StorageGRID verwalten

StorageGRID software

NetApp
July 23, 2026

Inhalt

StorageGRID verwalten

StorageGRID verwalten

${post_edited_translations.segment}

Über diese Anweisungen

Die wichtigsten Aufgaben bei der Konfiguration und Administration von StorageGRID ermöglichen Folgendes:

- Mit dem Grid Manager können Gruppen und Benutzer eingerichtet werden.
- Mandantenkonten ermöglichen es S3-Clientanwendungen, Objekte zu speichern und abzurufen.
- StorageGRID Netzwerke konfigurieren und verwalten
- Konfiguration von AutoSupport
- Knoteneinstellungen verwalten

Bevor Sie beginnen

- Sie haben ein allgemeines Verständnis des StorageGRID Systems.
- Sie verfügen über recht detaillierte Kenntnisse der Linux-Befehlsshells, der Netzwerktechnik sowie der Einrichtung und Konfiguration von Serverhardware.

Erste Schritte mit Grid Manager

Anforderungen an den Webbrowser für StorageGRID

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	${post_edited_translations.segment}
Google Chrome	138
Microsoft Edge	138
Mozilla Firefox	140

Das Browserfenster sollte auf eine empfohlene Breite eingestellt werden.

Browserbreite	Pixel
Minimum	1024
${post_edited_translations.segment}	1280

Melden Sie sich beim StorageGRID Grid Manager an

Auf die Anmeldeseite des Grid Manager wird zugegriffen, indem der vollqualifizierte Domainname (FQDN) oder die IP-Adresse eines Admin Node in die Adresszeile eines unterstützten Webbrowsers eingegeben wird.

Jedes StorageGRID System besteht aus einem primären Admin Node und beliebig vielen nicht-primären Admin Nodes. Eine Anmeldung am Grid Manager ist auf jedem Admin Node möglich, um das StorageGRID System zu verwalten. Einige Wartungsverfahren können jedoch nur vom primären Admin Node aus durchgeführt werden.

Verbindung zur HA-Gruppe

Wenn Admin-Knoten in einer hochverfügbaren (HA) Gruppe enthalten sind, erfolgt die Verbindung über die virtuelle IP-Adresse der HA-Gruppe oder eine vollqualifizierte Domain, die der virtuellen IP-Adresse zugeordnet ist. Der primäre Admin-Knoten sollte als primäre Schnittstelle der Gruppe ausgewählt werden, sodass beim Zugriff auf den Grid Manager der Zugriff auf den primären Admin-Knoten erfolgt, es sei denn, der primäre Admin-Knoten ist nicht verfügbar. Siehe "Hochverfügbarkeitsgruppen verwalten".

SSO verwenden

Die Anmeldeschritte unterscheiden sich geringfügig, wenn "Single Sign-On (SSO) wurde konfiguriert".

Anmeldung bei Grid Manager auf dem ersten Admin-Node

Bevor Sie beginnen

- Sie haben Ihre Anmeldedaten.
- Sie verwenden ein "unterstützte 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 vollqualifizierten Domainnamen, die IP-Adresse eines Admin-Knotens oder die virtuelle IP-Adresse einer HA-Gruppe von Admin-Knoten verwenden.

  Um auf den Grid Manager über einen anderen Port als den Standardport für HTTPS (443) zuzugreifen, ist die Portnummer in der URL anzugeben:

  `https://FQDN_or_Admin_Node_IP:port/`

  > SSO ist über den eingeschränkten Grid Manager Port nicht verfügbar. Port 443 muss verwendet werden.

Schritte

1. ${post_edited_translations.segment}
2. In der Adressleiste des Browsers die URL für den Grid Manager eingeben.
3. Wenn eine Sicherheitswarnung angezeigt wird, kann das Zertifikat mit dem Installationsassistenten des Browsers installiert werden. Siehe "Sicherheitszertifikate verwalten".

4. Melden Sie sich beim Grid Manager an.

   ${post_edited_translations.segment}

   SSO wird nicht verwendet

   a. Geben Sie Ihren Benutzernamen und Ihr Passwort für den Grid Manager ein.

   b. **Anmelden** auswählen.

   Verwendung von SSO

   - Wenn StorageGRID SSO verwendet und dies das erste Mal ist, dass Sie die URL in diesem Browser aufrufen:

     i. **Anmelden** auswählen. Die 0 kann im Feld Konto belassen werden.

     ii. Geben Sie Ihre Standard-SSO-Anmeldedaten auf der SSO-Anmeldeseite Ihrer Organisation ein.

     ${post_edited_translations.segment}

     A. ${post_edited_translations.segment}

     B. **Anmelden** auswählen.

     C. Mit den üblichen SSO-Anmeldedaten auf der SSO-Anmeldeseite der Organisation anmelden.

Nach der Anmeldung wird die Startseite des Grid Managers angezeigt, die das Dashboard enthält. Welche Informationen bereitgestellt werden, ist unter "Dashboard anzeigen und verwalten" zu finden.

Bei einem anderen Admin-Node anmelden

${post_edited_translations.segment}

SSO wird nicht verwendet

Schritte

1. In der Adresszeile des Browsers den vollqualifizierten Domainnamen oder die IP-Adresse des anderen Admin Node eingeben. Die Portnummer bei Bedarf angeben.
2. Geben Sie Ihren Benutzernamen und Ihr Passwort für den Grid Manager ein.
3. **Anmelden** auswählen.

Verwendung von SSO

Wenn StorageGRID SSO verwendet und Sie sich bei einem Admin-Knoten angemeldet haben, ist der Zugriff auf andere Admin-Knoten möglich, ohne sich erneut anmelden zu müssen.

Schritte

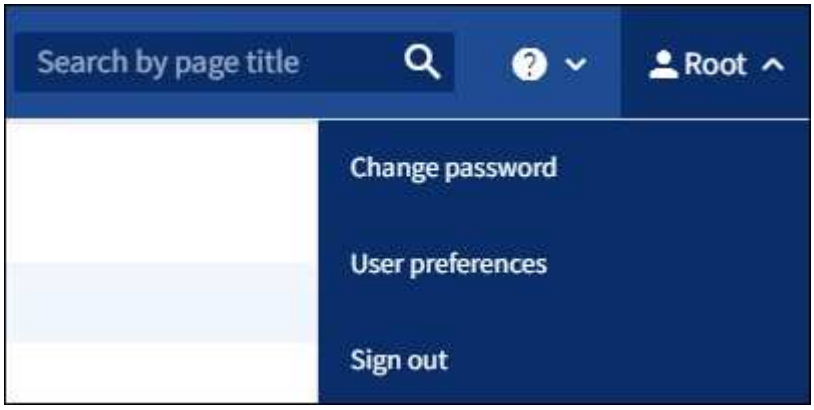
1. Den vollqualifizierten Domainnamen oder die IP-Adresse des anderen Admin-Knotens in die Adressleiste des Browsers eingeben.
2. Wenn Ihre SSO-Sitzung abgelaufen ist, geben Sie Ihre Anmeldeinformationen erneut ein.

Vom StorageGRID Grid Manager abmelden

Wenn Sie die Arbeit mit dem Grid Manager beendet haben, müssen Sie sich abmelden, um sicherzustellen, dass unbefugte Benutzer nicht auf das StorageGRID System zugreifen können. Abhängig von den Cookie-Einstellungen des Browsers werden Sie durch das Schließen des Browsers eventuell nicht aus dem System abgemeldet.

Schritte

1. ${post_edited_translations.segment}



2. ${post_edited_translations.segment}

Option	Beschreibung
SSO wird nicht verwendet	Sie sind vom Admin-Node abgemeldet. Die Anmeldeseite des Grid Managers wird angezeigt. **Hinweis:** Wenn Sie sich bei mehr als einem Admin-Knoten angemeldet haben, müssen Sie sich von jedem Knoten abmelden.
SSO aktiviert	Sie wurden von allen Admin-Knoten abgemeldet, auf die Sie zugegriffen haben. Die StorageGRID Anmeldeseite wird angezeigt. **Grid Manager** ist im Dropdown-Menü **Zuletzt verwendete Konten** als Standard aufgeführt, und das Feld **Account ID** zeigt 0 an. **Hinweis:** Wenn SSO aktiviert ist und Sie auch beim Tenant Manager angemeldet sind, müssen Sie auch "Vom Mieterkonto abmelden" zu "Abmelden von SSO".

Ändern Sie Ihr StorageGRID Grid Manager-Passwort

Wenn Sie ein lokaler Benutzer des Grid Managers sind, kann das eigene Passwort geändert werden.

Bevor Sie beginnen

Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.

Über diese Aufgabe

Wenn Sie sich als Verbundbenutzer bei StorageGRID anmelden oder wenn Single Sign-On (SSO) aktiviert ist, kann das Passwort nicht im Grid Manager geändert werden. Stattdessen muss das Passwort in der externen Identitätsquelle geändert werden, zum Beispiel in Active Directory oder OpenLDAP.

Schritte

1. Im Grid Manager Header ***Ihr Name*** > **Passwort ändern** auswählen.
2. Geben Sie Ihr aktuelles Passwort ein.
3. Geben Sie ein neues Passwort ein.

   Ihr Passwort muss mindestens 8 und höchstens 32 Zeichen lang sein. Passwörter sind Groß- und Kleinschreibungs-empfindlich.
4. Das neue Passwort erneut eingeben.
5. **Speichern** auswählen.

${post_edited_translations.segment}

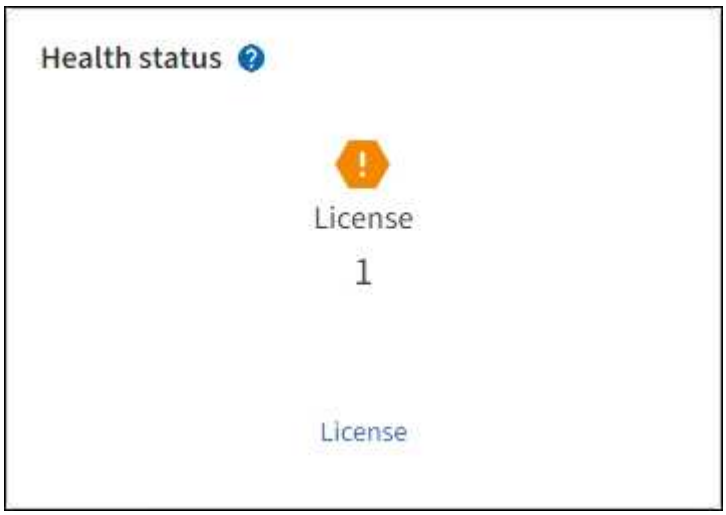
Sie können die Lizenzinformationen für Ihr StorageGRID System, wie die maximale Speicherkapazität Ihres Grids, jederzeit einsehen.

Bevor Sie beginnen

Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.

Über diese Aufgabe

Bei Problemen mit der Softwarelizenz für dieses StorageGRID System enthält die Statuskarte „Health“ auf dem Dashboard ein Lizenzstatussymbol und einen **License**-Link. Die Zahl gibt die Anzahl der lizenzbezogenen Probleme an.



Schritte

1. Die Lizenzseite ist über eine der folgenden Möglichkeiten zugänglich:
   - **Wartung** > **System** > **Lizenz** auswählen.
   - ${post_edited_translations.segment}

     ${post_edited_translations.segment}

2. Schreibgeschützte Details zur aktuellen Lizenz:
    - StorageGRID System-ID, die die eindeutige Identifikationsnummer für diese StorageGRID Installation ist
    - Lizenzseriennummer
    - Lizenztyp, entweder **Dauerlizenz** oder **Abonnement**
    - ${post_edited_translations.segment}
    - Unterstützte Speicherkapazität
    - Ablaufdatum der Lizenz. **N/A** wird für eine unbefristete Lizenz angezeigt.
    - Support-Enddatum

      Dieses Datum wird aus der aktuellen Lizenzdatei gelesen und kann veraltet sein, wenn der Support-Servicevertrag nach dem Erhalt der Lizenzdatei verlängert oder erneuert wurde. Zum Aktualisieren dieses Werts siehe "${post_edited_translations.segment}". Das tatsächliche Vertragsende lässt sich auch mit Active IQ anzeigen.

    - Inhalt der Lizenztextdatei

${post_edited_translations.segment}

Sie müssen die Lizenzinformationen für Ihr StorageGRID System jedes Mal 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.
- Du hast "spezifische Zugriffsberechtigungen".
- Sie besitzen die Bereitstellungspassphrase.

Schritte

1. **Wartung** > **System** > **Lizenz** auswählen.
2. Im Abschnitt „Lizenz aktualisieren“ **Durchsuchen** auswählen.
3. Suchen und wählen Sie die neue Lizenzdatei (`.txt` aus.

   Die neue Lizenzdatei wird validiert und angezeigt.

4. ${post_edited_translations.segment}
5. **Speichern** auswählen.

Die API verwenden

Verwenden Sie die StorageGRID Grid Management API

Systemmanagement-Aufgaben können mithilfe der Grid Management REST API anstelle der Grid Manager Benutzeroberfläche durchgeführt werden. Beispielsweise kann die API verwendet werden, um Vorgänge zu automatisieren oder mehrere Entitäten, wie

Benutzer, schneller zu erstellen.

Ressourcen der obersten Ebene

Die Grid Management API stellt die folgenden Ressourcen der obersten Ebene bereit:

- `/grid`: Der Zugriff ist auf Grid Manager Benutzer beschränkt und basiert auf den konfigurierten Gruppenberechtigungen.
- `/org`: Der Zugriff ist auf Benutzer beschränkt, die einer lokalen oder föderierten LDAP-Gruppe für ein Mandantenkonto angehören. Weitere Informationen finden sich unter "Ein Mandantenkonto verwenden".
- `/private`: Der Zugriff ist auf Grid Manager-Benutzer beschränkt und basiert auf den konfigurierten Gruppenberechtigungen. Die privaten APIs können sich ohne Vorankündigung ändern. StorageGRID private Endpunkte ignorieren außerdem die API-Version der Anfrage.

API-Anfragen ausführen

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

Die Swagger-Benutzeroberfläche bietet vollständige Details und Dokumentation für jede API-Operation.

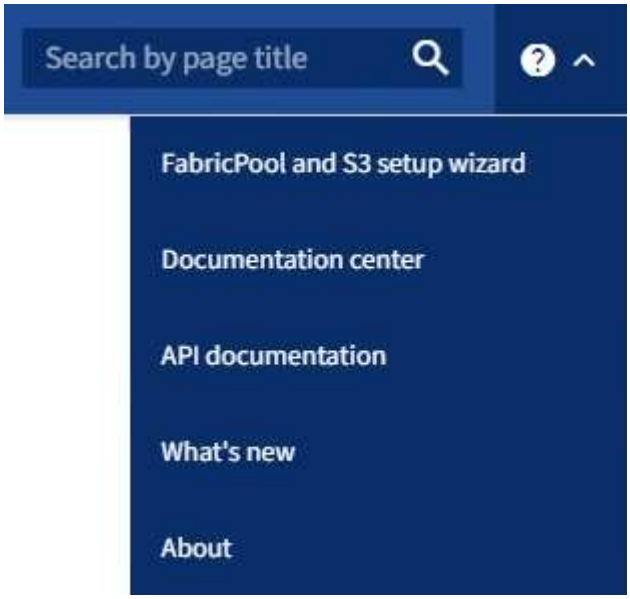
Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Du hast "spezifische Zugriffsberechtigungen".

> Alle API-Operationen, die Sie über die API-Dokumentationswebseite durchführen, sind Live-Operationen. Es ist darauf zu achten, dass Konfigurationsdaten oder andere Daten nicht versehentlich erstellt, aktualisiert oder gelöscht werden.

Schritte

1. Im Grid Manager Header das Hilfesymbol auswählen und anschließend **API-Dokumentation** wählen.



2. Um eine Operation mit der privaten API durchzuführen, auf der StorageGRID Management API-Seite **Zur**

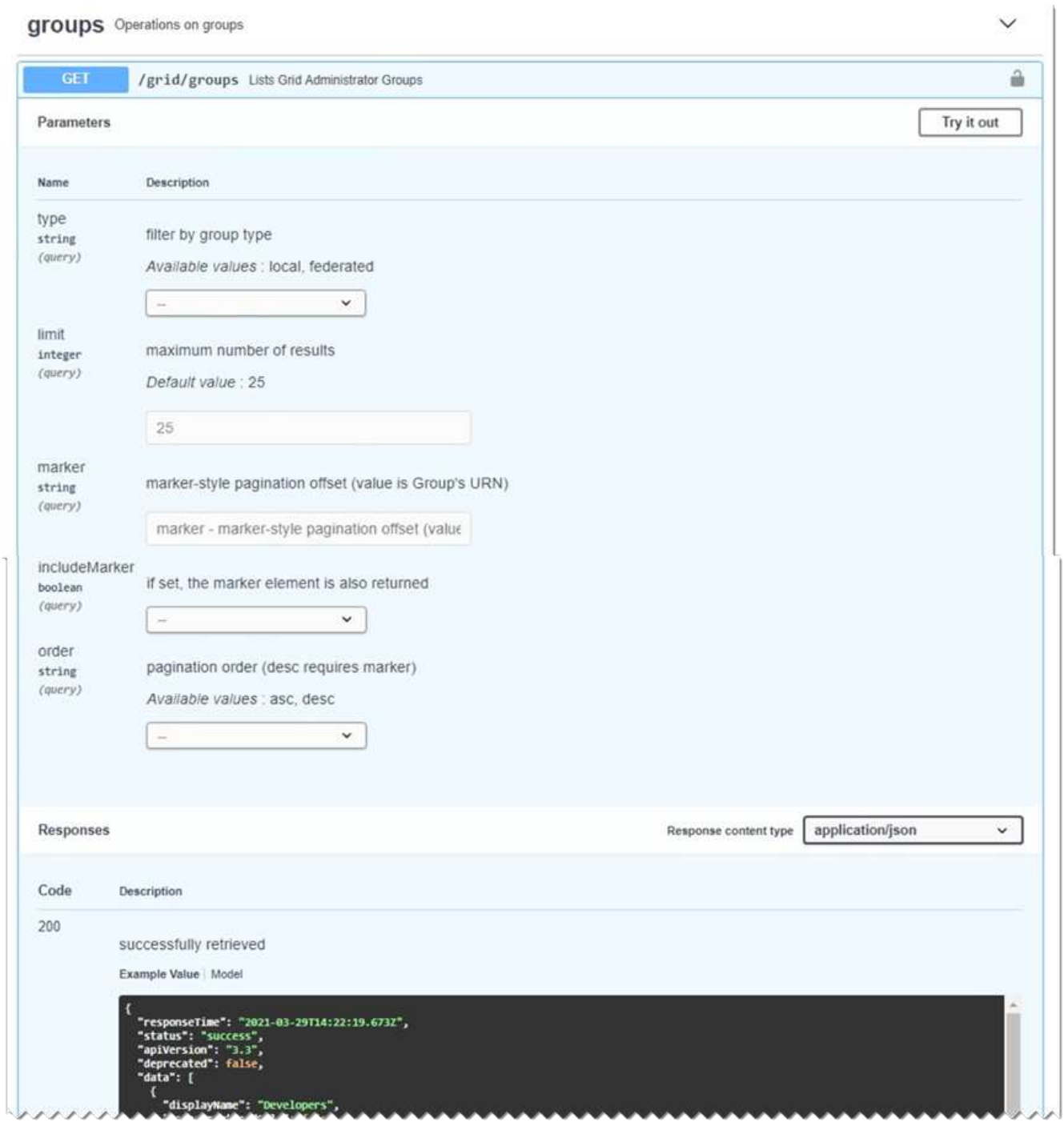
Dokumentation der privaten API gehen auswählen.

Die privaten APIs können sich ohne Vorankündigung ändern. Private Endpunkte von StorageGRID ignorieren außerdem die API-Version der Anfrage.

3. Den gewünschten Vorgang auswählen.

   Wenn eine API-Operation erweitert wird, sind die verfügbaren HTTP-Aktionen wie GET, PUT, UPDATE und DELETE sichtbar.

4. Eine HTTP-Aktion kann ausgewählt werden, um die Anfragedetails einschließlich der Endpunkt-URL, einer Liste aller erforderlichen oder optionalen Parameter, eines Beispiels für den Anfragetext (falls erforderlich) und der möglichen Antworten anzuzeigen.



5. Es ist zu ermitteln, ob die Anforderung zusätzliche Parameter wie eine Gruppen- oder Benutzer-ID erfordert. Anschließend sind diese Werte abzurufen. Möglicherweise muss zuerst eine andere API-Anforderung gesendet werden, um die benötigten Informationen zu erhalten.
6. Es kann geprüft werden, ob der Beispiel-Anfragetext angepasst werden muss. Ist dies der Fall, steht **Model** zur Verfügung, um die Anforderungen für jedes Feld anzuzeigen.
7. **Ausprobieren** auswählen.
8. Alle erforderlichen Parameter können angegeben oder der Anfragetext nach Bedarf angepasst werden.
9. **Ausführen** auswählen.
10. Der Antwortcode gibt Aufschluss darüber, ob die Anfrage erfolgreich war.

Grid Management API-Operationen in StorageGRID

${post_edited_translations.segment}

Diese Liste enthält nur Operationen, die in der öffentlichen API verfügbar sind.

- **Konten**: Vorgänge zur Verwaltung von Speicher-Mandantenkonten, einschließlich der Erstellung neuer Konten und des Abrufs der Speichernutzung für ein bestimmtes Konto.
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- **alert-silences**: Vorgänge bei Alarm-Stummschaltungen.
- **Warnungen**: Vorgänge bei Warnmeldungen.
- **audit**: Vorgänge zum Auflisten und Aktualisieren der Audit-Konfiguration.
- **auth**: Operationen zur Durchführung der Benutzersitzungsauthentifizierung.

