendung zu verwenden, haben Sie die VLAN-Schnittstelle bereits konfiguriert. Siehe "Konfigurieren Sie die VLAN-Schnittstellen".

Konfigurieren Sie Identity Federation und SSO

Wenn Sie Identitätsföderation oder Single Sign-On (SSO) für Ihr StorageGRID System verwenden möchten, haben Sie diese Funktionen aktiviert. Sie wissen auch, welche föderierte Gruppe Root-Zugriff auf das Mandantenkonto haben sollte, das die S3-Anwendung verwenden wird. Sehen"Verwenden Sie den Identitätsverbund" Und"Konfigurieren Sie Single Sign-On" .

Abrufen und Konfigurieren von Domänennamen

Sie wissen, welcher vollständig qualifizierte Domänenname (FQDN) für StorageGRID verwendet werden soll. DNS-Einträge (Domain Name Server) weisen diesen FQDN den virtuellen IP-Adressen (VIP) der HA-Gruppe zu, die Sie mit dem Assistenten erstellen.

Wenn Sie Anforderungen im virtuellen gehosteten Stil von S3 verwenden möchten, sollten Sie über verfügen"Domänennamen des S3-Endpunkts wurden konfiguriert". Die Verwendung von Anforderungen im virtuellen Hosted-Stil wird empfohlen.

Anforderungen für Load Balancer und Sicherheitszertifikate prüfen

Wenn Sie den StorageGRID Load Balancer einsetzen möchten, haben Sie die allgemeinen Überlegungen zum Lastausgleich besprochen. Sie verfügen über die hochgeladenen Zertifikate oder die Werte, die Sie zum Generieren eines Zertifikats benötigen.

Wenn Sie einen externen (Drittanbieter-)Load Balancer-Endpunkt verwenden möchten, verfügen Sie über den vollständig qualifizierten Domänennamen (FQDN), den Port und das Zertifikat für diesen Load Balancer.

Konfigurieren Sie alle Verbindungen des Grid-Verbunds

Wenn Sie es dem S3-Mandanten erlauben möchten, Kontodaten zu klonen und Bucket-Objekte mithilfe einer Grid-Federation-Verbindung in ein anderes Grid zu replizieren, bestätigen Sie Folgendes, bevor Sie

den Assistenten starten:

- Sie haben "Grid Federation-Verbindung konfiguriert".
- Der Status der Verbindung lautet **connected**.
- Sie haben Root-Zugriffsberechtigung.

Rufen Sie den S3-Setup-Assistenten auf und vervollständigen Sie sie

Sie können den S3-Einrichtungsassistenten verwenden, um StorageGRID für die Verwendung mit einer S3-Applikation zu konfigurieren. Der Einrichtungsassistent bietet die Werte, die die Anwendung benötigt, um auf einen StorageGRID-Bucket zuzugreifen und Objekte zu speichern.

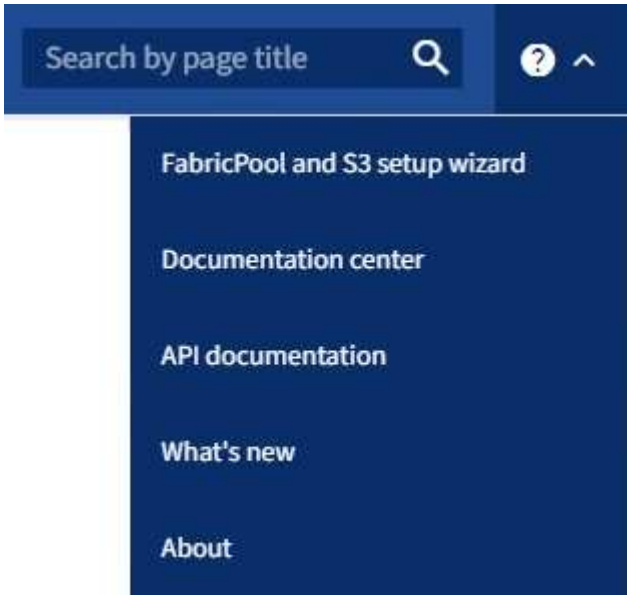
Bevor Sie beginnen

- Sie haben die "Root-Zugriffsberechtigung".
- Sie haben die zur Verwendung des Assistenten überprüft"Überlegungen und Anforderungen".

Greifen Sie auf den Assistenten zu

Schritte

1. Melden Sie sich mit einem beim Grid-Manager an"Unterstützter Webbrowser".
2. Wenn das Banner **FabricPool and S3 Setup Wizard** auf dem Dashboard angezeigt wird, wählen Sie den Link im Banner aus. Wenn das Banner nicht mehr angezeigt wird, wählen Sie in der Kopfzeile des Grid-Managers das Hilfesymbol aus und wählen Sie **FabricPool und S3-Setup-Assistent** aus.



3. Wählen Sie im Abschnitt S3-Anwendung der Seite FabricPool und S3-Setup-Assistent **Jetzt konfigurieren** aus.

Schritt 1 von 6: Konfigurieren Sie die HA-Gruppe

Eine HA-Gruppe ist eine Sammlung von Nodes, die jeweils den StorageGRID Lastausgleich enthalten. Eine HA-Gruppe kann Gateway-Nodes, Admin-Nodes oder beides enthalten.

Sie können eine HA-Gruppe verwenden, um die S3 Datenverbindungen verfügbar zu halten. Wenn die aktive

Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle den Workload mit geringen Auswirkungen auf den S3-Betrieb managen.

Weitere Informationen zu dieser Aufgabe finden Sie unter "Management von Hochverfügbarkeitsgruppen".

Schritte

1. Wenn Sie einen externen Load Balancer verwenden möchten, müssen Sie keine HA-Gruppe erstellen. Wählen Sie **diesen Schritt überspringen** und gehen Sie zu Schritt 2 von 6: Konfigurieren Sie den Load Balancer-Endpunkt.
2. Um den StorageGRID Load Balancer zu verwenden, können Sie eine neue HA-Gruppe erstellen oder eine vorhandene HA-Gruppe verwenden.

Erstellen Sie eine HA-Gruppe

a. Um eine neue HA-Gruppe zu erstellen, wählen Sie **HA-Gruppe erstellen**.

b. Füllen Sie für den Schritt **Enter Details** die folgenden Felder aus.

Feld	Beschreibung
Name DER HA-Gruppe	Ein eindeutiger Anzeigename für diese HA-Gruppe.
Beschreibung (optional)	Die Beschreibung dieser HA-Gruppe.

c. Wählen Sie im Schritt **Schnittstellen hinzufügen** die Knotenschnittstellen aus, die Sie in dieser HA-Gruppe verwenden möchten.

   Verwenden Sie die Spaltenüberschriften, um die Zeilen zu sortieren, oder geben Sie einen Suchbegriff ein, um Schnittstellen schneller zu finden.

   Sie können einen oder mehrere Nodes auswählen, aber Sie können nur eine Schnittstelle für jeden Node auswählen.

d. Bestimmen Sie für den Schritt **priorisiere Schnittstellen** die primäre Schnittstelle und alle Backup-Schnittstellen für diese HA-Gruppe.

   Ziehen Sie Zeilen, um die Werte in der Spalte **Priority order** zu ändern.

   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 enthält und die aktive Schnittstelle ausfällt, werden die virtuellen IP-Adressen (VIP-Adressen) zur ersten Backup-Schnittstelle in der Prioritätsreihenfolge verschoben. Wenn diese Schnittstelle ausfällt, wechseln die VIP-Adressen zur nächsten Backup-Schnittstelle usw. Wenn Fehler behoben sind, werden die VIP-Adressen auf die Schnittstelle mit der höchsten Priorität zurückverschoben.

e. Füllen Sie für den Schritt **IP-Adressen eingeben** die folgenden Felder aus.

Feld	Beschreibung
Subnetz-CIDR	Die Adresse des VIP-Subnetzes in CIDR-Notation — eine IPv4-Adresse gefolgt von einem Schrägstrich und der Subnetz-Länge (0-32). Die Netzwerkadresse darf keine Host-Bits festgelegt haben. `192.16.0.0/22`Beispiel: .
Gateway-IP-Adresse (optional)	Wenn sich die S3-IP-Adressen für den Zugriff auf StorageGRID nicht im selben Subnetz wie die StorageGRID-VIP-Adressen befinden, geben Sie die lokale StorageGRID-VIP-Gateway-IP-Adresse ein. Die IP-Adresse des lokalen Gateways muss sich im VIP-Subnetz befinden.

Feld	Beschreibung
Virtuelle IP-Adresse	Geben Sie mindestens eine und nicht mehr als zehn VIP-Adressen für die aktive Schnittstelle in der HA-Gruppe ein. Alle VIP-Adressen müssen sich innerhalb des VIP-Subnetzes befinden. Mindestens eine Adresse muss IPv4 sein. Optional können Sie weitere IPv4- und IPv6-Adressen angeben.

f. Wählen Sie **HA-Gruppe erstellen** und dann **Fertig stellen**, um zum S3-Setup-Assistenten zurückzukehren.

g. Wählen Sie **Weiter**, um zum Schritt Load Balancer zu gelangen.

Verwenden Sie die vorhandene HA-Gruppe

a. Um eine vorhandene HA-Gruppe zu verwenden, wählen Sie den Namen der HA-Gruppe aus **Select an HA Group** aus.

b. Wählen Sie **Weiter**, um zum Schritt Load Balancer zu gelangen.

Schritt 2 von 6: Konfigurieren Sie den Load Balancer-Endpunkt

StorageGRID verwendet einen Load Balancer für das Management des Workloads aus Client-Applikationen. Load Balancing maximiert Geschwindigkeit und Verbindungskapazität über mehrere Storage Nodes hinweg.

Sie können den StorageGRID Load Balancer-Dienst verwenden, der auf allen Gateway- und Admin-Nodes vorhanden ist, oder eine Verbindung zu einem externen Load Balancer (Drittanbieter) herstellen. Die Verwendung des StorageGRID Load Balancer wird empfohlen.

Weitere Informationen zu dieser Aufgabe finden Sie unter "Überlegungen zum Lastausgleich".

Um den StorageGRID Load Balancer Service zu verwenden, wählen Sie die Registerkarte **StorageGRID Load Balancer** aus und erstellen oder wählen Sie dann den gewünschten Load Balancer-Endpunkt aus. Um einen externen Load Balancer zu verwenden, wählen Sie die Registerkarte **External Load Balancer** und geben Sie Details zum System an, das Sie bereits konfiguriert haben.

Endpunkt erstellen

Schritte

1. Um einen Load Balancer-Endpunkt zu erstellen, wählen Sie **Endpunkt erstellen**.
2. Füllen Sie für den Schritt **Enter Endpoint Details** die folgenden Felder aus.

Feld	Beschreibung
Name	Ein beschreibender Name für den Endpunkt.
Port	Der StorageGRID-Port, den Sie für den Lastausgleich verwenden möchten. Dieses Feld ist für den ersten erstellten Endpunkt standardmäßig auf 10433 eingestellt, Sie können jedoch jeden nicht verwendeten externen Port eingeben. Wenn Sie 80 oder 443 eingeben, wird der Endpunkt nur auf Gateway-Nodes konfiguriert, da diese Ports auf Admin-Nodes reserviert sind. **Hinweis:** Von anderen Grid-Diensten verwendete Ports sind nicht zulässig. Sehen "Interne StorageGRID-Ports" .
Client-Typ	Muss **S3** sein.
Netzwerkprotokoll	Wählen Sie **HTTPS**. **Hinweis**: Die Kommunikation mit StorageGRID ohne TLS-Verschlüsselung wird unterstützt, aber nicht empfohlen.

3. Geben Sie für den Schritt **Bindungsmodus auswählen** den Bindungsmodus an. Der Bindungsmodus steuert, wie der Zugriff auf den Endpunkt über eine beliebige IP-Adresse oder über spezifische IP-Adressen und Netzwerkschnittstellen erfolgt.

Modus	Beschreibung
Global (Standard)	Clients können über die IP-Adresse eines beliebigen Gateway-Node oder Admin-Node, die virtuelle IP-Adresse (VIP) einer beliebigen HA-Gruppe in einem beliebigen Netzwerk oder einen entsprechenden FQDN auf den Endpunkt zugreifen. Verwenden Sie die **Global**-Einstellung (Standard), es sei denn, Sie müssen die Zugriffsmöglichkeiten dieses Endpunkts einschränken.
Virtuelle IPs von HA-Gruppen	Clients müssen eine virtuelle IP-Adresse (oder einen entsprechenden FQDN) einer HA-Gruppe verwenden, um auf diesen Endpunkt zuzugreifen. Endpunkte mit diesem Bindungsmodus können alle dieselbe Portnummer verwenden, solange sich die für die Endpunkte ausgewählten HA-Gruppen nicht überlappen.

Modus	Beschreibung
Node-Schnittstellen	Clients müssen die IP-Adressen (oder entsprechende FQDNs) der ausgewählten Knotenschnittstellen verwenden, um auf diesen Endpunkt zuzugreifen.
Node-Typ	Basierend auf dem von Ihnen ausgewählten Knotentyp müssen Clients entweder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Admin-Knotens oder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Gateway-Knotens verwenden, um auf diesen Endpunkt zuzugreifen.

4. Wählen Sie für den Schritt Tenant Access eine der folgenden Optionen aus:

Feld	Beschreibung
Alle Mandanten zulassen (Standard)	Alle Mandantenkonten können diesen Endpunkt verwenden, um auf ihre Buckets zuzugreifen.
Ausgewählte Mandanten zulassen	Nur die ausgewählten Mandantenkonten können diesen Endpunkt für den Zugriff auf ihre Buckets verwenden.
Ausgewählte Mandanten blockieren	Die ausgewählten Mandantenkonten können diesen Endpunkt nicht für den Zugriff auf ihre Buckets verwenden. Dieser Endpunkt kann von allen anderen Mandanten verwendet werden.

5. Wählen Sie für den Schritt **Zertifikat anhängen** eine der folgenden Optionen aus:

Feld	Beschreibung
Zertifikat hochladen (empfohlen)	Verwenden Sie diese Option, um ein CA-signiertes Serverzertifikat, einen privaten Zertifikatschlüssel und ein optionales CA-Paket hochzuladen.
Zertifikat wird generiert	Verwenden Sie diese Option, um ein selbstsigniertes Zertifikat zu generieren. Einzelheiten dazu finden Sie unter"Konfigurieren von Load Balancer-Endpunkten".
StorageGRID S3-Zertifikat verwenden	Verwenden Sie diese Option nur, wenn Sie bereits eine benutzerdefinierte Version des globalen StorageGRID-Zertifikats hochgeladen oder generiert haben. Weitere Informationen finden Sie unter "Konfigurieren Sie S3-API-Zertifikate" .

6. Wählen Sie **Finish**, um zum S3-Setup-Assistenten zurückzukehren.
7. Wählen Sie **Weiter**, um zum Mandanten- und Bucket-Schritt zu gelangen.

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

Verwenden Sie den vorhandenen Endpunkt des Load Balancer

Schritte

1. Um einen vorhandenen Endpunkt zu verwenden, wählen Sie seinen Namen aus dem **Select a Load Balancer Endpunkt** aus.
2. Wählen Sie **Weiter**, um zum Mandanten- und Bucket-Schritt zu gelangen.

Externen Load Balancer verwenden

Schritte

1. Um einen externen Load Balancer zu verwenden, füllen Sie die folgenden Felder aus.

Feld	Beschreibung
FQDN	Der vollständig qualifizierte Domänenname (FQDN) des externen Load Balancer.
Port	Die Portnummer, die die S3-Anwendung für die Verbindung mit dem externen Load Balancer verwendet.
Zertifikat	Kopieren Sie das Serverzertifikat für den externen Load Balancer und fügen Sie es in dieses Feld ein.

2. Wählen Sie **Weiter**, um zum Mandanten- und Bucket-Schritt zu gelangen.

Schritt 3 von 6: Erstellen Sie einen Mandanten und Bucket

Ein Mandant ist eine Einheit, die S3-Applikationen zum Speichern und Abrufen von Objekten in StorageGRID verwenden kann. Jeder Mandant verfügt über eigene Benutzer, Zugriffsschlüssel, Buckets, Objekte und bestimmte Funktionen.

Ein Bucket ist ein Container, mit dem die Objekte und Objektmetadaten eines Mandanten gespeichert werden können. Obwohl Mandanten möglicherweise über viele Buckets verfügen, hilft Ihnen der Assistent dabei, auf schnelle und einfache Weise einen Mandanten und einen Bucket zu erstellen. Wenn Sie zu einem späteren Zeitpunkt Buckets hinzufügen oder Optionen festlegen müssen, können Sie den Tenant Manager verwenden.

Weitere Informationen zu dieser Aufgabe finden Sie unter "Erstellen eines Mandantenkontos" und "S3-Bucket erstellen".

Schritte

1. 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.

2. Definieren Sie den Root-Zugriff für das Mandantenkonto, je nachdem, ob Ihr StorageGRID -System"Identitätsföderation" ,"Single Sign On (SSO)" oder beides.

Option	Tun Sie das
Wenn die Identitätsföderation nicht aktiviert ist	Geben Sie das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.

Option	Tun Sie das
Wenn die Identitätsföderation aktiviert ist	a. Wählen Sie eine vorhandene Verbundgruppe aus, die "Root-Zugriffsberechtigung"für den Mandanten vorhanden sein soll. b. Geben Sie optional das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.
Wenn sowohl Identitätsföderation als auch Single Sign-On (SSO) aktiviert sind	Wählen Sie eine vorhandene Verbundgruppe aus, die "Root-Zugriffsberechtigung"für den Mandanten vorhanden sein soll. Keine lokalen Benutzer können sich anmelden.

3. Wenn Sie möchten, dass der Assistent die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel für den Root-Benutzer erstellt, wählen Sie **Root-Benutzer S3-Zugriffsschlüssel automatisch erstellen**.

   Wählen Sie diese Option aus, wenn der einzige Benutzer für den Mandanten der Root-Benutzer ist. Wenn andere Benutzer diesen Mandanten verwenden, konfigurieren Sie "Verwenden Sie Tenant Manager"Schlüssel und Berechtigungen.

4. Wenn Sie jetzt einen Bucket für diesen Mandanten erstellen möchten, wählen Sie **Create Bucket for this Tenant** aus.

   Wenn S3 Object Lock für das Raster aktiviert ist, ist für den in diesem Schritt erstellten Bucket die S3 Object Lock nicht aktiviert. Wenn Sie einen S3-ObjektsperrBucket für diese S3-Applikation verwenden müssen, wählen Sie jetzt nicht, um einen Bucket zu erstellen. Verwenden Sie stattdessen Tenant Manager zu "Erstellen Sie den Bucket" einem späteren Zeitpunkt.

   a. Geben Sie den Namen des Buckets ein, den die S3-Applikation verwendet. `s3-bucket`Beispiel: .

      Sie können den Bucket-Namen nach dem Erstellen des Buckets nicht ändern.

   b. Wählen Sie die **Region** für diesen Bucket aus.

      Verwenden Sie die Standardregion (`us-east-1`), es sei denn, Sie werden zukünftig ILM verwenden, um Objekte basierend auf der Region des Buckets zu filtern.

5. Wählen Sie **Erstellen und fortfahren**.

Schritt 4 von 6: Daten herunterladen

Im Schritt zum Herunterladen von Daten können Sie eine oder zwei Dateien herunterladen, um die Details zu dem zu speichern, was Sie gerade konfiguriert haben.

Schritte

1. Wenn Sie **Root-Benutzer S3-Zugriffsschlüssel automatisch erstellen** ausgewählt haben, führen Sie einen oder beide der folgenden Schritte aus:
   - Wählen Sie **Zugriffsschlüssel herunterladen**, um eine Datei herunterzuladen `.csv`, die den Namen des Mandantenkontos, die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel enthält.
   - Wählen Sie das Kopiersymbol ( ), um die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel in die Zwischenablage zu kopieren.
2. Wählen Sie **Konfigurationswerte herunterladen**, um eine Datei herunterzuladen `.txt`, die die

Einstellungen für den Load Balancer-Endpunkt, den Mandanten, den Bucket und den Root-Benutzer enthält.

3. Speichern Sie diese Informationen an einem sicheren Ort.

> Schließen Sie diese Seite erst, wenn Sie beide Zugriffsschlüssel kopiert haben. Die Tasten sind nach dem Schließen dieser Seite nicht mehr verfügbar. Speichern Sie diese Informationen an einem sicheren Ort, da sie zum Abrufen von Daten von Ihrem StorageGRID-System verwendet werden können.

4. Wenn Sie dazu aufgefordert werden, aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Schlüssel heruntergeladen oder kopiert haben.
5. Wählen Sie **Weiter**, um zur ILM-Regel und zum Richtlinienschritt zu gelangen.

Schritt 5 von 6: Prüfen Sie die ILM-Regel und die ILM-Richtlinie für S3

Informationen Lifecycle Management-Regeln (ILM) steuern die Platzierung, Dauer und das Aufnahmeverhalten aller Objekte in Ihrem StorageGRID System. Mit der bei StorageGRID enthaltenen ILM-Richtlinie werden zwei replizierte Kopien aller Objekte erstellt. Diese Richtlinie ist gültig, bis Sie mindestens eine neue Richtlinie aktivieren.

Schritte

1. Überprüfen Sie die Informationen auf der Seite.
2. Wenn Sie bestimmte Anweisungen für die Objekte hinzufügen möchten, die zum neuen Mandanten oder Bucket gehören, erstellen Sie eine neue Regel und eine neue Richtlinie. Siehe "ILM-Regel erstellen" und "Verwenden Sie ILM-Richtlinien".
3. Wählen Sie * Ich habe diese Schritte überprüft und verstehe, was ich tun muss*.
4. Aktivieren Sie das Kontrollkästchen, um anzugeben, dass Sie die nächsten Schritte verstehen.
5. Wählen Sie **Weiter**, um zu **Zusammenfassung** zu gelangen.

Schritt 6 von 6: Zusammenfassung überprüfen

Schritte

1. Überprüfen Sie die Zusammenfassung.
2. Notieren Sie sich in den nächsten Schritten die Details, die die zusätzliche Konfiguration beschreiben, die möglicherweise erforderlich ist, bevor Sie eine Verbindung zum S3-Client herstellen. Wenn Sie beispielsweise **als root anmelden** auswählen, gelangen Sie zum Tenant Manager, wo Sie Mandantenbenutzer hinzufügen, zusätzliche Buckets erstellen und Bucket-Einstellungen aktualisieren können.
3. Wählen Sie **Fertig**.
4. Konfigurieren Sie die Anwendung mit der Datei, die Sie von StorageGRID heruntergeladen haben, oder mit den manuell erhaltenen Werten.

Managen von HA-Gruppen

Was sind Hochverfügbarkeitsgruppen (High Availability Groups, HA-Gruppen)?

Hochverfügbarkeitsgruppen (HA-Gruppen) bieten hochverfügbare Datenverbindungen für S3-Clients und hochverfügbare Verbindungen zu Grid Manager und Tenant Manager.

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.

Jede HA-Gruppe bietet Zugriff auf die Shared Services auf den ausgewählten Nodes.

- HA-Gruppen, die Gateway-Nodes, Admin-Nodes oder beide umfassen, stellen hochverfügbare Datenverbindungen für S3-Clients bereit.
- HA-Gruppen, die nur Admin-Nodes enthalten, bieten hochverfügbare Verbindungen zum Grid Manager und dem Mandanten-Manager.
- Eine HA-Gruppe, die nur Services Appliances und VMware-basierte Software Nodes umfasst"S3-Mandanten, die S3 Select nutzen", kann hochverfügbare Verbindungen für bereitstellen. 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 „aktive“ Schnittstelle 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 dann verwendet, wenn die primäre (derzeit aktive) Schnittstelle nicht mehr verfügbar ist.

Anzeigen des aktuellen HA-Gruppen-Status eines Node

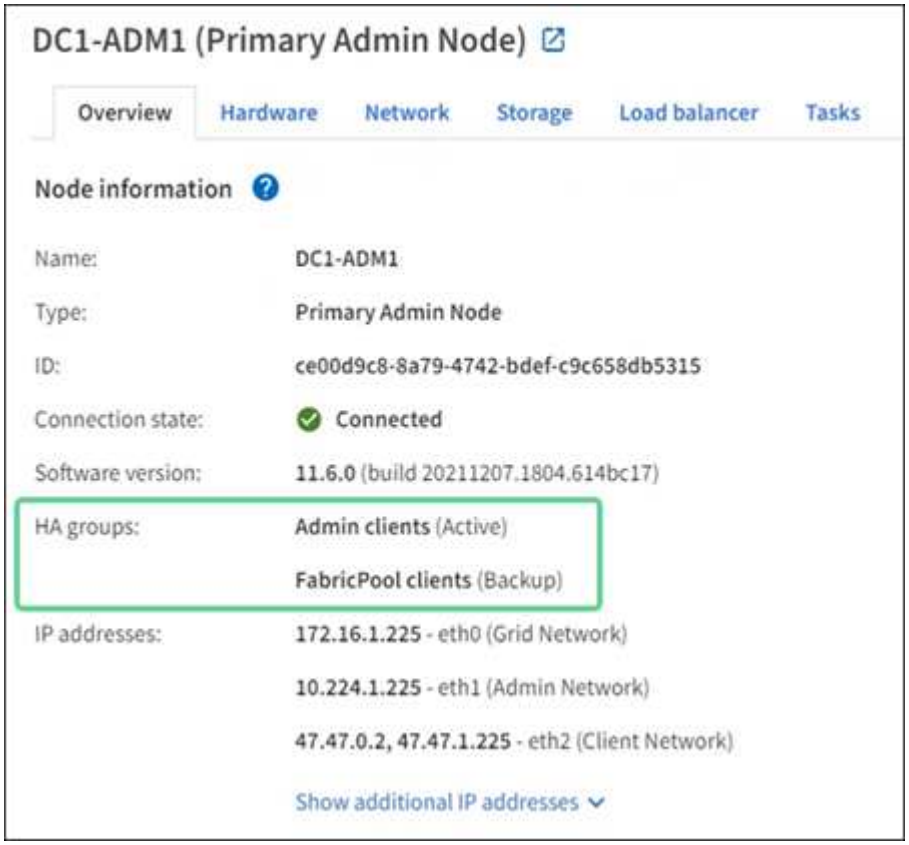
Um zu sehen, ob ein Knoten einer HA-Gruppe zugewiesen ist, und um seinen aktuellen Status zu bestimmen, wählen Sie **Knoten** > ***Knoten***.

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 Dienst hohe Verfügbarkeit (keepalibed) manuell angehalten wurde.
- **Fault**: Die HA-Gruppe kann nicht auf diesem Knoten gehostet werden, weil einer oder mehrere der folgenden:
  - 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 Failover nicht von den Diensten für den Grid Manager oder den Tenant 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-Clients bereitstellen.
- 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 Nodes**: Fügen Sie den Load Balancer Service 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-Clientzugriff – Load Balancer-Dienst	• Admin-Nodes • Gateway-Nodes

Zweck der HA-Gruppe	Fügen Sie diesem Typ Nodes der HA-Gruppe hinzu
S3-Client-Zugriff für "S3 Select"	• Service-Appliances • VMware-basierte Software-Nodes **Hinweis**: HA-Gruppen werden bei der Verwendung von S3 Select empfohlen, aber nicht erforderlich.