  Die Grid Management API unterstützt das Bearer Token Authentifizierungsschema. Für die Anmeldung werden ein Benutzername und ein Passwort im JSON-Body der Authentifizierungsanfrage angegeben (das heißt, `POST /api/v3/authorize`). Wenn der Benutzer erfolgreich authentifiziert wurde, wird ein Sicherheitstoken zurückgegeben. Dieses Token muss im Header nachfolgender API-Anfragen bereitgestellt werden ("Authorization: Bearer *token*"). Das Token läuft nach 16 Stunden ab.

  Wenn Single Sign-On für das StorageGRID System aktiviert ist, sind andere Schritte zur Authentifizierung erforderlich. Siehe „Authentifizierung an der API, wenn Single Sign-On aktiviert ist“.

  Weitere Informationen zur Verbesserung der Sicherheit bei der Authentifizierung finden Sie unter „Schutz vor Cross-Site Request Forgery“.

- **Clientzertifikate**: Vorgänge zur Konfiguration von Clientzertifikaten, sodass StorageGRID mithilfe externer Überwachungstools sicher aufgerufen werden kann.
- **config**: Operationen im Zusammenhang mit der Produktfreigabe und den Versionen der Grid Management API. Es besteht die Möglichkeit, die Produktfreigabeversion sowie die von dieser Freigabe unterstützten Hauptversionen der Grid Management API aufzulisten und veraltete Versionen der API zu deaktivieren.
- **deactivated-features**: Vorgänge zum Anzeigen von Funktionen, die möglicherweise deaktiviert wurden.
- **dns-servers**: Vorgänge zum Auflisten und Ändern konfigurierter externer DNS-Server.

- ${post_edited_translations.segment}
- **endpoint-domain-names**: Operationen zum Auflisten und Ändern von S3-Endpunkt-Domänennamen.
- ${post_edited_translations.segment}
- **Expansion**: Operationen bei der Expansion (Prozedurebene).
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- **grid-networks**: Vorgänge zum Auflisten und Ändern der Grid-Netzwerkliste.
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- **ilm**: Vorgänge im Bereich des Information Lifecycle Management (ILM).
- **in-progress-procedures**: Ruft die Wartungsverfahren ab, die derzeit in Bearbeitung sind.
- ${post_edited_translations.segment}
- **Protokolle**: Vorgänge zum Sammeln und Herunterladen von Protokolldateien.v
- **Metriken**: Operationen an StorageGRID-Metriken, einschließlich sofortiger Metrikabfragen zu einem bestimmten Zeitpunkt und Bereichsabfragen von Metriken über einen Zeitraum. Die Grid Management API verwendet das Systemüberwachungstool Prometheus als Backend-Datenquelle. Informationen zur Erstellung von Prometheus-Abfragen sind auf der Prometheus-Website verfügbar.

  > Metriken, die *`private`* in ihrem Namen enthalten, sind ausschließlich für den internen Gebrauch bestimmt. Diese Metriken können sich zwischen StorageGRID Versionen ohne Vorankündigung ändern.

- **Knotendetails**: Operationen an Knotendetails.
- **Knotengesundheit**: Vorgänge zum Status der Knotengesundheit.
- **node-storage-state**: Vorgänge zum Speicherstatus des Knotens.
- **ntp-servers**: Operationen zum Auflisten oder Aktualisieren externer Network Time Protocol (NTP) Server.
- **Objekte**: Vorgänge an Objekten und Objektmetadaten.
- **Wiederherstellung**: Vorgänge für das Wiederherstellungsverfahren.
- **Wiederherstellungspaket**: Vorgänge zum Herunterladen des Wiederherstellungspakets.
- **Regionen**: Vorgänge zum Anzeigen und Erstellen von Regionen.
- **s3-object-lock**: Vorgänge an globalen S3 Object Lock-Einstellungen.
- **Serverzertifikat**: Vorgänge zum Anzeigen und Aktualisieren von Grid Manager Serverzertifikaten.
- **snmp**: Vorgänge an der aktuellen SNMP Konfiguration.
- **storage-watermarks**: Wasserzeichen für Storage-Node.
- **traffic-classes**: Vorgänge für Richtlinien zur Verkehrsklassifizierung.
- **untrusted-client-network**: Vorgänge an der Konfiguration des nicht vertrauenswürdigen Client-Netzwerks.
- **Benutzer**: Vorgänge zum Anzeigen und Verwalten von Grid Manager Benutzern.

Versionierung der Grid Management API in StorageGRID

Die Grid Management API verwendet Versionierung, um unterbrechungsfreie Upgrades zu unterstützen.

Beispielsweise gibt diese Request-URL die Version 4 der API an.

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

Die Hauptversion der API wird erhöht, wenn Änderungen vorgenommen werden, die nicht mit älteren Versionen kompatibel sind. Die Nebenversion der API wird erhöht, wenn Änderungen vorgenommen werden, die mit älteren Versionen kompatibel sind. Kompatible Änderungen umfassen das Hinzufügen neuer Endpunkte oder neuer Eigenschaften.

Das folgende Beispiel veranschaulicht, wie die API-Version je nach Art der vorgenommenen Änderungen erhöht wird.

Art der Änderung an der API	${post_edited_translations.segment}	Neue Version
${post_edited_translations.segment}	2,1	2,2
Nicht kompatibel mit älteren Versionen	2,1	3,0

Bei der erstmaligen Installation der StorageGRID Software ist nur die neueste Version der API aktiviert. Wenn jedoch ein Upgrade auf eine neue Funktionsversion von StorageGRID erfolgt, bleibt der Zugriff auf die ältere API-Version für mindestens eine StorageGRID Funktionsversion erhalten.

> Sie können die unterstützten Versionen konfigurieren. Im Abschnitt **config** der Swagger API-Dokumentation "Grid Management API" finden sich weitere Informationen. Die Unterstützung für die ältere Version sollte nach der Aktualisierung aller API-Clients auf die neuere Version deaktiviert werden.

Veraltete Anfragen werden auf folgende Weise als veraltet gekennzeichnet:

- Der Antwortheader ist „Deprecated: true“.
- Der JSON-Antworttext enthält "deprecated": true
- Eine Warnung bezüglich veralteter Technologien wird in nms.log hinzugefügt. Zum Beispiel:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

${post_edited_translations.segment}

Die `GET /versions`API-Anfrage gibt eine Liste der unterstützten API-Hauptversionen zurück. 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
  ]
}
```

Eine API-Version für eine Anfrage angeben

Sie können die API-Version mit einem Pfadparameter (`/api/v4`) oder einem Header (`Api-Version: 4`) angeben. Wenn beide Werte angegeben werden, überschreibt der Wert im Header den Wert im Pfad.

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

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Schutz vor Cross-Site Request Forgery (CSRF) in StorageGRID

Sie können zum Schutz vor Cross-Site-Request-Forgery-Angriffen (CSRF) auf StorageGRID beitragen, indem Sie CSRF-Token verwenden, um die Authentifizierung über Cookies zu verbessern. Der Grid Manager und der Tenant Manager aktivieren diese Sicherheitsfunktion automatisch; andere API-Clients können beim Anmelden auswählen, ob sie diese aktivieren möchten.

${post_edited_translations.segment}

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

Um die Funktion zu aktivieren, legen Sie den Parameter `csrfToken` während der Authentifizierung auf `true` fest. 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 dieser Wert auf „true“ festgelegt ist, wird ein `GridCsrfToken`-Cookie mit einem zufälligen Wert für Anmeldungen beim Grid Manager gesetzt, und das `AccountCsrfToken`-Cookie wird mit einem zufälligen Wert für Anmeldungen beim Tenant Manager gesetzt.

${post_edited_translations.segment}

- Der `X-Csrf-Token`-Header, wobei der Wert des Headers auf den Wert des CSRF-Token-Cookies festgelegt ist.
- Für Endpunkte, die einen formularcodierten Body akzeptieren: Ein `csrfToken` formularcodierter Anfragekörperparameter.

Zusätzliche Beispiele und Details sind in der Online-API-Dokumentation zu finden.

${post_edited_translations.segment}

Die API kann verwendet werden, wenn Single Sign-On aktiviert ist.

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

Wenn Sie "Single Sign-On (SSO) konfiguriert und aktiviert" haben und Active Directory als SSO-Anbieter verwenden, müssen Sie eine Reihe von API-Anfragen senden, um ein Authentifizierungstoken zu erhalten, das für die Grid Management API oder die Tenant Management API gültig ist.

Bei aktivierter Single Sign-On-Funktion erfolgt die Anmeldung an der API.

${post_edited_translations.segment}

Bevor Sie beginnen

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

Über diese Aufgabe

Um ein Authentifizierungs-Token zu erhalten, kann eines der folgenden Beispiele verwendet werden:

- Das `storagegrid-ssoauth.py` Python-Skript befindet sich im StorageGRID Installationsverzeichnis (`./rpms` für RHEL, `./debs` für Ubuntu oder Debian und `./vsphere` für VMware.
- Ein Beispielworkflow für curl-Anfragen.

  Der curl Workflow kann zu einem Timeout führen, wenn er zu langsam ausgeführt wird. Möglicherweise

wird folgender Fehler angezeigt: `A valid SubjectConfirmation was not found on this Response`.

> Der im Beispiel gezeigte curl Workflow schützt das Passwort nicht davor, von anderen Benutzern eingesehen zu werden.

Wenn ein Problem mit der URL-Codierung vorliegt, wird möglicherweise folgender Fehler angezeigt: `Unsupported SAML version`.

Schritte

1. Wählen Sie eine der folgenden Methoden, um ein Authentifizierungstoken zu erhalten:
   - Das Python-Skript `storagegrid-ssoauth.py` verwenden. Weiter mit Schritt 2.
   - Verwenden Sie curl Anfragen. Wechseln Sie zu Schritt 3.
2. Wenn Sie das `storagegrid-ssoauth.py` Skript verwenden möchten, übergeben Sie das Skript an den Python-Interpreter und führen das Skript aus.

   Geben Sie bei Aufforderung Werte für die folgenden Argumente ein:

   - Die SSO-Methode. ADFS oder adfs eingeben.
   - Der SSO Benutzername
   - Die Domäne, in der StorageGRID installiert ist
   - Die Adresse für StorageGRID
   - Die Mandantenkonto-ID, falls Sie auf die Tenant Management 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 Autorisierungstoken wird in der Ausgabe bereitgestellt. Sie können das Token nun für andere Anfragen verwenden, ähnlich wie Sie die API verwenden würden, wenn kein SSO verwendet wird.

3. ${post_edited_translations.segment}

   a. ${post_edited_translations.segment}

```
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'
```

Für den Zugriff auf die Grid Management API ist 0 als `TENANTACCOUNTID` zu verwenden.

b. Um eine signierte Authentifizierungs-URL zu erhalten, wird eine POST-Anfrage an `/api/v3/authorize-saml` gesendet und die zusätzliche JSON-Codierung aus der Antwort entfernt.

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-Codierungsschicht.

```
{
    "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. Den `SAMLRequest` aus der Antwort für die Verwendung in nachfolgenden Befehlen speichern.

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

d. Eine vollständige URL mit der Client Request-ID von AD FS erhalten.

Eine Möglichkeit besteht darin, das Anmeldeformular mit der URL aus der vorherigen Antwort anzufordern.

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

Die Antwort enthält 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. Die Client-Anforderungs-ID aus der Antwort speichern.

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

f. Ihre Zugangsdaten werden an die Formularaktion aus der vorherigen Antwort gesendet.

```
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 302-Weiterleitung zurück, mit zusätzlichen Informationen in den Headern.

Wenn für Ihr SSO-System die Multi-Faktor-Authentifizierung (MFA) aktiviert ist, enthält das Formular ebenfalls das zweite Passwort oder andere Anmeldeinformationen.

```
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. Den `MSISAuth`Cookie aus der Antwort speichern.

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

h. Eine GET-Anfrage wird an den angegebenen Speicherort mit den Cookies aus dem Authentifizierung-POST gesendet.

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

Die Antwortheader enthalten AD FS-Sitzungsinformationen für die spätere Abmeldung, und der Antworttext enthält die SAMLResponse in einem versteckten 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. Die Daten `SAMLResponse` aus dem versteckten Feld speichern:

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

j. Mit den gespeicherten `SAMLResponse` kann eine StorageGRID`/api/saml-response`-Anfrage gestellt werden, um ein StorageGRID Authentifizierungs-Token zu generieren.

   Für `RelayState` verwenden Sie die Mandantenkonto-ID oder 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 enthält das Authentifizierungs-Token.

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

a. Das Authentifizierungstoken in der Antwort als `MYTOKEN` speichern.

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

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

${post_edited_translations.segment}

Wenn Single Sign-On (SSO) aktiviert wurde, müssen Sie eine Reihe von API-Anfragen senden, um sich von der Grid Management API oder der Tenant Management API abzumelden. Diese Anweisungen gelten, wenn Sie Active Directory als SSO-Identitätsanbieter verwenden

Über diese Aufgabe

Bei Bedarf können Sie sich von der StorageGRID API abmelden, indem Sie sich über die Single-Logout-Seite Ihrer Organisation abmelden. Alternativ können Sie das Single Logout (SLO) von StorageGRID auslösen, wofür ein gültiges StorageGRID Bearer-Token erforderlich ist.

Schritte

1. Um eine signierte Abmeldeanfrage zu generieren, wird `cookie "sso=true"` an die SLO API übergeben:

```
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
```

Eine Abmelde-URL wird 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. ${post_edited_translations.segment}

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

3. Eine Anfrage an die Logout-URL senden, um SLO auszulösen und zurück zu StorageGRID zu gelangen.

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

Es wird der Statuscode 302 zurückgegeben. Die Weiterleitungsadresse gilt nicht für die Abmeldung ausschließlich über die API.

```
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. ${post_edited_translations.segment}

Das Löschen des StorageGRID Bearer-Tokens funktioniert auf dieselbe Weise wie ohne SSO. Wenn das Cookie "sso=true" nicht bereitgestellt wird, wird der Benutzer von StorageGRID abgemeldet, ohne dass der SSO-Status beeinträchtigt wird.

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

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

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

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

Wenn Sie über "Single Sign-On (SSO) konfiguriert und aktiviert" verfügen und Entra ID als SSO-Anbieter verwenden, können Sie zwei Beispielskripte verwenden, um ein Authentifizierungstoken abzurufen, das für die Grid Management API oder die Tenant Management API gültig ist.

Anmeldung bei der API, wenn die Entra ID Single Sign-on-Funktion aktiviert ist

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

Bevor Sie beginnen

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

Über diese Aufgabe

${post_edited_translations.segment}

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

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

Um eine eigene API-Integration mit Entra ID zu erstellen, siehe das `storagegrid-ssoauth-azure.py` Skript. Das Python-Skript sendet zwei Anfragen direkt an StorageGRID (zuerst zum Abrufen der SAMLRequest und später zum Abrufen des Autorisierungstokens) und ruft außerdem das Node.js-Skript auf, um mit Entra ID zu interagieren und die SSO-Operationen auszuführen.

SSO-Operationen können mithilfe einer Reihe von API-Anfragen ausgeführt werden, jedoch ist dies nicht unkompliziert. Das Puppeteer Node.js Modul wird verwendet, um die Entra ID SSO-Oberfläche auszulesen.

Wenn ein Problem mit der URL-Codierung vorliegt, wird möglicherweise folgender Fehler angezeigt: `Unsupported SAML version.`

Schritte

1. ${post_edited_translations.segment}
   a. Node.js installieren (siehe "https://nodejs.org/en/download/").

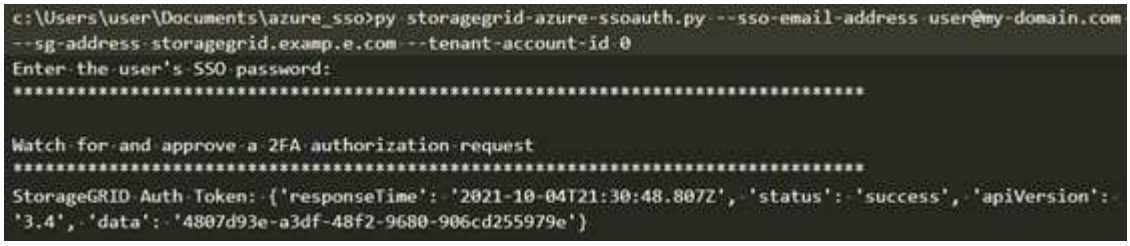
b. Die erforderlichen Node.js Module (puppeteer und jsdom) installieren:

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

2. Das Python-Skript wird dem Python-Interpreter übergeben, um das Skript auszuführen.

   Anschließend ruft das Python-Skript das entsprechende Node.js-Skript auf, um die Entra ID SSO-Interaktionen durchzuführen.

3. ${post_edited_translations.segment}
   - Die SSO-E-Mail-Adresse, die für die Anmeldung bei Entra ID verwendet wird
   - Die Adresse für StorageGRID
   - Die Mandantenkonto-ID, wenn auf die Tenant Management API zugegriffen werden soll
4. ${post_edited_translations.segment}



> Das Skript geht davon aus, dass die Multi-Faktor-Authentifizierung (MFA) mit Microsoft Authenticator durchgeführt wird. Möglicherweise ist eine Anpassung des Skripts erforderlich, um andere Formen der MFA zu unterstützen (wie zum Beispiel die Eingabe eines per SMS erhaltenen Codes).

Das StorageGRID Autorisierungstoken wird in der Ausgabe bereitgestellt. Sie können das Token nun für andere Anfragen verwenden, ähnlich wie Sie die API verwenden würden, wenn kein SSO verwendet wird.

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

Wenn Sie "Single Sign-On (SSO) konfiguriert und aktiviert" haben und PingFederate als SSO-Anbieter verwenden, muss eine Reihe von API-Anfragen gestellt werden, um ein Authentifizierungs-Token zu erhalten, das für die Grid Management API oder die Tenant Management API gültig ist.

Bei aktivierter Single Sign-On-Funktion erfolgt die Anmeldung an der API.

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

Bevor Sie beginnen

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

Über diese Aufgabe

Um ein Authentifizierungs-Token zu erhalten, kann eines der folgenden Beispiele verwendet werden:

- Das `storagegrid-ssoauth.py` Python-Skript befindet sich im StorageGRID Installationsverzeichnis

(`./rpms` für RHEL, `./debs` für Ubuntu oder Debian und `./vsphere` für VMware.

- Ein Beispielworkflow für curl-Anfragen.

  Der curl Workflow kann zu einem Timeout führen, wenn er zu langsam ausgeführt wird. Möglicherweise wird folgender Fehler angezeigt: `A valid SubjectConfirmation was not found on this Response`.

  > Der im Beispiel gezeigte curl Workflow schützt das Passwort nicht davor, von anderen Benutzern eingesehen zu werden.

  Wenn ein Problem mit der URL-Codierung vorliegt, wird möglicherweise folgender Fehler angezeigt: `Unsupported SAML version`.

Schritte

1. Wählen Sie eine der folgenden Methoden, um ein Authentifizierungstoken zu erhalten:
   - Das Python-Skript `storagegrid-ssoauth.py` verwenden. Weiter mit Schritt 2.
   - Verwenden Sie curl Anfragen. Wechseln Sie zu Schritt 3.
2. Wenn Sie das `storagegrid-ssoauth.py` Skript verwenden möchten, übergeben Sie das Skript an den Python-Interpreter und führen das Skript aus.

   Geben Sie bei Aufforderung Werte für die folgenden Argumente ein:

   - Die SSO-Methode. Es kann jede beliebige Variante von "pingfederate" eingegeben werden (PINGFEDERATE, pingfederate und so weiter).
   - Der SSO Benutzername
   - Die Domäne, in der StorageGRID installiert ist. Dieses Feld wird nicht für PingFederate verwendet. Das Feld kann leer bleiben oder es kann ein beliebiger Wert eingegeben werden.
   - Die Adresse für StorageGRID
   - Die Mandantenkonto-ID, falls Sie auf die Tenant Management 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 Autorisierungstoken wird in der Ausgabe bereitgestellt. Sie können das Token nun für andere Anfragen verwenden, ähnlich wie Sie die API verwenden würden, wenn kein SSO verwendet wird.

3. ${post_edited_translations.segment}

   a. ${post_edited_translations.segment}

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```

Für den Zugriff auf die Grid Management API ist 0 als `TENANTACCOUNTID` zu verwenden.

b. Um eine signierte Authentifizierungs-URL zu erhalten, wird eine POST-Anfrage an `/api/v3/authorize-saml` gesendet und die zusätzliche JSON-Codierung aus der Antwort entfernt.

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

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

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

```
{
    "apiVersion": "3.0",
    "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Den `SAMLRequest` aus der Antwort für die Verwendung in nachfolgenden Befehlen speichern.

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

d. Die Antwort und den Cookie exportieren und die Antwort ausgeben:

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

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

e. Den Wert 'pf.adapterId' exportieren und die Antwort ausgeben:

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

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

f. Exportieren Sie den 'href'-Wert (entfernen Sie den abschließenden Schrägstrich /), und geben Sie die Antwort aus:

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

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

g. Den Wert „action“ exportieren:

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

h. Cookies zusammen mit den Anmeldeinformationen senden:

```
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. Die Daten `SAMLResponse` aus dem versteckten Feld speichern:

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

j. Mit den gespeicherten `SAMLResponse` kann eine StorageGRID`/api/saml-response`-Anfrage gestellt werden, um ein StorageGRID Authentifizierungs-Token zu generieren.

   Für `RelayState` verwenden Sie die Mandantenkonto-ID oder 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 enthält das Authentifizierungs-Token.

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

a. Das Authentifizierungstoken in der Antwort als `MYTOKEN` speichern.

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

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

${post_edited_translations.segment}

Wenn Single Sign-On (SSO) aktiviert wurde, müssen Sie eine Reihe von API-Anfragen senden, um sich von der Grid Management API oder der Tenant Management API abzumelden. Diese Anweisungen gelten, wenn Sie PingFederate als SSO-Identitätsanbieter verwenden

Über diese Aufgabe

Bei Bedarf können Sie sich von der StorageGRID API abmelden, indem Sie sich über die Single-Logout-Seite Ihrer Organisation abmelden. Alternativ können Sie das Single Logout (SLO) von StorageGRID auslösen, wofür ein gültiges StorageGRID Bearer-Token erforderlich ist.

Schritte

1. Um eine signierte Abmeldeanfrage zu generieren, wird `cookie "sso=true"` an die SLO API übergeben:

```
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
```

Eine Abmelde-URL wird 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. ${post_edited_translations.segment}

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Eine Anfrage an die Logout-URL senden, um SLO auszulösen und zurück zu StorageGRID zu gelangen.

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

Es wird der Statuscode 302 zurückgegeben. Die Weiterleitungsadresse gilt nicht für die Abmeldung ausschließlich über die API.