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.

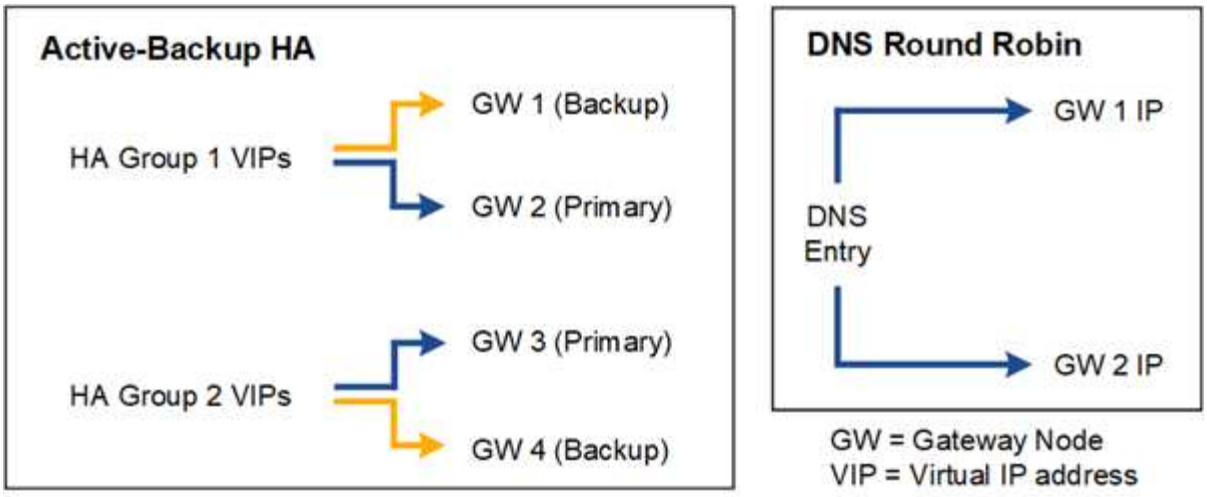
Wenn Sie sich bei einem Failover beim Grid Manager oder beim Tenant Manager angemeldet haben, werden Sie abgemeldet und müssen sich erneut anmelden, um Ihre Aufgabe fortzusetzen.

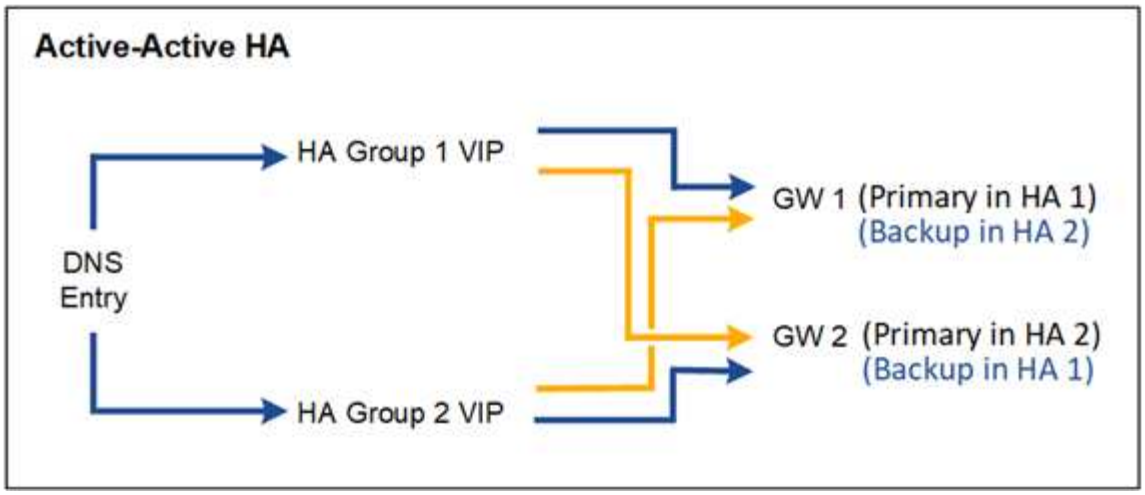
Einige Wartungsverfahren können nicht durchgeführt werden, wenn der primäre Admin-Node nicht verfügbar ist. Während des Failovers können Sie Ihr StorageGRID-System mit dem Grid-Manager überwachen.

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.

Ein StorageGRID -System kann maximal 255 HA-Gruppen haben.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem 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:
  - **Linux (vor der Installation des Knotens)**:"Erstellen von Node-Konfigurationsdateien"
  - **Linux (nach der Installation des Knotens)**:"Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Knoten"
  - **VMware (nach der Installation des Knotens)**:"Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Knoten"

„Linux“ bezieht sich auf eine RHEL-, Ubuntu- oder Debian-Bereitstellung. Eine Liste der unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool (IMT)" .

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

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerk** > **Hochverfügbarkeitsgruppen**.

2. Wählen Sie **Erstellen**.

Geben Sie Details für die HA-Gruppe ein

Schritte

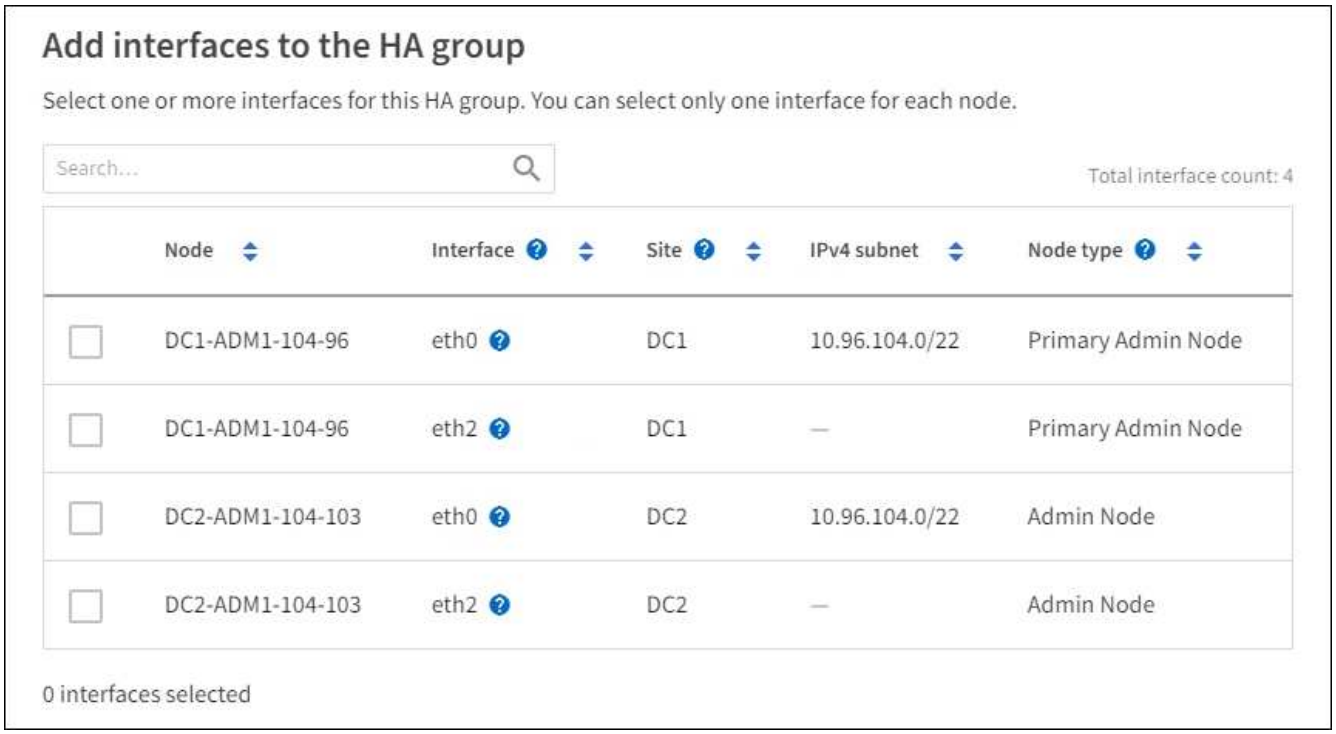
1. Geben Sie einen eindeutigen Namen für die HA-Gruppe ein.
2. Geben Sie optional eine Beschreibung für die HA-Gruppe ein.
3. Wählen Sie **Weiter**.

Fügen Sie der HA-Gruppe Schnittstellen hinzu

Schritte

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.



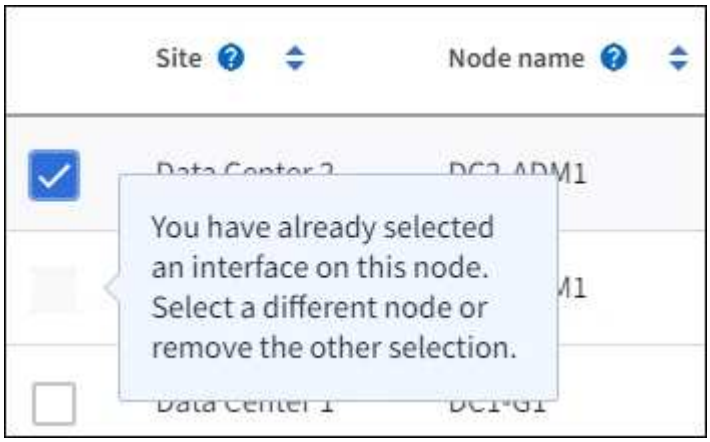
> Warten Sie nach dem Erstellen einer VLAN-Schnittstelle bis zu 5 Minuten, bis die neue Schnittstelle in der Tabelle angezeigt wird.

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 für HA-Schutz für S3-Client-Datenverkehr geeignet ist, wählen Sie Schnittstellen auf Admin-Nodes, Gateway-Nodes oder beides 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. Ein Backup-Gateway-Node kann beispielsweise keinen HA-Schutz für Admin-Node-Services bereitstellen. Ebenso kann ein Backup-Admin-Node nicht alle Wartungsverfahren durchführen, die der primäre Admin-Node bereitstellen kann.

- Wenn Sie keine Schnittstelle auswählen können, ist das Kontrollkästchen deaktiviert. Der QuickInfo enthält weitere Informationen.



- Eine Schnittstelle kann nicht ausgewählt werden, wenn ihr Subnetzwert oder Gateway mit einer anderen ausgewählten Schnittstelle in Konflikt steht.
- Sie können keine konfigurierte Schnittstelle auswählen, wenn diese keine statische IP-Adresse hat.

2. Wählen Sie **Weiter**.

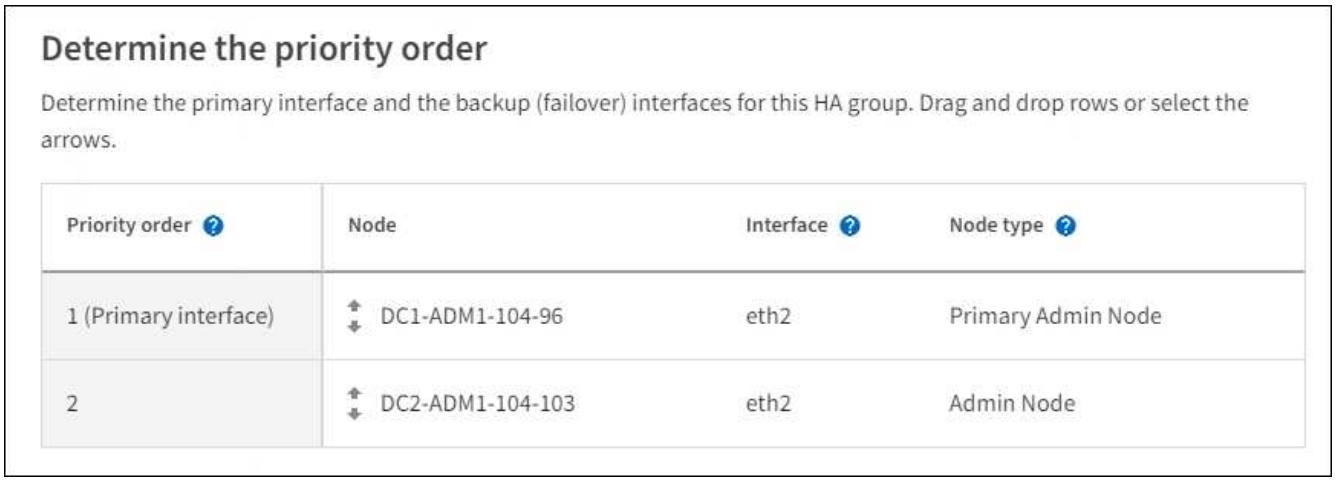
Legen Sie die Prioritätsreihenfolge fest

Wenn die HA-Gruppe mehr als eine Schnittstelle umfasst, können Sie feststellen, welche primäre Schnittstelle und welche Backup-Schnittstellen (Failover) sind. Wenn die primäre Schnittstelle fehlschlägt, werden die VIP-Adressen zur Schnittstelle mit der höchsten Priorität verschoben, die verfügbar ist. Wenn diese Schnittstelle ausfällt, werden die VIP-Adressen zur nächsten verfügbaren Schnittstelle mit der höchsten Priorität usw. verschoben.

Schritte

1. Ziehen Sie Zeilen in die Spalte **Priority order**, um die primäre Schnittstelle und alle Backup-Schnittstellen zu bestimmen.

   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 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.

2. Wählen Sie **Weiter**.

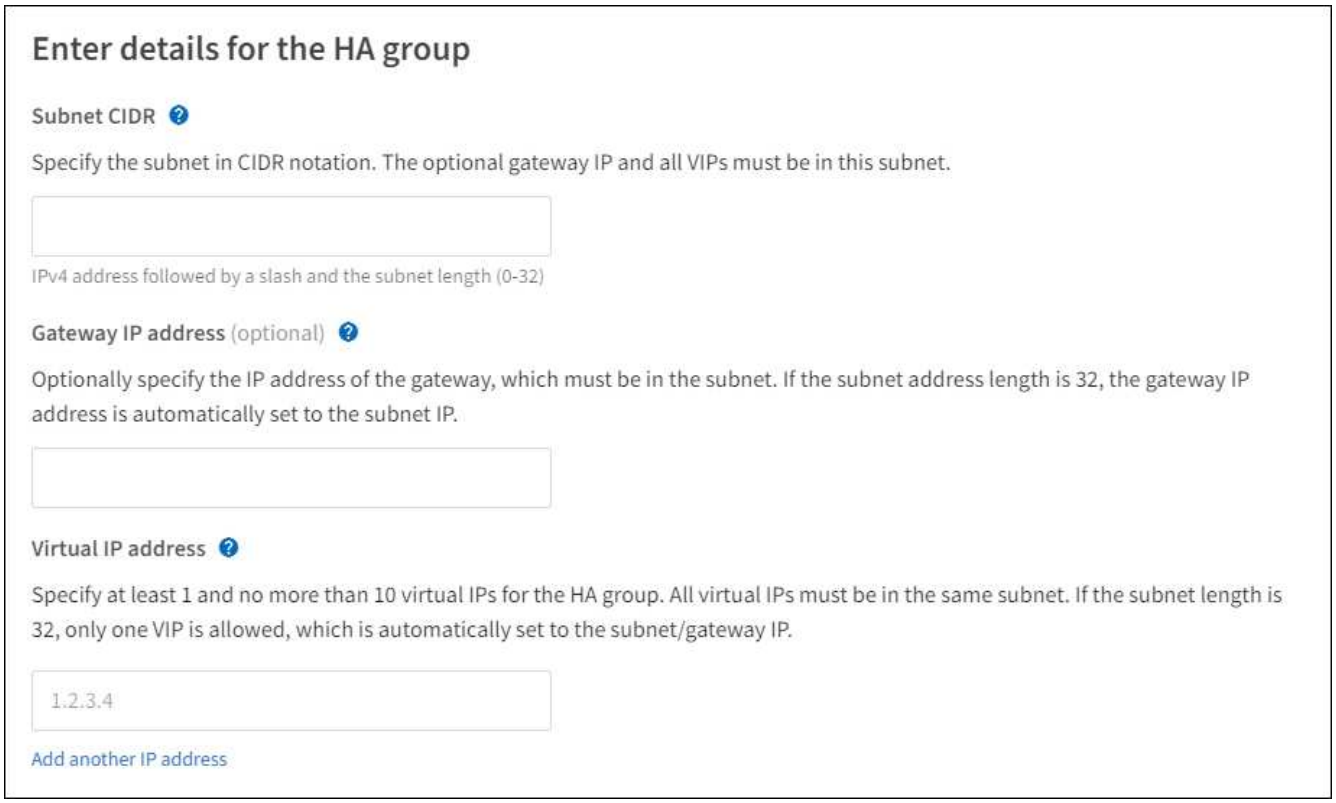
Geben Sie die IP-Adressen ein

Schritte

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. `192.16.0.0/22`Beispiel: .

   Wenn Sie ein 32-Bit-Präfix verwenden, dient die VIP-Netzwerkadresse auch als Gateway-Adresse und VIP-Adresse.



2. Wenn irgendwelche S3-Administrator- oder Mandanten-Clients von einem anderen Subnetz aus auf diese VIP-Adressen zugreifen, geben Sie optional 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 mindestens eine und nicht mehr als zehn VIP-Adressen für die aktive Schnittstelle in der HA-Gruppe ein. Alle VIP-Adressen müssen sich innerhalb des VIP-Subnetzes befinden, und alle müssen gleichzeitig auf der aktiven Schnittstelle aktiv sein.

   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.

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 oder deaktivieren 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. Optional können Sie Zeilen ziehen, 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**.

Entfernen Sie eine Hochverfügbarkeitsgruppe

Sie können eine oder mehrere HA-Gruppen (High Availability, Hochverfügbarkeit) gleichzeitig entfernen.

Sie können eine HA-Gruppe nicht entfernen, wenn sie an einen Load Balancer-Endpunkt gebunden ist. Zum Löschen einer HA-Gruppe müssen Sie sie von allen Endpunkten der Load Balancer entfernen, die sie verwenden.

Aktualisieren Sie alle betroffenen S3-Client-Applikationen, bevor Sie eine HA-Gruppe entfernen, um Client-Unterbrechungen zu vermeiden. 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. Überprüfen Sie die Spalte **Load Balancer Endpunkte** für jede HA-Gruppe, die Sie entfernen möchten. Wenn Load Balancer-Endpunkte aufgeführt sind:
   a. Gehen Sie zu **Konfiguration** > **Netzwerk** > **Load Balancer-Endpunkte**.
   b. Aktivieren Sie das Kontrollkästchen für den Endpunkt.
   c. Wählen Sie **Aktionen** > **Endpunktbindungsmodus bearbeiten**.
   d. Aktualisieren Sie den Bindungsmodus, um die HA-Gruppe zu entfernen.
   e. Wählen Sie **Änderungen speichern**.
3. Wenn keine Load Balancer-Endpunkte aufgeführt sind, aktivieren Sie das Kontrollkästchen für jede HA-Gruppe, die Sie entfernen möchten.
4. Wählen Sie **actions** > **Remove HA Group**.
5. 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

Überlegungen zum Lastausgleich

Mit Lastausgleich können Workloads bei der Aufnahme und dem Abruf von S3 Clients genutzt werden.

Was ist Load Balancing?

Wenn eine Client-Applikation Daten eines StorageGRID Systems speichert oder abruft, verwendet StorageGRID einen Load Balancer, um den Aufnahme- und Abruf-Workload zu managen. Load Balancing maximiert die Geschwindigkeit und die Verbindungskapazität, indem der Workload auf mehrere Storage Nodes verteilt wird.

Der StorageGRID Load Balancer-Service wird auf allen Admin-Nodes und allen Gateway-Knoten installiert und bietet Layer 7-Lastausgleich. Sie beendet die TLS-Beendigung von Client-Anforderungen, prüft die Anforderungen und stellt neue sichere Verbindungen zu den Storage-Nodes her.

Der Load Balancer-Service auf jedem Node wird unabhängig ausgeführt, wenn der Client-Datenverkehr an die Storage Nodes weitergeleitet wird. Durch eine Gewichtung leitet der Load Balancer-Service mehr Anfragen an Storage-Nodes mit höherer CPU-Verfügbarkeit weiter.

> Obwohl der StorageGRID Load Balancer-Dienst der empfohlene Lastausgleichsmechanismus ist, möchten Sie möglicherweise stattdessen einen Load Balancer eines Drittanbieters integrieren. Weitere Informationen erhalten Sie von Ihrem NetApp -Kundenbetreuer oder unter [Link einfügen]. "Verwenden Sie Load Balancer von Drittanbietern mit StorageGRID."Die

Wie viele Nodes für Lastausgleich benötige ich?

Als allgemeine Best Practice sollte jeder Standort in Ihrem StorageGRID-System zwei oder mehr Nodes mit dem Load Balancer Service umfassen. Ein Standort kann beispielsweise zwei Gateway-Nodes oder einen Admin-Node und einen Gateway-Node umfassen. Stellen Sie sicher, dass für jeden Load Balancing-Node eine geeignete Netzwerk-, Hardware- oder Virtualisierungsinfrastruktur bereitgestellt wird, unabhängig davon, ob Sie Services-Appliances, Bare-Metal-Nodes oder VM-basierte Nodes nutzen.

Was ist ein Endpunkt eines Load Balancers?

Ein Load Balancer-Endpunkt definiert den Port und das Netzwerkprotokoll (HTTPS oder HTTP), über das eingehende und ausgehende Client-Anwendungsanforderungen auf die Knoten zugreifen, die den Load Balancer-Dienst enthalten. Der Endpunkt definiert außerdem den Client-Typ (S3), den Bindungsmodus und optional eine Liste zulässiger oder blockierter Mandanten.

Um einen Load Balancer-Endpunkt zu erstellen, verwenden Sie entweder den Grid Manager oder schließen Sie die S3-Setup- und FabricPool Assistenten ab:

- "Konfigurieren von Load Balancer-Endpunkten"
- "Verwenden Sie den S3-Einrichtungsassistenten"
- "Verwenden Sie den FabricPool-Einrichtungsassistenten"

Überlegungen zum Load Balancer-Caching

Durch Caching wird die Leistung erheblich verbessert, wenn eine Arbeitslast mit einer Teilmenge von Daten arbeitet und mehrmals auf Objekte zugreift. Darüber hinaus ermöglicht das Caching den Fernzugriff auf den Objektspeicher ohne vollständige Grid-Bereitstellung. Das Zwischenspeichern des Lastenausgleichs ist nur für Gateway-Knoten verfügbar.

Beim Erstellen von Load Balancer-Endpunkten:

- Aktivieren Sie das Caching nur für Workloads, die zwischengespeichert werden können. Workloads, die häufiger auf nicht zwischengespeicherte Daten als auf zwischengespeicherte Daten zugreifen, weisen eine schlechtere Leistung auf, als wenn sie nicht vom Cache verarbeitet würden. In einigen Fällen können Workloads mit hohen Überschreib- und Auslagerungsraten auch die garantierte Schreiblebensdauer des Laufwerks überschreiten.
- Erwägen Sie das Hinzufügen zusätzlicher Endpunkte oder Knoten zum Zwischenspeichern einzelner Workloads, die sich gut für das Zwischenspeichern eignen.
- Verwenden Sie unterschiedliche Endpunkte für zwischenspeicherbare und nicht zwischenspeicherbare Workloads. Diese Trennung stellt sicher, dass Caching-Mechanismen angemessen angewendet werden und die nicht zwischenspeicherbare Datenverarbeitung nicht beeinträchtigen.
- Bewerten Sie eine potenziell zwischenspeicherbare Arbeitslast, indem Sie sie an den cachefähigen Endpunkt weiterleiten. Überwachen und überprüfen Sie die Cache-Trefferquote, um die Eignung der Arbeitslast für das Caching zu bestimmen. Diese Bewertung hilft bei der Optimierung der Leistung und stellt eine effiziente Nutzung der Cache-Ressourcen sicher.
- "Prüfung von Audit-Protokollen"um zu bestimmen, ob eine vorhandene Arbeitslast ein guter Kandidat für das Caching wäre. Bestimmen Sie für einen bestimmten Zeitraum, welcher Prozentsatz der GETs für eindeutige Objekte erfolgt. Um für das Caching geeignet zu sein, sollte dieser Wert unter 50 % liegen.

Beispiele für Workloads, die sich gut für das Caching eignen könnten

- Datenseen
- Hochleistungsrechnen (HPC)
- KI/ML-Schulung
- Content-Distribution-Netzwerke (CDN)
- Medien-Asset-Management
- Videoproduktion

- Es können mehrere Objektversionen zwischengespeichert werden.
- Bereichslesevorgänge werden unterstützt.

Beispiele für Workloads, die sich nicht gut für das Caching eignen

- Stoffpool
- Backup-Anwendungen
- Speicher-Tiering

Wenn für vom Cache bereitzustellende Inhalte eine Verschlüsselung im Ruhezustand erforderlich ist, "Knoten- oder Laufwerkverschlüsselung aktivieren" auf dem Cache-Knoten.

Arten von Objekten und Anfragen, die nicht zwischengespeichert werden

- Der `response-content-encoding` Abfrageparameter
- Der `partNumber` Abfrageparameter
- Bedingte Header
  - `If-Match`
  - `If-Modified-Since`
  - `If-None-Match`
  - `If-Unmodified-Since`
- Anfragen, die im Ruhezustand mit einem der folgenden Elemente verschlüsselt wurden:
  - SSE (serverseitige Verschlüsselung mit von StorageGRID verwalteten Schlüsseln)
  - SSE-C (serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln)
  - Verschlüsselung gespeicherter Objekte

Alle nicht zwischengespeicherten Anfragen werden an einen Upstream-LDR weitergeleitet, als wäre der Cache nicht aktiviert.

Verwandte Informationen

- "Fehlerbehebung beim Load Balancer-Caching"
- Weitere Informationen zum Load Balancer-Caching erhalten Sie beim technischen Support.

Überlegungen zum Port

Der Port für einen Load Balancer-Endpunkt ist für den ersten erstellten Endpunkt standardmäßig auf 10433 gesetzt. Sie können jedoch einen beliebigen nicht verwendeten externen Port zwischen 1 und 65535 angeben. Wenn Sie Port 80 oder 443 verwenden, verwendet der Endpunkt nur den Load Balancer-Dienst auf Gateway-Nodes. Diese Ports sind für Admin-Nodes reserviert. Wenn Sie denselben Port für mehr als einen Endpunkt verwenden, müssen Sie für jeden Endpunkt einen anderen Bindungsmodus angeben.

Von anderen Grid-Diensten verwendete Ports sind nicht zulässig. Sehen "Interne StorageGRID-Ports" .

Überlegungen zum Netzwerkprotokoll

In den meisten Fällen sollte für die Verbindungen zwischen Client-Anwendungen und StorageGRID die TLS-Verschlüsselung (Transport Layer Security) verwendet werden. Eine Verbindung mit StorageGRID ohne TLS-Verschlüsselung wird unterstützt, aber nicht empfohlen, insbesondere in Produktionsumgebungen. Wenn Sie das Netzwerkprotokoll für den StorageGRID Load Balancer-Endpunkt auswählen, sollten Sie **HTTPS** auswählen.