```
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. ${post_edited_translations.segment}

Das Löschen des StorageGRID Bearer-Tokens funktioniert auf dieselbe Weise wie ohne SSO. Wenn das Cookie "sso=true" nicht bereitgestellt wird, wird der Benutzer von StorageGRID abgemeldet, ohne dass der SSO-Status beeinträchtigt wird.

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

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

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

StorageGRID-Funktionen mit der API deaktivieren

Mithilfe der Grid Management API kann die vollständige Deaktivierung bestimmter Funktionen im StorageGRID System erfolgen. Wenn eine Funktion deaktiviert ist, kann niemand Berechtigungen zur Ausführung der mit dieser Funktion verbundenen Aufgaben erhalten.

Über diese Aufgabe

Das System „Deaktivierte Funktionen“ ermöglicht es, den Zugriff auf bestimmte Funktionen im StorageGRID System zu verhindern. Die Deaktivierung einer Funktion ist die einzige Möglichkeit, den Root-Benutzer oder Benutzer, die Administratorgruppen mit **Root access**-Berechtigung angehören, an der Nutzung dieser Funktion zu hindern.

Um zu verstehen, wie diese Funktionalität nützlich sein kann, ist folgendes Szenario zu berücksichtigen:

Unternehmen A ist ein Dienstleister, der die Speicherkapazität seines StorageGRID Systems durch die Erstellung von Mandantenkonten vermietet. Um die Sicherheit der Objekte seiner Mieter zu schützen, möchte Unternehmen A sicherstellen, dass seine eigenen Mitarbeiter nach der Bereitstellung eines Mandantenkontos niemals auf ein Mandantenkonto zugreifen können.

Unternehmen A kann dieses Ziel erreichen, indem die Funktion „Funktionen deaktivieren“ im Grid Management API verwendet wird. Durch die vollständige Deaktivierung der Funktion **Change tenant root password** im Grid Manager (sowohl in der UI als auch in der API) wird sichergestellt, dass Admin-Benutzer – einschließlich des Root-Benutzers und von Benutzern, die Gruppen mit der Berechtigung **Root access** angehören – das Passwort für den Root-Benutzer eines beliebigen Mandantenkontos nicht ändern können.

Schritte

1. Auf die Swagger-Dokumentation für die Grid Management API kann zugegriffen werden. Siehe "Die Grid Management API verwenden".
2. Den Endpunkt „Funktionen deaktivieren“ finden.
3. Um eine Funktion wie das Ändern des Root-Benutzer-Passworts des Mandanten zu deaktivieren, wird ein Body wie folgt an die API gesendet:

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

   Nach Abschluss der Anfrage wird die Funktion „Change tenant root password“ deaktiviert. Die Verwaltungsberechtigung **Change tenant root password** wird nicht mehr in der Benutzeroberfläche angezeigt, und jede API-Anfrage, die versucht, das Root-Passwort eines Mandanten zu ändern, schlägt mit „403 Forbidden“ fehl.

Deaktivierte Funktionen reaktivieren

Standardmäßig kann die Grid Management API verwendet werden, um eine deaktivierte Funktion zu reaktivieren. Wenn jedoch verhindert werden soll, dass deaktivierte Funktionen jemals wieder aktiviert werden, kann die Funktion **activateFeatures** selbst deaktiviert werden.

> Die Funktion **activateFeatures** kann nicht reaktiviert werden. Wenn Sie sich entscheiden, diese Funktion zu deaktivieren, ist zu beachten, dass die Möglichkeit, andere deaktivierte Funktionen erneut zu aktivieren, dauerhaft verloren geht. Um verlorene Funktionen wiederherzustellen, ist der technische Support zu kontaktieren.

Schritte

1. Auf die Swagger-Dokumentation für die Grid Management API kann zugegriffen werden.
2. Den Endpunkt „Funktionen deaktivieren“ finden.
3. Um alle Funktionen wieder zu aktivieren, wird ein Body wie folgt an die API gesendet:

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

   Nach Abschluss dieser Anfrage werden alle Funktionen, einschließlich der Funktion zum Ändern des Mandanten-Root-Passworts, reaktiviert. Die Verwaltungsberechtigung **Change tenant root password** wird nun in der Benutzeroberfläche angezeigt, und jede API-Anfrage, die versucht, das Root-Passwort eines Mandanten zu ändern, ist erfolgreich, sofern der Benutzer über die Verwaltungsberechtigung **Root access** oder **Change tenant root password** verfügt.

> Das vorherige Beispiel bewirkt, dass *alle* deaktivierten Funktionen wieder aktiviert werden. Wenn weitere Funktionen deaktiviert wurden, die deaktiviert bleiben sollen, müssen diese explizit in der PUT-Anfrage angegeben werden. Um beispielsweise die Funktion „Change tenant root password“ wieder zu aktivieren und die storageAdmin Management-Berechtigung weiterhin deaktiviert zu lassen, ist folgende PUT-Anfrage zu senden: `{ "grid": {"storageAdmin": true} }`

Zugriff auf StorageGRID steuern

${post_edited_translations.segment}

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.

Zugriff auf den Grid Manager steuern

Es wird festgelegt, wer auf den Grid Manager und die Grid Management API zugreifen kann, indem Gruppen und Benutzer aus einem Identitätsverbunddienst importiert oder lokale Gruppen und lokale Benutzer eingerichtet werden.

Die Verwendung von "Identitätsföderation" beschleunigt die Einrichtung von "${post_edited_translations.segment}" und "Benutzer", und sie ermöglicht es Benutzern, sich mit vertrauten Anmeldedaten bei StorageGRID anzumelden. Sie können die Identitätsföderation konfigurieren, wenn Sie Active Directory, OpenLDAP oder Oracle Directory Server verwenden.

> ${post_edited_translations.segment}

Sie legen fest, welche Aufgaben jeder Benutzer ausführen darf, indem Sie jeder Gruppe unterschiedliche "Berechtigungen" zuweisen. Beispielsweise können Benutzer einer Gruppe ILM-Regeln verwalten und Benutzer einer anderen Gruppe Wartungsaufgaben durchführen. Ein Benutzer muss mindestens einer Gruppe angehören, um auf das System zugreifen zu können.

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

Single Sign-On aktivieren

Das StorageGRID System unterstützt Single Sign-On (SSO) mithilfe des Security Assertion Markup Language 2.0 (SAML 2.0) Standards. Nachdem Sie "${post_edited_translations.segment}" haben, 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.

Bereitstellungspassphrase ändern

Die Bereitstellungs-Passphrase ist für viele Installations- und Wartungsverfahren sowie für das Herunterladen des StorageGRID Recovery-Pakets erforderlich. Die Passphrase ist auch erforderlich, um Backups der Grid-Topologieinformationen und Verschlüsselungsschlüssel für das StorageGRID System herunterzuladen. Sie können "die Passphrase ändern" nach Bedarf.

Passwörter für die Node Konsole ändern

Jeder Knoten in Ihrem Grid verfügt über ein Knotenkonsolen-Passwort, das Sie benötigen, um sich über SSH als „admin“ am Knoten anzumelden, oder als Root-Benutzer bei einer VM-Verbindung oder einer physischen Konsolenverbindung. Bei Bedarf können Sie "${post_edited_translations.segment}" für jeden Knoten.

Ändern Sie die StorageGRID Bereitstellungspassphrase

Mit diesem Verfahren lässt sich die StorageGRID Bereitstellungspassphrase ändern. Die Passphrase ist für Wiederherstellungs-, Erweiterungs- und Wartungsverfahren erforderlich. Die Passphrase ist außerdem erforderlich, um Backups des Wiederherstellungspakets herunterzuladen, die die Grid-Topologieinformationen, die Passwörter der Grid-Knotenkonsolen und die Verschlüsselungsschlüssel für das StorageGRID System enthalten.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie verfügen über Wartungs- oder Root-Zugriffsberechtigungen.
- Sie besitzen die aktuelle Bereitstellungspassphrase.

Über diese Aufgabe

Die Bereitstellungspassphrase wird für viele Installations- und Wartungsvorgänge sowie für "Herunterladen des Wiederherstellungspakets" benötigt. Die Bereitstellungspassphrase ist nicht in der `Passwords.txt` Datei aufgeführt. Die Bereitstellungspassphrase sollte dokumentiert und an einem sicheren Ort aufbewahrt werden.

Schritte

1. **Konfiguration** > **Zugriffskontrolle** > **Grid Passwörter** auswählen.
2. Unter **Bereitstellungspassphrase ändern** die Option **Änderung vornehmen** auswählen
3. Geben Sie Ihre aktuelle Bereitstellungs Passphrase ein.
4. Geben Sie die neue Passphrase ein. Die Passphrase muss mindestens 8 und höchstens 32 Zeichen lang sein. Bei Passphrasen wird zwischen Groß- und Kleinschreibung unterschieden.

Die Bereitstellungspassphrase ist an einem sicheren Ort aufzubewahren. Sie wird für Installations-, Erweiterungs- und Wartungsverfahren benötigt.

5. Die neue Passphrase erneut eingeben und **Speichern** auswählen.

   Das System zeigt ein grünes Erfolgsbanner an, wenn die Änderung der Bereitstellungspassphrase abgeschlossen ist.

6. **Wiederherstellungspaket** auswählen.
7. Geben Sie die neue Bereitstellungs-Passphrase ein, um das neue Wiederherstellungspaket herunterzuladen.

> Nach der Änderung der Bereitstellungspassphrase muss umgehend ein neues Wiederherstellungspaket heruntergeladen werden. Die Wiederherstellungspaketdatei ermöglicht die Wiederherstellung des Systems im Fehlerfall.

Konsolenpasswörter für Knoten in StorageGRID ändern

Jeder Knoten in Ihrem Grid verfügt über ein Knotenkonsolenpasswort, das zum Anmelden am Knoten verwendet wird. Standardmäßig hat jeder Knoten ein eindeutiges Passwort. Jedes Passwort kann in ein neues eindeutiges Passwort geändert werden, oder das Passwort für alle Knoten kann auf ein globales Passwort gesetzt werden. Die Passwörter werden im Wiederherstellungspaket gespeichert.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "${post_edited_translations.segment}".
- Sie besitzen die aktuelle Bereitstellungspassphrase.

Über diese Aufgabe

Sie verwenden ein Node-Konsolenpasswort, um sich per SSH als „admin“ an einem Node anzumelden oder als Root-Benutzer über eine VM/physische Konsolenverbindung. Node-Konsolenpasswörter lassen sich mit einer der folgenden Optionen ändern:

- Zufällige Passwörter werden automatisch auf jeden Knoten angewendet
- ${post_edited_translations.segment}
- Ein eindeutiges Passwort für einen oder mehrere Knoten angeben und anwenden

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

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

Assistenten aufrufen

Schritte

1. **Konfiguration** > **Zugriffskontrolle** > **Grid-Passwörter** auswählen.
2. Unter **Knotenkonsolenpasswörter ändern** die Option **Änderung vornehmen** auswählen.

Aktuelles Wiederherstellungspaket herunterladen

Vor dem Ändern der Konsolenpasswörter sollte das aktuelle Wiederherstellungspaket heruntergeladen werden. Die Passwörter in dieser Datei können verwendet werden, falls der Passwortänderungsprozess für einen Knoten fehlschlägt.

Schritte

1. Geben Sie die Bereitstellungs-Passphrase für Ihr Grid ein.
2. **Wiederherstellungspaket herunterladen** auswählen.
3. Die Wiederherstellungspaketdatei (`.zip`ist an zwei sichere und voneinander getrennte Orte zu kopieren.

> 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 zur Änderung des Passworts aus.
   - **Automatisch**: StorageGRID weist allen Knoten automatisch ein neues, zufälliges Konsolenpasswort zu.
   - **Benutzerdefiniert**: Sie stellen Konsolenpasswörter bereit.

Automatisch

1. Wählen Sie **Weiter**.

Benutzerdefiniert

1. Wählen Sie eine der folgenden Optionen aus:
   - **Globales Konsolenpasswort**: Dasselbe Konsolenpasswort wird auf alle Knoten angewendet.
   - **Eindeutige Konsolenpasswörter**: Auf einem oder mehreren Knoten ein anderes Passwort anwenden.
2. Wenn Sie **Globales Konsolenpasswort** ausgewählt haben, geben Sie das Passwort ein, das Sie für alle Knoten verwenden möchten.
3. Wenn Sie **Eindeutige Konsolenpasswörter** ausgewählt haben, ein eindeutiges Passwort für einen oder mehrere Knoten eingeben.
4. Wählen Sie **Weiter**.

Die Passwortänderung abschließen

1. Wenn das Bestätigungsdialogfeld erscheint, **Ja** auswählen, falls StorageGRID mit dem Ändern der Knotenkonsolenpasswörter beginnen soll.

Dieser Vorgang kann nach seinem Start nicht mehr abgebrochen werden.

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

2. Wenn das neue Wiederherstellungspaket bereit ist, **Neues Wiederherstellungspaket herunterladen** auswählen und das Wiederherstellungspaket speichern.
3. Die `.zip`Datei öffnen.
4. Bestätigen Sie, dass Sie auf die Inhalte zugreifen können, einschließlich der `Passwords.txt` Datei, die die neuen Passwörter für die Node-Konsole enthält.
5. Kopieren Sie die neue Wiederherstellungspaketdatei (`.zip` an zwei sichere und voneinander getrennte Orte.

   Das alte Wiederherstellungspaket darf nicht überschrieben werden.

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

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

   StorageGRID aktualisiert das Passwort für jeden Knoten.

   Tritt während des Aktualisierungsvorgangs ein Fehler auf, zeigt die Fortschrittsanzeige die Anzahl der Knoten an, deren Passwörter nicht geändert werden konnten. Das System versucht automatisch erneut, den Vorgang bei jedem Knoten durchzuführen, bei dem das Passwort nicht geändert werden konnte. Wenn der Vorgang endet und bei einigen Knoten das Passwort weiterhin nicht geändert wurde, erscheint die Schaltfläche **Retry**.

8. Wenn die Aktualisierung des Passworts für einen oder mehrere Knoten fehlgeschlagen ist:
   a. Die in der Tabelle aufgeführten Fehlermeldungen werden angezeigt.
   b. Die Probleme beheben.
   c. **Wiederholen** auswählen.

   Durch erneutes Versuchen werden nur die Passwörter der Knotenkonsole auf den Knoten geändert, bei denen vorherige Passwortänderungsversuche fehlgeschlagen sind.

9. Wenn die Fortschrittsanzeige anzeigt, dass keine Aktualisierungen mehr ausstehen, **Fertigstellen** auswählen.
10. Nachdem die Passwörter der Knotenkonsole für alle Knoten geändert wurden, ist die Datei erstes Wiederherstellungspaket, das Sie heruntergeladen haben zu löschen.

Ändern Sie die SSH-Zugriffspasswörter für StorageGRID Admin Nodes

Durch das Ändern der SSH-Zugriffspasswörter für Admin-Knoten werden auch die eindeutigen internen SSH-Schlüsselsätze für jeden Knoten im Grid aktualisiert. Der primäre Admin-Knoten verwendet diese SSH-Schlüssel, um auf Knoten mithilfe einer

sicheren, passwortlosen Authentifizierung zuzugreifen.

Verwenden Sie einen SSH-Schlüssel, um sich bei einem Node als `admin` oder als Root-Benutzer über eine VM- oder physische Konsolenverbindung anzumelden.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "${post_edited_translations.segment}".
- Sie besitzen die aktuelle Bereitstellungspassphrase.

Über diese Aufgabe

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

Für die SSH-Schlüssel, die zur Kommunikation zwischen den Knoten verwendet werden, gibt es separate SSH-Zugriffspasswörter. Diese werden durch dieses Verfahren nicht geändert.

Assistenten aufrufen

Schritte

1. **Konfiguration** > **Zugriffskontrolle** > **Grid-Passwörter** auswählen.
2. Unter **SSH-Schlüssel ändern** die Option **Änderung vornehmen** auswählen.

Aktuelles Wiederherstellungspaket herunterladen

Vor dem Ändern der SSH-Zugriffsschlüssel sollte das aktuelle Wiederherstellungspaket heruntergeladen werden. Die Schlüssel in dieser Datei können verwendet werden, falls der Schlüsseländerungsprozess für einen Knoten fehlschlägt.

Schritte

1. Geben Sie die Bereitstellungs-Passphrase für Ihr Grid ein.
2. **Wiederherstellungspaket herunterladen** auswählen.
3. Die Wiederherstellungspaketdatei (`.zip`ist an zwei sichere und voneinander getrennte Orte zu kopieren.

> 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 erscheint, **Ja** auswählen, falls die Änderung der SSH-Zugriffsschlüssel gestartet werden soll.

> Dieser Vorgang kann nach seinem Start nicht mehr abgebrochen werden.

SSH-Zugriffsschlüssel ändern

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

Schritte

1. Es kann einige Minuten dauern, bis das neue Wiederherstellungspaket generiert ist.
2. Wenn die Schaltfläche „Neues Wiederherstellungspaket herunterladen“ aktiviert ist, **Neues Wiederherstellungspaket herunterladen** auswählen und die neue Wiederherstellungspaketdatei (`.zip` an zwei sicheren, geschützten und getrennten Orten speichern.
3. Wenn der Download abgeschlossen ist:

   a. Die `.zip`Datei öffnen.

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

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

   > ! Das alte Wiederherstellungspaket darf nicht überschrieben werden.

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

4. Es kann einige Minuten dauern, bis die Schlüssel auf jedem Knoten aktualisiert sind.

   Wenn die Schlüssel für alle Knoten geändert werden, erscheint ein grünes Erfolgsbanner.

   Tritt während des Aktualisierungsprozesses ein Fehler auf, wird in einer Meldung die Anzahl der Knoten angezeigt, deren Schlüssel nicht geändert werden konnten. Das System versucht automatisch erneut, den Vorgang bei jedem Knoten durchzuführen, dessen Schlüssel nicht geändert werden konnte. Wenn der Vorgang endet und bei einigen Knoten der Schlüssel weiterhin nicht geändert wurde, erscheint die Schaltfläche **Retry**.

   Wenn die Schlüsselaktualisierung für einen oder mehrere Knoten fehlgeschlagen ist:

   a. Die in der Tabelle aufgeführten Fehlermeldungen werden angezeigt.

   b. Die Probleme beheben.

   c. **Wiederholen** auswählen.

      Durch das erneute Versuchen werden nur die SSH-Zugriffsschlüssel auf den Knoten geändert, bei denen vorherige Schlüsseländerungsversuche fehlgeschlagen sind.

5. Nachdem die SSH-Zugriffsschlüssel für alle Nodes geändert wurden, muss die erstes Wiederherstellungspaket, das Sie heruntergeladen haben gelöscht werden.
6. Optional kann unter **Wartung** > **System** > **Wiederherstellungspaket** eine zusätzliche Kopie des neuen Wiederherstellungspakets heruntergeladen werden.

Verwenden Sie die Identitätsföderation in StorageGRID

Durch die Verwendung von Identitätsföderation erfolgt die Einrichtung von Gruppen und Benutzern schneller, und Benutzer können sich mit vertrauten Anmeldeinformationen bei StorageGRID anmelden.

Identitätsföderation für Grid Manager konfigurieren

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

Bevor Sie beginnen

- Sie sind beim Grid Manager mit einem "unterstützte Webbrowser" angemeldet.
- Sie haben "spezifische Zugriffsberechtigungen".
- Sie verwenden Active Directory, Microsoft Entra ID, OpenLDAP oder Oracle Directory Server als Identitätsanbieter.

> ⓘ Wenn Sie einen LDAP v3-Dienst nutzen 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 planen, Single Sign-On (SSO) zu aktivieren, wurden die "Anforderungen und Überlegungen für Single Sign-On" überprüft.
- Wenn die Transport Layer Security (TLS) für die Kommunikation mit dem LDAP-Server vorgesehen ist, verwendet der Identitätsanbieter TLS 1.2 oder 1.3. Siehe "Unterstützte Verschlüsselungsverfahren für ausgehende TLS-Verbindungen".