Überlegungen für Load Balancer-Endpunktzertifikate

Wenn Sie **HTTPS** als Netzwerkprotokoll für den Load Balancer-Endpunkt auswählen, müssen Sie ein Sicherheitszertifikat angeben. Beim Erstellen des Load Balancer-Endpunkts können Sie eine der folgenden drei Optionen verwenden:

- **Laden Sie ein signiertes Zertifikat hoch (empfohlen)**. Dieses Zertifikat kann entweder von einer öffentlich vertrauenswürdigen oder einer privaten Zertifizierungsstelle (CA) signiert werden. Die Verwendung eines öffentlich vertrauenswürdigen CA-Serverzertifikats zum Sichern der Verbindung ist die beste Methode. Im Gegensatz zu generierten Zertifikaten können von einer CA signierte Zertifikate unterbrechungsfrei gedreht werden, was dazu beitragen kann, Ablaufprobleme zu vermeiden.

  Sie müssen die folgenden Dateien abrufen, bevor Sie den Load Balancer-Endpunkt erstellen:

  - Die Zertifikatdatei des benutzerdefinierten Servers.
  - Die Datei mit dem privaten Schlüssel des benutzerdefinierten Serverzertifikats.
  - Optional ein CA-Bündel der Zertifikate jeder zwischengeschalteten Zertifizierungsstelle.
- **Generieren Sie ein selbst signiertes Zertifikat**.
- **Verwenden Sie das globale StorageGRID S3-Zertifikat**. Sie müssen eine benutzerdefinierte Version dieses Zertifikats hochladen oder generieren, bevor Sie es für den Load Balancer-Endpunkt auswählen können. Siehe "Konfigurieren Sie S3-API-Zertifikate".

Welche Werte brauche ich?

Zum Erstellen des Zertifikats müssen Sie alle Domänennamen und IP-Adressen kennen, die S3-Client-Anwendungen für den Zugriff auf den Endpunkt verwenden.

Der Eintrag **Subject DN** (Distinguished Name) für das Zertifikat muss den vollständig qualifizierten Domänennamen enthalten, den die Client-Anwendung für StorageGRID verwendet. Beispiel:

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

Bei Bedarf kann das Zertifikat Platzhalter verwenden, um die vollständig qualifizierten Domänennamen aller Admin-Nodes und Gateway-Nodes darzustellen, auf denen der Load Balancer-Dienst ausgeführt wird. Zum Beispiel `*.storagegrid.example.com` verwendet den Platzhalter * für `adm1.storagegrid.example.com` und `gn1.storagegrid.example.com`.

Wenn Sie virtuelle Anfragen im Hosted-Stil von S3 verwenden möchten, muss das Zertifikat für jeden konfigurierten Eintrag einen Eintrag **alternativer Name** enthalten"Der Domänenname des S3-Endpunkts", einschließlich aller Platzhalternamen. Beispiel:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

Wenn Sie Platzhalter für Domänennamen verwenden, lesen Sie die "Härtungsrichtlinien für Serverzertifikate".

Außerdem müssen Sie für jeden Namen im Sicherheitszertifikat einen DNS-Eintrag definieren.

Wie verwalte ich auslaufende Zertifikate?

Wenn das Zertifikat, mit dem die Verbindung zwischen der S3-Anwendung und StorageGRID gesichert wird, abläuft, kann die Applikation möglicherweise vorübergehend den Zugriff auf StorageGRID verlieren.

Befolgen Sie die folgenden Best Practices, um Probleme mit dem Ablauf von Zertifikaten zu vermeiden:

- Überwachen Sie sorgfältig alle Warnungen, die darauf hinweisen, dass sich das Ablaufdatum des Zertifikats nähert, wie z. B. das * Ablaufdatum des Endpunktzertifikats des Load Balancer* und **Ablauf des globalen Serverzertifikats für S3 API**-Warnungen.
- Halten Sie die Versionen des Zertifikats für die StorageGRID- und S3-Anwendung immer synchron. Wenn Sie das für einen Load Balancer-Endpunkt verwendete Zertifikat ersetzen oder erneuern, müssen Sie das von der S3-Anwendung verwendete entsprechende Zertifikat ersetzen oder erneuern.
- Ein öffentlich signiertes CA-Zertifikat verwenden. Wenn Sie ein von einer Zertifizierungsstelle signiertes Zertifikat verwenden, können Sie bald abgelaufene Zertifikate unterbrechungsfrei ersetzen.
- Wenn Sie ein selbstsigniertes StorageGRID-Zertifikat generiert haben und dieses Zertifikat kurz vor dem Ablauf steht, müssen Sie das Zertifikat sowohl in StorageGRID als auch in der S3-Anwendung manuell ersetzen, bevor das vorhandene Zertifikat abläuft.

Überlegungen zum Bindungsmodus

Im Bindungsmodus können Sie festlegen, welche IP-Adressen für den Zugriff auf einen Load Balancer-Endpunkt verwendet werden können. Wenn ein Endpunkt einen Bindungsmodus verwendet, können Clientanwendungen nur auf den Endpunkt zugreifen, wenn sie eine zulässige IP-Adresse oder den entsprechenden vollständig qualifizierten Domänennamen (FQDN) verwenden. Client-Anwendungen, die eine andere IP-Adresse oder FQDN verwenden, können nicht auf den Endpunkt zugreifen.

Sie können einen der folgenden Bindungsmodi festlegen:

- **Global** (Standard): Client-Anwendungen können über die IP-Adresse eines beliebigen Gateway-Knotens oder Admin-Knotens, die virtuelle IP-Adresse (VIP) einer HA-Gruppe in einem beliebigen Netzwerk oder einen entsprechenden FQDN auf den Endpunkt zugreifen. Verwenden Sie diese Einstellung, es sei denn, Sie müssen den Zugriff auf einen Endpunkt einschränken.
- **Virtuelle IPs von HA-Gruppen**. Client-Anwendungen müssen eine virtuelle IP-Adresse (oder einen entsprechenden FQDN) einer HA-Gruppe verwenden.
- **Knotenschnittstellen**. Clients müssen die IP-Adressen (oder entsprechende FQDNs) der ausgewählten Knotenschnittstellen verwenden.
- **Knotentyp**. Basierend auf dem von Ihnen ausgewählten Knotentyp müssen Clients entweder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Admin-Knotens oder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Gateway-Knotens verwenden.

Überlegungen für den Mandantenzugriff

Der Mandantenzugriff ist eine optionale Sicherheitsfunktion, mit der Sie steuern können, welche StorageGRID-Mandantenkonten einen Load-Balancer-Endpunkt für den Zugriff auf ihre Buckets verwenden können. Sie können allen Mandanten den Zugriff auf einen Endpunkt erlauben (Standard), oder Sie können eine Liste der zulässigen oder blockierten Mandanten für jeden Endpunkt festlegen.

Sie können diese Funktion nutzen, um eine bessere Sicherheitsisolierung zwischen Mandanten und ihren Endpunkten zu ermöglichen. Mit dieser Funktion können Sie beispielsweise sicherstellen, dass die streng geheimen oder streng klassifizierten Materialien eines Mandanten für andere Mieter nicht zugänglich sind.

> Für die Zugriffssteuerung wird der Mandant aus den Zugriffsschlüsseln ermittelt, die in der Client-Anfrage verwendet werden. Wenn im Rahmen der Anfrage keine Zugriffsschlüssel angegeben werden (z. B. mit anonymem Zugriff), wird der Bucket-Eigentümer zur Ermittlung des Mandanten verwendet.

Beispiel für Mandantenzugriff

Um zu verstehen, wie diese Sicherheitsfunktion funktioniert, betrachten Sie das folgende Beispiel:

1. Sie haben zwei Lastausgleichsendpunkte wie folgt erstellt:
   - **Öffentlicher** Endpunkt: Nutzt Port 10443 und erlaubt den Zugriff auf alle Mandanten.
   - **Top secret** Endpunkt: Verwendet Port 10444 und erlaubt nur den Zugriff auf den **Top secret** Mieter. Alle anderen Mandanten werden für den Zugriff auf diesen Endpunkt gesperrt.
2. Der `top-secret.pdf` befindet sich in einem Eimer im Besitz des **Top Secret** Mieters.

Um auf den zuzugreifen `top-secret.pdf`, kann ein Benutzer im **Top Secret**-Mieter eine GET-Anfrage an ausstellen `https://w.x.y.z:10444/top-secret.pdf`. Da dieser Mandant den Endpunkt 10444 verwenden darf, kann der Benutzer auf das Objekt zugreifen. Wenn ein Benutzer eines anderen Mandanten jedoch dieselbe Anforderung an dieselbe URL ausgibt, erhält er eine Meldung über „Zugriff verweigert“. Der Zugriff wird verweigert, selbst wenn die Anmeldeinformationen und die Signatur gültig sind.

CPU-Verfügbarkeit

Der Load Balancer-Service auf jedem Admin-Node und Gateway-Node wird unabhängig ausgeführt, wenn der S3-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, die S3-Clients bei der Verbindung zum StorageGRID Load Balancer auf Gateway- und Admin-Nodes verwenden können. Sie können Endpunkte auch für den Zugriff auf Grid Manager, Tenant Manager oder beide verwenden.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Root-Zugriffsberechtigung".
- Sie haben die überprüft"Überlegungen zum Lastausgleich".
- Wenn Sie zuvor einen Port, den Sie für den Load Balancer-Endpunkt verwenden möchten, neu zugeordnet haben, haben Sie "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 Load Balancer-Endpunkt von verwendet wird"S3 Mandanten für S3 Select", darf er die IP-Adressen oder FQDNs von Bare-Metal-Knoten nicht verwenden. Für die für S3 Select verwendeten Load Balancer-Endpunkte sind nur Service-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 Domänennamen und IP-Adressen, die S3-Clients für den Zugriff auf den Endpunkt verwenden. Sie müssen auch das Thema (Distinguished Name) kennen.
  - Wenn Sie das StorageGRID S3-API-Zertifikat verwenden möchten (das auch für direkte Verbindungen zu Storage-Nodes verwendet werden kann), haben Sie das Standardzertifikat bereits durch ein benutzerdefiniertes Zertifikat ersetzt, das von einer externen Zertifizierungsstelle signiert wurde. Siehe "Konfigurieren Sie S3-API-Zertifikate".

Erstellen Sie einen Endpunkt für den Load Balancer

Jeder S3-Client-Load-Balancer-Endpunkt gibt einen Port, einen Clienttyp (S3) und ein Netzwerkprotokoll (HTTP oder HTTPS) an. Die Endpunkte des Lastenausgleichsmoduls der Verwaltungsschnittstelle geben einen Port, einen Schnittstellentyp und ein nicht vertrauenswürdiges Clientnetzwerk an.

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerk** > **Load Balancer-Endpunkte**.
2. Um einen Endpunkt für einen S3-Client zu erstellen, wählen Sie die Registerkarte **S3-Client**.
3. Um einen Endpunkt für den Zugriff auf Grid Manager, Tenant Manager oder beides zu erstellen, wählen Sie die Registerkarte **Verwaltungsschnittstelle** aus.
4. Wählen Sie **Erstellen**.

Geben Sie Details zu Endpunkten ein

Schritte

1. Wählen Sie die entsprechenden Anweisungen aus, um Details für den Typ des Endpunkts einzugeben,

den Sie erstellen möchten.

S3-Client

Feld	Beschreibung
Name	Ein beschreibbarer Name für den Endpunkt, der in der Tabelle auf der Seite Load Balancer Endpunkte angezeigt wird.
Port	Der StorageGRID-Port, den Sie für den Lastausgleich verwenden möchten. Dieses Feld ist für den ersten erstellten Endpunkt standardmäßig auf 10433 eingestellt. Sie können jedoch jeden nicht verwendeten externen Port zwischen 1 und 65535 eingeben. Wenn Sie **80** oder **8443** eingeben, wird der Endpunkt nur auf Gateway Nodes konfiguriert, es sei denn, Sie haben Port 8443 freigegeben. Anschließend können Sie Port 8443 als S3-Endpunkt verwenden, und der Port wird sowohl auf dem Gateway als auch auf den Admin-Nodes konfiguriert.
Client-Typ	Muss **S3** sein.
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.
Caching aktivieren	Aktivieren oder Deaktivieren"Caching auf den Gateway-Knoten" für diesen Load Balancer-Endpunkt. Wenn Probleme mit dem Caching auftreten, lesen Sie"Fehlerbehebung beim Load Balancer-Caching" .

Managementoberfläche

Feld	Beschreibung
Name	Ein beschreibbarer Name für den Endpunkt, der in der Tabelle auf der Seite Load Balancer Endpunkte angezeigt wird.

Feld	Beschreibung
Port	Der StorageGRID-Port, über den Sie auf den Grid-Manager, den Mandantenmanager oder beide zugreifen möchten. • Grid Manager: **8443** • Mieter-Manager: **9443** • Grid Manager und Tenant Manager: **443** **Hinweis**: Sie können diese voreingestellten Ports oder andere verfügbare Ports verwenden.
Schnittstellentyp	Aktivieren Sie das Optionsfeld für die StorageGRID-Schnittstelle, auf die Sie über diesen Endpunkt zugreifen möchten.
Nicht Vertrauenswürdiges Client-Netzwerk	Wählen Sie **Ja**, wenn dieser Endpunkt für nicht vertrauenswürdige Client-Netzwerke zugänglich sein soll. Andernfalls wählen Sie **Nein**. Wenn Sie **Yes** auswählen, ist der Port auf allen nicht vertrauenswürdigen Client-Netzwerken geöffnet. **Hinweis**: Sie können einen Port nur so konfigurieren, dass er für nicht vertrauenswürdige Client-Netzwerke geöffnet oder geschlossen wird, wenn Sie den Load Balancer-Endpunkt erstellen.

1. Wählen Sie **Weiter**.

Wählen Sie einen Bindungsmodus aus

Schritte

1. Wählen Sie einen Bindungsmodus für den Endpunkt aus, um den Zugriff auf den Endpunkt über eine beliebige IP-Adresse oder über spezifische IP-Adressen und Netzwerkschnittstellen zu steuern.

   Einige Bindungsmodi stehen entweder für Client-Endpunkte oder für Managementschnittstellen zur Verfügung. Hier sind alle Modi für beide Endpunkttypen aufgeführt.

Modus	Beschreibung
Global (Standard für Client-Endpunkte)	Clients können über die IP-Adresse eines beliebigen Gateway-Node oder Admin-Node, die virtuelle IP-Adresse (VIP) einer beliebigen HA-Gruppe in einem beliebigen Netzwerk oder einen entsprechenden FQDN auf den Endpunkt zugreifen. Verwenden Sie die Einstellung **Global**, es sei denn, Sie müssen den Zugriff auf diesen Endpunkt einschränken.

Modus	Beschreibung
Virtuelle IPs von HA-Gruppen	Clients müssen eine virtuelle IP-Adresse (oder einen entsprechenden FQDN) einer HA-Gruppe verwenden, um auf diesen Endpunkt zuzugreifen. Endpunkte mit diesem Bindungsmodus können alle dieselbe Portnummer verwenden, solange sich die für die Endpunkte ausgewählten HA-Gruppen nicht überlappen.
Node-Schnittstellen	Clients müssen die IP-Adressen (oder entsprechende FQDNs) der ausgewählten Knotenschnittstellen verwenden, um auf diesen Endpunkt zuzugreifen.
Node-Typ (nur Client-Endpunkte)	Basierend auf dem von Ihnen ausgewählten Knotentyp müssen Clients entweder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Admin-Knotens oder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Gateway-Knotens verwenden, um auf diesen Endpunkt zuzugreifen.
Alle Admin-Nodes (Standard für Endpunkte der Managementoberfläche)	Clients müssen die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Admin-Knotens verwenden, um auf diesen Endpunkt zuzugreifen.

Wenn mehr als ein Endpunkt denselben Port verwendet, verwendet StorageGRID diese Prioritätsreihenfolge, um zu entscheiden, welcher Endpunkt verwendet werden soll: **Virtuelle IPs von HA-Gruppen** > **Knotenschnittstellen** > **Knotentyp** > **global**.

Wenn Sie Endpunkte der Managementoberfläche erstellen, sind nur Admin-Nodes zulässig.

2. Wenn Sie **virtuelle IPs von HA-Gruppen** ausgewählt haben, wählen Sie eine oder mehrere HA-Gruppen aus.

   Wenn Sie Endpunkte für die Managementoberfläche erstellen, wählen Sie VIPs aus, die nur Admin-Nodes zugeordnet sind.

3. 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.
4. Wenn Sie **Node type** ausgewählt haben, wählen Sie entweder Admin-Nodes aus, die sowohl den primären Admin-Node als auch alle nicht-primären Admin-Nodes enthalten, oder Gateway-Nodes.

Kontrolle des Mandantenzugriffs

Ein Endpunkt der Managementoberfläche kann den Mandantenzugriff nur steuern, wenn der Endpunkt über den verfügtSchnittstellentyp des Tenant Manager.

Schritte

1. Wählen Sie für den Schritt **Tenant Access** eine der folgenden Optionen aus:

Feld	Beschreibung
Alle Mandanten zulassen (Standard)	Alle Mandantenkonten können diesen Endpunkt verwenden, um auf ihre Buckets zuzugreifen. Sie müssen diese Option auswählen, wenn Sie noch keine Mandantenkonten erstellt haben. Nachdem Sie Mandantenkonten hinzugefügt haben, können Sie den Load Balancer-Endpunkt bearbeiten, um bestimmte Konten zuzulassen oder zu blockieren.
Ausgewählte Mandanten zulassen	Nur die ausgewählten Mandantenkonten können diesen Endpunkt für den Zugriff auf ihre Buckets verwenden.
Ausgewählte Mandanten blockieren	Die ausgewählten Mandantenkonten können diesen Endpunkt nicht für den Zugriff auf ihre Buckets verwenden. Dieser Endpunkt kann von allen anderen Mandanten verwendet werden.

2. Wenn Sie einen **HTTP**-Endpunkt erstellen, müssen Sie kein Zertifikat anhängen. Wählen Sie **Erstellen**, um den neuen Load Balancer-Endpunkt hinzuzufügen. Dann gehen Sie zu Nachdem Sie fertig sind. Andernfalls wählen Sie **Weiter**, um das Zertifikat anzuhängen.

Zertifikat anhängen

Schritte

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-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.
   - **StorageGRID S3 Zertifikat** verwenden. Wählen Sie diese Option aus, wenn Sie das globale S3-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 Standard-S3-API-Zertifikat durch ein benutzerdefiniertes Zertifikat ersetzt haben, das von einer externen Zertifizierungsstelle signiert wurde. Siehe "Konfigurieren Sie S3-API-Zertifikate".

   - **Management Interface Zertifikat** verwenden. Wählen Sie diese Option aus, wenn Sie das Zertifikat für die globale Verwaltungsschnittstelle verwenden möchten, das auch für direkte Verbindungen zu Admin-Knoten verwendet werden kann.
2. Wenn Sie das StorageGRID S3-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 Schlüsseldatei (`.key`).

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

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

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

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

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

  Beispiel: `storagegrid_certificate.pem`

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

d. Wählen Sie **Erstellen**. + der Endpunkt des Load Balancer wird erstellt. Das benutzerdefinierte Zertifikat wird für alle nachfolgenden neuen Verbindungen zwischen S3-Clients oder der Managementoberfläche und dem Endpunkt verwendet.

Zertifikat wird generiert

a. Wählen Sie **Zertifikat erstellen**.

b. Geben Sie die Zertifikatsinformationen an:

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

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

c. Wählen Sie **Erzeugen**.

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

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

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

   Beispiel: `storagegrid_certificate.pem`

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

e. Wählen Sie **Erstellen**.

   Der Endpunkt des Load Balancer wird erstellt. Das benutzerdefinierte Zertifikat wird für alle nachfolgenden neuen Verbindungen zwischen S3-Clients oder der Managementoberfläche und diesem Endpunkt verwendet.

Nachdem Sie fertig sind

Schritte

1. Wenn Sie einen DNS verwenden, stellen Sie sicher, dass der DNS einen Datensatz enthält, mit dem der vollständig qualifizierte StorageGRID-Domänenname (FQDN) jeder IP-Adresse zugeordnet wird, die Clients zum Verbindungsaufbau verwenden.

   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 Clients mithilfe der IP-Adresse eines Gateway-Node oder Admin-Node eine Verbindung zum StorageGRID Load Balancer-Service her.

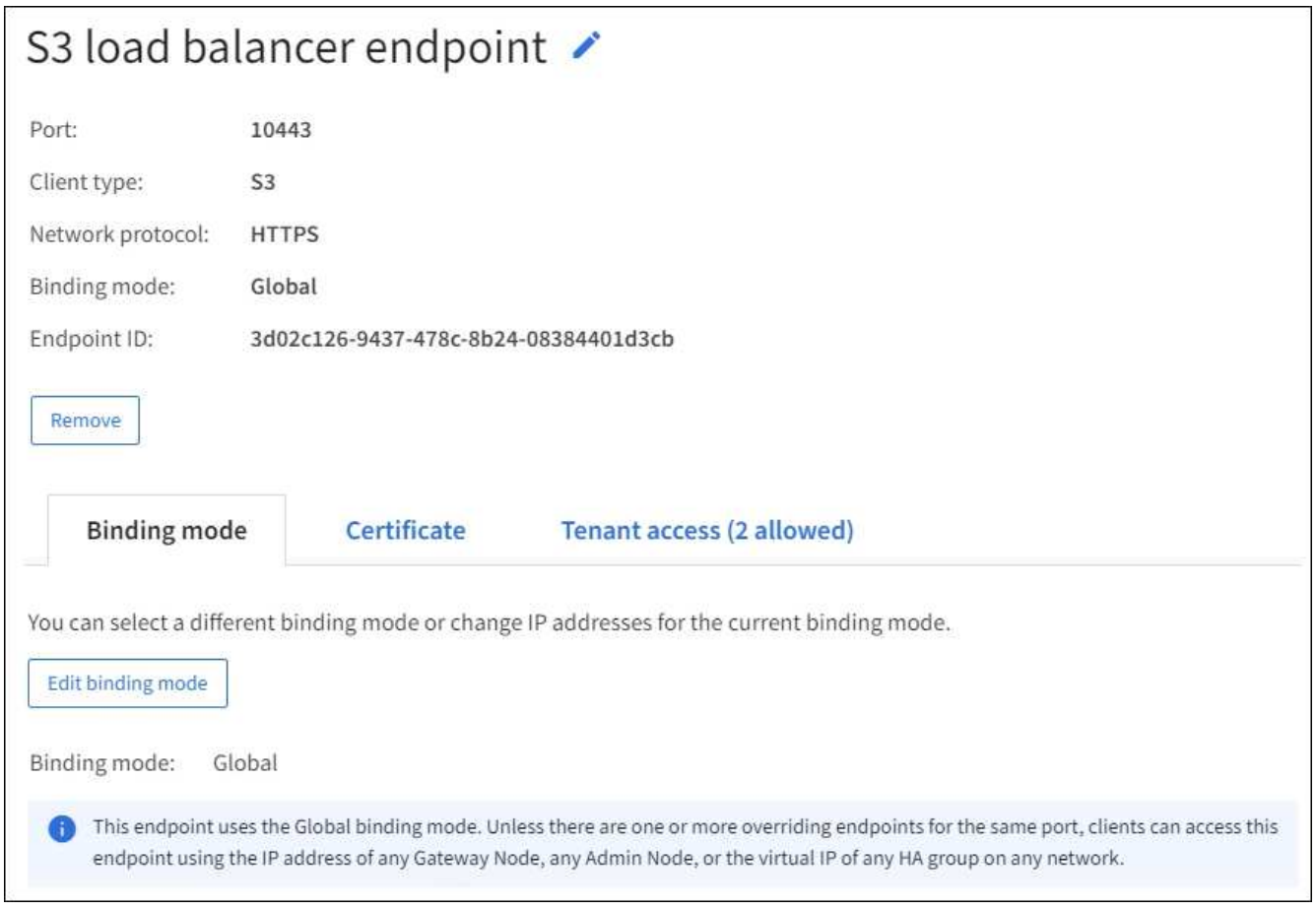
  Außerdem müssen Sie sicherstellen, dass der DNS-Datensatz alle erforderlichen Endpunkt-Domain-Namen referenziert, einschließlich Platzhalternamen.

2. Bereitstellen der für die Verbindung mit dem Endpunkt erforderlichen Informationen für S3-Clients:
   - 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 bestimmte Einstellungen für einen Endpunkt ändern.

- Um grundlegende Informationen für alle Lastausgleichsendpunkte anzuzeigen, lesen Sie die Tabellen auf der Seite Lastausgleichsendpunkte.
- Um alle Details zu einem bestimmten Endpunkt einschließlich Zertifikatmetadaten anzuzeigen, wählen Sie in der Tabelle den Namen des Endpunkts aus. Die angezeigten Informationen variieren je nach Endpunkttyp und Konfiguration.



- Um einen Endpunkt zu bearbeiten, verwenden Sie das Menü **actions** auf der Seite Load Balancer Endpoints.

> Wenn Sie den Zugriff auf Grid Manager während der Bearbeitung des Ports eines Endpunkts der Managementoberfläche verlieren, aktualisieren Sie die URL und den Port, um den Zugriff wiederherzustellen.

> 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 Symbol Bearbeiten . c. Geben Sie den neuen Namen ein. d. Wählen Sie **Speichern**.
Endpunkt-Port bearbeiten	a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie **actions** > **Edit Endpoint Port** c. Geben Sie eine gültige Portnummer ein. d. Wählen Sie **Speichern**.	*N/a*
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**.

Aufgabe	Menü „Aktionen“	Detailseite
Endpunktzertifikat bearbeiten	a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie **Aktionen** > **Endpunktzertifikat bearbeiten** aus. c. Laden Sie nach Bedarf ein neues benutzerdefiniertes Zertifikat hoch oder generieren Sie es oder beginnen Sie mit der Verwendung des globalen S3-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 nach Bedarf ein neues benutzerdefiniertes Zertifikat hoch oder generieren Sie es oder beginnen Sie mit der Verwendung des globalen S3-Zertifikats. e. Wählen Sie **Änderungen speichern**.
Bearbeiten Sie den Mandantenzugriff	a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie **actions** > **Edit Tenant Access**. c. Wählen Sie eine andere Zugriffsoption aus, wählen Sie Mandanten aus der Liste aus oder entfernen Sie sie aus oder führen Sie beides aus. d. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Endpunktnamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte **Tenant Access**. c. Wählen Sie **Mandantenzugriff bearbeiten**. d. Wählen Sie eine andere Zugriffsoption aus, wählen Sie Mandanten aus der Liste aus oder entfernen Sie sie aus oder führen Sie beides aus. 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 alle betroffenen S3-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.

> Wenn Sie den Zugriff auf Grid Manager verlieren, während Sie einen Endpunkt der Managementoberfläche entfernen, aktualisieren Sie die URL.

- So entfernen Sie einen oder mehrere Endpunkte:
  a. Aktivieren Sie auf der Seite Load Balancer das Kontrollkästchen für jeden Endpunkt, den Sie entfernen möchten.
  b. Wählen Sie **Aktionen** > **Entfernen**.
  c. Wählen Sie **OK**.
- So entfernen Sie einen Endpunkt auf der Detailseite:

a. Wählen Sie auf der Seite Load Balancer den Endpunktnamen aus.

b. Wählen Sie auf der Detailseite * Entfernen.

c. Wählen Sie **OK**.

Konfigurieren Sie die Domänennamen des S3-Endpunkts

Um Anforderungen im virtuellen Hosted-Stil von S3 zu unterstützen, müssen Sie die Liste der S3-Endpunkt-Domänennamen, mit denen S3-Clients eine Verbindung herstellen, mit dem Grid Manager konfigurieren.

Die Verwendung einer IP-Adresse für einen Domänennamen des Endpunkts wird nicht unterstützt. Zukünftige Versionen verhindern diese Konfiguration.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben "Bestimmte Zugriffsberechtigungen".
- Sie haben bestätigt, dass ein Grid-Upgrade nicht ausgeführt wird.

Nehmen Sie keine Änderungen an der Domänennamenkonfiguration vor, wenn ein Grid-Upgrade durchgeführt 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 der "Zertifikat, das der Client für HTTPS-Verbindungen zu StorageGRID verwendet"für alle vom Client benötigten Domänennamen signiert ist.

  Wenn der Endpunkt beispielsweise lautet `s3.company.com`, müssen Sie sicherstellen, dass das für HTTPS-Verbindungen verwendete Zertifikat den Endpunkt und den Platzhalter Subject Alternative Name (SAN) des Endpunkts umfasst `s3.company.com`: `*.s3.company.com`.

- Konfigurieren Sie den vom Client verwendeten DNS-Server. Fügen Sie DNS-Datensätze für die IP-Adressen ein, die Clients zum Verbindungsaufbau verwenden, und stellen Sie sicher, dass die Datensätze auf alle erforderlichen S3-Endpunkt-Domänennamen verweisen, einschließlich aller 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 er unterschiedliche S3-Endpunkt-Domänennamen erkennt.

- Clients, die sich mit einem Load-Balancer-Endpunkt oder direkt mit einem Storage-Node verbinden, können das globale S3-API-Zertifikat so anpassen, dass alle erforderlichen S3-Endpunkt-Domänennamen berücksichtigt werden.

> Wenn Sie keine S3-Endpunkt-Domänennamen hinzufügen und die Liste leer ist, wird die Unterstützung für Anforderungen im virtuellen Hosted-Stil von S3 deaktiviert.

Fügen Sie einen S3-Endpunkt-Domänennamen hinzu

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerk** > **S3-Endpunktdomänennamen**.
2. Geben Sie den Domainnamen in das Feld **Domain Name 1** ein. Wählen Sie **Add another Domain Name**, um weitere Domainnamen hinzuzufügen.
3. Wählen Sie **Speichern**.
4. Stellen Sie sicher, dass die von Clients verwendeten Serverzertifikate mit den erforderlichen S3-Endpunkt-Domänennamen übereinstimmen.
   - Wenn Clients eine Verbindung zu einem Load Balancer-Endpunkt herstellen, der ein eigenes Zertifikat verwendet, "Aktualisieren Sie das dem Endpunkt zugeordnete Zertifikat".
   - Wenn Clients eine Verbindung zu einem Load Balancer-Endpunkt herstellen, der das globale S3-API-Zertifikat oder direkt zu Storage Nodes verwendet, "Aktualisieren Sie das globale S3-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`, wird der DNS-Server auf den richtigen Endpunkt aufgelöst und das Zertifikat authentifiziert den Endpunkt wie erwartet.

Benennen Sie einen S3-Endpunkt-Domänennamen um

Wenn Sie einen Namen ändern, der von S3-Anwendungen verwendet wird, schlagen Anforderungen im virtuellen Hosted-Stil fehl.

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerk** > **S3-Endpunktdomänennamen**.
2. Wählen Sie das Feld für den Domänennamen aus, das Sie bearbeiten möchten, und nehmen Sie die erforderlichen Änderungen vor.
3. Wählen Sie **Speichern**.
4. Wählen Sie **Ja**, um Ihre Änderung zu bestätigen.

Löschen Sie einen S3-Endpunkt-Domänennamen

Wenn Sie einen Namen entfernen, der von S3-Anwendungen verwendet wird, schlagen Anforderungen im virtuellen Hosted-Stil fehl.

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerk** > **S3-Endpunktdomänennamen**.

2. Wählen Sie das Löschsymbol ✕ neben dem Domänennamen aus.
3. Wählen Sie **Ja**, um den Löschvorgang zu bestätigen.

Verwandte Informationen

- "S3-REST-API VERWENDEN"
- "Zeigen Sie IP-Adressen an"
- "Konfigurieren Sie Hochverfügbarkeitsgruppen"

Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen

Zum Speichern oder Abrufen von Objekten stellen S3-Clientanwendungen eine Verbindung zum Load Balancer-Dienst her, der auf allen Admin-Knoten und Gateway-Knoten enthalten ist, oder zum Local Distribution Router (LDR)-Dienst, der auf allen Storage-Nodes enthalten ist.

Client-Applikationen können mithilfe der IP-Adresse eines Grid-Node und der Portnummer des Service auf diesem Node eine Verbindung zu StorageGRID herstellen. Optional können Sie Gruppen für Hochverfügbarkeit (High Availability, HA) von Load-Balancing-Nodes erstellen, um hochverfügbare Verbindungen bereitzustellen, die virtuelle IP-Adressen (VIP) verwenden. Wenn Sie eine Verbindung zu StorageGRID über einen vollständig qualifizierten Domänennamen (FQDN) anstelle einer IP- oder VIP-Adresse herstellen möchten, können Sie DNS-Einträge konfigurieren.

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. Wenn Sie bereits Load Balancer-Endpunkte und HA-Gruppen (Hochverfügbarkeitsgruppen) erstellt haben, finden Sie unter Wo finden Sie IP-Adressendiese Werte im Grid Manager.

Wo eine Verbindung hergestellt wird	Dienst, mit dem der Client verbunden ist	IP-Adresse	Port
HA-Gruppe	Lastausgleich	Virtuelle IP-Adresse einer HA-Gruppe	Port, der dem Endpunkt des Lastausgleichs zugewiesen ist
Admin-Node	Lastausgleich	IP-Adresse des Admin-Knotens	Port, der dem Endpunkt des Lastausgleichs zugewiesen ist
Gateway-Node	Lastausgleich	IP-Adresse des Gateway-Node	Port, der dem Endpunkt des Lastausgleichs zugewiesen ist
Storage-Node	LDR	IP-Adresse des Speicherknoten	S3-Standard-Ports: • HTTPS: 18082 • HTTP: 18084

Beispiel-URLs

Um eine Client-Applikation mit dem Endpunkt Load Balancer einer HA-Gruppe von Gateway Nodes zu verbinden, verwenden Sie eine wie unten gezeigt strukturierte URL:

`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 des Endpunkts des Load Balancer 10443 lautet, könnte eine Applikation die folgende URL verwenden, um eine Verbindung zum StorageGRID herzustellen:

`https://192.0.2.5:10443`

Wo finden Sie IP-Adressen

1. Melden Sie sich mit einem beim Grid-Manager an"Unterstützter Webbrowser".
2. So suchen Sie die IP-Adresse eines Grid-Knotens:
   a. Wählen Sie **Knoten** aus.
   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**.
   b. Notieren Sie sich die Portnummer für den zu verwendenden Endpunkt.

      > Wenn die Portnummer 80 oder 443 ist, wird der Endpunkt nur auf Gateway-Nodes konfiguriert, da diese Ports auf Admin-Nodes reserviert sind. Alle anderen Ports werden sowohl an Gateway-Knoten als auch an Admin-Nodes konfiguriert.

   c. Wählen Sie den Namen des Endpunkts aus der Tabelle aus.

d. Bestätigen Sie, dass der **Client-Typ** (S3) mit der Client-Anwendung übereinstimmt, die den Endpunkt verwendet.

Netzwerke und Verbindungen verwalten

Netzwerkeinstellungen konfigurieren

Sie können verschiedene Netzwerkeinstellungen vom Grid Manager konfigurieren, um den Betrieb Ihres StorageGRID Systems zu optimieren.

Konfigurieren Sie die VLAN-Schnittstellen

"Erstellung von Virtual LAN-Schnittstellen (VLAN"Isolieren und partitionieren Sie den Datenverkehr für Sicherheit, Flexibilität und Performance. Jede VLAN-Schnittstelle ist einer oder mehreren übergeordneten Schnittstellen auf Admin-Nodes und Gateway-Nodes zugeordnet. Die VLAN-Schnittstellen können in HA-Gruppen und in Load Balancer Endpunkten eingesetzt werden, um den Client- oder Admin-Datenverkehr nach Applikation oder Mandanten zu trennen.

Richtlinien für die Verkehrsklassifizierung

Sie können "Richtlinien zur Verkehrsklassifizierung"verschiedene Arten von Netzwerkverkehr identifizieren und verarbeiten, einschließlich des Datenverkehrs in Bezug auf bestimmte Buckets, Mandanten, Client-Subnetze oder Load-Balancer-Endpunkte. Diese Richtlinien unterstützen die Begrenzung und das Monitoring des Datenverkehrs.

Richtlinien für StorageGRID-Netzwerke

Mit dem Grid Manager können Sie StorageGRID-Netzwerke und -Verbindungen konfigurieren und verwalten.

Informationen zum Verbinden von S3-Clients finden Sie unter"S3-Client-Verbindungen konfigurieren".

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-Client-Anwendungen 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-Knoten benötigt für jedes Netzwerk, dem er zugewiesen ist, eine dedizierte Netzwerkschnittstelle, eine IP-Adresse, eine Subnetzmaske und ein Gateway.
- Ein Grid-Knoten 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. Sie können beispielsweise eine Trunk-Schnittstelle zu einem Administrator- oder Gateway-Knoten hinzufügen, "VLAN-Schnittstellen"um den Datenverkehr verschiedener Anwendungen oder Mandanten zu trennen. Sie können auch eine Zugriffsschnittstelle hinzufügen, die in einem verwendet "Hochverfügbarkeitsgruppe (High Availability Group, HA-Gruppe"werden soll.

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"
  - **Linux (vor der Installation des Knotens)**:"Erstellen von Node-Konfigurationsdateien"
  - **Linux (nach der Installation des Knotens)**:"Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Knoten"

> „Linux“ bezieht sich auf eine RHEL-, Ubuntu- oder Debian-Bereitstellung. Eine Liste der unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool (IMT)" .

Zeigen Sie IP-Adressen an

Sie können die IP-Adresse für jeden Grid-Node im StorageGRID System anzeigen. Sie können sich dann mithilfe dieser IP-Adresse am Grid Node an der Befehlszeile anmelden und verschiedene Wartungsverfahren durchführen.

Bevor Sie beginnen

Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".

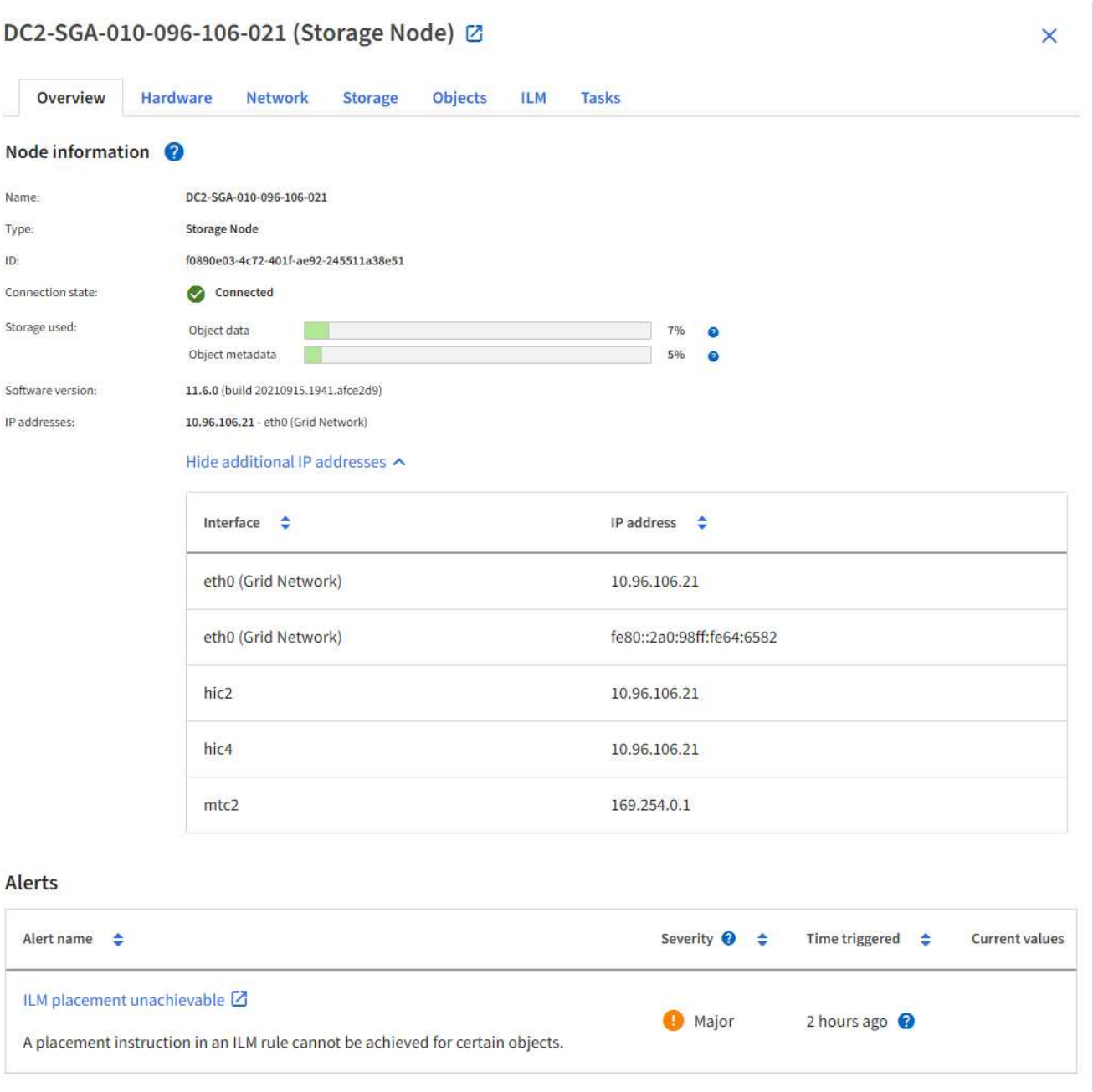
Über diese Aufgabe

Informationen zum Ändern von IP-Adressen finden Sie unter "Konfigurieren Sie IP-Adressen".

Schritte

1. Wählen Sie **Knoten** > ***Rasterknoten*** > **Übersicht**.
2. Wählen Sie **Mehr anzeigen** rechts neben dem Titel der IP-Adressen.

   Die IP-Adressen für diesen Grid-Node werden in einer Tabelle aufgeführt.



Konfigurieren Sie die VLAN-Schnittstellen

Erstellen Sie virtuelle LAN-Schnittstellen (VLAN) auf Admin-Knoten und Gateway-Knoten und verwenden Sie sie in HA-Gruppen und Load Balancer-Endpunkten, um den Datenverkehr aus Sicherheits-, Flexibilitäts- und Leistungsgründen zu isolieren und zu partitionieren. Die ausgewählten Knoten in der HA-Gruppe können die VLAN-Schnittstellen verwenden, um bis zu 10 virtuelle IP-Adressen gemeinsam zu nutzen, sodass beim Ausfall eines Knotens ein anderer Knoten den Datenverkehr zu und von den virtuellen IP-Adressen übernimmt.

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. Beispielsweise können Sie 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 den S3-Client-Datenverkehr verwendet wird, wählen Sie Schnittstellen 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"
  - **Linux (vor der Installation des Knotens)**:"Erstellen von Node-Konfigurationsdateien"
  - **Linux (nach der Installation des Knotens)**:"Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Knoten"

> „Linux“ bezieht sich auf eine RHEL-, Ubuntu- oder Debian-Bereitstellung. Eine Liste der unterstützten Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool (IMT)" .

Erstellen einer VLAN-Schnittstelle

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem 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

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerk** > **VLAN-Schnittstellen**.
2. Wählen Sie **Erstellen**.

Geben Sie Details zu den VLAN-Schnittstellen ein

Schritte

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. Zwei VLAN-Schnittstellen mit derselben ID können jedoch nicht dieselbe Schnittstelle auf einem Node gemeinsam nutzen. Wenn Sie eine ID angeben, die bereits verwendet wurde, wird eine Meldung angezeigt.

2. Geben Sie optional eine kurze Beschreibung für die VLAN-Schnittstelle ein.
3. Wählen Sie **Weiter**.

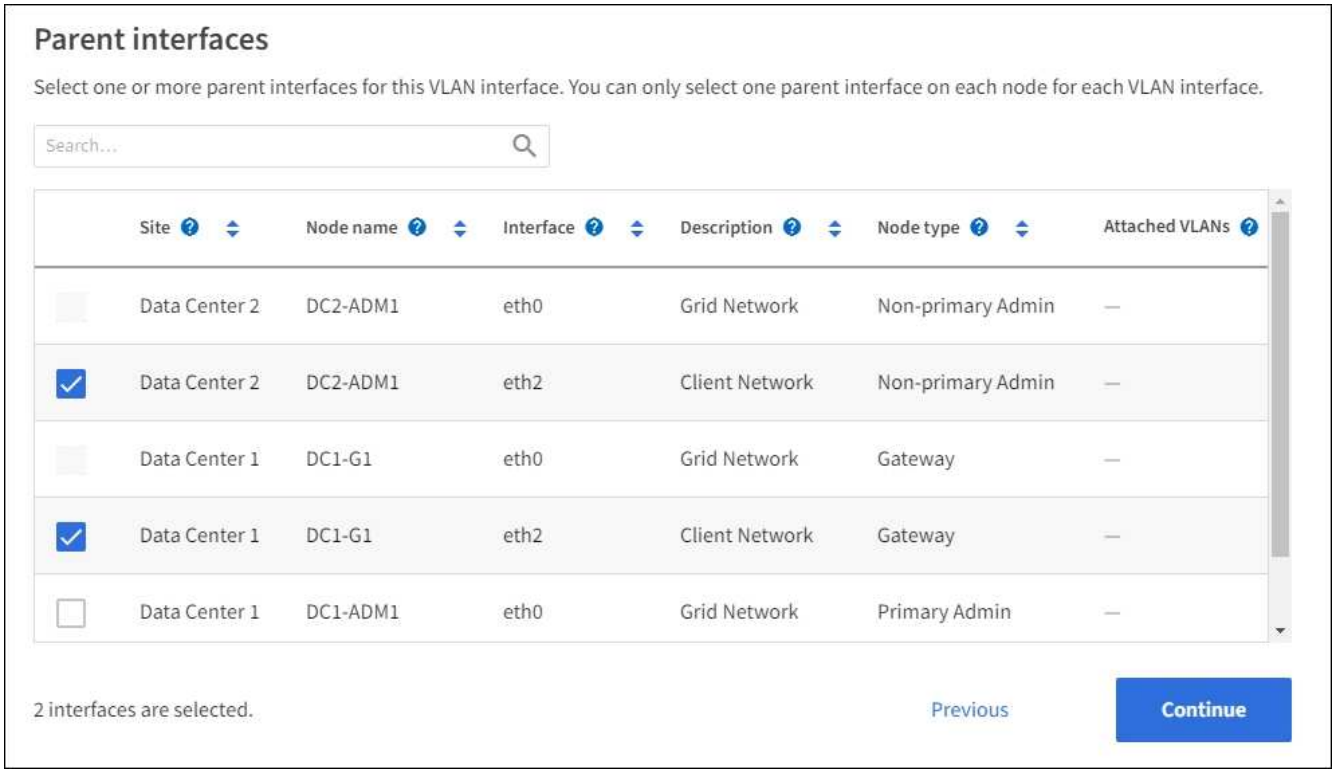
Wählen Sie übergeordnete Schnittstellen

In der Tabelle sind die verfügbaren Schnittstellen für alle Admin-Nodes und Gateway-Nodes an jedem Standort im Raster aufgeführt. Schnittstellen des Admin-Netzwerks (eth1) können nicht als übergeordnete Schnittstellen verwendet werden und werden nicht angezeigt.

Schritte

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

Schritte

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 möchten, 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 und in der Tabelle **Netzwerkschnittstellen** für den Knoten aufgeführt wird (**Knoten** > ***übergeordneter Schnittstellenknoten*** > **Netzwerk**).

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.

  Angenommen, VLAN 200 ist an den übergeordneten Schnittstellen auf den Knoten A und B angeschlossen. Wenn eine HA-Gruppe die VLAN-200-Schnittstelle für Knoten A und die eth2-Schnittstelle für Knoten B verwendet, können Sie die nicht verwendete übergeordnete Schnittstelle für Knoten B entfernen, aber Sie können die verwendete übergeordnete Schnittstelle für Knoten 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 oder deaktivieren 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.

Aktivieren Sie StorageGRID CORS für eine Verwaltungsschnittstelle

Als Grid-Administrator können Sie Cross-Origin Resource Sharing (CORS) für Management-API-Anfragen an StorageGRID aktivieren, wenn Sie möchten, dass Daten in StorageGRID über Management-APIs einer anderen Domäne zugänglich sind.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Der"Root-Zugriffsberechtigung" bietet Zugriff auf alle CORS-Konfigurationsanforderungen.

Über diese Aufgabe

CORS ist ein Sicherheitsmechanismus, der es Client-Webanwendungen in einer Domäne ermöglicht, auf Ressourcen in einer anderen Domäne zuzugreifen. Angenommen, Sie möchten ein Überwachungs-Dashboard für StorageGRID in der Domäne erstellen `http://www.example.com` . Durch die Aktivierung von CORS in StorageGRID für `http://www.example.com` und "Grid Manager", die StorageGRID Domäne antwortet auf Grid Management API-Anfragen von `http://www.example.com` .

Management-API (mgmt-api)-Anfragen mit `application/json` oder `multipart/formdata` Anfragen für `Content-Type` werden für CORS unterstützt.

Schritte

1. Gehen Sie im Grid Manager zu **KONFIGURATION** > **Netzwerk** > **CORS-Einstellungen der**

Verwaltungsschnittstelle.

2. Wählen Sie **Grid Manager**, **Tenant Manager** oder beide Optionen.
   - **Grid Manager**: Aktiviert CORS für domänenübergreifende Grid Management-API-Anfragen.
   - **Tenant Manager**: Aktiviert CORS für domänenübergreifende Tenant Management-API-Anfragen.
3. Geben Sie die URL für die andere Domäne in das Feld **Domänen** ein.

   Wählen Sie **Weitere Domäne hinzufügen**, wenn Sie CORS in StorageGRID für mehr als eine Domäne aktivieren möchten.

4. Wählen Sie **Speichern**.

Verwandte Informationen

"Konfigurieren Sie StorageGRID CORS für Buckets und Objekte"

Verwalten von Richtlinien zur Verkehrsklassifizierung

Was sind Richtlinien zur Verkehrsklassifizierung?

Mithilfe von Richtlinien zur Datenverkehrsklassifizierung können Sie verschiedene Arten von Netzwerkverkehr identifizieren und überwachen. Diese Richtlinien unterstützen Sie bei der Verkehrsbeschränkung und -Überwachung und verbessern so Ihre Quality-of-Service-Angebote.

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
- Subnetz
- Mandant
- 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 einer Richtlinie die folgenden Begrenzungstypen hinzufügen:

- Aggregatbandbreite
- Bandbreite pro Anforderung
- Gleichzeitige Anfragen

- Anforderungsrate

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. Die von der Anforderung verbrauchte Bandbreite wird nicht mit anderen weniger spezifischen übereinstimmenden Richtlinien verglichen, die Richtlinien zur Gesamtbandbreite enthalten. 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.

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	Maximal zulässige Leistung	Kosten
Gold	1 PB Speicherplatz zulässig	ILM-Regel für 3 Kopien	25 .000 Anforderungen/Sek. 5 GB/s (40 Gbit/s) Bandbreite	Kosten pro Monat
Silber	250 TB Speicher erlaubt	ILM-Regel für 2 Kopien	10 .000 Anforderungen/Sek. 1.25 GB/s (10 Gbit/s) Bandbreite	Kosten pro Monat
Bronze	100 TB Speicher erlaubt	ILM-Regel für 2 Kopien	5 .000 Anforderungen/Sek. 1 GB/s (8 Gbit/s) Bandbreite	Kosten pro Monat

Richtlinien für die Verkehrsklassifizierung erstellen

Sie können Richtlinien zur Verkehrsklassifizierung erstellen, wenn Sie den Netzwerk-Traffic nach Bucket, Bucket-Regex, CIDR, Load-Balancer-Endpunkt oder Mandant überwachen und optional begrenzen möchten. Optional können Sie Obergrenzen für eine Richtlinie basierend auf der Bandbreite, der Anzahl gleichzeitiger Anfragen oder der Anfragerate festlegen.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem 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**.
2. Wählen Sie **Erstellen**.
3. Geben Sie einen Namen und eine Beschreibung (optional) für die Richtlinie ein und wählen Sie **Weiter**.

   Beschreiben Sie beispielsweise, auf welche Weise diese Richtlinie zur Klassifizierung von Verkehrsdaten zutrifft und welche Begrenzung sie hat.

4. Wählen Sie **Regel hinzufügen** und geben Sie die folgenden Details an, um eine oder mehrere übereinstimmende Regeln für die Richtlinie zu erstellen. Jede Richtlinie, die Sie erstellen, sollte mindestens eine übereinstimmende Regel haben. Wählen Sie **Weiter**.

Feld	Beschreibung
Typ	Wählen Sie die Verkehrstypen aus, für die die entsprechende Regel gilt. Traffic-Typen sind Bucket, Bucket-Regex, CIDR, Load Balancer-Endpunkt und Mandant.

Feld	Beschreibung
Match-Wert	Geben Sie den Wert ein, der dem ausgewählten Typ entspricht. • Bucket: Geben Sie einen oder mehrere Bucket-Namen ein. • Bucket-regex: Geben Sie einen oder mehrere reguläre Ausdrücke ein, die für einen Satz von Bucket-Namen verwendet werden. Der reguläre Ausdruck ist nicht verankert. Verwenden Sie den Anker ^, um am Anfang des Bucket-Namens zu übereinstimmen, und verwenden Sie den Anker €, um am Ende des Namens zu übereinstimmen. Die Übereinstimmung mit regulären Ausdrücken unterstützt eine Teilmenge der PCRE-Syntax (Perl Compatible Regular Expression). • CIDR: Geben Sie ein oder mehrere IPv4-Subnetze in CIDR-Notation ein, die mit dem gewünschten Subnetz übereinstimmen. • Load-Balancer-Endpunkt: Wählen Sie einen Endpunktnamen aus. Dies sind die Lastausgleichsendpunkte, die Sie auf der definiert "Konfigurieren von Load Balancer-Endpunkten"haben. • Tenant: Tenant Matching verwendet die Zugriffsschlüssel-ID. Wenn die Anforderung keine Zugriffsschlüssel-ID enthält (z. B. anonymer Zugriff), wird die Eigentümerschaft des abgerufenen Buckets verwendet, um den Mandanten zu bestimmen.
Umgekehrtes Match	Wenn Sie den gesamten Netzwerkverkehr *except* mit dem gerade definierten Typ und Match-Wert abstimmen möchten, aktivieren Sie das Kontrollkästchen **inverse Übereinstimmung**. Andernfalls lassen Sie das Kontrollkästchen deaktiviert. Wenn Sie beispielsweise möchten, dass diese Richtlinie auf alle Endpunkte mit Ausnahme eines Lastausgleichs angewendet wird, geben Sie den auszuschließenden Lastausgleichsendpunkt an, und wählen Sie **inverse Übereinstimmung** 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.