Über diese Aufgabe

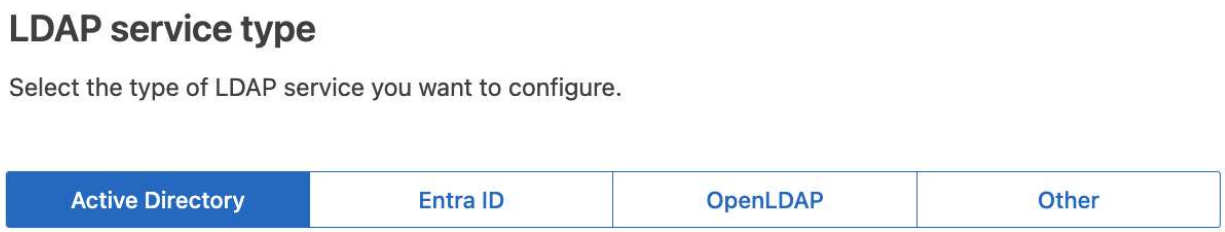
Sie können eine Identitätsquelle für den Grid Manager konfigurieren, wenn Gruppen aus einem anderen System wie Active Directory, Microsoft Entra ID, OpenLDAP oder Oracle Directory Server importiert werden sollen. Die folgenden Gruppentypen können importiert werden:

- Administratorgruppen. Die Benutzer in Administratorgruppen können sich beim Grid Manager anmelden und Aufgaben ausführen, basierend auf den der Gruppe zugewiesenen Verwaltungsberechtigungen.
- Benutzergruppen für Mandanten, die keine eigene Identitätsquelle verwenden. Benutzer in Mandantengruppen können sich beim Tenant Manager anmelden und Aufgaben ausführen, basierend auf den der Gruppe im Tenant Manager zugewiesenen Berechtigungen. Siehe "Mandantenkonto erstellen" und "Ein Mandantenkonto verwenden" für Details.

Konfiguration eingeben

Schritte

1. **Konfiguration** > **Zugriffskontrolle** > **Identitätsföderation** auswählen.
2. **Identitätsföderation aktivieren** auswählen.
3. Im Abschnitt LDAP-Diensttyp wählen Sie den Typ des LDAP-Dienstes aus, den Sie konfigurieren möchten.



Andere kann ausgewählt werden, um Werte für einen LDAP-Server zu konfigurieren, der Oracle Directory Server verwendet.

4. Wenn Sie **Other** ausgewählt haben, füllen Sie die Felder im Abschnitt LDAP-Attribute aus. Andernfalls zum nächsten Schritt wechseln.
   - **Benutzer Unique Name**: Der Name des Attributs, das die eindeutige Kennung eines LDAP-Benutzers enthält. Dieses Attribut entspricht `sAMAccountName` für Active Directory und `uid` für OpenLDAP. Bei der Konfiguration von Oracle Directory Server ist `uid` einzugeben.
   - **Benutzer-UUID**: Der Name des Attributs, das die permanente eindeutige Kennung eines LDAP-Benutzers enthält. Dieses Attribut entspricht `objectGUID` für Active Directory und `entryUUID` für OpenLDAP. Wenn Oracle Directory Server konfiguriert wird, `nsuniqueid` eintragen. Der Wert jedes Benutzers für das angegebene Attribut muss eine 32-stellige Hexadezimalzahl im 16-Byte- oder String-Format sein, wobei Bindestriche ignoriert werden.
   - **Eindeutiger Gruppenname**: Der Name des Attributs, das die eindeutige Kennung einer LDAP-Gruppe enthält. Dieses Attribut entspricht `sAMAccountName` für Active Directory und `cn` für OpenLDAP. Bei der Konfiguration von Oracle Directory Server ist `cn` einzugeben.
   - **Gruppen-UUID**: Der Name des Attributs, das die permanente eindeutige Kennung einer LDAP-Gruppe enthält. Dieses Attribut entspricht `objectGUID` für Active Directory und `entryUUID` für OpenLDAP. Wenn Oracle Directory Server konfiguriert wird, `nsuniqueid` eintragen. Der Wert jeder Gruppe für das angegebene Attribut muss eine 32-stellige Hexadezimalzahl im 16-Byte- oder String-Format sein, wobei Bindestriche ignoriert werden.
5. Für alle LDAP-Diensttypen sind die erforderlichen LDAP-Server- und Netzwerkverbindungsinformationen im Abschnitt „LDAP-Server konfigurieren“ anzugeben.
   - **Hostname**: Der vollqualifizierte Domainname (FQDN) oder die IP-Adresse des LDAP-Servers.
   - **Port**: Der Port, der zur Verbindung mit dem LDAP-Server verwendet wird.

     Der Standardport für STARTTLS ist 389, und der Standardport für LDAPS ist 636. Allerdings kann jeder beliebige Port verwendet werden, sofern die Firewall korrekt konfiguriert ist.

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

     Für Active Directory können Sie auch den Down-Level Logon Name oder den User Principal Name angeben.

     Der angegebene Benutzer muss die Berechtigung haben, Gruppen und Benutzer aufzulisten und auf die folgenden Attribute zuzugreifen:

- `sAMAccountName` oder `uid`
- `objectGUID`, `entryUUID`, oder `nsuniqueid`
- `cn`
- `memberOf` oder `isMemberOf`
- **Active Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, und `userPrincipalName`
- **Entra ID**: `accountEnabled` und `userPrincipalName`

◦ **Passwort**: Das zum Benutzernamen gehörende Passwort.

> Wenn Sie das Passwort in Zukunft ändern, muss es auf dieser Seite aktualisiert werden.

◦ **Gruppenbasis-DN**: Der vollständige Pfad des individuellen Namens (DN) eines LDAP-Teilbaums, in dem nach Gruppen gesucht werden soll. Im folgenden Active Directory-Beispiel können alle Gruppen, deren individueller Name relativ zum Basis-DN (DC=storagegrid,DC=example,DC=com) ist, als föderierte Gruppen verwendet werden.

> Die Werte für den **eindeutigen Gruppennamen** müssen innerhalb des **Gruppenbasis-DN**, zu dem sie gehören, eindeutig sein.

◦ **User Base DN**: Der vollständige Pfad des individuellen Namens (DN) eines LDAP-Teilbaums, in dem nach Benutzern gesucht werden soll.

> Die Werte für den **Benutzer eindeutigen Namen** müssen innerhalb der **Benutzerbasis-DN**, zu der sie gehören, eindeutig sein.

◦ **Bind-Benutzernamenformat** (optional): Das Standard-Benutzernamensmuster, das StorageGRID verwenden sollte, wenn das Muster nicht automatisch ermittelt werden kann.

Die Angabe des **Bind-Benutzernamenformats** wird empfohlen, da dies Benutzern die Anmeldung ermöglicht, falls StorageGRID keine Bindung mit dem Dienstkonto herstellen kann.

Eines dieser Muster kann eingegeben werden:

- **UserPrincipalName-Muster (AD und Entra ID)**: `[USERNAME]@*example*.com`
- **Namensmuster für die Anmeldung auf niedrigerer Ebene (AD und Entra ID)**: `*example*\[USERNAME]`
- **Individueller Name Muster**: `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

  [USERNAME] muss exakt wie angegeben übernommen werden.

6. Im Abschnitt Transport Layer Security (TLS) eine Sicherheitseinstellung auswählen.
   ◦ **STARTTLS verwenden**: STARTTLS sichert die Kommunikation mit dem LDAP-Server. Dies ist die empfohlene Option für Active Directory, OpenLDAP oder Other, wird jedoch für Microsoft Entra ID nicht unterstützt.
   ◦ **LDAPS verwenden**: Die Option LDAPS (LDAP über SSL) verwendet TLS, um eine Verbindung zum LDAP-Server herzustellen. Diese Option ist für Microsoft Entra ID erforderlich.

- **Kein TLS verwenden**: Der Netzwerkverkehr zwischen dem StorageGRID System und dem LDAP-Server ist nicht gesichert. Diese Option wird für Microsoft Entra ID nicht unterstützt.

> Die Option **TLS nicht verwenden** wird nicht unterstützt, wenn Ihr Active Directory Server die LDAP-Signierung erzwingt. STARTTLS oder LDAPS ist erforderlich.

7. Wenn Sie STARTTLS oder LDAPS ausgewählt haben, wählen Sie das Zertifikat aus, das zur Sicherung der Verbindung verwendet wird.
   - **CA-Zertifikat des Betriebssystems verwenden**: Das standardmäßig auf dem Betriebssystem installierte Grid-CA-Zertifikat wird verwendet, um Verbindungen abzusichern.
   - **Benutzerdefiniertes CA-Zertifikat verwenden**: Ein benutzerdefiniertes Sicherheitszertifikat wird verwendet.

     Wenn diese Einstellung ausgewählt wird, das benutzerdefinierte Sicherheitszertifikat in das Textfeld für das CA-Zertifikat kopieren und einfügen.

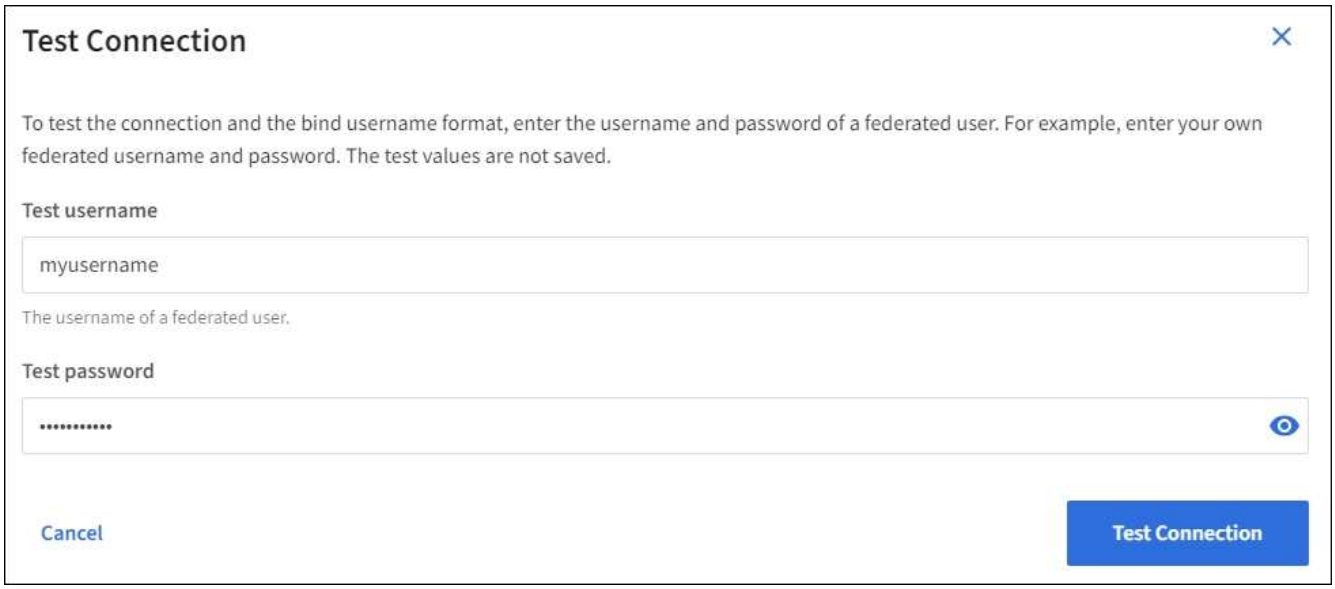
Die Verbindung testen und die Konfiguration speichern

Nach Eingabe aller Werte muss die Verbindung getestet werden, bevor die Konfiguration gespeichert werden kann. StorageGRID überprüft die Verbindungseinstellungen für den LDAP-Server und das Format des Bind-Benutzernamens, sofern einer angegeben wurde.

Schritte

1. **Verbindung testen** auswählen.
2. Falls Sie kein Bind-Benutzernamenformat angegeben haben:
   - Die Meldung „Verbindungstest erfolgreich“ erscheint, wenn die Verbindungseinstellungen gültig sind. **Speichern** auswählen, um die Konfiguration zu speichern.
   - Die Meldung „Testverbindung konnte nicht hergestellt werden“ erscheint, wenn die Verbindungseinstellungen ungültig sind. **Schließen** auswählen. Anschließend etwaige Probleme beheben und die Verbindung erneut testen.
3. Wenn ein Bind-Benutzernamensformat angegeben wurde, sind der Benutzername und das Passwort eines gültigen Verbundbenutzers einzugeben.

   Geben Sie beispielsweise Ihren eigenen Benutzernamen und Ihr eigenes Passwort ein. Im Benutzernamen dürfen keine Sonderzeichen wie @ oder / enthalten sein.



- Die Meldung „Verbindungstest erfolgreich“ erscheint, wenn die Verbindungseinstellungen gültig sind. **Speichern** auswählen, um die Konfiguration zu speichern.
- Eine Fehlermeldung erscheint, wenn die Verbindungseinstellungen, das Format des Bind-Benutzernamens oder der Testbenutzername und das Testpasswort ungültig sind. Nach Behebung aller Probleme kann die Verbindung erneut getestet werden.

Synchronisierung mit der Identitätsquelle erzwingen

Das StorageGRID System synchronisiert periodisch föderierte Gruppen und Benutzer aus der Identitätsquelle. Sie können den Start der Synchronisierung erzwingen, wenn Sie Benutzerberechtigungen so schnell wie möglich aktivieren oder einschränken möchten.

Schritte

1. Zur Seite „Identitätsföderation“ wechseln.
2. Oben auf der Seite **Sync server** auswählen.

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

   Die Warnung **Fehler bei der Synchronisierung der Identitätsföderation** wird ausgelöst, wenn ein Problem bei der Synchronisierung von föderierten Gruppen und Benutzern aus der Identitätsquelle auftritt.

Identitätsföderation deaktivieren

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. Die von Ihnen konfigurierten Einstellungen bleiben jedoch erhalten, was eine einfache erneute Aktivierung der Identitätsföderation in der Zukunft ermöglicht.

Über diese Aufgabe

Bevor Sie die Identitätsföderation deaktivieren, ist Folgendes zu beachten:

- Verbundbenutzer können sich nicht anmelden.
- Verbundbenutzer, die aktuell angemeldet sind, behalten den Zugriff auf das StorageGRID System bis zum

Ablauf ihrer Sitzung, können sich aber nach Ablauf ihrer Sitzung nicht mehr anmelden.

- Eine Synchronisierung zwischen dem StorageGRID System und der Identitätsquelle findet nicht 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. Siehe "Single Sign-On deaktivieren".

Schritte

1. Zur Seite „Identitätsföderation“ wechseln.
2. ${post_edited_translations.segment}

Richtlinien für die Konfiguration eines OpenLDAP Servers

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

> Bei Identitätsquellen, die weder Active Directory noch Microsoft Entra ID sind, blockiert StorageGRID den S3-Zugriff für extern deaktivierte Benutzer nicht automatisch. Zum Blockieren des S3-Zugriffs müssen alle S3-Schlüssel des Benutzers gelöscht oder der Benutzer aus allen Gruppen entfernt werden.

Memberof und Refint Overlays

Die memberof- und refint-Overlays sollten aktiviert sein. Weitere Informationen enthält die Anleitung zur Verwaltung der umgekehrten Gruppenmitgliedschaft in der "${post_edited_translations.segment}".

${post_edited_translations.segment}

${post_edited_translations.segment}

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

Zusätzlich sollte sichergestellt sein, dass die in der Hilfe für Username genannten Felder für eine optimale Leistung indiziert sind.

Informationen zur umgekehrten Gruppenmitgliedschaftsverwaltung befinden sich in der "${post_edited_translations.segment}".

Administratorgruppen in StorageGRID verwalten

Sie können Administratorgruppen erstellen, um die Sicherheitsberechtigungen für einen oder mehrere Administratorbenutzer zu verwalten. Benutzer müssen einer Gruppe angehören, um Zugriff auf das StorageGRID System zu erhalten.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.

- Du hast "spezifische Zugriffsberechtigungen".
- ${post_edited_translations.segment}

${post_edited_translations.segment}

Mit Administratorgruppen kann festgelegt werden, welche Benutzer auf welche Funktionen und Vorgänge im Grid Manager und in der Grid Management API zugreifen können.

Assistenten aufrufen

Schritte

1. **Konfiguration** > **Zugriffskontrolle** > **Administratorgruppen** auswählen.
2. ${post_edited_translations.segment}

Wählen Sie einen Gruppentyp

Sie können eine lokale Gruppe erstellen oder eine Verbundgruppe importieren.

- Eine lokale Gruppe kann erstellt werden, wenn Berechtigungen lokalen Benutzern zugewiesen werden sollen.
- ${post_edited_translations.segment}

${post_edited_translations.segment}

Schritte

1. ${post_edited_translations.segment}
2. Geben Sie einen Anzeigenamen für die Gruppe ein, den Sie später bei Bedarf aktualisieren können. Zum Beispiel „Maintenance Users“ oder „ILM Administrators“.
3. Geben Sie einen eindeutigen Namen für die Gruppe ein, der später nicht mehr geändert werden kann.
4. Wählen Sie **Weiter**.

Föderierte Gruppe

Schritte

1. **Verbundgruppe** auswählen.
2. Geben Sie den Namen der Gruppe, die Sie importieren möchten, genau so ein, wie er in der konfigurierten Identitätsquelle erscheint.
   - Für Active Directory und Microsoft Entra ID ist der sAMAccountName zu verwenden.
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
3. Wählen Sie **Weiter**.

Gruppenberechtigungen verwalten

Schritte

1. Für **Zugriffsmodus** auswählen, ob Benutzer in der Gruppe Einstellungen ändern und Vorgänge im Grid Manager und der Grid Management API durchführen können oder ob sie nur Einstellungen und Funktionen

anzeigen können.

- **Lese-/Schreibzugriff** (Standard): Benutzer können Einstellungen ändern und die durch ihre Verwaltungsberechtigungen erlaubten Vorgänge ausführen.
- **Schreibgeschützt**: Benutzer können Einstellungen und Funktionen nur anzeigen. Sie können keine Änderungen vornehmen oder Vorgänge im Grid Manager oder in der Grid Management API ausführen. Lokale schreibgeschützte Benutzer können ihre eigenen Passwörter ändern.

> Wenn ein Benutzer mehreren Gruppen angehört und eine dieser Gruppen auf **Schreibgeschützt** gesetzt ist, hat der Benutzer nur Lesezugriff auf alle ausgewählten Einstellungen und Funktionen.

2. Wählen Sie ein oder mehrere "Administratorgruppenberechtigungen" aus.

   ${post_edited_translations.segment}

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

${post_edited_translations.segment}

Schritte

1. ${post_edited_translations.segment}

   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. Siehe "Benutzer verwalten" für Details.

2. **Gruppe erstellen** und **Fertigstellen** auswählen.

${post_edited_translations.segment}

Sie können Details zu bestehenden Gruppen anzeigen, eine Gruppe bearbeiten oder eine Gruppe duplizieren.

- Grundlegende Informationen zu allen Gruppen finden sich in der Tabelle auf der Seite „Gruppen“.
- Alle Details einer bestimmten Gruppe sowie die Bearbeitung einer Gruppe sind über das Menü **Aktionen** oder die Detailseite möglich.

Aufgabe	Aktionsmenü	Detailseite
Gruppendetails anzeigen	a. Aktivieren Sie das Kontrollkästchen für die Gruppe. b. ${post_edited_translations.segment}	Den Gruppennamen in der Tabelle auswählen.
Anzeigenamen bearbeiten (nur lokale Gruppen)	a. Aktivieren Sie das Kontrollkästchen für die Gruppe. b. **Aktionen** > **Gruppennamen bearbeiten** auswählen. c. Geben Sie den neuen Namen ein. d. Wählen Sie **Save changes**.	a. ${post_edited_translations.segment} b. Das Bearbeitungssymbol auswählen. c. Geben Sie den neuen Namen ein. d. Wählen Sie **Save changes**.

Aufgabe	Aktionsmenü	Detailseite
${post_edited_translations.segment}	a. Aktivieren Sie das Kontrollkästchen für die Gruppe. b. ${post_edited_translations.segment} c. Optional kann der Zugriffsmodus der Gruppe geändert werden. d. Optional kann "Administratorgruppenberechtigungen" ausgewählt oder abgewählt werden. e. Wählen Sie **Save changes**.	a. ${post_edited_translations.segment} b. Optional kann der Zugriffsmodus der Gruppe geändert werden. c. Optional kann "Administratorgruppenberechtigungen" ausgewählt oder abgewählt werden. d. Wählen Sie **Save changes**.

${post_edited_translations.segment}

Schritte

1. Aktivieren Sie das Kontrollkästchen für die Gruppe.
2. **Aktionen** > **Gruppe duplizieren** auswählen.
3. ${post_edited_translations.segment}

Gruppe löschen

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

Schritte

1. Auf der Seite „Gruppen“ das Kontrollkästchen für jede zu entfernende Gruppe auswählen.
2. **Aktionen** > **Gruppe löschen** auswählen.
3. **Gruppen löschen** auswählen.

Administratorgruppenberechtigungen in StorageGRID

Beim Erstellen von Admin-Benutzergruppen wählen Sie eine oder mehrere Berechtigungen aus, um den Zugriff auf bestimmte Funktionen des Grid Managers zu steuern. Jeder Benutzer kann dann einer oder mehreren dieser Admin-Gruppen zugewiesen werden, wodurch festgelegt wird, welche Aufgaben dieser Benutzer ausführen kann.

Jeder Gruppe muss mindestens eine Berechtigung zugewiesen werden; andernfalls können sich Benutzer, die dieser Gruppe angehören, nicht beim Grid Manager oder der Grid Management API anmelden.

Standardmäßig kann jeder Benutzer, der einer Gruppe angehört, die über mindestens eine Berechtigung verfügt, die folgenden Aufgaben ausführen:

- Anmeldung beim Grid Manager
- Dashboard anzeigen

- Die Knotenseiten
- Aktuelle und behobene Warnmeldungen
- Eigenes Passwort ändern (nur lokale Benutzer)
- Bestimmte Informationen, die auf den Seiten „Konfiguration“ und „Wartung“ bereitgestellt werden, können angezeigt werden.

Interaktion zwischen Berechtigungen und Zugriffsmodus

Für alle Berechtigungen bestimmt die **Zugriffsmodus**-Einstellung der Gruppe, ob Benutzer Einstellungen ändern und Aktionen ausführen können oder ob sie die zugehörigen Einstellungen und Funktionen nur anzeigen können. Wenn ein Benutzer mehreren Gruppen angehört und eine dieser Gruppen auf **Schreibgeschützt** eingestellt ist, hat der Benutzer nur Lesezugriff auf alle ausgewählten Einstellungen und Funktionen.

In den folgenden Abschnitten werden die Berechtigungen beschrieben, die Sie beim Erstellen oder Bearbeiten einer Admin-Gruppe zuweisen können. Alle nicht explizit genannten Funktionen erfordern die Berechtigung **Root access**.

Root-Zugriff

Diese Berechtigung gewährt Zugriff auf alle Grid-Administrationsfunktionen.

Root-Passwort des Mandanten ändern

Diese Berechtigung ermöglicht den Zugriff auf die Option **Root-Passwort ändern** auf der Tenants-Seite, wodurch gesteuert werden kann, wer das Passwort für den lokalen Root-Benutzer des Mandanten ändern darf. Diese Berechtigung wird auch für die Migration von S3-Schlüsseln verwendet, wenn die S3-Schlüsselimportfunktion aktiviert ist. Benutzer, die diese Berechtigung nicht haben, können die Option **Root-Passwort ändern** nicht sehen.

> Um Zugriff auf die Seite „Mandanten“ zu gewähren, die die Option **Root-Passwort ändern** enthält, muss auch die Berechtigung **Mandantenkonten** zugewiesen werden.

ILM

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

- Regeln
- Richtlinien
- Richtlinien-Tags
- Storage Pools
- Storage-Grades
- Regionen
- Objektmetadatenabfrage

> Benutzer benötigen die Berechtigung **Andere Grid-Konfiguration**, um Speicherklassen zu verwalten.

Wartung

Benutzer benötigen die Wartungsberechtigung, um diese Optionen zu verwenden:

- **Konfiguration** > **Zugriffskontrolle**:
  - Grid-Passwörter
- **Konfiguration** > **Netzwerk**:
  - S3 Endpoint-Domänennamen
- **Wartung** > **Aufgaben**:
  - Außerdienststellung
  - ${post_edited_translations.segment}
  - Objektexistenzprüfung
  - Wiederherstellung
- **Wartung** > **System**:
  - ${post_edited_translations.segment}
  - Software Update
- **Support** > **Tools**:
  - Protokolle

Benutzer ohne Wartungsberechtigung können diese Seiten zwar ansehen, aber nicht bearbeiten:

- **Wartung** > **Netzwerk**:
  - DNS-Server
  - Grid-Netzwerk
  - NTP-Server
- **Wartung** > **System**:
  - Lizenz
- **Konfiguration** > **Netzwerk**:
  - S3 Endpoint-Domänennamen
- **Konfiguration** > **Sicherheit**:
  - Zertifikate
- **Konfiguration** > **Überwachung**:
  - Audit und Syslog Server

Benachrichtigungen verwalten

Diese Berechtigung ermöglicht den Zugriff auf Optionen zur Verwaltung von Warnmeldungen. Benutzer müssen über diese Berechtigung verfügen, um Stummschaltungen, Warnbenachrichtigungen und Warnregeln zu verwalten.

Metrikabfrage

Diese Berechtigung gewährt Zugriff auf:

- ${post_edited_translations.segment}
- Benutzerdefinierte Prometheus-Metrikabfragen mithilfe des Abschnitts **Metrics** der Grid Management API
- Grid Manager Dashboard-Karten, die Kennzahlen enthalten

Objektmetadatenabfrage

Diese Berechtigung ermöglicht den Zugriff auf die Seite **ILM** > **Objektmetadaten-Lookup**.

Andere Grid-Konfiguration

Diese Berechtigung gewährt Zugriff auf diese zusätzlichen Grid-Konfigurationsoptionen:

- ${post_edited_translations.segment}
  - Storage-Grades
- **Konfiguration** > **System**:
- **Support** > **Sonstiges**:
  - Verbindungskosten

Storage-Appliance-Administrator

${post_edited_translations.segment}

- Zugriff auf den E-Series SANtricity System Manager auf Speichergeräten über den Grid Manager.
- Die Möglichkeit, auf der Registerkarte „Laufwerke verwalten“ für Appliances, die diese Vorgänge unterstützen, Fehlerbehebungs- und Wartungsaufgaben auszuführen.

Mieterkonten

Diese Berechtigung ermöglicht Folgendes:

- Auf der Seite „Mandanten“ können Mandantenkonten erstellt, bearbeitet und entfernt werden.
- Vorhandene Verkehrsklassifizierungsrichtlinien anzeigen
- Dashboard-Karten des Grid Manager mit Mandantendetails anzeigen

Benutzer in StorageGRID verwalten

Sie können lokale und föderierte Benutzer anzeigen. Sie können auch lokale Benutzer erstellen und diese lokalen Administratorgruppen zuweisen, um festzulegen, auf welche Grid Manager Funktionen diese Benutzer zugreifen können.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Du hast "spezifische Zugriffsberechtigungen".

${post_edited_translations.segment}

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

Es können nur lokale Benutzer erstellt werden. Die externe Identitätsquelle dient zur Verwaltung von föderierten Benutzern und Gruppen.

Der Grid Manager enthält einen vordefinierten lokalen Benutzer namens „root“. Sie können den Root-Benutzer nicht entfernen.

${post_edited_translations.segment}

Assistenten aufrufen

Schritte

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}

${post_edited_translations.segment}

Schritte

1. Den vollständigen Namen des Benutzers, einen eindeutigen Benutzernamen und ein Passwort eingeben.
2. ${post_edited_translations.segment}
3. Wählen Sie **Weiter**.

Gruppen zuweisen

Schritte

1. Optional kann der Benutzer einer oder mehreren Gruppen zugeordnet werden, um die Berechtigungen des Benutzers festzulegen.

   Wenn Sie noch keine Gruppen erstellt haben, können Sie den Benutzer speichern, ohne Gruppen auszuwählen. Dieser Benutzer kann auf der Seite „Gruppen“ einer Gruppe hinzugefügt werden.

   Wenn ein Benutzer mehreren Gruppen angehört, sind die Berechtigungen kumulativ. Siehe "${post_edited_translations.segment}" für Details.

2. ${post_edited_translations.segment}

Lokale Benutzer anzeigen und bearbeiten

Sie können Details zu bestehenden lokalen und föderierten Benutzern einsehen. Ein lokaler Benutzer kann geändert werden, um den vollständigen Namen, das Passwort oder die Gruppenzugehörigkeit des Benutzers zu ändern. Ein Benutzer kann außerdem vorübergehend vom Zugriff auf den Grid Manager und die Grid Management API ausgeschlossen werden.

Sie können nur lokale Benutzer bearbeiten. Die Verwaltung föderierter Benutzer erfolgt über die externe Identitätsquelle.

- Grundlegende Informationen zu allen lokalen und föderierten Benutzern sind in der Tabelle auf der Seite „Benutzer“ aufgeführt.
- Alle Details eines bestimmten Benutzers können über das Menü **Aktionen** oder die Detailseite angezeigt werden, ebenso ist das Bearbeiten eines lokalen Benutzers oder das Ändern des Passworts eines lokalen Benutzers dort möglich.

  Alle Änderungen werden beim nächsten Ab- und erneuten Anmelden des Benutzers im Grid Manager

angewendet.

Lokale Benutzer können ihre eigenen Passwörter über die Option **Passwort ändern** im Grid Manager Banner ändern.

Aufgabe	Aktionsmenü	Detailseite
Benutzerdetails	a. Das Kontrollkästchen für den Benutzer auswählen. b. ${post_edited_translations.segment}	Der Name des Benutzers in der Tabelle wird ausgewählt.
Vollständigen Namen bearbeiten (nur lokale Benutzer)	a. Das Kontrollkästchen für den Benutzer auswählen. b. ${post_edited_translations.segment} c. Geben Sie den neuen Namen ein. d. Wählen Sie **Save changes**.	a. Der Name des Benutzers kann ausgewählt werden, um die Details anzuzeigen. b. Das Bearbeitungssymbol auswählen. c. Geben Sie den neuen Namen ein. d. Wählen Sie **Save changes**.
${post_edited_translations.segment}	a. Das Kontrollkästchen für den Benutzer auswählen. b. ${post_edited_translations.segment} c. ${post_edited_translations.segment} d. ${post_edited_translations.segment} e. Wählen Sie **Save changes**.	a. Der Name des Benutzers kann ausgewählt werden, um die Details anzuzeigen. b. ${post_edited_translations.segment} c. ${post_edited_translations.segment} d. Wählen Sie **Save changes**.
Passwort ändern (nur für lokale Benutzer)	a. Das Kontrollkästchen für den Benutzer auswählen. b. ${post_edited_translations.segment} c. Die Registerkarte „Passwort“ auswählen. d. ${post_edited_translations.segment} e. **Passwort ändern** auswählen.	a. Der Name des Benutzers kann ausgewählt werden, um die Details anzuzeigen. b. Die Registerkarte „Passwort“ auswählen. c. ${post_edited_translations.segment} d. **Passwort ändern** auswählen.
Gruppen ändern (nur lokale Benutzer)	a. Das Kontrollkästchen für den Benutzer auswählen. b. ${post_edited_translations.segment} c. ${post_edited_translations.segment} d. ${post_edited_translations.segment} e. **Gruppen bearbeiten** auswählen, um andere Gruppen auszuwählen. f. Wählen Sie **Save changes**.	a. Der Name des Benutzers kann ausgewählt werden, um die Details anzuzeigen. b. ${post_edited_translations.segment} c. ${post_edited_translations.segment} d. **Gruppen bearbeiten** auswählen, um andere Gruppen auszuwählen. e. Wählen Sie **Save changes**.

${post_edited_translations.segment}

${post_edited_translations.segment}

Schritte

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. Die UUID oder der Benutzername für einen oder mehrere Verbundbenutzer wird eingegeben.

   ${post_edited_translations.segment}

4. **Importieren** auswählen.

   ${post_edited_translations.segment}

   a. **Nicht importierte Benutzer** erweitern und **Benutzer kopieren** auswählen.
   b. Den Import erneut versuchen, indem **Vorherige** ausgewählt und die kopierten Benutzer in das Dialogfeld **Verbundbenutzer importieren** eingefügt werden.

   ${post_edited_translations.segment}

Einen Benutzer duplizieren

${post_edited_translations.segment}

Schritte

1. Das Kontrollkästchen für den Benutzer auswählen.
2. **Aktionen** > **Benutzer duplizieren** auswählen.
3. Den Assistenten zum Duplizieren von Benutzern abschließen.

Einen Benutzer löschen

Ein lokaler Benutzer kann gelöscht werden, um diesen Benutzer dauerhaft aus dem System zu entfernen.

Der Root-Benutzer kann nicht gelöscht werden.

Schritte

1. Auf der Seite „Benutzer“ das Kontrollkästchen für jeden Benutzer auswählen, der entfernt werden soll.
2. ${post_edited_translations.segment}
3. **Benutzer löschen** auswählen.

Single Sign-On (SSO) nutzen

Erfahren Sie mehr über StorageGRID SSO

Wenn Single Sign-On (SSO) aktiviert ist, ist der Zugriff auf Grid Manager, Tenant Manager, die Grid Management API oder die Tenant Management API für Benutzer nur möglich, wenn ihre Anmeldeinformationen über den von Ihrer Organisation implementierten SSO-Anmeldeprozess autorisiert werden. 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.

${post_edited_translations.segment}

Anmelden, wenn SSO aktiviert ist

Wenn SSO aktiviert ist und Sie sich bei StorageGRID anmelden, werden Sie zur SSO-Seite Ihrer Organisation weitergeleitet, um Ihre Anmeldeinformationen zu bestätigen.

Schritte

1. Geben Sie den vollqualifizierten Domainnamen oder die IP-Adresse eines beliebigen StorageGRID Admin Node in einem Webbrowser ein.

   Die StorageGRID Anmeldeseite wird angezeigt.

   - Wenn Sie die URL zum ersten Mal mit 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 kürzlich verwendetes Konto auszuwählen oder eine Konto-ID einzugeben.

   > Die StorageGRID Sign-in-Seite wird nicht angezeigt, wenn die vollständige URL für ein Mandantenkonto eingegeben wird (das heißt, eine vollqualifizierte Domain oder IP-Adresse gefolgt von `/?accountId=20-digit-account-id`). Stattdessen erfolgt eine sofortige Weiterleitung zur SSO Sign-in-Seite Ihrer Organisation, wo Mit Ihren SSO-Anmeldeinformationen anmelden möglich ist.

2. Geben Sie an, ob Sie auf den Grid Manager oder den Tenant Manager zugreifen möchten:
   - Um auf den Grid Manager zuzugreifen, das Feld **Konto-ID** leer lassen, **0** als Konto-ID eingeben oder **Grid Manager** auswählen, falls dieser in der Liste der zuletzt verwendeten Konten erscheint.
   - ${post_edited_translations.segment}
3. **Anmelden** auswählen

   StorageGRID leitet Sie zur SSO-Anmeldeseite Ihrer Organisation weiter. Zum Beispiel:

4. Mit Ihren SSO-Anmeldeinformationen anmelden.

   Wenn Ihre SSO-Anmeldeinformationen korrekt sind:

   a. Der Identitätsanbieter (IdP) stellt eine Authentifizierungsantwort für StorageGRID bereit.
   b. StorageGRID validiert die Authentifizierungsantwort.
   c. Wenn die Antwort gültig ist und Sie einer föderierten Gruppe mit StorageGRID-Zugriffsberechtigungen angehören, sind Sie beim Grid Manager oder beim Tenant Manager angemeldet, abhängig davon, welches Konto Sie ausgewählt haben.

   > Wenn das Dienstkonto nicht erreichbar ist, können Sie sich trotzdem anmelden, sofern Sie ein bestehender Benutzer sind, der einer Verbundgruppe mit StorageGRID Zugriffsberechtigungen angehört.

5. Optional ist auch der Zugriff auf andere Admin-Knoten, den Grid Manager oder den Tenant Manager möglich, sofern die entsprechenden Berechtigungen vorliegen.

   Sie müssen Ihre SSO-Anmeldeinformationen nicht erneut eingeben.

${post_edited_translations.segment}

${post_edited_translations.segment}

Schritte

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}

   Die StorageGRID Sign in-Seite wird angezeigt. Das Dropdown-Menü **Recent Accounts** wurde aktualisiert und enthält nun **Grid Manager** oder den Namen des Mandanten, sodass zukünftig schneller auf diese Benutzeroberflächen zugegriffen werden kann.

   Die Tabelle fasst zusammen, was beim Abmelden geschieht, wenn Sie eine einzelne Browsersitzung verwenden. Wenn Sie über mehrere Browsersitzungen bei StorageGRID angemeldet sind, müssen Sie sich von allen Browsersitzungen separat abmelden.

${post_edited_translations.segment}	Und Sie melden sich ab von…	Sie sind abgemeldet…
Grid Manager auf einem oder mehreren Admin Nodes	Grid Manager auf einem beliebigen Admin-Node	Grid Manager auf allen Admin Nodes **Hinweis:** Wenn Sie Entra ID für SSO verwenden, kann es einige Minuten dauern, bis Sie von allen Admin Nodes abgemeldet sind.
Mandantenmanager auf einem oder mehreren Admin-Nodes	Mandantenmanager auf einem beliebigen Admin-Node	Mandantenmanager auf allen Admin-Nodes
Sowohl Grid Manager als auch Tenant Manager	Grid Manager	Nur der Grid Manager. Um sich von SSO abzumelden, ist auch eine Abmeldung vom Tenant Manager erforderlich.

Anforderungen und Überlegungen für StorageGRID SSO

Vor der Aktivierung von Single Sign-On (SSO) für ein StorageGRID System sind die Anforderungen und Überlegungen zu prüfen.

Anforderungen an Identitätsanbieter

${post_edited_translations.segment}

- Active Directory Federation Service (AD FS)

- Microsoft Entra ID
- PingFederate

Sie müssen die Identitätsföderation für Ihr StorageGRID System konfigurieren, bevor Sie einen SSO-Identitätsanbieter einrichten können. Der Typ des LDAP-Dienstes, den Sie für die Identitätsföderation verwenden, bestimmt, welche Art von SSO Sie implementieren können.

Konfigurierter LDAP-Diensttyp	Optionen für SSO Identitätsanbieter
Active Directory	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

AD FS Anforderungen

Es können beliebige der folgenden Versionen von AD FS verwendet werden:

- ${post_edited_translations.segment}
- Windows Server 2019 AD FS
- ${post_edited_translations.segment}

Windows Server 2016 sollte "${post_edited_translations.segment}" oder höher verwenden.

Zusätzliche Anforderungen

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

Überlegungen zu 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. Damit sich Benutzer anmelden können, muss die Verbindung zum LDAP-Server wiederhergestellt werden.

Anforderungen an Serverzertifikate

Standardmäßig verwendet StorageGRID auf jedem Admin-Knoten ein Managementoberflächenzertifikat, um den Zugriff auf den Grid Manager, den Tenant Manager, die Grid Management API und die Tenant Management API zu sichern. Bei der Konfiguration von Vertrauensstellungen zwischen vertrauenden Parteien (AD FS), Unternehmensanwendungen (Entra ID) oder Dienstanbieterverbindungen (PingFederate) für StorageGRID wird das Serverzertifikat als Signaturzertifikat für StorageGRID-Anfragen verwendet.

Falls Sie dies noch nicht "Ein benutzerdefiniertes Zertifikat für die Managementoberfläche konfiguriert" haben, sollte es jetzt erfolgen. Wenn ein benutzerdefiniertes Serverzertifikat installiert wird, wird es für alle Admin Nodes verwendet und kann in allen StorageGRID relying party trusts, enterprise applications oder SP connections genutzt werden.

Die Verwendung des Standardserverzertifikats eines Administratorknotens in einer Vertrauensstellung der vertrauenden Seite, einer Unternehmensanwendung oder SP Verbindung wird nicht empfohlen. Wenn der Knoten ausfällt und wiederhergestellt wird, wird ein neues Standardserverzertifikat generiert. Vor der Anmeldung am wiederhergestellten Knoten ist die Vertrauensstellung der vertrauenden Seite, die Unternehmensanwendung oder die SP Verbindung mit dem neuen Zertifikat zu aktualisieren.

Sie können auf das Serverzertifikat eines Admin-Knotens zugreifen, indem Sie sich an der Befehlsshell des Knotens anmelden und zum `/var/local/mgmt-api` Verzeichnis wechseln. Ein benutzerdefiniertes Serverzertifikat trägt den Namen `custom-server.crt`. Das Standard-Serverzertifikat des Knotens trägt den Namen `server.crt`.

Port-Anforderungen

Single Sign-On (SSO) ist auf den eingeschränkten Ports des Grid Manager oder Tenant Manager nicht verfügbar. Der Standard-HTTPS-Port (443) muss verwendet werden, wenn Benutzer sich mit Single Sign-On authentifizieren sollen. Siehe "Zugriffskontrolle an der externen Firewall".

Bestätigen Sie, dass sich Verbundbenutzer bei StorageGRID anmelden können

Bevor Sie Single Sign-On (SSO) aktivieren, muss bestätigt werden, dass sich mindestens ein Verbundbenutzer beim Grid Manager und beim Tenant Manager für alle bestehenden Mandantenkonten anmelden kann.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Du hast "spezifische Zugriffsberechtigungen".
- Sie haben die Identitätsföderation bereits konfiguriert.

Schritte

1. Falls bereits Mandantenkonten vorhanden sind, ist zu bestätigen, dass keiner der Mandanten seine eigene Identitätsquelle verwendet.

   Wenn Sie SSO aktivieren, wird eine im Tenant Manager konfigurierte Identitätsquelle durch die im Grid Manager konfigurierte Identitätsquelle überschrieben. Benutzer, die zur Identitätsquelle des Tenants gehören, können sich nicht mehr anmelden, es sei denn, sie verfügen über ein Konto bei der Grid Manager Identitätsquelle.

   a. Bei jedem Mieterkonto im Tenant Manager anmelden.
   b. **Zugriffsverwaltung** > **Identitätsföderation** auswählen.
   c. Bestätigen Sie, dass das Kontrollkästchen **Identitätsföderation aktivieren** nicht ausgewählt ist.
   d. ${post_edited_translations.segment}

2. Bestätigen, dass ein Verbundbenutzer auf den Grid Manager zugreifen kann:
   a. ${post_edited_translations.segment}
   b. Stellen Sie sicher, dass mindestens eine Verbundgruppe aus der Active Directory Identitätsquelle importiert wurde und dass ihr die Root-Zugriffsberechtigung zugewiesen wurde.
   c. Abmelden.

d. Bestätigen Sie, dass eine erneute Anmeldung beim Grid Manager als Benutzer der Verbundgruppe möglich ist.

3. ${post_edited_translations.segment}

   a. Im Grid Manager **Mandanten** auswählen.

   b. ${post_edited_translations.segment}

   c. Auf der Registerkarte „Details eingeben“ **Weiter** auswählen.

   d. Wenn das Kontrollkästchen **Eigene Identitätsquelle verwenden** ausgewählt ist, das Kontrollkästchen deaktivieren und **Speichern** auswählen.

      Die Mieterseite wird angezeigt.

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

   f. Im Mandantenmanager **Zugriffsverwaltung** > **Gruppen** auswählen.

   g. Stellen Sie sicher, dass mindestens einer föderierten Gruppe des Grid Managers die Root-Zugriffsberechtigung für diesen Mandanten zugewiesen wurde.

   h. Abmelden.

   i. ${post_edited_translations.segment}

Verwandte Informationen

- "Anforderungen und Überlegungen zum Single Sign-On"
- "${post_edited_translations.segment}"
- "Ein Mandantenkonto verwenden"_

SSO in StorageGRID konfigurieren

Sie können dem Konfigurationsassistenten für Single Sign-On (SSO) folgen und den Sandbox-Modus aktivieren, um SSO zu konfigurieren und zu testen, bevor es für alle StorageGRID Benutzer aktiviert wird. Nachdem SSO aktiviert wurde, besteht die Möglichkeit, bei Bedarf in den Sandbox-Modus zurückzukehren, um die Konfiguration zu ändern oder erneut zu testen.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Root-Zugriffsberechtigung".
- Sie haben die Identitätsföderation für Ihr StorageGRID System konfiguriert.
- Für den Identitätsverbund-Diensttyp **LDAP** wurde entweder Active Directory oder Entra ID ausgewählt, abhängig vom SSO-Identitätsanbieter, der verwendet werden soll.