5. Wählen Sie optional **Limit hinzufügen** und wählen Sie die folgenden Details aus, um eine oder mehrere Grenzwerte hinzuzufügen, um den Netzwerkverkehr zu steuern, der von einer Regel abgeglichen wird.

> StorageGRID sammelt Kennzahlen, auch wenn Sie keine Limits hinzufügen, sodass Sie Verkehrstrends besser verstehen können.

Feld	Beschreibung
Typ	Die Art der Begrenzung, die auf den Netzwerkverkehr angewendet werden soll, der der Regel entspricht. Beispielsweise können Sie die Bandbreite oder die Anforderungsrate begrenzen. **Hinweis**: Sie können Richtlinien erstellen, um die Gesamtbandbreite zu begrenzen oder die Bandbreite pro Anfrage zu begrenzen. StorageGRID kann jedoch nicht beide Bandbreitenarten gleichzeitig einschränken. Wenn die aggregierte Bandbreite verwendet wird, ist die Bandbreite pro Anforderung nicht verfügbar. Umgekehrt ist die aggregierte Bandbreite nicht verfügbar, wenn die Bandbreite pro Anforderung verwendet wird. 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 die „besten“ Matches für Bandbreitenlimits in der folgenden Reihenfolge: • Exakte IP-Adresse (/32-Maske) • Exakter Bucket-Name • Eimer-Regex • Mandant • Endpunkt • Nicht exakte CIDR-Übereinstimmungen (nicht /32) • Umgekehrte Übereinstimmungen
Gilt für	Gibt an, ob diese Begrenzung auf Client-Leseanforderungen (GET oder HEAD) oder Schreibanforderungen (PUT, POST oder DELETE) zutrifft.
Wert	Der Wert, auf den der Netzwerkverkehr begrenzt wird, abhängig von der ausgewählten Einheit. Geben Sie beispielsweise 10 ein, und wählen Sie MiB/s aus, um zu verhindern, dass der Netzwerkverkehr, der dieser Regel entspricht, 10 MiB/s überschreitet **Hinweis**: Je nach Einstellung der Einheiten sind die verfügbaren Einheiten entweder binär (z. B. gib) oder dezimal (z. B. GB). Um die Einstellung Einheiten zu ändern, wählen Sie oben rechts im Grid-Manager das Dropdown-Menü Benutzer aus, und wählen Sie dann **Benutzereinstellungen** aus.
Einheit	Die Einheit, die den eingegebenen Wert beschreibt.

Wenn Sie beispielsweise ein Bandbreitenlimit von 4 GB/s für eine SLA-Stufe erstellen möchten, erstellen Sie zwei aggregierte Bandbreitenlimits: GET/HEAD mit 4 GB/s und PUT/POST/DELETE mit 4 GB/s.

6. Wählen Sie **Weiter**.

7. Lesen und prüfen Sie die Richtlinie zur Verkehrsklassifizierung. Verwenden Sie die Schaltfläche * Zurück*, um zurückzugehen und Änderungen vorzunehmen. Wenn Sie mit der Richtlinie zufrieden sind, wählen Sie **Speichern und fortfahren**.

   S3-Client-Traffic wird nun gemäß der Traffic-Klassifizierungsrichtlinie behandelt.

Nachdem Sie fertig sind

"Zeigen Sie Metriken zum Netzwerkverkehr an" Um zu überprüfen, ob die Richtlinien die von Ihnen erwarteten Verkehrsgrenzwerte durchsetzen.

Richtlinie zur Verkehrsklassifizierung bearbeiten

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.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Root-Zugriffsberechtigung".

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerk** > **Verkehrsklassifizierung**.

   Die Seite für die Verkehrsklassifizierungsrichtlinien wird angezeigt, und die vorhandenen Richtlinien werden in einer Tabelle aufgeführt.

2. Bearbeiten Sie die Richtlinie über das Menü Aktionen oder die Detailseite. Siehe "Erstellen von Richtlinien zur Verkehrsklassifizierung" für das, was Sie teilnehmen.

   Menü „Aktionen“

   a. Aktivieren Sie das Kontrollkästchen für die Richtlinie.

   b. Wählen Sie **Actions** > **Edit**.

   Detailseite

   a. Wählen Sie den Richtliniennamen aus.

   b. Klicken Sie neben dem Richtliniennamen auf die Schaltfläche **Bearbeiten**.

3. Bearbeiten Sie für den Schritt Richtliniennamen eingeben optional den Richtliniennamen oder die Beschreibung, und wählen Sie **Weiter** aus.
4. Fügen Sie für den Schritt übereinstimmende Regeln hinzufügen optional eine Regel hinzu oder bearbeiten Sie die Werte **Typ** und **Match** der bestehenden Regel und wählen Sie **Weiter**.
5. Für den Schritt Grenzen festlegen können Sie optional ein Limit hinzufügen, bearbeiten oder löschen und dann **Weiter** auswählen.
6. Überprüfen Sie die aktualisierte Richtlinie, und wählen Sie **Speichern und fortfahren**.

   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

Sie können eine Verkehrsklassifizierungsrichtlinie löschen, wenn Sie sie nicht mehr benötigen. Achten Sie darauf, die richtige Richtlinie zu löschen, da eine Richtlinie beim Löschen nicht abgerufen werden kann.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Root-Zugriffsberechtigung".

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerk** > **Verkehrsklassifizierung**.

   Die Seite für die Verkehrsklassifizierungsrichtlinien wird mit den vorhandenen Richtlinien in einer Tabelle angezeigt.

2. Löschen Sie die Richtlinie über das Menü Aktionen oder die Detailseite.

   Menü „Aktionen“

   a. Aktivieren Sie das Kontrollkästchen für die Richtlinie.

   b. Wählen Sie **Aktionen** > **Entfernen**.

   Seite mit den Details der Richtlinie

   a. Wählen Sie den Richtliniennamen aus.

   b. Klicken Sie neben dem Richtliniennamen auf die Schaltfläche **Entfernen**.

3. Wählen Sie **Ja**, 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 anzeigen, die auf der Seite für die Verkehrsklassifizierungsrichtlinien verfügbar sind.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Berechtigung für Root-Zugriff oder Mandantenkonten".

Über diese Aufgabe

Für alle vorhandenen Richtlinien zur Verkehrsklassifizierung können Sie Metriken für den Load Balancer-Dienst anzeigen, um zu ermitteln, ob die Richtlinie den Datenverkehr im Netzwerk erfolgreich einschränkt. Anhand der Daten in den Diagrammen können Sie feststellen, 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 für die Verkehrsklassifizierungsrichtlinien wird angezeigt, und die vorhandenen Richtlinien werden in der Tabelle aufgeführt.

2. Wählen Sie den Richtliniennamen für die Verkehrsklassifizierung aus, für den Sie Metriken anzeigen möchten.
3. Wählen Sie die Registerkarte **Metriken**.

   Die Richtliniendiagramme für die Verkehrsklassifizierung werden angezeigt. Die Diagramme zeigen Metriken nur für den Datenverkehr an, der mit der ausgewählten Richtlinie übereinstimmt.

   Die folgenden Diagramme sind auf der Seite enthalten.

   - Anforderungsrate: Dieses Diagramm zeigt die Bandbreite an, die dieser Richtlinie entspricht, die von allen Load Balancern verarbeitet wird. Die empfangenen Daten umfassen Anforderungskopfzeilen für alle Anfragen und die Körperdatengröße für Antworten mit Körperdaten. „Gesendet“ enthält Antwortkopfzeilen für alle Anfragen und die Größe der Antwortkörperdaten für Anforderungen, die Körperdaten in die Antwort einschließen.

     Wenn die Anforderungen abgeschlossen sind, zeigt dieses Diagramm nur die Bandbreitennutzung an. Bei langsamen oder großen Objektanforderungen kann die tatsächliche unmittelbare Bandbreite von den in diesem Diagramm gemeldeten Werten abweichen.

   - Fehlerreaktionsrate: Dieses Diagramm bietet eine ungefähre Rate, mit der Anfragen, die dieser Richtlinie entsprechen, Fehler (HTTP-Statuscode >= 400) an Clients zurückgeben.
   - Durchschnittliche Anforderungsdauer (kein Fehler): Diese Grafik bietet eine durchschnittliche Dauer erfolgreicher Anfragen, die dieser Richtlinie entsprechen.
   - Verwendung der Richtlinienbandbreite: Dieses Diagramm gibt die Bandbreite an, die dieser Richtlinie entspricht, die von allen Lastverteilern verarbeitet wird. Die empfangenen Daten umfassen Anforderungskopfzeilen für alle Anfragen und die Körperdatengröße für Antworten mit Körperdaten. „Gesendet“ enthält Antwortkopfzeilen für alle Anfragen und die Größe der Antwortkörperdaten für Anforderungen, die Körperdaten in die Antwort einschließen.

4. Positionieren Sie den Cursor über einem Liniendiagramm, um ein Popup-Fenster mit Werten für einen bestimmten Teil des Diagramms anzuzeigen.
5. Wählen Sie **Grafana Dashboard** direkt unter dem Metrics-Titel, um alle Diagramme für eine Richtlinie anzuzeigen. Zusätzlich zu den vier Diagrammen aus der Registerkarte **Metriken** können Sie zwei weitere Diagramme anzeigen:

   - Schreibanforderungsrate nach Objektgröße: Die Rate für PUT/POST/DELETE-Anfragen, die dieser Richtlinie entsprechen. Die Positionierung auf einer einzelnen Zelle zeigt die Raten pro Sekunde an. Die in der Hover-Ansicht angezeigten Raten werden auf Ganzzahlen gekürzt und können 0 melden, wenn im Bucket Anfragen ohne Null angezeigt werden.
   - Leseanforderungsrate nach Objektgröße: Die Rate für GET/HEAD-Anfragen, die dieser Richtlinie entsprechen. Die Positionierung auf einer einzelnen Zelle zeigt die Raten pro Sekunde an. Die in der Hover-Ansicht angezeigten Raten werden auf Ganzzahlen gekürzt und können 0 melden, wenn im Bucket Anfragen ohne Null angezeigt werden.

6. Alternativ können Sie über das Menü **Support** auf die Diagramme zugreifen.
   a. Wählen Sie **Support** > **Tools** > **Metriken**.

b. Wählen Sie im Abschnitt **Grafana** die Option **Richtlinie zur Traffic-Klassifizierung** aus.

c. Wählen Sie die Richtlinie aus dem Menü oben links auf der Seite aus.

d. Positionieren Sie den Cursor über einem Diagramm, um ein Popup-Fenster anzuzeigen, in dem Datum und Uhrzeit der Probe, Objektgrößen, die in der Anzahl zusammengefasst werden, und die Anzahl der Anfragen pro Sekunde in diesem Zeitraum angezeigt werden.

   Richtlinien für die Verkehrsklassifizierung werden anhand ihrer ID identifiziert. Richtlinien-IDs werden auf der Seite für die Verkehrsklassifizierungsrichtlinien aufgeführt.

7. Analysieren Sie die Diagramme, um zu ermitteln, wie oft die Richtlinie den Datenverkehr einschränkt und ob Sie die Richtlinie anpassen müssen.

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 für die Verwendung mit externen Systemen unterstützten TLS-Chiffren wurden ausgewählt, um die Kompatibilität mit einer Reihe externer Systeme sicherzustellen. Die Liste ist größer als die Liste der Chiffren, die für die Verwendung mit S3-Clientanwendungen unterstützt werden. Um Verschlüsselungen zu konfigurieren, gehen Sie zu **Konfiguration** > **Sicherheit** > **Sicherheitseinstellungen** und wählen Sie **TLS- und SSH-Richtlinien**.

> TLS-Konfigurationsoptionen wie Protokollversionen, Chiffren, Schlüsselaustauschalgorithmen und MAC-Algorithmen sind in StorageGRID nicht konfigurierbar. Wenden Sie sich an Ihren NetApp Ansprechpartner, wenn Sie spezifische Anfragen zu diesen Einstellungen haben.

Vorteile von aktiven, inaktiven und gleichzeitigen HTTP-Verbindungen

Die Konfiguration von HTTP-Verbindungen kann sich auf die Performance des StorageGRID-Systems auswirken. Die Konfigurationen unterscheiden sich je nachdem, ob die HTTP-Verbindung aktiv oder inaktiv ist oder Sie mehrere Verbindungen gleichzeitig haben.

Sie können die Performance-Vorteile für die folgenden Arten von HTTP-Verbindungen identifizieren:

- Inaktive HTTP-Verbindungen
- Aktive HTTP-Verbindungen
- Gleichzeitige HTTP-Verbindungen

Vorteile, wenn inaktive HTTP-Verbindungen offen gehalten werden

Halten Sie HTTP-Verbindungen offen, wenn Clientanwendungen inaktiv sind, um spätere Transaktionen zu ermöglichen. Halten Sie eine inaktive HTTP-Verbindung maximal 10 Minuten lang offen. StorageGRID schließt

möglicherweise automatisch eine HTTP-Verbindung, die länger als 10 Minuten geöffnet und inaktiv ist.

Open- und Idle-HTTP-Verbindungen bieten folgende Vorteile:

- Niedrigere Latenz von dem Zeitpunkt, zu dem das StorageGRID System feststellt, dass eine HTTP-Transaktion durchgeführt werden muss, bis zum Zeitpunkt, zu dem das StorageGRID System die Transaktion ausführen kann

  Die geringere Latenz ist der Hauptvorteil, insbesondere aufgrund der für die Einrichtung von TCP/IP- und TLS-Verbindungen benötigten Zeit.

- Erhöhte Datenübertragungsrate durch Priming des TCP/IP Slow-Start-Algorithmus mit zuvor durchgeführten Transfers
- Sofortige Benachrichtigung über mehrere Klassen von Fehlerbedingungen, die die Verbindung zwischen Client-Anwendung und StorageGRID-System unterbrechen

Entscheiden Sie, wie lange eine inaktive Verbindung offen gehalten werden soll, indem Sie die Vorteile eines langsamen Starts und die Ressourcenzuweisung gegeneinander abwägen.

Vorteile von aktiven HTTP-Verbindungen

Bei Verbindungen direkt zu Storage Nodes sollten Sie die Dauer einer aktiven HTTP-Verbindung auf maximal 10 Minuten begrenzen, selbst wenn die HTTP-Verbindung kontinuierlich Transaktionen durchführt.

Die Bestimmung der maximalen Dauer, die eine Verbindung offen halten sollte, ist ein Kompromiss zwischen den Vorteilen der Verbindungspersistenz und der idealen Zuweisung der Verbindung zu internen Systemressourcen.

Bei Client-Verbindungen zu Storage-Nodes bietet die Beschränkung aktiver HTTP-Verbindungen folgende Vorteile:

- Ermöglicht einen optimalen Lastausgleich über das StorageGRID System hinweg.

  Mit der Zeit ist eine HTTP-Verbindung möglicherweise nicht mehr optimal, da sich die Anforderungen an den Lastenausgleich ändern. Das System erzielt die beste Lastverteilung, wenn Clientanwendungen für jede Transaktion eine separate HTTP-Verbindung herstellen. Bei dieser Methode gehen jedoch die wertvollen Vorteile dauerhafter Verbindungen zunichte.

- Ermöglicht Client-Anwendungen, HTTP-Transaktionen an LDR-Dienste mit verfügbarem Speicherplatz zu leiten.
- Ermöglicht das Starten von Wartungsvorgängen.

  Einige Wartungsverfahren beginnen erst, nachdem alle laufenden HTTP-Verbindungen abgeschlossen sind.

Bei Client-Verbindungen zum Load Balancer-Service kann eine Begrenzung der Dauer offener Verbindungen nützlich sein, um einige Wartungsverfahren zeitnah starten zu können. Wenn die Dauer der Clientverbindungen nicht begrenzt ist, kann es mehrere Minuten dauern, bis aktive Verbindungen automatisch beendet werden.

Vorteile gleichzeitiger HTTP-Verbindungen

Sie sollten mehrere TCP/IP-Verbindungen zum StorageGRID-System offen halten, um Parallelität zu ermöglichen, was die Performance steigert. Die optimale Anzahl paralleler Verbindungen hängt von einer

Vielzahl von Faktoren ab.

Gleichzeitige HTTP-Verbindungen bieten die folgenden Vorteile:

- Geringere Latenz

  Transaktionen können sofort gestartet werden, anstatt auf die Durchführung anderer Transaktionen zu warten.

- Erhöhter Durchsatz

  Das StorageGRID System kann parallele Transaktionen durchführen und den aggregierten Transaktionsdurchsatz erhöhen.

Client-Anwendungen sollten mehrere HTTP-Verbindungen einrichten. Wenn eine Client-Anwendung eine Transaktion durchführen muss, kann sie eine vorhandene Verbindung auswählen und sofort verwenden, die derzeit keine Transaktion verarbeitet.

Die Topologie jedes StorageGRID -Systems weist einen anderen Spitzendurchsatz für gleichzeitige Transaktionen und Verbindungen auf. Der Spitzendurchsatz hängt von den Rechen-, Netzwerk- und Speicherressourcen, den WAN-Verbindungen und der Anzahl der Server, Dienste und Anwendungen ab, die das StorageGRID -System unterstützt.

StorageGRID -Systeme unterstützen häufig mehrere Clientanwendungen. Berücksichtigen Sie dies, wenn Sie die maximale Anzahl gleichzeitiger Verbindungen bestimmen. Wenn die Client-Anwendung aus mehreren Software-Entitäten besteht, die jeweils Verbindungen zum StorageGRID -System herstellen, addieren Sie alle Verbindungen zwischen den Entitäten. In den folgenden Situationen müssen Sie möglicherweise die maximale Anzahl gleichzeitiger Verbindungen anpassen:

- Die Topologie des StorageGRID Systems beeinflusst die maximale Anzahl gleichzeitiger Transaktionen und Verbindungen, die das System unterstützen kann.
- Client-Applikationen, die über ein Netzwerk mit begrenzter Bandbreite mit dem StorageGRID-System interagieren, müssen möglicherweise das Maß an Parallelität verringern, um sicherzustellen, dass einzelne Transaktionen in einem angemessenen Zeitraum durchgeführt werden.
- Wenn viele Client-Applikationen das StorageGRID System gemeinsam nutzen, muss möglicherweise der Grad an Parallelität reduziert werden, um das Überschreiten der Systemgrenzen zu vermeiden.

Trennung von HTTP-Verbindungspools für Lese- und Schreibvorgänge

Es können separate Pools von HTTP-Verbindungen für Lese- und Schreibvorgänge genutzt werden, inklusive Kontrolle darüber, wie viele aus einem Pool jeweils verwendet werden. Separate Pools von HTTP-Verbindungen ermöglichen eine bessere Kontrolle von Transaktionen und einen besseren Lastausgleich.

Client-Applikationen können Lasten erzeugen, die sich auf Abruf dominant (Lesen) oder stark speichern (Schreiben). Mit separaten Pools von HTTP-Verbindungen für Lese- und Schreibtransaktionen können Sie den Umfang der einzelnen Pools für Lese- und Schreibtransaktionen anpassen.

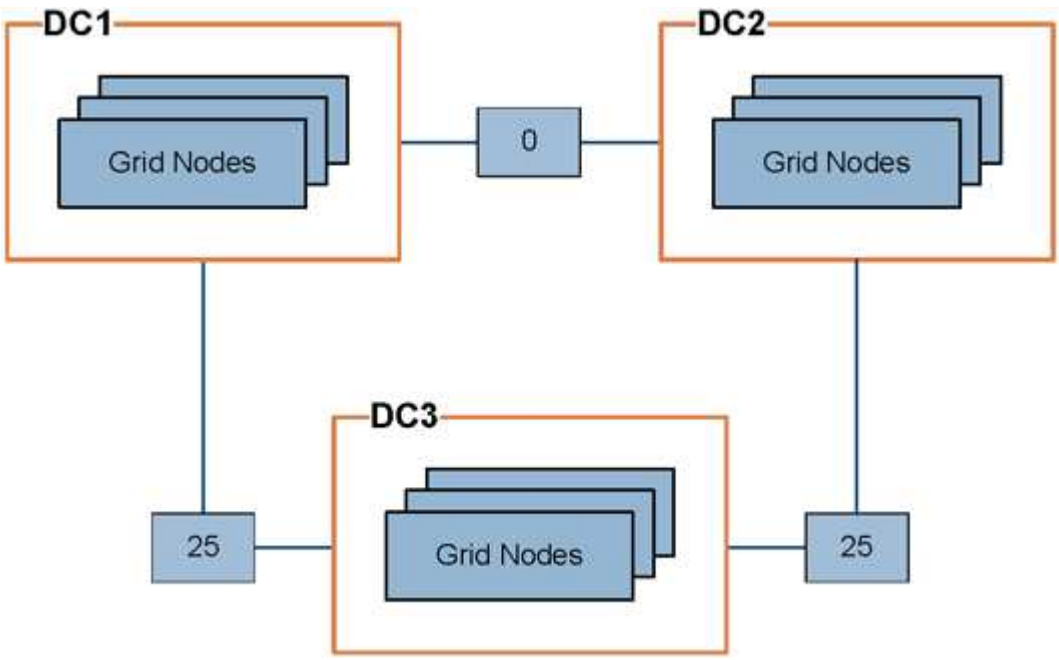
Verwalten Sie Verbindungskosten

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.

Was sind Verbindungskosten?

- 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.
- Verbindungskosten werden vom Load Balancer-Service auf Admin-Nodes und Gateway-Nodes zum direkten Client-Verbindungen verwendet. Siehe "Überlegungen zum Lastausgleich".

Das Diagramm zeigt ein drei Standortraster mit Verbindungskosten, die zwischen Standorten konfiguriert sind:



- Der Load Balancer auf Admin-Nodes und Gateway-Nodes verteilt Client-Verbindungen zu allen Storage-Nodes am selben Datacenter-Standort und zu allen Datacenter-Standorten, für die keine Linkkosten anfallen.

  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 in dem Beispiel eine Client-Anwendung bei DC2 ein Objekt abruft, das sowohl bei DC1 als auch bei DC3 gespeichert ist, wird das Objekt von DC1 abgerufen, da die Verbindungskosten von DC1 zu DC2 0 sind, was niedriger ist als die Verbindungskosten von DC3 zu 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

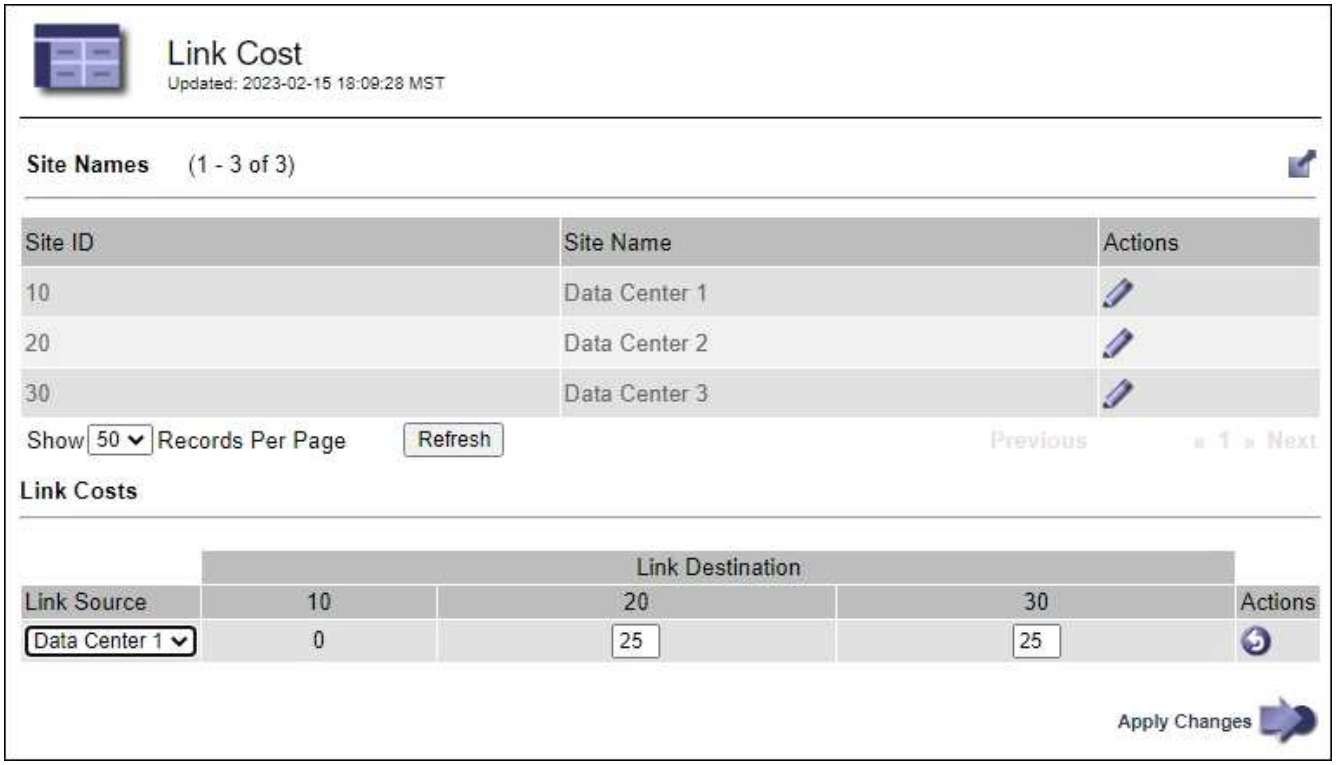
Sie können die Verbindungskosten zwischen Datacenter-Standorten aktualisieren, um die Latenz zwischen Standorten wiederzugeben.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die"Andere Rasterkonfigurationsberechtigung" .

Schritte

1. Wählen Sie **Support** > **Sonstiges** > **Linkkosten**.



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 die Änderungen zu verwerfen, wählen Sie **Rückgängig**.

3. Wählen Sie **Änderungen Anwenden**.

Verwenden Sie AutoSupport

Was ist AutoSupport?

Mit der AutoSupport-Funktion kann StorageGRID Systemzustands- und Statuspakete an den technischen Support von NetApp senden.

Durch die Verwendung von AutoSupport können Probleme schneller gelöst werden. Der technische Support kann den Speicherbedarf Ihres Systems überwachen und Ihnen dabei helfen, festzustellen, ob Sie neue Knoten oder Sites hinzufügen müssen. Optional kann AutoSupport Pakete an ein zusätzliches Ziel senden.

StorageGRID bietet zwei Arten von AutoSupport:

- **StorageGRID AutoSupport** meldet Probleme mit der StorageGRID-Software. Standardmäßig aktiviert, wenn Sie StorageGRID zum ersten Mal installieren. Sie können"Ändern Sie die AutoSupport-Standardkonfiguration", wenn nötig.

> Wenn StorageGRID AutoSupport nicht aktiviert ist, wird eine Meldung auf dem Grid Manager-Dashboard angezeigt. Die Nachricht enthält einen Link zur AutoSupport Konfigurationsseite. Wenn Sie die Nachricht schließen, wird sie erst wieder angezeigt, wenn Ihr Browser-Cache geleert wird, auch wenn AutoSupport deaktiviert bleibt.

- **Appliance Hardware AutoSupport** meldet Probleme mit der StorageGRID Appliance. Sie müssen "Konfigurieren Sie Hardware-AutoSupport auf jeder Appliance".

Was ist Active IQ?

Active IQ ist ein Cloud-basierter digitaler Berater, der prädiktive Analysen und Community-Wissen aus der installierten Basis von NetApp nutzt. 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 Active IQ Dashboards und Funktionen auf der NetApp Support-Website verwenden möchten, müssen Sie AutoSupport aktivieren.

"Active IQ Digital Advisor Dokumentation"

Informationen im AutoSupport-Paket enthalten

Ein AutoSupport-Paket enthält die folgenden Dateien und Details.

Dateiname	Felder	Beschreibung
AUTOSUPPORT-HISTORY.XML	AutoSupport-Sequenznummer + Ziel für diese AutoSupport + Lieferstatus + Zustellversuche + AutoSupport-Betreff + Liefer-URI + letzter Fehler + AutoSupport PUT Dateiname + Erstellungszeit + AutoSupport komprimierter Größe + AutoSupport dekomprimierter Größe + Gesamtaufzeichnungszeit (ms)	AutoSupport-Verlaufsdatei.
AUTOSUPPORT.XML	Knoten + Protokoll für Support-Kontakt + Support-URL für HTTP/HTTPS + Support-Adresse + AutoSupport OnDemand-Status + AutoSupport OnDemand-Server-URL + AutoSupport OnDemand-Abfrageintervall	AutoSupport-Statusdatei. Enthält Details zum verwendeten Protokoll, URL und Adresse des technischen Supports, Abfrageintervall und OnDemand-AutoSupport, falls aktiviert oder deaktiviert.
BUCKETS.XML	Bucket-ID + Konto-ID + Build-Version + Speicherortbeschränkung Konfiguration + Compliance aktiviert + Compliance-Konfiguration + S3-Objektsperre aktiviert + S3-Objektsperrkonfiguration + Consistency Configuration + CORS aktiviert + CORS-Konfiguration + Letzte Zugriffszeit aktiviert + Policy aktiviert + Richtlinienkonfiguration + Benachrichtigungen aktiviert + Benachrichtigungskonfiguration + Cloud Mirror aktiviert + Cloud Mirror-Konfiguration + Suche aktiviert + Suchkonfiguration + Bucket-Tagging aktiviert + Bucket-Tagging-Konfiguration + Versionierungskonfiguration	Bietet Konfigurationsdetails und Statistiken auf Bucket-Ebene. Beispiele für Bucket-Konfigurationen sind Plattformservices, Compliance und Bucket-Konsistenz.

Dateiname	Felder	Beschreibung
GRID-KONFIGURATIONEN.XML	Attribut-ID + Attributname + Wert + Index + Tabellen-ID + Tabellenname	Informationsdatei für die gesamte Konfiguration. Enthält Informationen zu Grid-Zertifikaten, reserviertem Speicherplatz für Metadaten, Grid-weiten Konfigurationseinstellungen (Compliance, S3 Object Lock, Objektkomprimierung, Warnmeldungen, Syslog- und ILM-Konfiguration), Profildetails zur Fehlerkorrektur, DNS-Name und "NMS-Name".
GRID-SPEC.XML	Grid-Spezifikationen, RAW-XML	Wird für die Konfiguration und Bereitstellung von StorageGRID verwendet. Enthält Grid-Spezifikationen, NTP-Server-IP, DNS-Server-IP, Netzwerktopologie und Hardware-Profile der Nodes.
GRID-TASKS.XML	Knoten + Servicepfad + Attribut-ID + Attributname + Wert + Index + Tabellen-ID + Tabellenname	Statusdatei für Grid Tasks (Maintenance Procedures). Enthält Details zu den aktiven, beendeten, abgeschlossenen, fehlgeschlagenen und ausstehenden Aufgaben des Rasters.
GRID.JSON	Grid + Revision + Softwareversion + Beschreibung + Lizenz + Passwörter + DNS + NTP + Sites + Nodes	Grid-Informationen.
ILM-CONFIGURATION.XML	Attribut-ID + Attributname + Wert + Index + Tabellen-ID + Tabellenname	Liste der Attribute für ILM-Konfigurationen
ILM-STATUS.XML	Knoten + Servicepfad + Attribut-ID + Attributname + Wert + Index + Tabellen-ID + Tabellenname	Informationsdatei zu ILM-Kennzahlen Enthält ILM-Auswertungsraten für jeden Node und für das gesamte Grid.
ILM.XML	ILM-RAW XML	Aktive ILM-Richtliniendatei Enthält Details zu aktiven ILM-Richtlinien, z. B. Storage-Pool-ID, Aufnahmeverhalten, Filter, Regeln und Beschreibung
LOG.TGZ	*N/a*	Herunterladbare Protokolldatei. Enthält `bycast-err.log` und `servermanager.log` von jedem Knoten.

Dateiname	Felder	Beschreibung
MANIFEST.XML	Erfassungsreihenfolge + AutoSupport-Inhaltsdateiname für diese Daten + Beschreibung dieses Datenelements + Anzahl der erfassten Bytes + Zeitaufwand für die Erfassung + Status dieses Datenelements + Beschreibung des Fehlers + AutoSupport-Inhaltstyps für diese Daten	Enthält AutoSupport-Metadaten und kurze Beschreibungen aller AutoSupport-Dateien.
NMS-ENTITIES.XML	Attributindex + Entity OID + Node ID + Device Model ID + Device Model Version + Entity Name	Gruppen- und Serviceeinheiten im "NMS-Struktur". Enthält Details zur Grid-Topologie. Der Node kann auf Basis der auf dem Node ausgeführten Services ermittelt werden.
OBJECTS-STATUS.XML	Knoten + Servicepfad + Attribut-ID + Attributname + Wert + Index + Tabellen-ID + Tabellenname	Objektstatus, einschließlich Hintergrundscan-Status, aktiver Transfer, Übertragungsrate, Gesamtübertragungen, Löschrate, beschädigte Fragmente, verlorene Objekte, fehlende Objekte, Reparaturversuch, Scan-Rate, geschätzter Scan-Zeitraum und Reparaturstatus.
SERVER-STATUS.XML	Knoten + Servicepfad + Attribut-ID + Attributname + Wert + Index + Tabellen-ID + Tabellenname	Serverkonfigurationen. Enthält diese Details für jeden Node: Plattformtyp, Betriebssystem, installierter Arbeitsspeicher, verfügbarer Arbeitsspeicher, Storage-Konnektivität, Seriennummer des Storage-Appliance-Chassis, Anzahl der ausgefallenen Storage-Controller, Temperatur des Computing-Controller-Chassis, Compute-Hardware, Seriennummer des Computing-Controllers, Stromversorgung, Laufwerkgröße und Festplattentyp.
SERVICE-STATUS.XML	Knoten + Servicepfad + Attribut-ID + Attributname + Wert + Index + Tabellen-ID + Tabellenname	Informationsdatei für den Service-Node. Enthält Details wie zugewiesenen Tabellenplatz, freien Tabellenplatz, Reaper-Metriken der Datenbank, Dauer der Bausteinreparatur, Dauer des Reparaturauftrags, automatischer Neustart des Jobs und automatische Beendigung des Jobs.

Dateiname	Felder	Beschreibung
STORAGE-GRADE.XML	Storage-Grade-ID + Storage-Grade-Name + Storage-Node-ID + Storage-Node-Pfad	Definitionsdatei für Speichergrade für jeden Speicher-Node.
SUMMARY-ATTRIBUTES.XML	Gruppen-OID + Gruppenpfad + Attribut-ID der Zusammenfassung + Attributname der Zusammenfassung + Wert + Index + Tabellen-ID + Tabellenname	Systemstatusdaten auf hoher Ebene, die Informationen zur StorageGRID-Nutzung zusammenfassen. Liefert Details, wie z. B. Name des Grids, Namen von Standorten, Anzahl der Storage-Nodes pro Grid und pro Standort, Lizenztyp, Lizenzkapazität und -Nutzung, Software-Support-Bedingungen und Details zu S3-Vorgängen.
SYSTEM-ALERTS.XML	Name + Schweregrad + Knotenname + Alarmstatus + Standortname + ausgelöste Zeit für Alarm + aufgelöste Zeit für Alarm + Regel-ID + Knoten-ID + Standort-ID + stummgeschaltet + andere Anmerkungen + andere Beschriftungen	Aktuelle Systemwarnungen, die auf potenzielle Probleme im StorageGRID-System hinweisen
USERAGENTS.XML	Benutzeragent + Anzahl der Tage + gesamte HTTP-Anfragen + insgesamt aufgenommene Bytes + insgesamt abgerufene Bytes + PUT-Anfragen + GET-Anfragen + Anfragen + Anfragen + Anfragen + Anfragen NACH Anfragen + OPTIONEN Anfragen + Durchschnittliche Anfragezeit (ms) + Durchschnittliche PUT-Anfragezeit (ms) + Durchschnittliche Anfragezeit (ms) + Durchschnittliche LÖSCHZEIT (ms) + Durchschnittliche Anfragezeit (ms) + Durchschnittliche Anfragezeit für Anfragen NACH Anfragen (ms) + Durchschnittliche OPTIONEN (ms)	Statistiken basierend auf den Agenten des Anwendungsbenutzers. Beispielsweise die Anzahl der PUT/GET/DELETE/HEAD-Vorgänge pro Benutzeragent und die Gesamtbyte-Größe jedes Vorgangs.

Dateiname	Felder	Beschreibung
X-HEADER-DATEN	X-NetApp-asup-generated-on + X-NetApp-asup-hostname + X-NetApp-asup-os-Version + X-NetApp-asup-serial-num + X-NetApp-asup-subject + X-NetApp-asup-System-id + X-NetApp-asup-model-Name	AutoSupport-Header-Daten

Konfigurieren Sie AutoSupport

Standardmäßig ist die StorageGRID AutoSupport-Funktion bei der ersten Installation von StorageGRID aktiviert. Sie müssen jedoch Hardware-AutoSupport auf jeder Appliance konfigurieren. Sie können die AutoSupport-Konfiguration nach Bedarf ändern.

Wenn Sie die Konfiguration von StorageGRID AutoSupport ändern möchten, nehmen Sie die Änderungen nur auf dem primären Administratorknoten vor. Sie müssen Hardware-AutoSupport konfigurieren auf jedem Gerät.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Root-Zugriffsberechtigung".
- Wenn Sie HTTPS zum Senden von AutoSupport-Paketen verwenden, haben Sie den ausgehenden Internetzugang zum primären Admin-Knoten entweder direkt oder (eingehende Verbindungen nicht erforderlich) bereitgestellt"Verwenden eines Proxy-Servers".
- Wenn HTTP auf der Seite StorageGRID AutoSupport ausgewählt ist, müssen Sie "Proxy-Server konfiguriert"AutoSupport-Pakete als HTTPS weiterleiten. Die AutoSupport Server von NetApp lehnen Pakete ab, die über HTTP gesendet werden.
- Wenn Sie SMTP als Protokoll für AutoSupport-Pakete verwenden, haben Sie einen SMTP-Mailserver konfiguriert.

Über diese Aufgabe

Sie können eine beliebige Kombination der folgenden Optionen verwenden, um AutoSupport-Pakete an den technischen Support zu senden:

- **Wöchentlich**: Verschicken Sie AutoSupport-Pakete automatisch einmal pro Woche. Standardeinstellung: Aktiviert.
- **Event-Triggered**: Sendet automatisch AutoSupport-Pakete jede Stunde oder wenn bedeutende Systemereignisse auftreten. Standardeinstellung: Aktiviert.
- **On Demand**: Lassen Sie technischen Support verlangen, dass Ihr StorageGRID-System AutoSupport-Pakete automatisch sendet, was nützlich ist, wenn sie aktiv an einem Problem arbeiten (erfordert HTTPS AutoSupport Übertragungsprotokoll). Standardeinstellung: Deaktiviert.
- **Vom Benutzer ausgelöst**: AutoSupport-Pakete jederzeit manuell senden.
- **Protokollsammlung**:"Sammeln Sie manuell Protokolldateien und Systemdaten und senden Sie ein AutoSupport Paket" .

Geben Sie das Protokoll für AutoSupport-Pakete an

Sie können jedes der folgenden Protokolle zum Senden von AutoSupport-Paketen verwenden:

- **HTTPS**: Dies ist die Standard-Einstellung und wird für Neuinstallationen empfohlen. Dieses Protokoll verwendet Port 443. Wenn Sie möchtenAktivieren Sie die Funktion „AutoSupport On Demand“, müssen Sie HTTPS verwenden.
- **HTTP**: Wenn Sie HTTP auswählen, müssen Sie einen Proxyserver konfigurieren, um AutoSupport-Pakete als HTTPS weiterzuleiten. Die AutoSupport Server von NetApp lehnen Pakete ab, die über HTTP gesendet werden. Dieses Protokoll verwendet Port 80.
- **SMTP**: Verwenden Sie diese Option, wenn Sie möchten, dass AutoSupport-Pakete per E-Mail gesendet werden.

Das von Ihnen festgelegte Protokoll wird zum Senden aller Arten von AutoSupport-Paketen verwendet.

Schritte

1. Wählen Sie **Support** > **Tools** > * AutoSupport* > **Einstellungen**.
2. Wählen Sie das Protokoll aus, das zum Senden von AutoSupport-Paketen verwendet werden soll.
3. Wenn Sie **HTTPS** ausgewählt haben, wählen Sie aus, ob Sie ein NetApp-Support-Zertifikat (TLS-Zertifikat) verwenden möchten, um die Verbindung zum technischen Support-Server zu sichern.
   - **Zertifikat prüfen** (Standard): Stellt sicher, dass die Übertragung von AutoSupport-Paketen 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 vom Ereignis ausgelösten Pakete werden mit dem ausgewählten Protokoll gesendet.

Wöchentliche AutoSupport deaktivieren

Standardmäßig ist das StorageGRID-System so konfiguriert, dass einmal pro Woche ein AutoSupport-Paket an den technischen Support gesendet wird.

Um zu bestimmen, wann das wöchentliche AutoSupport-Paket gesendet wird, gehen Sie auf die Registerkarte **AutoSupport** > **Results**. Im Abschnitt **Weekly AutoSupport** sehen Sie sich den Wert für **Next Scheduled Time** an.

Sie können das automatische Senden von wöchentlichen AutoSupport-Paketen jederzeit deaktivieren.

Schritte

1. Wählen Sie **Support** > **Tools** > * AutoSupport* > **Einstellungen**.
2. Deaktivieren Sie das Kontrollkästchen **Weekly AutoSupport** aktivieren.
3. Wählen Sie **Speichern**.

Deaktivieren Sie ereignisgesteuerte AutoSupport

Standardmäßig ist das StorageGRID System so konfiguriert, dass jede Stunde ein AutoSupport-Paket an den technischen Support gesendet wird.

Sie können ereignisgesteuerte AutoSupport jederzeit deaktivieren.

Schritte

1. Wählen Sie **Support** > **Tools** > * AutoSupport* > **Einstellungen**.
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 verlangen, dass AutoSupport-Pakete automatisch gesendet werden. Der technische Support kann auch das Abfrageintervall für AutoSupport-on-Demand-Abfragen festlegen.

Der technische Support kann AutoSupport On Demand nicht aktivieren oder deaktivieren.

Schritte

1. Wählen Sie **Support** > **Tools** > * AutoSupport* > **Einstellungen**.
2. Wählen Sie **HTTPS** für das Protokoll aus.
3. Aktivieren Sie das Kontrollkästchen **Weekly 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* > **Einstellungen**.
2. Deaktivieren Sie das Kontrollkästchen **nach Softwareupdates suchen**.
3. Wählen Sie **Speichern**.

Fügen Sie ein weiteres AutoSupport Ziel hinzu

Wenn Sie AutoSupport aktivieren, werden Health- und Statuspakete an den technischen Support gesendet. Sie können ein zusätzliches Ziel für alle AutoSupport-Pakete angeben.

Informationen zum Überprüfen oder Ändern des Protokolls zum Senden von AutoSupport-Paketen finden Sie in den Anweisungen an Geben Sie das Protokoll für AutoSupport-Pakete an.

Sie können das SMTP-Protokoll nicht verwenden, um AutoSupport-Pakete an ein zusätzliches Ziel zu senden.

Schritte

1. Wählen Sie **Support** > **Tools** > * AutoSupport* > **Einstellungen**.
2. Wählen Sie **Zusätzliches AutoSupport-Ziel aktivieren**.
3. Geben Sie Folgendes an:

   Hostname

   Der Hostname oder die IP-Adresse des Servers eines zusätzlichen AutoSupport-Zielservers.

   Sie können nur ein weiteres Ziel eingeben.

   Port

   Der Port, über den eine Verbindung zu einem zusätzlichen AutoSupport-Zielserver hergestellt wird. Der Standardwert ist Port 80 für HTTP oder Port 443 für HTTPS.

   Zertifikatvalidierung

   Ob ein TLS-Zertifikat verwendet wird, um die Verbindung zum zusätzlichen Ziel zu sichern.

   - Wählen Sie **Zertifikat überprüfen**, um die Zertifikatvalidierung zu verwenden.
   - Wählen Sie **Zertifikat nicht verifizieren**, um Ihre AutoSupport-Pakete ohne Zertifikatvalidierung zu senden.

     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.

4. Wenn Sie **Zertifikat überprüfen** ausgewählt haben, gehen Sie wie folgt vor:
   a. Navigieren Sie zum Speicherort des Zertifizierungsstellenzertifikats.
   b. Laden Sie die CA-Zertifikatdatei hoch.

   Die Metadaten des CA-Zertifikats werden angezeigt.

5. Wählen Sie **Speichern**.

   Alle zukünftigen wöchentlichen, ereignisgetriggerten und vom Benutzer ausgelösten AutoSupport Pakete werden an das zusätzliche Ziel gesendet.

[[AutoSupport für Appliances]]Konfigurieren von AutoSupport für Appliances

AutoSupport für Appliances meldet StorageGRID Hardwareprobleme und StorageGRID AutoSupport meldet StorageGRID Softwareprobleme. Mit einer Ausnahme meldet StorageGRID AutoSupport sowohl Hardware- als auch Softwareprobleme. Sie müssen AutoSupport auf jeder Appliance konfigurieren, mit Ausnahme der SGF6112, die keine zusätzliche Konfiguration erfordert. AutoSupport wird für Service-Appliances und Storage Appliances anders implementiert.

Sie verwenden SANtricity, um AutoSupport für jede Storage Appliance zu aktivieren. Sie können SANtricity AutoSupport während der ersten Appliance-Einrichtung oder nach der Installation einer Appliance konfigurieren:

- Für SG6000 und SG5700 Appliances, "Konfigurieren Sie AutoSupport in SANtricity System Manager"

AutoSupport Pakete von E-Series Appliances können in StorageGRID AutoSupport enthalten sein, wenn Sie die AutoSupport-Bereitstellung per Proxy in konfigurieren"SANtricity System Manager".

StorageGRID AutoSupport meldet keine Hardwareprobleme, z. B. DIMM- oder HIC-Fehler (Host Interface Card). Einige Komponentenfehler können jedoch auslösen"Warnmeldungen zu Hardware". Bei StorageGRID Appliances mit einem Baseboard Management Controller (BMC) können Sie E-Mail und SNMP Traps konfigurieren, um Hardwarefehler zu melden:

- "E-Mail-Benachrichtigungen für BMC-Warnungen einrichten"
- "Konfigurieren Sie die SNMP-Einstellungen für BMC"

Verwandte Informationen

"NetApp Support"

Starten Sie manuell ein AutoSupport-Paket

Um den technischen Support bei der Fehlerbehebung in Ihrem StorageGRID System zu unterstützen, können Sie manuell ein AutoSupport Paket senden.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie verfügen über Root-Zugriff oder die Berechtigung „Andere Rasterkonfiguration“.

Schritte

1. Wählen Sie **Support** > **Tools** > * AutoSupport*.
2. Wählen Sie auf der Registerkarte **Aktionen vom Benutzer ausgelöste AutoSupport** senden.

   StorageGRID versucht, ein AutoSupport Paket an die NetApp Support-Site zu senden. Wenn der Versuch erfolgreich ist, werden die Werte **Neuestes Ergebnis** und **Letzter erfolgreicher Zeitpunkt** auf der Registerkarte **Ergebnisse** aktualisiert. Wenn ein Problem auftritt, wird der Wert „Neuestes Ergebnis“ auf „Fehlgeschlagen“ aktualisiert und StorageGRID versucht nicht, das AutoSupport Paket erneut zu senden.

3. Aktualisieren Sie nach 1 Minute die AutoSupport -Seite in Ihrem Browser, um auf die aktuellsten Ergebnisse zuzugreifen.

Darüber hinaus können Sie"umfangreichere Logfiles und Systemdaten erfassen" und senden Sie sie an die NetApp Support Site.

Fehlerbehebung bei AutoSupport-Paketen

Wenn der Versuch, ein AutoSupport Paket zu senden, fehlschlägt, ergreift das StorageGRID System je nach Art des AutoSupport Pakets unterschiedliche Maßnahmen. Sie können den Status von AutoSupport -Paketen überprüfen, indem Sie **Support** > **Tools** > * AutoSupport* > **Ergebnisse** auswählen.

Wenn das AutoSupport-Paket nicht gesendet werden kann, erscheint auf der Registerkarte **Ergebnisse** der Seite **AutoSupport** „Fehlgeschlagen“.

Wenn Sie einen Proxyserver konfiguriert haben, um AutoSupport-Pakete an NetApp weiterzuleiten, sollten Sie "Überprüfen Sie, ob die Konfigurationseinstellungen des Proxy-Servers korrekt sind".

Fehler beim wöchentlichen AutoSupport-Paket

Wenn ein wöchentliches AutoSupport-Paket nicht gesendet werden kann, führt das StorageGRID-System die folgenden Aktionen durch:

1. Aktualisiert das Attribut für das aktuellste Ergebnis, um es erneut zu versuchen.
2. Versucht, das AutoSupport-Paket 15 Mal alle vier Minuten für eine Stunde erneut zu senden.
3. Nach einer Stunde des Sendefehlens aktualisiert das Attribut „Aktuelles Ergebnis“ auf „Fehlgeschlagen“.
4. Versucht, ein AutoSupport-Paket zum nächsten geplanten Zeitpunkt erneut zu senden.
5. Behält den regulären AutoSupport-Zeitplan bei, wenn das Paket fehlschlägt, weil der NMS-Dienst nicht verfügbar ist und wenn ein Paket vor sieben Tagen gesendet wird.
6. Wenn der NMS-Service wieder verfügbar ist, sendet ein AutoSupport-Paket sofort, wenn ein Paket nicht für mindestens sieben Tage gesendet wurde.

Fehler beim AutoSupport-Paket, der vom Benutzer ausgelöst wurde oder von einem Ereignis ausgelöst wurde

Wenn ein vom Benutzer oder durch ein Ereignis ausgelöstes AutoSupport-Paket nicht gesendet wird, führt das StorageGRID System die folgenden Aktionen durch:

1. Zeigt eine Fehlermeldung an, wenn der Fehler bekannt ist. Wenn ein Benutzer beispielsweise das SMTP-Protokoll ohne Angabe der korrekten E-Mail-Konfigurationseinstellungen wählt, wird der folgende Fehler angezeigt: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. Versucht nicht, das Paket 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 richtig konfiguriert ist und ob Ihr E-Mail-Server ausgeführt wird (**Support** > **Alarme (Legacy)** > **Legacy-E-Mail-Setup**). Auf der AutoSupport -Seite wird möglicherweise die folgende Fehlermeldung angezeigt: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Erfahren Sie, wie man "Konfigurieren Sie die E-Mail-Servereinstellungen".

Beheben Sie einen Fehler beim AutoSupport-Paket

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 Seite AutoSupport angezeigt werden: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Senden Sie E-Series AutoSupport-Pakete über StorageGRID

Sie können AutoSupport-Pakete für den E-Series SANtricity System Manager über einen StorageGRID-Administratorknoten anstatt über den Management-Port der Storage

Appliance an den technischen Support senden.

Unter finden "E-Series Hardware AutoSupport" Sie weitere Informationen zur Verwendung von AutoSupport mit E-Series Appliances.

Bevor Sie beginnen

- Sie sind mit einem beim Grid-Manager angemeldet"Unterstützter Webbrowser".
- Sie haben die "Zugriffsberechtigung für den Administrator der Storage-Appliance oder den Root-Zugriff".
- Sie haben SANtricity AutoSupport konfiguriert:
  - Für SG6000 und SG5700 Appliances, "Konfigurieren Sie AutoSupport in SANtricity System Manager"

> Sie müssen über SANtricity-Firmware 8.70 oder höher verfügen, um mit dem Grid Manager auf SANtricity System Manager zuzugreifen.

Über diese Aufgabe

Die AutoSupport-Pakete der E-Series enthalten Details zur Storage Hardware und sind spezifischer als andere AutoSupport-Pakete, die vom StorageGRID System gesendet werden.