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

Konfigurierter LDAP-Diensttyp	Optionen für SSO Identitätsanbieter
Entra ID	Entra ID

Über diese Aufgabe

Wenn SSO aktiviert ist und ein Benutzer versucht, sich an einem Admin-Node anzumelden, sendet StorageGRID eine Authentifizierungsanfrage an den SSO-Identitätsanbieter. Der SSO-Identitätsanbieter sendet daraufhin eine Authentifizierungsantwort an StorageGRID, die angibt, ob die Authentifizierungsanfrage erfolgreich war. Für erfolgreiche Anfragen:

- Die Antwort von Active Directory oder PingFederate enthält eine universell eindeutige Kennung (UUID) für den Benutzer.
- Die Antwort von Entra ID enthält einen User Principal Name (UPN).

Damit StorageGRID (dem Dienstanbieter) und der SSO-Identitätsanbieter sicher über Benutzerauthentifizierungsanfragen kommunizieren können, sind diese Aufgaben zu erledigen:

1. Einstellungen in StorageGRID konfigurieren.
2. Mit der Software des SSO-Identitätsanbieters wird für jeden Admin-Node eine Vertrauensstellung der vertrauenden Seite (AD FS), eine Enterprise Application (Entra ID) oder ein Service Provider (PingFederate) erstellt.
3. Zu StorageGRID zurückkehren, um SSO zu aktivieren.

Der Sandbox-Modus vereinfacht diese Hin- und Her-Konfiguration und ermöglicht es, alle Einstellungen zu testen, bevor SSO aktiviert wird. Im Sandbox-Modus können sich Benutzer nicht mit SSO anmelden.

Assistenten aufrufen

Schritte

1. Wählen Sie **Konfiguration** > **Zugriffskontrolle** > **Single sign-on**. Die Single sign-on-Seite wird angezeigt.

   Wenn die Schaltfläche „SSO-Einstellungen konfigurieren“ deaktiviert ist, sollte überprüft werden, ob der Identitätsanbieter als föderierte Identitätsquelle konfiguriert wurde. Siehe "Anforderungen und Überlegungen zum Single Sign-On".

2. **SSO-Einstellungen konfigurieren** auswählen. Die Seite „Details zum Identitätsanbieter angeben“ erscheint.

Angaben zum Identitätsanbieter bereitstellen

Schritte

1. Den **SSO-Typ** aus der Dropdown-Liste auswählen.
2. Wenn Sie Active Directory als SSO-Typ ausgewählt haben, ist der **Verbunddienstname** für den Identitätsanbieter genau so einzugeben, wie er im Active Directory Federation Service (AD FS) erscheint.

   Um den Namen des Verbunddienstes zu finden, gehen Sie zum Windows Server-Manager. **Tools** > **AD FS Management** auswählen. Im Menü „Action“ die Option **Edit Federation Service Properties** auswählen. Der Federation Service Name wird im zweiten Feld angezeigt.

3. Geben Sie an, welches TLS-Zertifikat zur Sicherung der Verbindung verwendet wird, wenn der Identitätsanbieter SSO-Konfigurationsinformationen als Antwort auf StorageGRID Anfragen sendet.
   - **CA-Zertifikat des Betriebssystems verwenden**: Das standardmäßig auf dem Betriebssystem installierte CA-Zertifikat wird zur Absicherung der Verbindung verwendet.
   - **Benutzerdefiniertes CA-Zertifikat verwenden**: Ein benutzerdefiniertes CA-Zertifikat wird verwendet, um die Verbindung zu sichern.

     Wenn Sie diese Einstellung auswählen, den Text des benutzerdefinierten Zertifikats kopieren und in das Textfeld **CA Certificate** einfügen.
   - **Kein TLS verwenden**: Es wird kein TLS-Zertifikat verwendet, um die Verbindung zu sichern.

     Wenn Sie das CA-Zertifikat ändern, "Den mgmt-api Service auf den Admin-Knoten neu starten" und testen Sie sofort, ob ein SSO-Zugriff auf den Grid Manager erfolgreich ist.
4. **Weiter** auswählen. Die Seite „Identifikator der vertrauenden Partei angeben“ wird angezeigt.

Relying-Party-Kennung angeben

1. Füllen Sie die Felder auf der Seite „Vertrauende Parteikennung angeben“ entsprechend dem ausgewählten SSO-Typ aus.

Active Directory

a. Geben Sie die **Relying party identifier** für StorageGRID an. Dieser Wert steuert den Namen, der für jede Relying party trust in AD FS verwendet wird.

   - Wenn Ihr Grid beispielsweise nur einen Admin-Knoten hat und nicht damit zu rechnen ist, dass in Zukunft weitere Admin-Knoten hinzugefügt werden, geben Sie `SG` oder `StorageGRID` ein.
   - Wenn Ihr Grid mehr als einen Admin Node enthält, muss die Zeichenfolge `[HOSTNAME]` in die Kennung eingefügt werden. Beispielsweise `SG-[HOSTNAME]`. Das Einfügen dieser Zeichenfolge führt zu einer Tabelle, die die Relying-Party-Kennung für jeden Admin Node im Grid basierend auf dem Hostnamen des Nodes anzeigt.

   > Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID System eine Vertrauensstellung einrichten. Eine Vertrauensstellung für jeden Admin-Knoten gewährleistet, dass sich Benutzer sicher an jedem Admin-Knoten an- und ausloggen können.

b. **Speichern und Sandbox-Modus aktivieren** auswählen.

Entra ID

a. Im Abschnitt „Enterprise Application“ ist der **Enterprise application name** für StorageGRID anzugeben. Dieser Wert legt den Namen fest, der für jede Enterprise Application in Entra ID verwendet wird.

   - Wenn Ihr Grid beispielsweise nur einen Admin-Knoten hat und nicht damit zu rechnen ist, dass in Zukunft weitere Admin-Knoten hinzugefügt werden, geben Sie `SG` oder `StorageGRID` ein.
   - Wenn Ihr Grid mehr als einen Admin Node enthält, sollte die Zeichenfolge `[HOSTNAME]` im Bezeichner enthalten sein. Zum Beispiel `SG-[HOSTNAME]`. Das Einfügen dieser Zeichenfolge führt zu einer Tabelle, die für jeden Admin Node in Ihrem System einen Enterprise Application Name basierend auf dem Hostnamen des Knotens anzeigt.

   > Sie müssen für jeden Admin Node in Ihrem StorageGRID System eine Unternehmensanwendung erstellen. Eine eigene Unternehmensanwendung für jeden Admin Node stellt sicher, dass sich Benutzer sicher bei jedem Admin Node anmelden und wieder ausloggen können.

b. Die Schritte in "Unternehmensanwendungen in Entra ID erstellen" führen zur Erstellung einer Unternehmensanwendung für jeden in der Tabelle aufgeführten Admin Node.

c. Kopieren Sie aus Entra ID die Föderationsmetadaten-URL für jede Unternehmensanwendung. Anschließend diese URL in das entsprechende Feld **Federation metadata URL** in StorageGRID einfügen.

d. Nachdem Sie eine Federation-Metadaten-URL für alle Admin-Knoten kopiert und eingefügt haben, **Speichern und Sandbox-Modus aktivieren** auswählen.

PingFederate

a. Im Abschnitt „Service Provider (SP)“ ist die **SP-Verbindungs-ID** für StorageGRID anzugeben. Dieser Wert bestimmt den Namen, den Sie für jede SP-Verbindung in PingFederate verwenden.

   - Wenn Ihr Grid beispielsweise nur einen Admin-Knoten hat und nicht damit zu rechnen ist, dass in Zukunft weitere Admin-Knoten hinzugefügt werden, geben Sie `SG` oder `StorageGRID`

ein.

- Wenn Ihr Grid mehr als einen Admin-Node enthält, ist die Zeichenfolge `[HOSTNAME]` in die Kennung aufzunehmen. Zum Beispiel `SG-[HOSTNAME]`. Die Einbindung dieser Zeichenfolge führt zu einer Tabelle, die die SP-Verbindungs-ID für jeden Admin-Node in Ihrem System basierend auf dem Hostnamen des Nodes anzeigt.

> Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID-System eine SP-Verbindung erstellen. Eine SP-Verbindung für jeden Admin-Knoten stellt sicher, dass sich Benutzer sicher an jedem Admin-Knoten an- und ausloggen können.

b. Geben Sie die Metadaten-URL der Föderation für jeden Admin-Knoten im Feld **Federation metadata URL** an.

Folgendes Format wird verwendet:

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

c. **Speichern und Sandbox-Modus aktivieren** auswählen.

Vertrauensstellungen der vertrauenden Seite, Unternehmensanwendungen oder SP Verbindungen konfigurieren

Nachdem Sie die Konfiguration gespeichert und den Sandbox-Modus aktiviert haben, kann die Konfiguration für den von Ihnen ausgewählten SSO-Typ abgeschlossen und getestet werden.

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

Active Directory

Schritte

1. Zu Active Directory Federation Services (AD FS) wechseln.
2. Eine oder mehrere Vertrauensstellungen für StorageGRID werden erstellt, wobei jeweils die in der Tabelle auf der Seite „SSO konfigurieren“ aufgeführten Relying-Party-Bezeichner verwendet werden.

   Für jeden in der Tabelle aufgeführten Admin-Knoten muss eine Vertrauensstellung erstellt werden.

   Anweisungen sind unter "Erstellen von Vertrauensstellungen für vertrauende Parteien in AD FS" zu finden.

Entra ID

Schritte

1. Auf der Single sign-on-Seite des Admin-Knotens, bei dem Sie aktuell angemeldet sind, die Schaltfläche zum Herunterladen und Speichern der SAML-Metadaten auswählen.
2. Anschließend sind diese Schritte für alle anderen Admin-Knoten in Ihrem Grid zu wiederholen:
   a. Melden Sie sich am Node an.
   b. **Konfiguration** > **Zugriffskontrolle** > **Single sign-on** auswählen.
   c. Die SAML-Metadaten für diesen Knoten herunterladen und speichern.
3. Wechseln Sie zum Azure Portal.
4. Führen Sie die Schritte in "Unternehmensanwendungen in Entra ID erstellen" aus, um die SAML-Metadatendatei für jeden Admin-Node in die entsprechende Entra ID Enterprise Application hochzuladen.

PingFederate

Schritte

1. Auf der Single sign-on-Seite des Admin-Knotens, bei dem Sie aktuell angemeldet sind, die Schaltfläche zum Herunterladen und Speichern der SAML-Metadaten auswählen.
2. Anschließend sind diese Schritte für alle anderen Admin-Knoten in Ihrem Grid zu wiederholen:
   a. Melden Sie sich am Node an.
   b. **Konfiguration** > **Zugriffskontrolle** > **Single sign-on** auswählen.
   c. Die SAML-Metadaten für diesen Knoten herunterladen und speichern.
3. Zu PingFederate wechseln.
4. "Eine oder mehrere Service Provider (SP) Verbindungen für StorageGRID erstellen". Die SP-Verbindungs-ID für jeden Admin-Knoten (angezeigt in der Tabelle auf der Seite „SSO konfigurieren“) und die SAML-Metadaten, die für diesen Admin-Knoten heruntergeladen wurden, sind zu verwenden.

   Für jeden in der Tabelle aufgeführten Admin-Knoten muss eine SP-Verbindung erstellt werden.

Testkonfiguration

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

Active Directory

Schritte

1. Auf der Seite „SSO konfigurieren“ befindet sich der Link im Schritt „Konfiguration testen“ des Assistenten.

   ${post_edited_translations.segment}

2. Wählen Sie den Link aus oder kopieren Sie die URL und fügen Sie sie in einen Browser ein, um auf die Anmeldeseite Ihres Identitätsanbieters zuzugreifen.
3. ${post_edited_translations.segment}
4. Geben Sie Ihren Verbundbenutzernamen und Ihr Passwort ein.
   - ${post_edited_translations.segment}
   - 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. ${post_edited_translations.segment}

Entra ID

Schritte

1. ${post_edited_translations.segment}
2. **Diese Anwendung testen** auswählen.
3. Die Anmeldeinformationen eines Verbundbenutzers eingeben.
   - ${post_edited_translations.segment}
   - 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. ${post_edited_translations.segment}

PingFederate

Schritte

1. Auf der Seite „SSO konfigurieren“ ist der erste Link in der Meldung zum Sandbox-Modus auszuwählen.

   Jeweils ein Link kann ausgewählt und getestet werden.

2. Die Anmeldeinformationen eines Verbundbenutzers eingeben.
   - ${post_edited_translations.segment}
   - 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. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

Single Sign-On aktivieren

Sobald bestätigt wurde, dass Sie sich per SSO an jedem Admin-Knoten anmelden können, lässt sich SSO für das gesamte StorageGRID System aktivieren.

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

Schritte

1. Im Schritt „Testkonfiguration“ des Assistenten zur SSO-Konfiguration **SSO aktivieren** auswählen.
2. Die Warnmeldung prüfen und **SSO aktivieren** auswählen.

   Single Sign-on ist jetzt aktiviert. Die Single Sign-on Seite wird angezeigt und enthält nun die Details für das soeben konfigurierte SSO.

3. Zum Bearbeiten der Konfiguration **Bearbeiten** auswählen.
4. Zum Deaktivieren von Single Sign-On **SSO deaktivieren** auswählen.

Wenn das Azure-Portal verwendet wird und von demselben Computer aus auf StorageGRID zugegriffen wird, von dem auch auf Entra ID zugegriffen wird, ist sicherzustellen, dass der Azure-Portal-Benutzer ebenfalls ein autorisierter StorageGRID Benutzer ist (ein Benutzer in einer Verbundgruppe, die in StorageGRID importiert wurde), oder es erfolgt ein Ausloggen vom Azure-Portal, bevor versucht wird, sich bei StorageGRID anzumelden.

Erstellen von Relying-Party-Vertrauensstellungen in AD FS für StorageGRID

Sie müssen Active Directory Federation Services (AD FS) verwenden, um für jeden Admin Node in Ihrem System eine Vertrauensstellung der vertrauenden Seite zu erstellen. Vertrauensstellungen der vertrauenden Seite können mithilfe von PowerShell-Befehlen, durch Importieren von SAML-Metadaten aus StorageGRID oder durch manuelle Eingabe der Daten erstellt werden.

Bevor Sie beginnen

- Sie haben Single Sign-On für StorageGRID konfiguriert und **AD FS** als SSO-Typ ausgewählt.
- Sie haben "Sandbox-Modus wurde aktiviert" im Grid Manager.
- Sie kennen den vollqualifizierten Domainnamen (oder die IP-Adresse) und die Kennung der vertrauenden Partei für jeden Admin Node in Ihrem System. Diese Werte sind in der Detailtabelle der Admin Nodes auf der StorageGRID Configure SSO-Seite zu finden.

  Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID System eine Vertrauensstellung einrichten. Eine Vertrauensstellung für jeden Admin-Knoten gewährleistet, dass sich Benutzer sicher an jedem Admin-Knoten an- und ausloggen können.

- Sie haben Erfahrung mit der Erstellung von Vertrauensstellungen für vertrauende Parteien in AD FS oder Sie haben Zugriff auf die Microsoft AD FS-Dokumentation.
- ${post_edited_translations.segment}
- Wenn Sie die Vertrauensstellung der vertrauenden Seite manuell erstellen, verfügen Sie über das benutzerdefinierte Zertifikat, das für die StorageGRID Managementoberfläche hochgeladen wurde, oder Sie wissen, wie Sie sich über die Befehlsshell bei einem Admin Node anmelden.

Über diese Aufgabe

Diese Anleitung gilt für Windows Server 2016 AD FS. Wenn Sie eine andere Version von AD FS verwenden,

werden Sie geringfügige Unterschiede im Ablauf feststellen. In der Microsoft AD FS-Dokumentation finden sich weitere Informationen bei Fragen.

Erstellen einer Vertrauensstellung der vertrauenden Seite mithilfe von Windows PowerShell

Mit Windows PowerShell lassen sich schnell eine oder mehrere Vertrauensstellungen für vertrauende Parteien erstellen.

Schritte

1. Im Windows-Startmenü mit der rechten Maustaste auf das PowerShell-Symbol klicken und **Als Administrator ausführen** auswählen.
2. An der PowerShell-Eingabeaufforderung den folgenden Befehl eingeben:

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

   - Für *`Admin_Node_Identifier`* den Admin-Knoten ist der Relying Party Identifier exakt so einzugeben, wie er auf der Single Sign-on-Seite angezeigt wird. Zum Beispiel `SG-DC1-ADM1`.
   - Für *`Admin_Node_FQDN`* den gleichen Admin-Knoten den vollqualifizierten Domänennamen eingeben. (Falls erforderlich, kann stattdessen die IP-Adresse des Knotens verwendet werden. Wenn jedoch eine IP-Adresse eingegeben wird, ist zu beachten, dass diese Relying-Party-Vertrauensstellung aktualisiert oder neu erstellt werden muss, falls sich diese IP-Adresse jemals ändert.)
3. Wählen Sie im Windows Server-Manager **Tools** > **AD FS Management** aus.

   ${post_edited_translations.segment}

4. **AD FS** > **Vertrauensstellungen der vertrauenden Seite** auswählen.

   Die Liste der vertrauenden Partei-Vertrauensstellungen wird angezeigt.

5. Eine Zugriffssteuerungsrichtlinie zur neu erstellten Vertrauensstellung der vertrauenden Seite hinzufügen:
   a. Die soeben erstellte Vertrauensstellung der vertrauenden Partei befindet sich an folgender Stelle.
   b. Mit der rechten Maustaste auf die Vertrauensstellung klicken und **Zugriffssteuerungsrichtlinie bearbeiten** auswählen.
   c. Wählen Sie eine Zugriffskontrollrichtlinie aus.
   d. **Anwenden** und anschließend **OK** auswählen
6. Eine Claim Issuance Policy zum neu erstellten Relying Party Trust hinzufügen:
   a. Die soeben erstellte Vertrauensstellung der vertrauenden Partei befindet sich an folgender Stelle.
   b. Klicken Sie mit der rechten Maustaste auf den Trust und wählen Sie **Claim-Issuance-Richtlinie bearbeiten**.
   c. **Regel hinzufügen** auswählen.
   d. Auf der Seite „Regelvorlage auswählen“ in der Liste **LDAP-Attribute als Ansprüche senden** auswählen und **Weiter** wählen.
   e. Auf der Seite „Regel konfigurieren“ einen Anzeigenamen für diese Regel eingeben.

      Beispielsweise **ObjectGUID zu Name ID** oder **UPN zu Name ID**.

   f. Für den Attributspeicher wird **Active Directory** ausgewählt.

g. ${post_edited_translations.segment}

h. In der Spalte „Ausgehender Anspruchstyp“ der Zuordnungstabelle wird **Name ID** aus der Dropdown-Liste ausgewählt.

i. **Fertigstellen** und anschließend **OK** auswählen.

7. ${post_edited_translations.segment}

   a. ${post_edited_translations.segment}

   b. Bestätigen Sie, dass die Felder auf den Registerkarten **Endpunkte**, **Kennungen** und **Signatur** ausgefüllt sind.

      Falls die Metadaten fehlen, sollte überprüft werden, ob die Federation-Metadatenadresse korrekt ist, oder die Werte können manuell eingegeben werden.

8. ${post_edited_translations.segment}

9. Wenn Sie fertig sind, kehren Sie zu StorageGRID zurück und "${post_edited_translations.segment}", um zu bestätigen, dass sie korrekt konfiguriert sind.

${post_edited_translations.segment}

Sie können die Werte für jede Relying-Party-Trust-Beziehung importieren, indem Sie auf die SAML-Metadaten für jeden Admin-Node zugreifen.

Schritte

1. ${post_edited_translations.segment}
2. Unter Aktionen die Option **Vertrauensstellung der vertrauenden Partei hinzufügen** auswählen.
3. Auf der Willkommensseite **Claims aware** auswählen und **Start** wählen.
4. **Daten über die vertrauende Partei importieren, die online oder in einem lokalen Netzwerk veröffentlicht wurden** auswählen.
5. ${post_edited_translations.segment}

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

   Für *`Admin_Node_FQDN`* den gleichen Admin-Knoten den vollqualifizierten Domänennamen eingeben. (Falls erforderlich, kann stattdessen die IP-Adresse des Knotens verwendet werden. Wenn jedoch eine IP-Adresse eingegeben wird, ist zu beachten, dass diese Relying-Party-Vertrauensstellung aktualisiert oder neu erstellt werden muss, falls sich diese IP-Adresse jemals ändert.)

6. Den Assistenten für die Vertrauensstellung der vertrauenden Partei abschließen, die Vertrauensstellung der vertrauenden Partei speichern und den Assistenten schließen.

   > Beim Eingeben des Anzeigenamens ist der Relying Party Identifier für den Admin Node zu verwenden, genau wie er auf der Single Sign-on-Seite im Grid Manager angezeigt wird. Zum Beispiel `SG-DC1-ADM1`.

7. Fügen Sie eine Anspruchsregel hinzu:

   a. Klicken Sie mit der rechten Maustaste auf den Trust und wählen Sie **Claim-Issuance-Richtlinie bearbeiten**.

   b. **Regel hinzufügen** auswählen:

c. Auf der Seite „Regelvorlage auswählen“ in der Liste **LDAP-Attribute als Ansprüche senden** auswählen und **Weiter** wählen.

d. Auf der Seite „Regel konfigurieren“ einen Anzeigenamen für diese Regel eingeben.

   Beispielsweise **ObjectGUID zu Name ID** oder **UPN zu Name ID**.

e. Für den Attributspeicher wird **Active Directory** ausgewählt.

f. ${post_edited_translations.segment}

g. In der Spalte „Ausgehender Anspruchstyp“ der Zuordnungstabelle wird **Name ID** aus der Dropdown-Liste ausgewählt.

h. **Fertigstellen** und anschließend **OK** auswählen.

8. ${post_edited_translations.segment}

   a. ${post_edited_translations.segment}

   b. Bestätigen Sie, dass die Felder auf den Registerkarten **Endpunkte**, **Kennungen** und **Signatur** ausgefüllt sind.

      Falls die Metadaten fehlen, sollte überprüft werden, ob die Federation-Metadatenadresse korrekt ist, oder die Werte können manuell eingegeben werden.

9. ${post_edited_translations.segment}

10. Wenn Sie fertig sind, kehren Sie zu StorageGRID zurück und "${post_edited_translations.segment}" um zu bestätigen, dass sie korrekt konfiguriert sind.

Eine Vertrauensstellung der vertrauenden Seite manuell erstellen

Wenn Sie die Daten für die vertrauenden Teilvertrauensstellungen nicht importieren, können Sie die Werte manuell eingeben.

Schritte

1. ${post_edited_translations.segment}
2. Unter Aktionen die Option **Vertrauensstellung der vertrauenden Partei hinzufügen** auswählen.
3. Auf der Willkommensseite **Claims aware** auswählen und **Start** wählen.
4. **Daten über die vertrauende Partei manuell eingeben** auswählen und **Weiter** auswählen.
5. Den Assistenten für die Vertrauensstellung der vertrauenden Partei abschließen:

   a. Geben Sie einen Anzeigenamen für diesen Admin Node ein.

      Für Konsistenz ist der Relying Party Identifier für den Admin Node genau so zu verwenden, wie er auf der Single Sign-on-Seite im Grid Manager angezeigt wird. Zum Beispiel `SG-DC1-ADM1`.

   b. Der Schritt zur Konfiguration eines optionalen Token-Verschlüsselungszertifikats kann übersprungen werden.

   c. Auf der Seite „URL konfigurieren“ das Kontrollkästchen **Unterstützung für das SAML 2.0 WebSSO-Protokoll aktivieren** auswählen.

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

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

Für *Admin_Node_FQDN* geben Sie den vollqualifizierten Domainnamen für den Admin Node ein. (Falls erforderlich, kann stattdessen die IP-Adresse des Knotens verwendet werden. Wenn hier jedoch eine IP-Adresse eingegeben wird, ist zu beachten, dass diese relying party trust aktualisiert oder neu erstellt werden muss, falls sich die IP-Adresse jemals ändert.)

e. Auf der Seite „Kennungen konfigurieren“ ist die Kennung der vertrauenden Partei für denselben Admin-Knoten anzugeben:

Admin_Node_Identifier

Für *Admin_Node_Identifier* den Admin-Knoten ist der Relying Party Identifier exakt so einzugeben, wie er auf der Single Sign-on-Seite angezeigt wird. Zum Beispiel `SG-DC1-ADM1`.

f. Die Einstellungen werden überprüft, die Vertrauensstellung der vertrauenden Seite gespeichert und der Assistent geschlossen.

Das Dialogfeld „Richtlinie zur Schadensmeldung bearbeiten“ wird angezeigt.

Falls das Dialogfeld nicht angezeigt wird, klicken Sie mit der rechten Maustaste auf das Trust und wählen Sie **Richtlinie zur Anspruchsausstellung bearbeiten**.

6. Um den Assistenten für Anspruchsregeln zu starten, **Regel hinzufügen** auswählen:
   a. Auf der Seite „Regelvorlage auswählen“ in der Liste **LDAP-Attribute als Ansprüche senden** auswählen und **Weiter** wählen.
   b. Auf der Seite „Regel konfigurieren“ einen Anzeigenamen für diese Regel eingeben.

      Beispielsweise **ObjectGUID zu Name ID** oder **UPN zu Name ID**.

   c. Für den Attributspeicher wird **Active Directory** ausgewählt.
   d. ${post_edited_translations.segment}
   e. In der Spalte „Ausgehender Anspruchstyp“ der Zuordnungstabelle wird **Name ID** aus der Dropdown-Liste ausgewählt.
   f. **Fertigstellen** und anschließend **OK** auswählen.
7. ${post_edited_translations.segment}
8. Auf der Registerkarte **Endpunkte** wird der Endpunkt für Single Logout (SLO) konfiguriert:
   a. **SAML hinzufügen** auswählen.
   b. Wählen Sie **Endpunkttyp** > **SAML Logout**.
   c. **Bindung** > **Umleitung** auswählen.
   d. Im Feld **Vertrauenswürdige URL** ist die URL anzugeben, die für das Single Logout (SLO) von diesem Admin-Node verwendet wird:

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

   Für *Admin_Node_FQDN* geben Sie den vollqualifizierten Domainnamen des Admin Node ein. (Falls erforderlich, kann stattdessen die IP-Adresse des Node verwendet werden. Wenn jedoch eine IP-Adresse eingegeben wird, ist zu beachten, dass diese relying party trust aktualisiert oder neu erstellt werden muss, falls sich die IP-Adresse jemals ändert.)

a. Wählen Sie **OK**.

9. Auf der Registerkarte **Signatur** wird das Signaturzertifikat für diese Relying-Party-Vertrauensstellung angegeben:
   a. Das benutzerdefinierte Zertifikat hinzufügen:
      - Wenn Sie über das benutzerdefinierte Verwaltungszertifikat verfügen, das Sie in StorageGRID hochgeladen haben, wählen Sie dieses Zertifikat aus.
      - Falls das benutzerdefinierte Zertifikat nicht vorhanden ist, am Admin Node anmelden, in das `/var/local/mgmt-api` Verzeichnis des Admin Node wechseln und die `custom-server.crt` Zertifikatsdatei hinzufügen.

> Die Verwendung des Standardzertifikats des Admin-Knotens (`server.crt` ist nicht empfohlen. Wenn der Admin-Knoten ausfällt, wird das Standardzertifikat bei der Wiederherstellung des Knotens neu generiert und die Vertrauensstellung der vertrauenden Seite muss aktualisiert werden.

   b. **Anwenden** und anschließend **OK** auswählen.

      Die Eigenschaften der Relying Party werden gespeichert und geschlossen.

10. ${post_edited_translations.segment}
11. Wenn Sie fertig sind, kehren Sie zu StorageGRID zurück und "${post_edited_translations.segment}" um zu bestätigen, dass sie korrekt konfiguriert sind.

Erstellen Sie Unternehmensanwendungen in Entra ID für StorageGRID

Entra ID wird verwendet, um eine Unternehmensanwendung für jeden Admin-Knoten in Ihrem System zu erstellen.

Bevor Sie beginnen

- Sie haben mit der Konfiguration von Single Sign-On für StorageGRID begonnen und **Entra ID** als SSO-Typ ausgewählt.
- Sie haben "Sandbox-Modus wurde aktiviert" im Grid Manager.
- Sie haben den **Enterprise application name** für jeden Admin-Node in Ihrem System. Diese Werte können aus der Admin-Node-Detailtabelle auf der Seite „SSO konfigurieren“ kopiert werden.

> Sie müssen für jeden Admin Node in Ihrem StorageGRID System eine Unternehmensanwendung erstellen. Eine eigene Unternehmensanwendung für jeden Admin Node stellt sicher, dass sich Benutzer sicher bei jedem Admin Node anmelden und wieder ausloggen können.

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

Entra ID aufrufen

Schritte

1. Melden Sie sich bei der "Azure Portal"an.

2. Navigieren Sie zu "Entra ID".
3. Wählen Sie "Unternehmensanwendungen".

Unternehmensanwendungen erstellen und StorageGRID SSO-Konfiguration speichern

Um die SSO-Konfiguration für Entra ID in StorageGRID zu speichern, ist es erforderlich, mit Entra ID für jeden Admin-Knoten eine Unternehmensanwendung zu erstellen. Die Föderationsmetadaten-URLs werden aus Entra ID kopiert und in die entsprechenden Felder für **Federation metadata URL** auf der Seite „SSO konfigurieren“ eingefügt.

Schritte

1. ${post_edited_translations.segment}
    a. Im Bereich Entra ID Enterprise-Anwendungen die Option **Neue Anwendung** auswählen.
    b. **Eigene Anwendung erstellen** auswählen.
    c. Für den Namen ist der **Enterprise application name** einzugeben, der aus der Tabelle „Admin-Knotendetails“ auf der Seite „SSO konfigurieren“ kopiert wurde.
    d. Die Option **Integrate any other application you don’t find in the gallery (Non-gallery)** bleibt ausgewählt.
    e. Wählen Sie **Create**.
    f. Wählen Sie den Link **Los geht’s** im Feld **2. Einmalanmeldung einrichten** oder den Link **Einmalanmeldung** in der linken Marge.
    g. Das Kontrollkästchen **SAML** auswählen.
    h. ${post_edited_translations.segment}
    i. ${post_edited_translations.segment}
2. Nachdem Sie für jeden Admin-Knoten eine Metadaten-URL für die Föderation eingefügt und alle anderen erforderlichen Änderungen an der SSO-Konfiguration vorgenommen haben, auf der Seite „SSO konfigurieren“ **Speichern** auswählen.

${post_edited_translations.segment}

${post_edited_translations.segment}

Schritte

1. Diese Schritte sind für jeden Admin Node zu wiederholen.
    a. Bei StorageGRID vom Admin-Knoten aus anmelden.
    b. **Konfiguration** > **Zugriffskontrolle** > **Single sign-on** auswählen.
    c. Die Schaltfläche auswählen, um die SAML-Metadaten für diesen Admin-Knoten herunterzuladen.
    d. Die Datei speichern, die anschließend in Entra ID hochgeladen wird.

SAML-Metadaten in jede Unternehmensanwendung hochladen

Nach dem Herunterladen einer SAML-Metadatendatei für jeden StorageGRID Admin Node sind in Entra ID die folgenden Schritte durchzuführen:

Schritte

1. Zurück zum Azure Portal.

2. ${post_edited_translations.segment}

> Möglicherweise ist es erforderlich, die Seite „Unternehmensanwendungen“ zu aktualisieren, damit zuvor hinzugefügte Anwendungen in der Liste angezeigt werden.

   a. Zur Eigenschaftenseite der Unternehmensanwendung wechseln.
   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}
   d. Die SAML-Konfiguration abschließen.
   e. Die Schaltfläche **Metadatendatei hochladen** auswählen und die SAML-Metadatendatei auswählen, die für den entsprechenden Admin Node heruntergeladen wurde.
   f. Nachdem die Datei geladen wurde, **Speichern** auswählen und anschließend **X**, um das Fenster zu schließen. Die Seite „Single Sign-On mit SAML einrichten“ wird wieder angezeigt.

3. "Jede Anwendung testen".

Erstellen Sie Dienstanbieterverbindungen in PingFederate für StorageGRID

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

Bevor Sie beginnen

- Sie haben Single Sign-On für StorageGRID konfiguriert und **Ping Federate** als SSO-Typ ausgewählt.
- Sie haben "Sandbox-Modus wurde aktiviert" im Grid Manager.
- Sie verfügen über die **SP-Verbindungskennung** für jeden Admin Node in Ihrem System. Sie finden diese Werte in der Detailtabelle der Admin Nodes auf der Seite „Configure SSO“.
- Sie haben die **SAML-Metadaten** für jeden Admin Node in Ihrem System heruntergeladen.
- Sie haben Erfahrung in der Erstellung von SP Verbindungen im PingFederate Server.
- Sie haben die "Administrator-Referenzhandbuch" für den PingFederate Server. Die PingFederate Dokumentation enthält detaillierte Schritt-für-Schritt-Anleitungen und Erklärungen.
- Sie haben die "Administratorberechtigung" für den PingFederate Server.

Über diese Aufgabe

Diese Anleitung fasst zusammen, wie der PingFederate Server Version 10.3 als SSO-Anbieter für StorageGRID konfiguriert wird. Wenn eine andere Version von PingFederate verwendet wird, müssen diese Anweisungen möglicherweise angepasst werden. In der PingFederate Server-Dokumentation finden Sie ausführliche Anweisungen für Ihre Version.

Voraussetzungen in PingFederate abschließen

Bevor Sie die SP Verbindungen für StorageGRID erstellen können, müssen Sie die erforderlichen Voraufgaben in PingFederate abschließen. Informationen aus diesen Voraufgaben werden bei der Konfiguration der SP Verbindungen verwendet.

Datenspeicher erstellen

Falls noch nicht geschehen, einen Datenspeicher erstellen, um PingFederate mit dem AD FS LDAP-Server zu

verbinden. Die Werte verwenden, die beim "Konfiguration der Identitätsföderation" in StorageGRID verwendet wurden.

- **Typ**: Verzeichnis (LDAP)
- **LDAP-Typ**: Active Directory
- **Name des Binärattributs**: **objectGUID** ist auf der Registerkarte LDAP-Binärattribute exakt wie angegeben einzugeben.

Passwort-Anmeldeinformationsvalidator erstellen

Falls noch nicht geschehen, einen Passwort-Anmeldeinformationsprüfer erstellen.

- **Typ**: LDAP-Benutzername Passwort Credential Validator
- **Datenspeicher**: Der von Ihnen erstellte Datenspeicher wird ausgewählt.
- **Suchbasis**: Informationen aus LDAP eingeben (z. B. DC=saml,DC=sgws).
- **Suchfilter**: sAMAccountName=${username}
- **Gültigkeitsbereich**: Teilbaum

IdP Adapterinstanz erstellen

Falls noch nicht geschehen, eine IdP-Adapterinstanz erstellen.

Schritte

1. Wechseln Sie zu **Authentifizierung** > **Integration** > **IdP Adapter**.
2. **Neue Instanz erstellen** auswählen.
3. Auf der Registerkarte „Typ“ ist **HTML Form IdP Adapter** auszuwählen.
4. Auf der Registerkarte „IdP-Adapter“ die Option **Neue Zeile zu 'Credential Validators' hinzufügen** auswählen.
5. Wählen Sie die Passwort-Anmeldeinformationsprüfer aus, die Sie erstellt haben.
6. Auf der Registerkarte Adapterattribute ist das Attribut **username** für **Pseudonym** auszuwählen.
7. **Speichern** auswählen.

Signaturzertifikat erstellen oder importieren

Falls noch nicht geschehen, das Signaturzertifikat erstellen oder importieren.

Schritte

1. Wechseln Sie zu **Sicherheit** > **Signatur- und Entschlüsselungsschlüssel & Zertifikate**.
2. Das Signaturzertifikat wird erstellt oder importiert.

Eine SP Verbindung in PingFederate erstellen

Wenn eine SP-Verbindung in PingFederate erstellt wird, wird die SAML-Metadaten-Datei importiert, die zuvor von StorageGRID für den Admin-Node heruntergeladen wurde. Die Metadatendatei enthält viele der benötigten spezifischen Werte.

Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID-System eine SP-Verbindung erstellen, damit sich Benutzer sicher an jedem Knoten an- und abmelden können. Diese Anweisungen dienen dazu, die erste SP-Verbindung zu erstellen. Anschließend zu Zusätzliche SP Verbindungen erstellen können alle weiteren benötigten Verbindungen erstellt werden.

SP Verbindungstyp auswählen

Schritte

1. Wechseln Sie zu **Anwendungen** > **Integration** > **SP Connections**.
2. **Verbindung erstellen** auswählen.
3. **Für diese Verbindung keine Vorlage verwenden** auswählen.
4. **Browser SSO Profiles** und **SAML 2.0** als Protokoll auswählen.

SP Metadaten importieren

Schritte

1. Auf der Registerkarte „Metadaten importieren“ wird **Datei** ausgewählt.
2. Wählen Sie die SAML-Metadatendatei aus, die Sie von der Seite „SSO konfigurieren“ für den Admin Node heruntergeladen haben.
3. Die Metadatenübersicht und die Informationen auf der Registerkarte „Allgemeine Informationen“ werden angezeigt.

   Die Partner-Entitäts-ID und der Verbindungsname sind auf die StorageGRID SP Verbindung-ID festgelegt. (zum Beispiel 10.96.105.200-DC1-ADM1-105-200). Die Basis-URL ist die IP des StorageGRID Admin Node.

4. **Weiter** auswählen.

IdP Browser-SSO konfigurieren

Schritte

1. Auf der Registerkarte „Browser SSO“ die Option „Browser SSO konfigurieren“ auswählen.
2. Auf der Registerkarte SAML-Profile die Optionen **SP-initiiertes SSO**, **SP-initiales SLO**, **IdP-initiiertes SSO** und **IdP-initiiertes SLO** auswählen.
3. **Weiter** auswählen.
4. Auf der Registerkarte „Assertion Lifetime“ werden keine Änderungen vorgenommen.
5. Auf der Registerkarte „Assertion Creation“ die Option **Assertion Creation konfigurieren** auswählen.
   a. Auf der Registerkarte „Identitätszuordnung“ wird **Standard** ausgewählt.
   b. Auf der Registerkarte „Attributvertrag“ wird **SAML_SUBJECT** als Attributvertrag und das importierte, nicht spezifizierte Namensformat verwendet.
6. Wählen Sie unter „Vertrag verlängern“ die Option **Löschen**, um das `urn:oid` zu entfernen, das nicht verwendet wird.

Adapterinstanz zuordnen

Schritte

1. Auf der Registerkarte „Zuordnung der Authentifizierungsquelle“ die Option **Neue Adapterinstanz**

zuordnen auswählen.

2. Auf der Registerkarte „Adapterinstanz“ die von Ihnen erstellte Adapterinstanz Instanz auswählen.
3. Auf der Registerkarte „Mapping-Methode“ ist **Zusätzliche Attribute aus einem Datenspeicher abrufen** auszuwählen.
4. Auf der Registerkarte „Attributquelle & Benutzersuche“ **Attributquelle hinzufügen** auswählen.
5. Geben Sie auf der Registerkarte „Datenspeicher“ eine Beschreibung an und wählen Sie die Datenspeicher aus, die Sie hinzugefügt haben.
6. Auf der Registerkarte „LDAP-Verzeichnissuche“:
   - Geben Sie den **Basis-DN** ein, der exakt mit dem Wert übereinstimmen muss, den Sie in StorageGRID für den LDAP-Server eingegeben haben.
   - Für den Suchbereich **Unterbaum** auswählen.
   - Für die Root-Objektklasse nach einem der folgenden Attribute suchen und entweder **objectGUID** oder **userPrincipalName** hinzufügen.
7. Auf der Registerkarte LDAP Binary Attribute Encoding Types ist für das Attribut **objectGUID** der Typ **Base64** auszuwählen.
8. Auf der Registerkarte LDAP-Filter **sAMAccountName=${username}** eingeben.
9. Auf der Registerkarte „Attributvertragserfüllung“ im Dropdown-Menü „Quelle“ **LDAP (Attribut)** auswählen und im Dropdown-Menü „Wert“ entweder **objectGUID** oder **userPrincipalName** auswählen.
10. Die Attributquelle wird überprüft und anschließend gespeichert.
11. Auf der Registerkarte „Failsave-Attributquelle“ die Option **SSO-Transaktion abbrechen** auswählen.
12. Die Zusammenfassung kann überprüft und **Fertig** ausgewählt werden.
13. **Fertig** auswählen.

Protokolleinstellungen konfigurieren

Schritte

1. Auf der Registerkarte **SP Connection** > **Browser SSO** > **Protocol Settings** ist **Configure Protocol Settings** auszuwählen.
2. Auf der Registerkarte „Assertion Consumer Service URL“ die Standardwerte übernehmen, die aus den StorageGRID SAML-Metadaten importiert wurden (**POST** für Binding und `/api/saml-response` für Endpoint URL).
3. Auf der Registerkarte SLO Service URLs die Standardwerte übernehmen, die aus den StorageGRID SAML-Metadaten importiert wurden (**REDIRECT** für Binding und `/api/saml-logout` für Endpoint URL).
4. Auf der Registerkarte „Zulässige SAML-Bindungen“ sind **ARTIFACT** und **SOAP** zu deaktivieren. Nur **POST** und **REDIRECT** sind erforderlich.
5. Auf der Registerkarte „Signaturrichtlinie“ bleiben die Kontrollkästchen **Authn-Anfragen müssen signiert werden** und **Assertion immer signieren** ausgewählt.
6. Auf der Registerkarte „Verschlüsselungsrichtlinie“ ist **Keine** auszuwählen.
7. Die Zusammenfassung kann überprüft und mit **Fertig** die Protokolleinstellungen gespeichert werden.
8. Die Zusammenfassung kann überprüft und mit **Fertig** die Browser SSO-Einstellungen gespeichert werden.

Anmeldeinformationen konfigurieren

Schritte

1. Wählen Sie auf der Registerkarte SP Connection die Option **Anmeldeinformationen**.
2. Auf der Registerkarte „Anmeldeinformationen“ die Option **Anmeldeinformationen konfigurieren** auswählen.
3. Wählen Sie die Unterzeichnungszertifikat aus, die Sie erstellt oder importiert haben.
4. **Weiter** auswählen, um zu **Einstellungen für die Signaturprüfung verwalten** zu gelangen.
   a. Auf der Registerkarte „Vertrauensmodell“ die Option „Nicht verankert“ auswählen.
   b. Auf der Registerkarte „Signaturverifizierungszertifikat“ werden die Informationen zum Signaturzertifikat angezeigt, die aus den StorageGRID SAML-Metadaten importiert wurden.
5. Die Zusammenfassungsbildschirme werden überprüft und mit **Speichern** wird die SP Verbindung gespeichert.