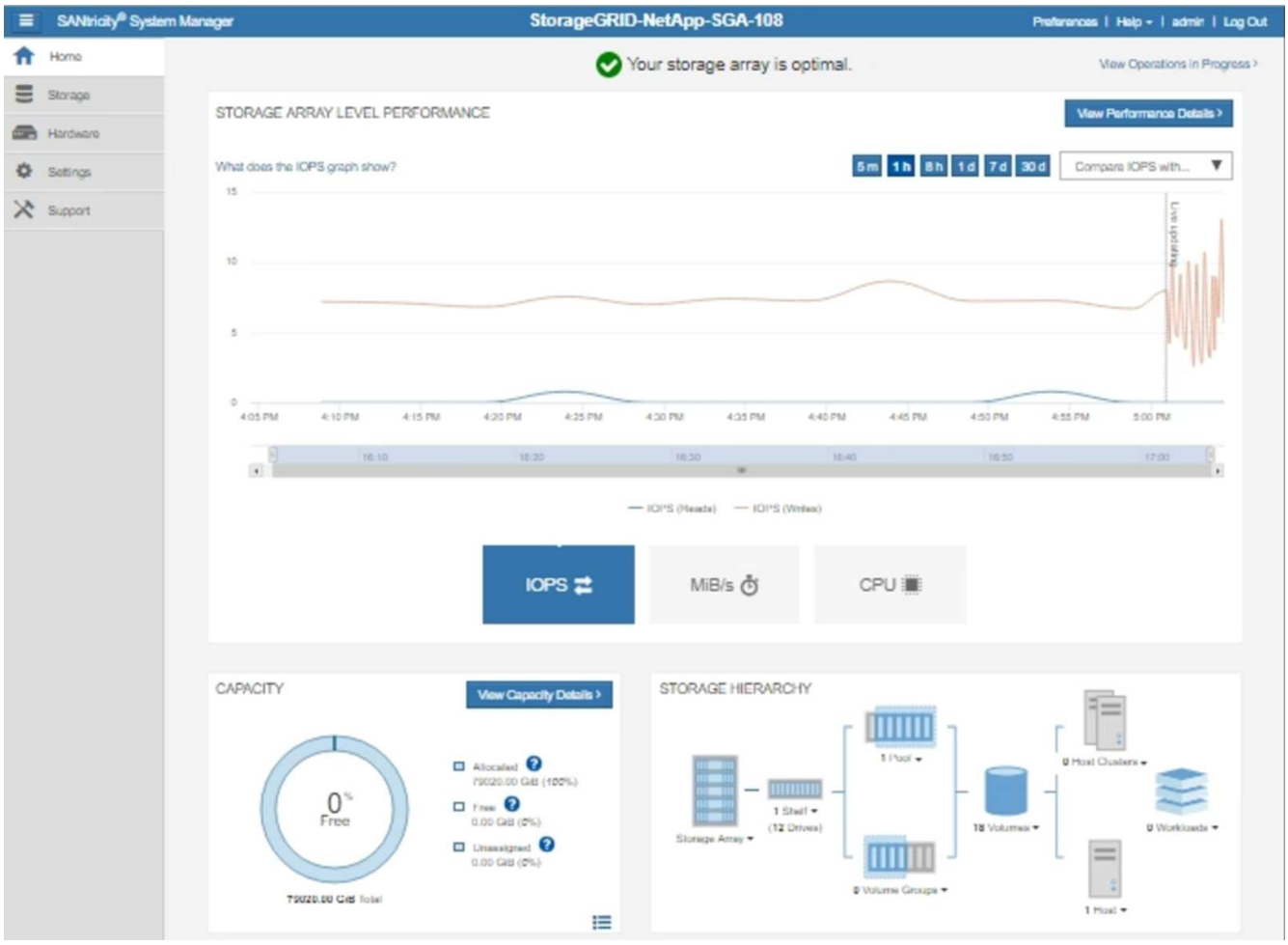
Sie können eine spezielle Proxy-Server-Adresse im SANtricity-System-Manager konfigurieren, um AutoSupport-Pakete über einen StorageGRID-Admin-Knoten ohne Verwendung des Management-Ports der Appliance zu übertragen. AutoSupport-Pakete, die auf diese Weise übertragen werden"Administratorknoten des bevorzugten Absenders", werden von der gesendet und verwenden alle"Administrator-Proxy-Einstellungen", die im Grid-Manager konfiguriert wurden.

> Dieses Verfahren gilt nur für die Konfiguration eines StorageGRID-Proxyservers für E-Series AutoSupport-Pakete. Weitere Informationen zur AutoSupport Konfiguration der E-Series finden Sie im "NetApp E-Series und SANtricity Dokumentation".

Schritte

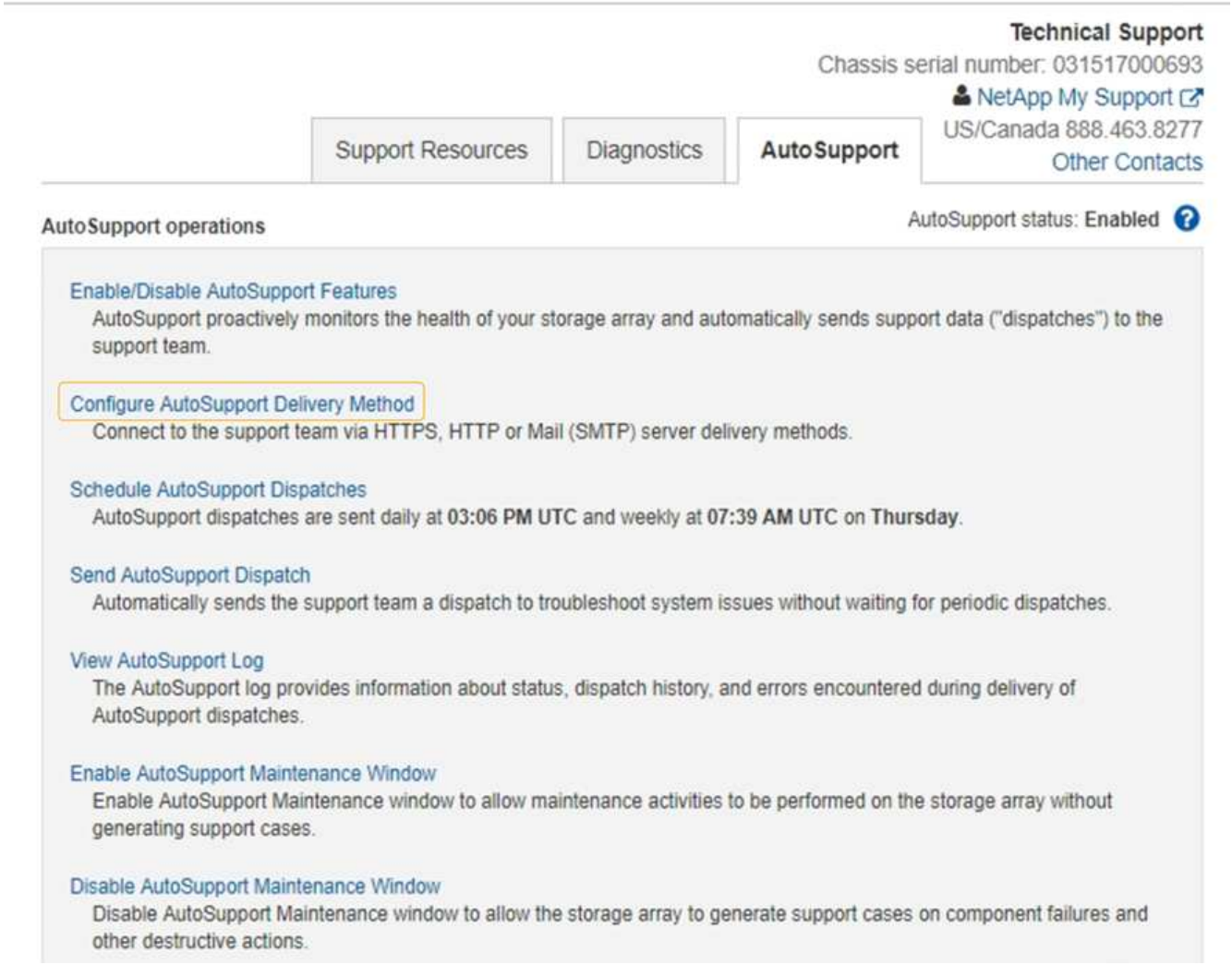
1. Wählen Sie im Grid Manager **Knoten** aus.
2. Wählen Sie in der Liste der Knoten links den Speicher-Appliance-Node aus, den Sie konfigurieren möchten.
3. Wählen Sie **SANtricity System Manager**.

   Die Startseite von SANtricity System Manager wird angezeigt.



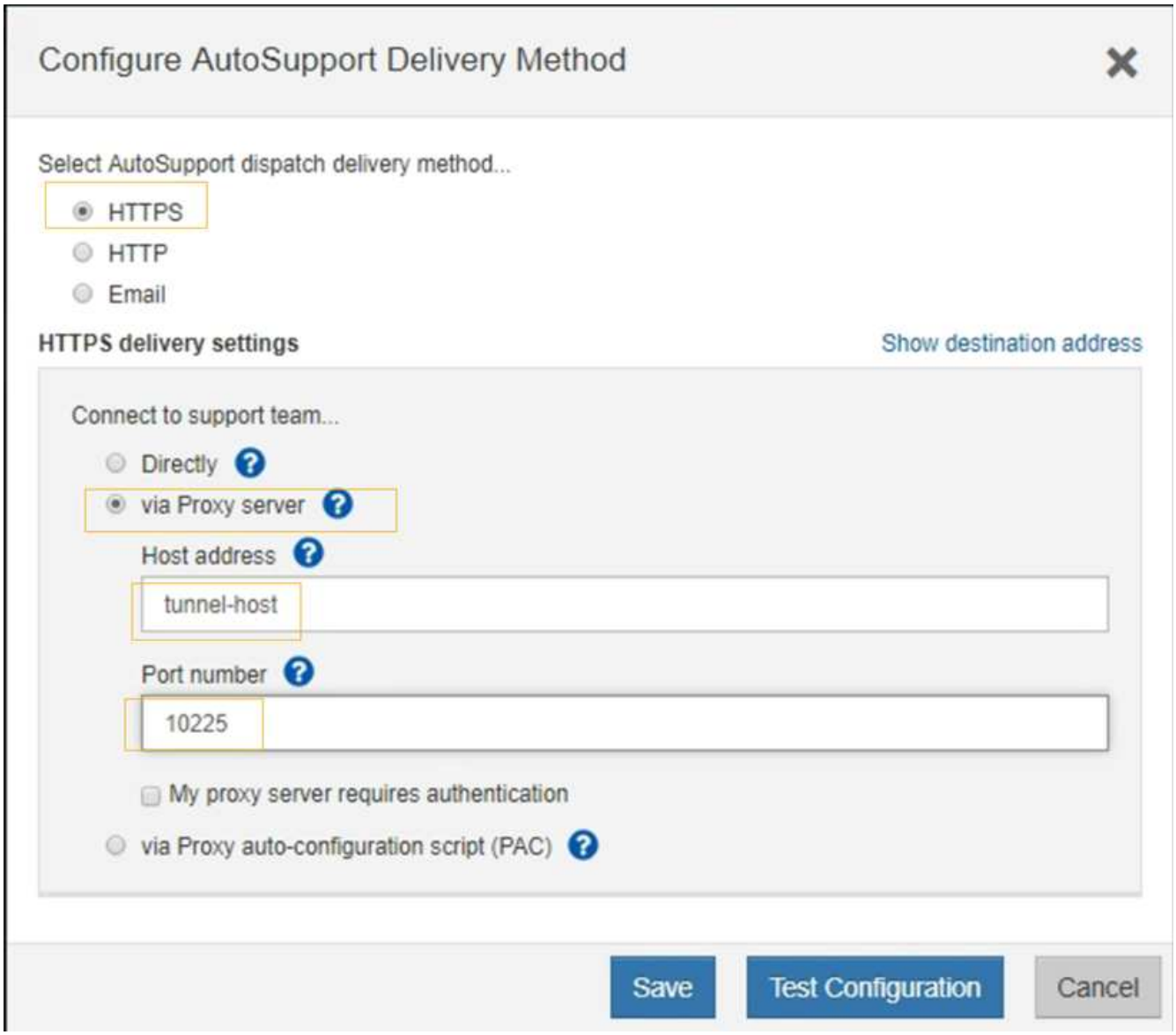
4. Wählen Sie **Support** > **Supportcenter** > * AutoSupport*.

   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 HTTPS aktiviert, ist vorinstalliert.

7. Wählen Sie **über Proxy-Server**.
8. Geben Sie für die **Host-Adresse** ein `tunnel-host`.

   `tunnel-host` Ist die besondere Adresse, an die Sie einen Admin-Node zum Senden von E-Series AutoSupport-Paketen verwenden können.

9. Geben Sie für die **Portnummer** ein `10225`.

   `10225` Ist die Portnummer auf dem StorageGRID-Proxyserver, der AutoSupport-Pakete vom E-Series Controller der Appliance empfängt.

10. Wählen Sie **Testkonfiguration** aus, um die Routing- und Konfigurationseinstellungen Ihres AutoSupport Proxy-Servers zu testen.

    Wenn Sie richtig sind, wird in einem grünen Banner die Meldung „Ihre AutoSupport-Konfiguration wurde

überprüft“ angezeigt.

Wenn der Test fehlschlägt, wird eine Fehlermeldung in einem roten Banner angezeigt. Überprüfen Sie Ihre StorageGRID-DNS-Einstellungen und Netzwerk, stellen Sie sicher, dass der "Administratorknoten des bevorzugten Absenders"eine Verbindung zur NetApp-Supportwebsite herstellen kann, und versuchen Sie den Test erneut.

11. Wählen Sie **Speichern**.

    Die Konfiguration wird gespeichert, und es wird eine Bestätigungsmeldung angezeigt: „AutoSupport-Bereitstellungsmethode wurde konfiguriert.“

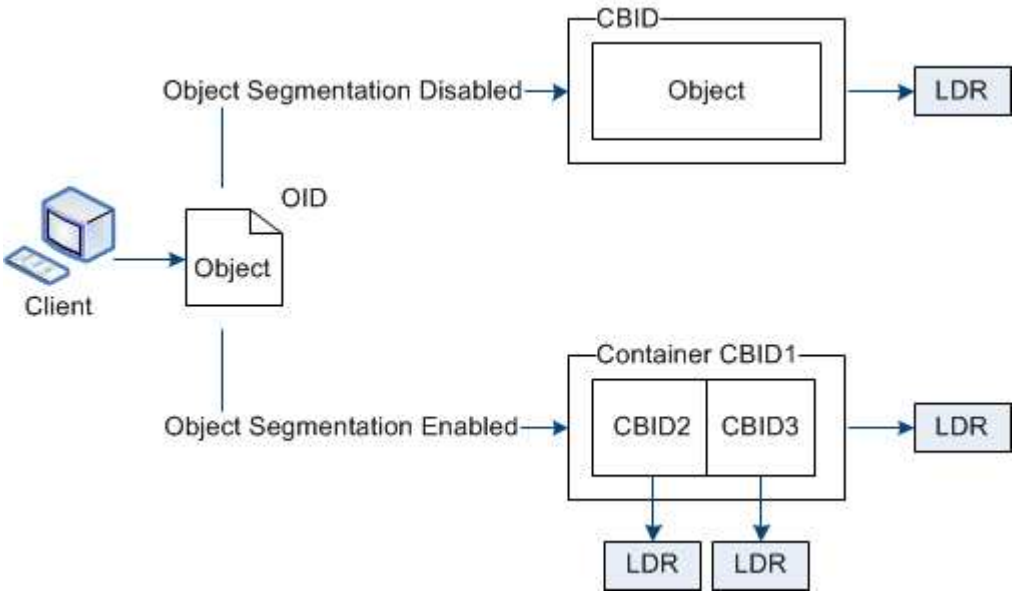
Managen Sie Storage-Nodes

Verwenden Sie Speicheroptionen

Was ist Objektsegmentierung?

Bei der Objektsegmentierung wird ein Objekt in eine Sammlung kleinerer Objekte fester Größe aufgeteilt, um die Storage- 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.

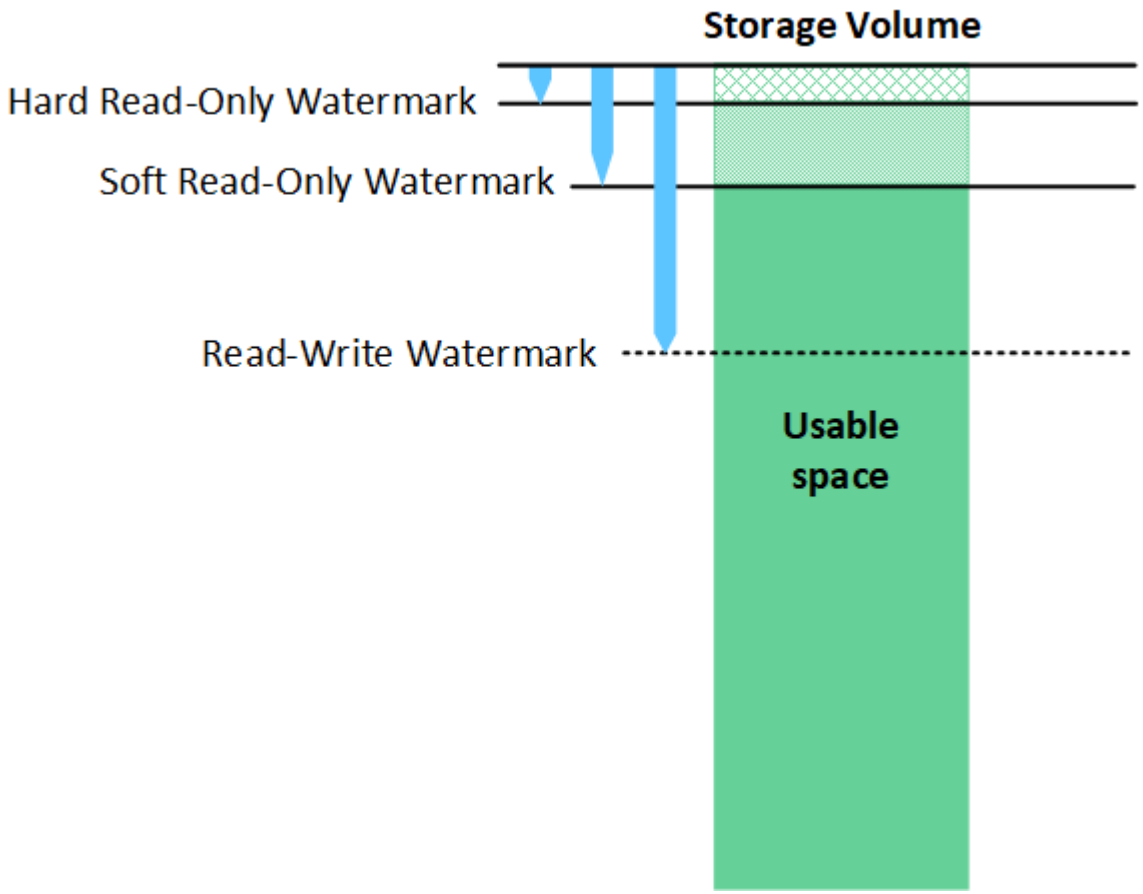
Der Container und die Segmente werden nicht unbedingt auf demselben Storage Node gespeichert. Container und Segmente können auf jedem Storage-Node innerhalb des in der ILM-Regel angegebenen Speicherpools gespeichert werden.

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:

```
segment container + segment 1 + segment 2 = three stored objects
```

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. Informationen über den für Objektmetadaten reservierten Speicherplatz auf Volume 0 finden Sie unter "Management von Objekt-Metadaten-Storage".

Was ist das weiche, schreibgeschützte Wasserzeichen?

Das Wasserzeichen **Storage Volume soft read-only** ist das erste Wasserzeichen, das angibt, dass der nutzbare Speicherplatz eines Storage Node für Objektdaten voll wird.

Wenn jedes Volume in einem Speicher-Node weniger freien Speicherplatz als das weiche schreibgeschützte Wasserzeichen des Volumes hat, wechselt der Speicher-Node in den *Read-Only-Modus*. Schreibgeschützter

Modus bedeutet, dass der Storage Node für den Rest des StorageGRID Systems schreibgeschützte Dienste anbietet, aber alle ausstehenden Schreibanforderungen erfüllt.

Nehmen wir beispielsweise an, jedes Volume in einem Storage Node hat ein weiches schreibgeschütztes 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 das fest lesbare Wasserzeichen?

Das Wasserzeichen **Speichervolumen nur auf hartem Lesezugriff** ist das nächste Wasserzeichen, um anzuzeigen, dass der nutzbare Speicherplatz eines Knotens für Objektdaten voll wird.

Wenn der freie Speicherplatz auf einem Volume geringer ist als das fest lesbare Wasserzeichen des Volumes, schlägt der Schreibvorgang auf das Volume fehl. Schreibvorgänge auf andere Volumes können jedoch so lange fortgesetzt werden, bis der freie Speicherplatz auf diesen Volumes kleiner als die harten schreibgeschützten Wasserzeichen ist.

Nehmen wir beispielsweise an, jedes Volume in einem Storage Node hat einen schreibgeschützten Wasserzeichen von 5 GB. Sobald jedes Volume weniger als 5 GB freien Speicherplatz hat, akzeptiert der Speicherknoten keine Schreibanforderungen mehr.

Das nur-Lese-Wasserzeichen ist immer kleiner als das weiche, schreibgeschützte Wasserzeichen.

Was ist das Lese-/Schreibwasserzeichen?

Das Lese-/Schreib-Wasserzeichen **Storage Volume** gilt nur für Storage Nodes, die in den schreibgeschützten Modus übergegangen sind. Er bestimmt, wann der Node wieder Lese-/Schreibzugriff werden kann. Wenn der freie Speicherplatz auf einem Speichervolume in einem Speicherknoten größer ist als das Lese-/Schreibwasserzeichen dieses Volumes, wechselt der Knoten automatisch zurück in den Lese-/Schreibzustand.

Angenommen, der Storage-Node ist in den schreibgeschützten Modus migriert. Nehmen Sie auch an, dass jedes Volume eine Lese-/Schreib-Wassermarke von 30 GB hat. Sobald der freie Speicherplatz eines beliebigen Volumes auf 30 GB ansteigt, wird der Node erneut zum Lesen/Schreiben.

Das Lese-/Schreibwasserzeichen ist immer größer als das weiche, schreibgeschützte Wasserzeichen und das nur-Lese-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.

Bevor Sie beginnen

- Sie haben das Upgrade auf StorageGRID 11.6 oder höher abgeschlossen.
- Sie sind im Grid Manager mit einem 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 **Support** > **Sonstiges** > **Speicherwasserzeichen**.
2. Aktivieren Sie auf der Seite Speicherwasserzeichen das Kontrollkästchen optimierte Werte verwenden.
   - Wenn das Kontrollkästchen aktiviert ist, werden alle drei Wasserzeichen für jedes Speicher-Volume auf jedem Speicher-Node optimiert, basierend auf der Größe des Speicher-Node und der relativen Kapazität des Volumes.

     Dies ist die Standardeinstellung und die empfohlene Einstellung. Aktualisieren Sie diese Werte nicht. Optional können Sie Anzeigen optimierter Speicherabdrücke.

   - Wenn das Kontrollkästchen optimierte Werte verwenden deaktiviert ist, werden benutzerdefinierte (nicht optimierte) Wasserzeichen verwendet. Es wird nicht empfohlen, benutzerdefinierte Wasserzeichen zu verwenden. Verwenden Sie die Anweisungen für"Fehlerbehebung Warnungen bei niedriger Schreibschutzmarke überschreiben", um festzustellen, ob Sie die Einstellungen anpassen können oder sollten.

     Wenn Sie benutzerdefinierte Wasserzeicheneinstellungen angeben, müssen Sie Werte größer als 0 eingeben.

Anzeigen optimierter Storage-Wasserzeichen

StorageGRID verwendet zwei Prometheus-Kennzahlen, um die optimierten Werte anzuzeigen, die es für das schreibgeschützte weiche Wasserzeichen des Storage-Volumes berechnet hat. Sie können die minimalen und maximalen optimierten Werte für jeden Speicherknoten in Ihrem Raster anzeigen.

1. Wählen Sie **Support** > **Tools** > **Metriken**.
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 minimale optimierte Wert des weichen schreibgeschützten Wasserzeichens für alle Speicher-Volumes auf jedem Storage Node angezeigt. Wenn dieser Wert größer ist als die benutzerdefinierte Einstellung für das Speichervolume-Softread-only-Wasserzeichen, wird die Warnmeldung **Low read-only Watermark override** für den Speicherknoten 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 maximale optimierte Wert des weichen schreibgeschützten Wasserzeichens für alle Speicher-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.

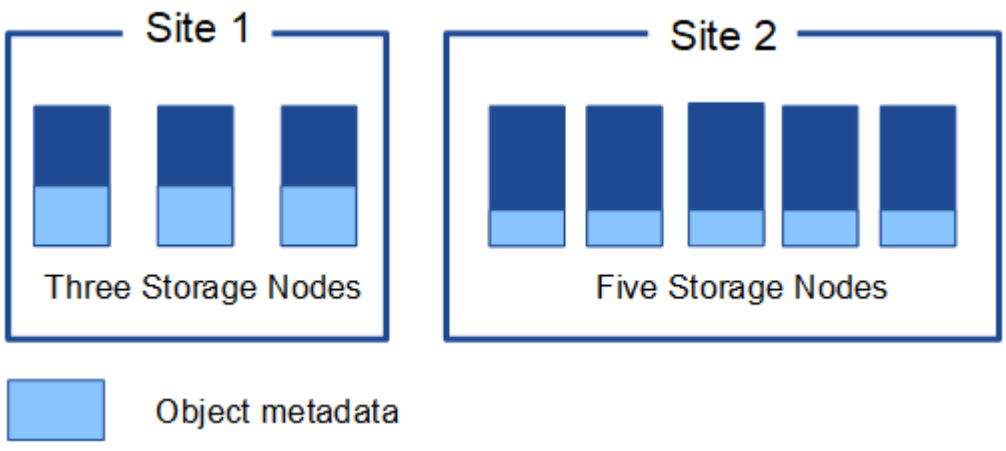
Für ein Objekt in StorageGRID enthalten die Objektmetadaten die folgenden Informationstypen:

- Systemmetadaten, einschließlich einer eindeutigen ID für jedes Objekt (UUID), des Objektnamens, des Namens des S3-Buckets, des Namens oder der ID des Mandantenkontos, der logischen Größe des Objekts, des Datums und der Uhrzeit, zu der das Objekt zum ersten Mal erstellt wurde sowie des Datums und der Uhrzeit, zu der das Objekt zuletzt geändert wurde.
- 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?

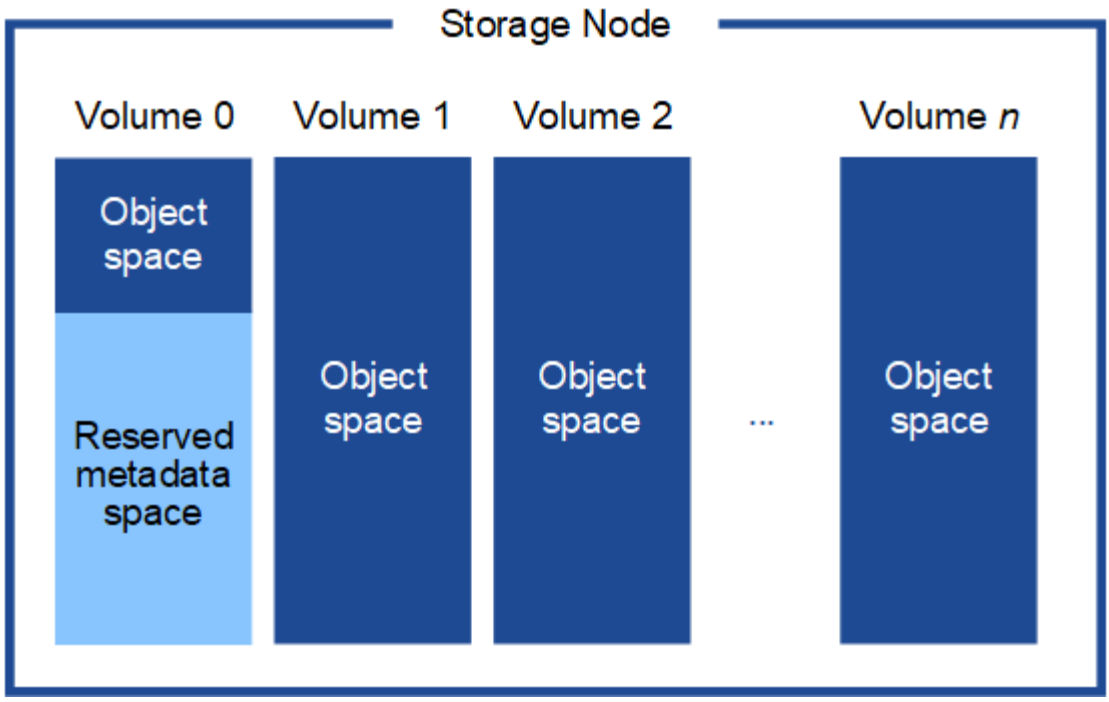
StorageGRID speichert Objektmetadaten in einer Cassandra-Datenbank, die unabhängig von Objektdaten gespeichert werden. Um Redundanz zu gewährleisten und Objekt-Metadaten vor Verlust zu schützen, speichert StorageGRID drei Kopien der Metadaten für alle Objekte im System an jedem Standort.

Diese Abbildung zeigt die Speicherknoten an zwei Standorten. Jeder Standort verfügt über die gleiche Menge an Objektmetadaten. Die Metadaten jedes Standorts werden unter alle Storage-Nodes an diesem Standort unterteilt.



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.

Der Speicherplatz, der für Objektmetadaten auf einem bestimmten Storage Node reserviert ist, hängt von mehreren Faktoren ab, die im Folgenden beschrieben werden.

Einstellung für reservierten Speicherplatz für Metadaten

Die Einstellung „*Metadata reserved space*“ ist eine systemweite Einstellung, die den Speicherplatz darstellt, der für Metadaten auf Volume 0 jedes Storage-Node reserviert wird. Wie in der Tabelle gezeigt, basiert der Standardwert dieser Einstellung auf:

- 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 für Metadaten
11,5 bis 12,0	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)

Für die Erstinstallation von StorageGRID verwendete Version	RAM-Größe auf Speicherknoten	Standardeinstellung für reservierten Speicherplatz für Metadaten
	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)

Zeigen Sie die Einstellung für den reservierten Speicherplatz für Metadaten an

Befolgen Sie diese Schritte, um die Einstellung für den reservierten Speicherplatz für Metadaten für Ihr StorageGRID-System anzuzeigen.

Schritte

1. Wählen Sie **Konfiguration** > **System** > **Speichereinstellungen**.
2. Erweitern Sie auf der Seite Speichereinstellungen den Abschnitt **reservierter Speicherplatz für Metadaten**.

Bei StorageGRID 11.8 oder höher muss der Wert für den reservierten Speicherplatz für Metadaten mindestens 100 GB und nicht mehr als 1 PB betragen.

Die Standardeinstellung für eine neue StorageGRID 11.6 oder höher-Installation, bei der jeder Speicherknoten mindestens 128 GB RAM hat, beträgt 8,000 GB (8 TB).

Tatsächlich reservierter Speicherplatz für Metadaten

Im Gegensatz zur Einstellung des systemweiten reservierten Speicherplatzes für Metadaten wird für jeden Storage Node der *tatsächliche reservierte Speicherplatz* für Objektmetadaten ermittelt. Der tatsächlich für Metadaten reservierte Speicherplatz hängt bei jedem Storage-Node von der Größe von Volume 0 für den Node und der Einstellung des für Metadaten reservierten Speicherplatzes für das gesamte System ab.

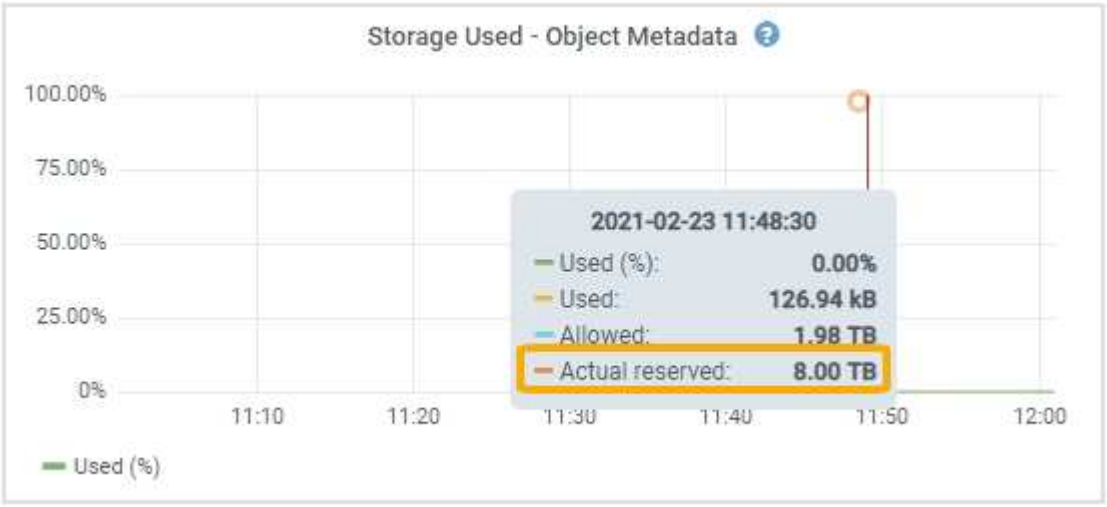
Größe von Volume 0 für den Node	Tatsächlich reservierter Speicherplatz für Metadaten
Weniger als 500 GB (nicht in der Produktion)	10% des Volumens 0
500 GB oder mehr + oder + nur Metadaten-Speicher-Nodes	Die kleineren Werte: • Band 0 • Einstellung für reservierten Speicherplatz für Metadaten **Hinweis**: Nur ein Rangedb ist für Metadaten-only Storage Nodes erforderlich.

Zeigen Sie den tatsächlich reservierten Speicherplatz für Metadaten an

Führen Sie die folgenden Schritte aus, um den tatsächlich reservierten Speicherplatz für Metadaten auf einem bestimmten Storage-Node anzuzeigen.

Schritte

1. Wählen Sie im Grid Manager **Knoten** > ***Speicherknoten***.
2. Wählen Sie die Registerkarte **Storage** aus.
3. Setzen Sie den Cursor auf das Diagramm Speicher verwendet - Objekt Metadaten 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 für diesen Storage-Node kleiner ist als Volume 0, entspricht der tatsächlich reservierte Speicherplatz für diesen Node der Einstellung für den reservierten Speicherplatz für Metadaten.

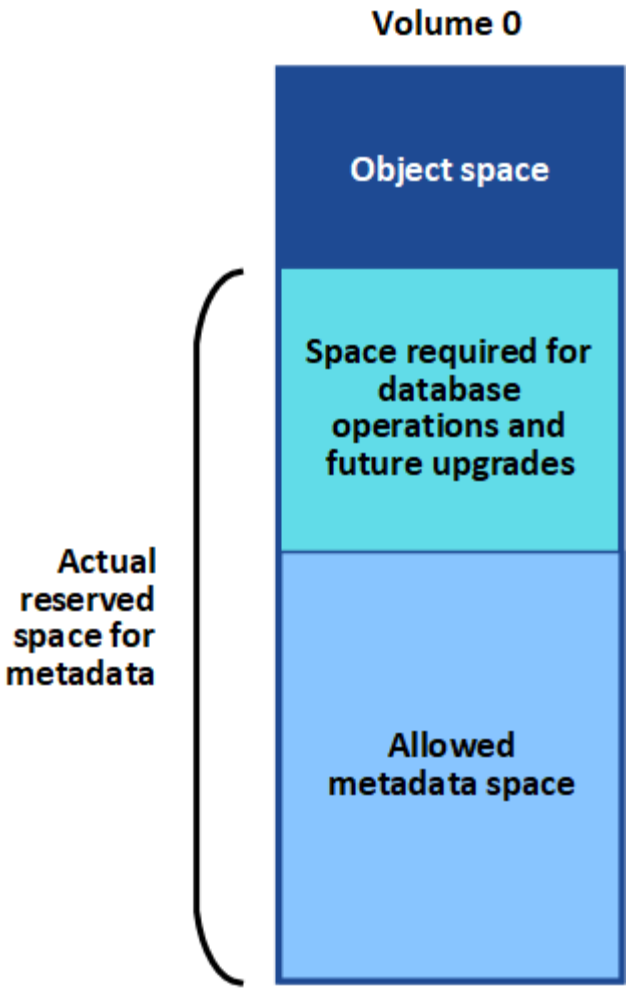
Beispiel für den tatsächlich reservierten Metadatenspeicherplatz

Angenommen, Sie installieren ein neues StorageGRID System mit Version 11.7 oder höher. 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-reservierte Speicherplatz** ist auf 8 TB eingestellt. (Dies ist der Standardwert für eine neue StorageGRID 11.6-Installation oder höher, 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 **Metadata reserved space**.)

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.

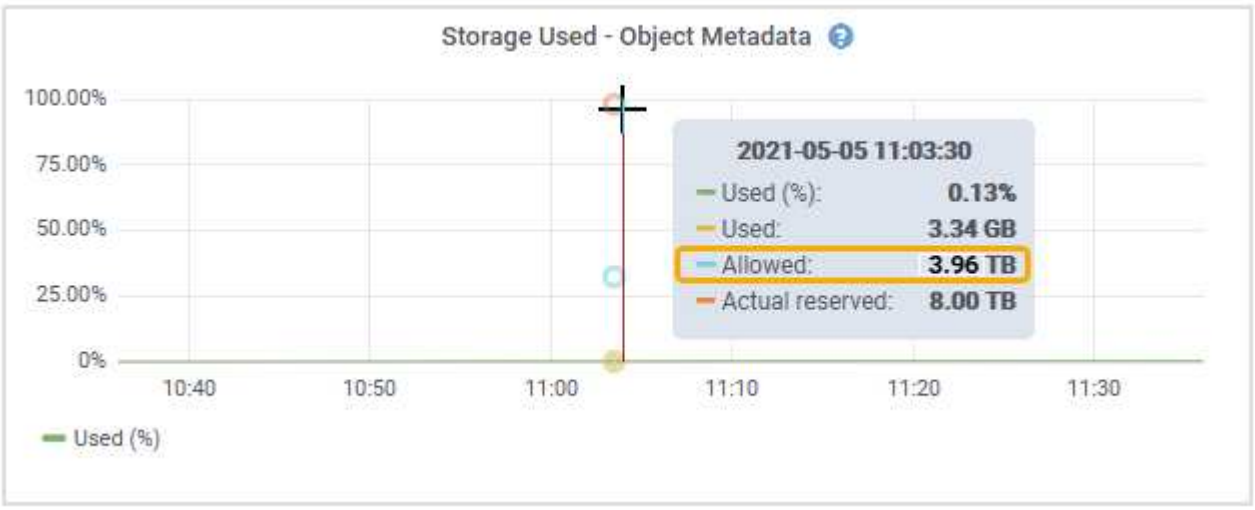
		Speichermenge auf Speicherknoten	
	≪ 128 GB	>= 128 GB	**Tatsächlich reservierter Platz für Metadaten**
≪= 4 TB	60 % des tatsächlich reservierten Speicherplatzes für Metadaten maximal 1.32 TB	60 % des tatsächlich reservierten Speicherplatzes für Metadaten maximal 1.98 TB	4 TB

Zeigen Sie den zulässigen Metadatenbereich an

Führen Sie die folgenden Schritte aus, um den zulässigen Metadatenspeicher für einen Storage-Node anzuzeigen.

Schritte

1. Wählen Sie im Grid Manager **Knoten** aus.
2. Wählen Sie den Speicherknoten aus.
3. Wählen Sie die Registerkarte **Storage** aus.
4. Setzen Sie den Cursor auf das Diagramm Speicher verwendet - Objekt Metadaten und suchen Sie den Wert **erlaubt**.



Im Screenshot ist der **allowed**-Wert 3.96 TB, was der Maximalwert 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-reservierte Speicherplatz** ist auf 8 TB eingestellt. (Dies ist der Standardwert für StorageGRID 11.6 oder höher, wenn jeder Speicher-Node 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 **Metadata reserved space**.)
- Der erlaubte Platz für Metadaten auf SN1 ist 3 TB, basierend auf der Berechnung in der gezeigt Tabelle für zulässigem Speicherplatz für Metadaten: (tatsächlich reservierter Speicherplatz für Metadaten − 1 TB) × 60%, bis zu einem Maximum von 3.96 TB.

Storage-Nodes unterschiedlicher Größen beeinflussen die Objektkapazität

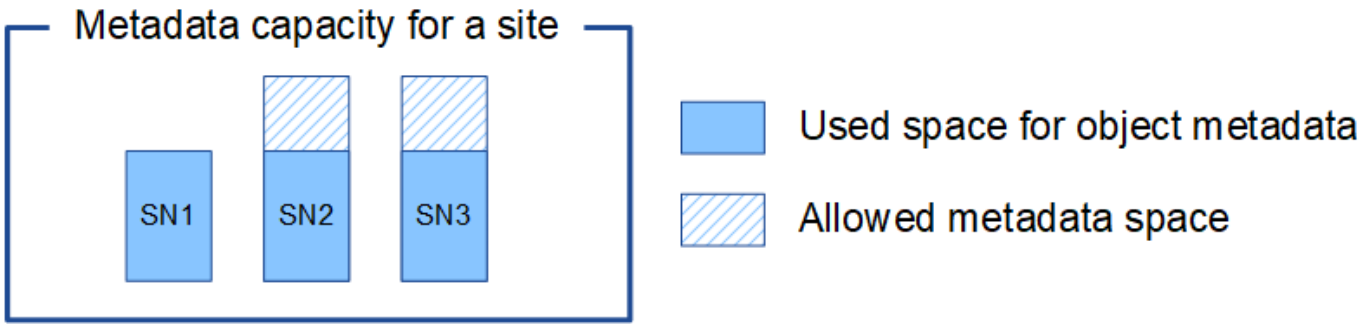
Wie oben beschrieben, verteilt StorageGRID Objektmetadaten gleichmäßig über Storage-Nodes an jedem Standort. Wenn ein Standort Storage-Nodes unterschiedlicher Größen enthält, bestimmt der kleinste Node am Standort die Metadaten-Kapazität des Standorts.

Beispiel:

- Sie haben ein Raster mit drei Storage Nodes unterschiedlicher Größe an einem einzigen Standort.
- Die Einstellung **Metadaten reservierter Speicherplatz** 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	2,2TB	2,2TB	1,32TB
SN2	5TB	4TB	1,98TB
SN3	6TB	4TB	1,98TB

Da Objektmetadaten gleichmäßig auf die Storage-Nodes an einem Standort verteilt werden, kann jeder Node in diesem Beispiel nur 1.32 TB Metadaten enthalten. Die zusätzlichen 0.66 TB an erlaubten Metadaten für SN2 und SN3 können 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 Überwachen der Objektmetadatenkapazität für jeden Speicher-Node finden Sie in den Anweisungen für "Monitoring von StorageGRID".
- Um die Objektmetadatenkapazität Ihres Systems durch Hinzufügen neuer Storage-Nodes zu erhöhen"Erweitern Sie ein Raster".

Erhöhen Sie die Einstellung für reservierten Speicherplatz für Metadaten

Möglicherweise können Sie die Systemeinstellung „reservierter Speicherplatz für Metadaten“ erhöhen, wenn die Storage-Nodes bestimmte Anforderungen für RAM und verfügbaren Speicherplatz erfüllen.

Was Sie benötigen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".

- Sie haben die"Root-Zugriffsberechtigung oder Berechtigung „Andere Rasterkonfiguration“" .

Über diese Aufgabe

Möglicherweise können Sie den systemweiten reservierten Metadatenspeicherplatz manuell auf bis zu 8 TB erhöhen.

Sie können nur den Wert der Einstellung für systemweiten reservierten Speicherplatz für Metadaten erhöhen, wenn beide dieser Anweisungen wahr sind:

- Die Speicherknoten an einem beliebigen Standort in Ihrem System haben jeweils 128 GB oder mehr RAM.
- Die Speicherknoten an jedem Standort in Ihrem System verfügen jeweils über genügend Platz auf dem Speichervolumen 0.

Wenn Sie diese Einstellung erhöhen, reduzieren Sie gleichzeitig den für den Objektspeicher verfügbaren Platz auf dem Speichervolumen 0 aller Storage-Nodes. Aus diesem Grund möchten Sie möglicherweise den reservierten Speicherplatz für Metadaten auf einen Wert kleiner als 8 TB setzen, der auf den erwarteten Anforderungen für Objektmetadaten basiert.

> Im Allgemeinen ist es besser, einen höheren Wert anstelle eines niedrigeren Wertes zu verwenden. Wenn die Einstellung für reservierten Speicherplatz für Metadaten zu groß ist, können Sie sie später verkleinern. Wenn Sie den Wert später erhöhen, muss das System dagegen möglicherweise Objektdaten verschieben, um Speicherplatz freizugeben.

Eine detaillierte Erklärung darüber, wie sich die Einstellung „reservierter Speicherplatz für Metadaten“ auf den zulässigen Speicherplatz für Objekt-Metadatenspeicherung auf einem bestimmten Storage Node auswirkt, finden Sie unter "Management von Objekt-Metadaten-Storage".

Schritte

1. Legen Sie die aktuelle Einstellung für den reservierten Metadatenspeicherplatz fest.
   a. Wählen Sie **Konfiguration** > **System** > **Speichereinstellungen**.
   b. Notieren Sie den Wert von **Reservierter Speicherplatz für Metadaten**.
2. Stellen Sie sicher, dass auf dem Speicher-Volume 0 jedes Speicherknoten genügend Speicherplatz zur Verfügung steht, um diesen Wert zu erhöhen.
   a. Wählen Sie **Knoten** aus.
   b. Wählen Sie den ersten Storage-Node im Raster aus.
   c. Wählen Sie die Registerkarte Storage aus.
   d. Suchen Sie im Abschnitt Volumes den Eintrag **/var/local/rangedb/0**.
   e. Vergewissern Sie sich, dass der verfügbare Wert gleich oder größer ist als der Unterschied zwischen dem neuen Wert, den Sie verwenden möchten, und dem aktuellen Wert für reservierten Metadatenspeicherplatz.

      Wenn die Einstellung für reservierten Speicherplatz für Metadaten beispielsweise aktuell 4 TB beträgt und Sie diesen auf 6 TB erhöhen möchten, muss der verfügbare Wert 2 TB oder mehr sein.

   f. Wiederholen Sie diese Schritte für alle Speicherknoten.
      - Wenn ein oder mehrere Speicherknoten nicht über genügend Speicherplatz verfügen, kann der Wert für den reservierten Metadatenspeicherplatz nicht erhöht werden. Fahren Sie mit diesem Verfahren nicht fort.

- Wenn jeder Speicherknoten genügend Platz auf Volume 0 hat, fahren Sie mit dem nächsten Schritt fort.

3. Stellen Sie sicher, dass Sie mindestens 128 GB RAM auf jedem Speicherknoten haben.
   a. Wählen Sie **Knoten** aus.
   b. Wählen Sie den ersten Storage-Node im Raster aus.
   c. Wählen Sie die Registerkarte **Hardware** aus.
   d. Bewegen Sie den Mauszeiger über das Diagramm „Speicherauslastung“. Vergewissern Sie sich, dass **Total Memory** mindestens 128 GB beträgt.
   e. Wiederholen Sie diese Schritte für alle Speicherknoten.
      - Wenn mindestens ein Speicherknoten nicht über genügend Gesamtspeicher verfügt, kann der Wert für den reservierten Metadatenspeicherplatz nicht erhöht werden. Fahren Sie mit diesem Verfahren nicht fort.
      - Wenn jeder Speicherknoten mindestens 128 GB Gesamtspeicher hat, fahren Sie mit dem nächsten Schritt fort.
4. Aktualisieren Sie die Einstellung für reservierten Metadatenspeicherplatz.
   a. Wählen Sie **Konfiguration** > **System** > **Speichereinstellungen**.
   b. Wählen Sie **Reservierter Speicherplatz für Metadaten**.
   c. Geben Sie den neuen Wert ein.

      Um beispielsweise 8 TB einzugeben, geben Sie **8000000000000** (8, gefolgt von 12 Nullen) ein.

   d. Wählen Sie **Speichern**.

Gespeicherte Objekte komprimieren

Sie können die Objektkomprimierung aktivieren, um die Größe der in StorageGRID gespeicherten Objekte zu reduzieren und so weniger Storage zu belegen.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben "Bestimmte Zugriffsberechtigungen".

Über diese Aufgabe

Standardmäßig ist die Objektkomprimierung deaktiviert. Wenn Sie die Komprimierung aktivieren, versucht StorageGRID beim Speichern jedes Objekts mithilfe einer verlustfreien 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 die Objektkomprimierung aktivieren, beachten Sie Folgendes:

- Sie sollten nicht **komprimieren gespeicherte Objekte** auswählen, es sei denn, Sie wissen, dass die gespeicherten Daten komprimierbar sind.
- Applikationen, die Objekte in StorageGRID speichern, komprimieren möglicherweise Objekte, bevor sie gespeichert werden. Wenn eine Client-Anwendung ein Objekt bereits komprimiert hat, bevor es in StorageGRID gespeichert wird, verringert die Auswahl dieser Option die Größe eines Objekts nicht weiter.

- Wählen Sie nicht **gespeicherte Objekte komprimieren** wenn Sie NetApp FabricPool mit StorageGRID verwenden.
- Wenn **Compress Stored Objects** ausgewählt ist, sollten S3-Client-Anwendungen die Ausführung von GetObject-Operationen vermeiden, die einen Bereich von Bytes angeben, die zurückgegeben werden sollen. Diese Vorgänge beim Lesen von Range sind ineffizient, da StorageGRID Objekte effektiv dekomprimieren muss, um auf die angeforderten Bytes zuzugreifen. GetObject Operationen, die einen kleinen Bereich von Bytes von einem sehr großen Objekt anfordern, sind besonders ineffizient; zum Beispiel ist es ineffizient, einen 10 MB Bereich von einem 50 GB komprimierten 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** > **Speichereinstellungen** > **Objektkomprimierung**.
2. Aktivieren Sie das Kontrollkästchen **gespeicherte Objekte komprimieren**.
3. Wählen Sie **Speichern**.

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 die Anleitung für "Erweitern eines StorageGRID Systems".

Hinzufügen von Shelfs zur Storage-Erweiterung

Einige Storage-Nodes der StorageGRID Appliance, z. B. SG6060 oder SG6160, 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 die Anleitung für "Erweitern eines StorageGRID Systems".

Storage-Nodes Hinzufügen

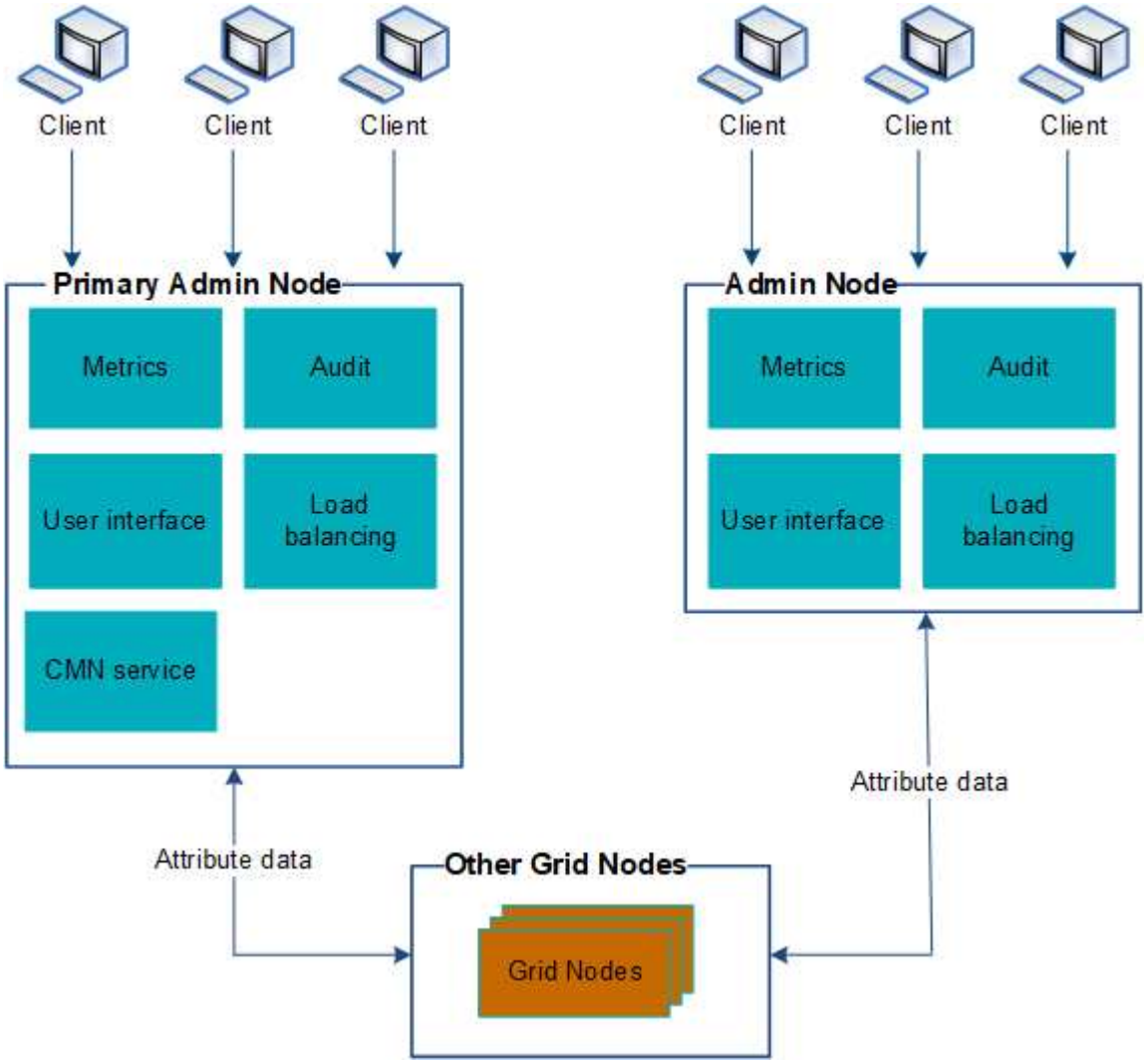
Sie können die Storage-Kapazität durch Hinzufügen von Storage-Nodes erhöhen. Beim Hinzufügen von Storage müssen die aktuell aktiven ILM-Regeln und Kapazitätsanforderungen sorgfältig berücksichtigt werden. Siehe die Anleitung für "Erweitern eines StorageGRID Systems".

Managen Sie Admin-Nodes

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 Administratorknoten nicht mehr verfügbar ist, wird die Attributverarbeitung fortgesetzt, Warnmeldungen werden weiterhin ausgelöst und E-Mail-Benachrichtigungen und AutoSupport-Pakete werden weiterhin gesendet. Wenn Sie jedoch mehrere Administratorknoten haben, bietet dieser keinen Failover-Schutz außer Benachrichtigungen und AutoSupport-Paketen.



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 aktive 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 bietet mehr Funktionen als nicht-primäre Admin-Nodes. Beispielsweise müssen einige Wartungsverfahren mit dem primären Admin-Node durchgeführt werden.

Weitere Informationen zu Admin-Knoten finden Sie unter "Was ist ein Admin-Node".

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben "Bestimmte Zugriffsberechtigungen".

Schritte

1. Wählen Sie **Knoten** aus.
2. Geben Sie **primary** in das Suchfeld ein.

   Identifizieren Sie in den Suchergebnissen den Knoten mit dem in der Spalte Typ angezeigten „Primary Admin Node“. Ein primärer Admin-Knoten sollte aufgelistet werden.