Zusätzliche SP Verbindungen erstellen

Sie können die erste SP-Verbindung kopieren, um die SP-Verbindungen zu erstellen, die Sie für jeden Admin-Knoten in Ihrem Grid benötigen. Für jede Kopie werden neue Metadaten hochgeladen.

> Die SP Verbindungen für verschiedene Admin-Knoten verwenden identische Einstellungen, mit Ausnahme der Partner Entity ID, der Base URL, der Connection ID, des Connection Name, der Signature Verification und der SLO Response URL.

Schritte

1. Wählen Sie **Aktion** > **Kopieren**, um eine Kopie der ursprünglichen SP-Verbindung für jeden zusätzlichen Admin-Knoten zu erstellen.
2. Geben Sie die Verbindungs-ID und den Verbindungsnamen für die Kopie ein und wählen Sie **Speichern**.
3. Wählen Sie die Metadatendatei aus, die dem Admin-Node entspricht:
   a. **Aktion** > **Mit Metadaten aktualisieren** auswählen.
   b. **Datei auswählen** auswählen und die Metadaten hochladen.
   c. **Weiter** auswählen.
   d. **Speichern** auswählen.
4. Der Fehler aufgrund des ungenutzten Attributs wird behoben:
   a. Die neue Verbindung auswählen.
   b. **Browser SSO konfigurieren > Assertionserstellung konfigurieren > Attributvertrag** auswählen.
   c. Löschen Sie den Eintrag für **urn:oid**.
   d. **Speichern** auswählen.

SSO in StorageGRID deaktivieren

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

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Du hast "spezifische Zugriffsberechtigungen".

Schritte

1. **Konfiguration** > **Zugriffskontrolle** > **Single sign-on** auswählen.

   Die Single Sign-on-Seite wird angezeigt.

2. **SSO deaktivieren** auswählen.
3. **Ja** auswählen.

   Es erscheint eine Warnmeldung, dass sich lokale Benutzer nun anmelden können.

Beim nächsten Anmelden bei StorageGRID erscheint die StorageGRID-Anmeldeseite, und Sie müssen den Benutzernamen und das Passwort für einen lokalen oder föderierten StorageGRID Benutzer eingeben.

SSO für einen StorageGRID Admin-Node vorübergehend deaktivieren und wieder aktivieren

Sie können sich möglicherweise nicht beim Grid Manager anmelden, wenn das Single Sign-On (SSO)-System ausfällt. In diesem Fall kann SSO für einen Admin-Knoten vorübergehend deaktiviert und anschließend wieder aktiviert werden. Zum Deaktivieren und anschließenden erneuten Aktivieren von SSO ist der Zugriff auf die Befehlsshell des Knotens erforderlich.

Bevor Sie beginnen

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

Über diese Aufgabe

Nachdem Sie SSO für einen Admin-Knoten deaktiviert haben, können Sie sich beim Grid Manager als lokaler Root-Benutzer anmelden. Um Ihr StorageGRID System zu schützen, muss die Befehlsshell des Knotens verwendet werden, um SSO auf dem Admin-Knoten unmittelbar nach dem Abmelden wieder zu aktivieren.

> Die Deaktivierung von SSO für einen Admin-Knoten hat keine Auswirkungen auf die SSO-Einstellungen anderer Admin-Knoten im Grid. Das Kontrollkästchen **Enable SSO** auf der Seite Single Sign-on im Grid Manager bleibt ausgewählt, und alle bestehenden SSO-Einstellungen werden beibehalten, sofern sie nicht aktualisiert werden.

Schritte

1. ${post_edited_translations.segment}
   a. Geben Sie den folgenden Befehl ein: `ssh admin@Admin_Node_IP`
   b. Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.
   c. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
   d. Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.

      Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` zu `#`.

2. Führen Sie folgenden Befehl aus:`disable-saml`

   Eine Meldung weist darauf hin, dass der Befehl nur für diesen Admin Node gilt.

3. Bestätigen Sie, dass SSO deaktiviert werden soll.

   Eine Meldung weist darauf hin, dass Single Sign-On auf dem Knoten deaktiviert ist.

4. ${post_edited_translations.segment}

   Die Anmeldeseite des Grid Managers wird jetzt angezeigt, da SSO deaktiviert wurde.

5. Mit dem Benutzernamen root und dem Passwort des lokalen Root-Benutzers anmelden.
6. Wenn Sie SSO vorübergehend deaktiviert haben, weil die SSO-Konfiguration korrigiert werden musste:
   a. **Konfiguration** > **Zugriffskontrolle** > **Single sign-on** auswählen.
   b. Die fehlerhaften oder veralteten SSO-Einstellungen können geändert werden.
   c. **Speichern** auswählen.

      Durch Auswahl von **Speichern** auf der Single Sign-on-Seite wird SSO für das gesamte Grid 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 die Aufgabe oder Aufgaben aus, die erforderlich sind.
   b. **Abmelden** auswählen und den Grid Manager schließen.
   c. SSO kann auf dem Admin-Node erneut aktiviert werden. Einer der folgenden Schritte ist möglich:

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

        Eine Meldung weist darauf hin, dass der Befehl nur für diesen Admin Node gilt.

      Bestätigen Sie, dass Sie SSO aktivieren möchten.

   Eine Meldung weist darauf hin, dass Single Sign-On auf dem Knoten aktiviert ist.

      - Grid-Knoten neu starten: `reboot`

8. Über einen Webbrowser kann vom selben Admin-Knoten aus auf den Grid Manager zugegriffen werden.
9. Bestätigt wird, dass die StorageGRID Sign in-Seite angezeigt wird und dass zur Anmeldung beim Grid Manager die SSO-Anmeldedaten eingegeben werden müssen.

Grid Federation verwenden

Erfahren Sie mehr über StorageGRID Grid-Föderation

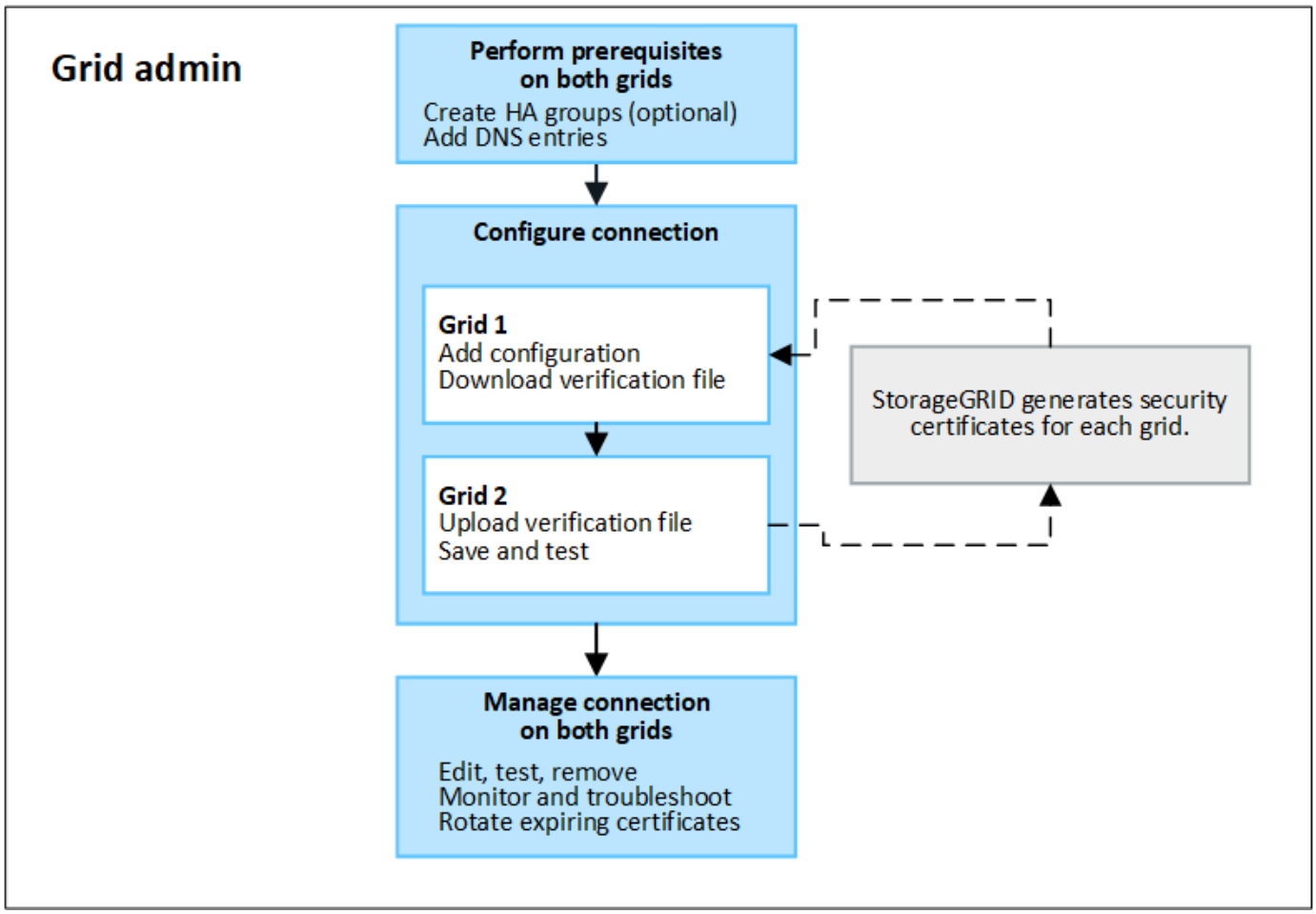
Mit der Grid-Federation ist das Klonen von Mandanten und das Replizieren ihrer Objekte zwischen zwei StorageGRID Systemen zur Notfallwiederherstellung möglich.

Was ist eine Grid Federation Verbindung?

Eine Grid-Federation-Verbindung ist eine bidirektionale, vertrauenswürdige und sichere Verbindung zwischen Admin- und Gateway-Knoten in zwei StorageGRID Systemen.

Workflow für Grid Federation

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



Überlegungen und Anforderungen für Grid Federation Verbindungen

- Die für die Grid Federation verwendeten Grids müssen StorageGRID Versionen verwenden, die entweder identisch sind oder sich in maximal einer Hauptversion unterscheiden.

  Einzelheiten zu den Versionsvoraussetzungen finden Sie in der "Versionshinweise". Sie müssen sich mit Ihrem NetApp Konto anmelden oder ein Konto erstellen, um auf die Versionshinweise zuzugreifen.

- Ein Grid kann eine oder mehrere Grid-Federationsverbindungen zu anderen Grids haben. Jede Grid-Federationsverbindung ist unabhängig von anderen Verbindungen. Wenn beispielsweise Grid 1 eine Verbindung zu Grid 2 und eine zweite Verbindung zu Grid 3 hat, besteht keine implizite Verbindung zwischen Grid 2 und Grid 3.
- Grid Federation-Verbindungen sind bidirektional. Nach der Verbindungsherstellung besteht die Möglichkeit, die Verbindung von beiden Grids aus zu überwachen und zu verwalten.
- Mindestens eine Grid Federation-Verbindung muss vorhanden sein, bevor "Konto klonen" oder

"gridübergreifende Replikation" verwendet werden können.

Netzwerk- und IP-Adressanforderungen

- Grid Federation-Verbindungen können im Grid Network, im Admin Network oder im Client Network auftreten.
- Eine Grid-Federation-Verbindung verbindet ein Grid mit einem anderen Grid. Die Konfiguration jedes Grids legt einen Grid-Federation-Endpunkt im jeweils anderen Grid fest, der aus Admin-Knoten, Gateway-Knoten oder beiden bestehen kann.
- Die bewährte Methode ist, "Hochverfügbarkeitsgruppen (HA)" von Gateway- und Admin-Knoten in jedem Grid zu verbinden. Durch die Verwendung von HA-Gruppen wird sichergestellt, dass Grid-Federation-Verbindungen online bleiben, wenn Knoten nicht verfügbar sind. Wenn die aktive Schnittstelle in einer der beiden HA-Gruppen ausfällt, kann die Verbindung eine Backup-Schnittstelle nutzen.
- Es wird nicht empfohlen, eine Grid Federation Verbindung über die IP-Adresse eines einzelnen Admin-Knotens oder Gateway-Knotens herzustellen. Wenn dieser Knoten nicht verfügbar ist, steht auch die Grid Federation Verbindung nicht zur Verfügung.
- "Gridübergreifende Replikation"Die Verwaltung von Objekten erfordert, dass die Storage Nodes in jedem Grid auf die konfigurierten Admin- und Gateway Nodes im jeweils anderen Grid zugreifen können. Für jedes Grid sollte bestätigt werden, dass alle Storage Nodes eine Route mit hoher Bandbreite zu den als Admin Nodes oder Gateway Nodes für die Verbindung genutzten Knoten haben.

FQDNs zur Lastverteilung der Verbindung verwenden

Für eine Produktionsumgebung sollten vollqualifizierte Domainnamen (FQDNs) verwendet werden, um jedes Grid in der Verbindung zu identifizieren. Anschließend sind die entsprechenden DNS-Einträge wie folgt zu erstellen:

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

Bei Verwendung mehrerer DNS-Einträge wird die Nutzung der Verbindung wie folgt auf verschiedene Anfragen verteilt (Lastausgleich):

- DNS-Einträge, die den VIP-Adressen mehrerer HA-Gruppen zugeordnet sind, werden zwischen den aktiven Knoten in den HA-Gruppen lastausgeglichen.
- DNS-Einträge, die den IP-Adressen mehrerer Admin-Knoten oder Gateway-Knoten zugeordnet sind, werden zwischen den zugeordneten Knoten per Lastausgleich verteilt.

Port-Anforderungen

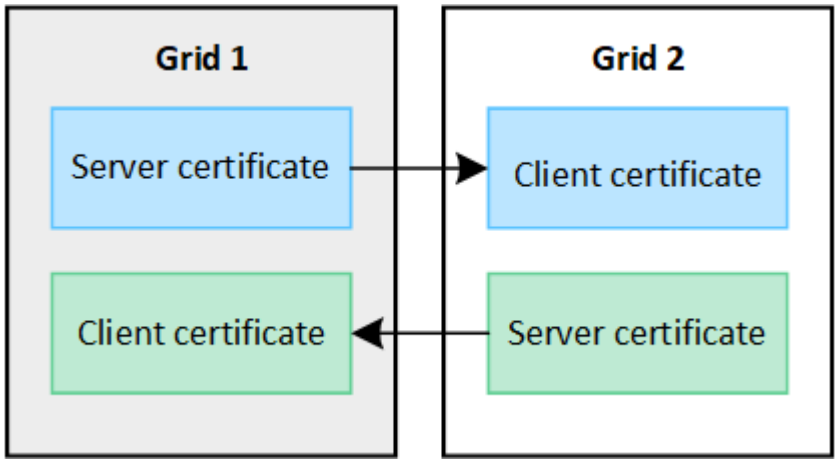
Beim Erstellen einer Grid Federation Verbindung kann eine beliebige ungenutzte Portnummer von 23000 bis 23999 angegeben werden. Beide Grids in dieser Verbindung verwenden denselben Port.

Es ist sicherzustellen, dass kein Knoten in einem der beiden Grids diesen Port für andere Verbindungen verwendet.

Zertifikatsanforderungen

Wenn eine Grid-Federation-Verbindung konfiguriert wird, generiert StorageGRID automatisch vier SSL-Zertifikate:

- Server- und Clientzertifikate zur Authentifizierung und Verschlüsselung von Informationen, die von Grid 1 zu Grid 2 gesendet werden
- Server- und Clientzertifikate zur Authentifizierung und Verschlüsselung von Informationen, die von Grid 2 an Grid 1 übertragen werden



Standardmäßig sind die Zertifikate 730 Tage (2 Jahre) gültig. Wenn diese Zertifikate sich dem Ablaufdatum nähern, weist die Warnmeldung **Expiration of grid federation certificate** darauf hin, dass die Zertifikate erneuert werden sollten, was über den Grid Manager möglich ist.

> Wenn die Zertifikate an einem der beiden Enden der Verbindung ablaufen, funktioniert die Verbindung nicht mehr. Die Datenreplikation bleibt ausstehend, bis die Zertifikate aktualisiert werden.

Mehr erfahren

- "Grid Federation Verbindungen erstellen"
- "Grid Federation-Verbindungen verwalten"
- "Fehler in der Grid-Federation beheben"

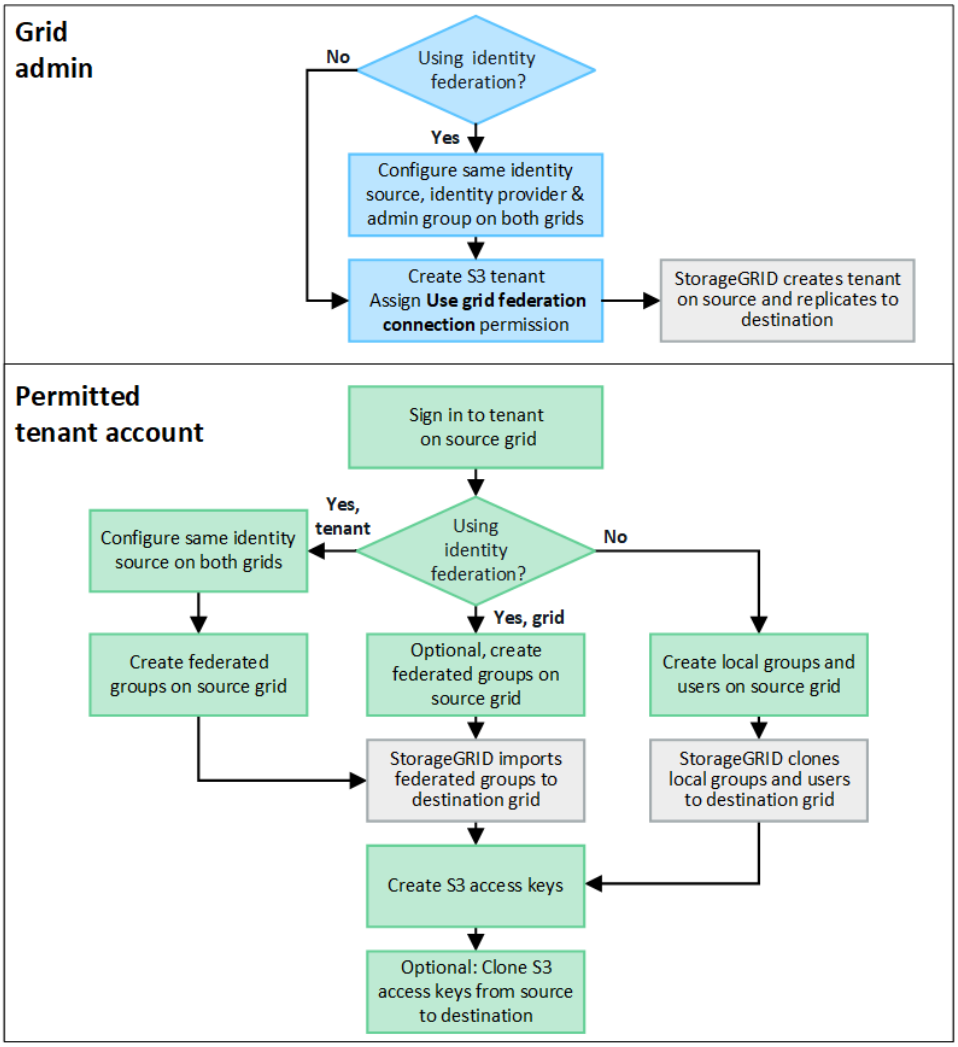
Erfahren Sie mehr über das Klonen von Konten in StorageGRID

Account Clone ist die automatische Replikation eines Mandantenkontos, von Mandantengruppen, Mandantenbenutzern und optional von S3-Zugriffsschlüsseln zwischen den StorageGRID Systemen in einer "Grid Federation Verbindung".

Account-Klon ist erforderlich für "gridübergreifende Replikation". Das Klonen von Kontoinformationen von einem Quell StorageGRID System zu einem Ziel StorageGRID System stellt sicher, dass Mandantenbenutzer und -gruppen auf die entsprechenden Buckets und Objekte in beiden Grids zugreifen können.

Workflow für die Kontoklonierung

Das Workflow-Diagramm zeigt die Schritte, die Grid-Administratoren und berechtigte Mandanten zur Einrichtung der Kontoklonierung durchführen. Diese Schritte werden nach dem "Die Grid Federation Verbindung ist konfiguriert" durchgeführt.



Grid Admin-Workflow

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

SSO für Kontoklonen konfigurieren (optional)

Wenn eines der StorageGRID Systeme in der Grid Federation-Verbindung SSO verwendet, müssen beide Grids SSO verwenden. Vor der Erstellung der Mandantenkonten für die Grid Federation müssen die Grid-Administratoren der Quell- und Ziel-Grids des Mandanten diese Schritte durchführen.

Schritte

1. Konfigurieren Sie dieselbe Identitätsquelle für beide Grids. Siehe "Identitätsföderation verwenden".
2. Es ist derselbe SSO-Identitätsanbieter (IdP) für beide Grids zu konfigurieren. Siehe "Einmalanmeldung konfigurieren".
3. "Dieselbe Administratorgruppe erstellen" auf beiden Grids durch Importieren derselben Verbundgruppe.

   Wenn der Mandant erstellt wird, wird diese Gruppe ausgewählt, damit sie die anfängliche Root-Zugriffsberechtigung sowohl für das Quell- als auch für das Zielmandantenkonto erhält.

Wenn diese Administratorgruppe auf beiden Grids vor der Erstellung des Mandanten nicht existiert, wird der Mandant nicht an das Ziel repliziert.

${post_edited_translations.segment}

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

Schritte

1. Konfigurieren Sie dieselbe Identitätsquelle für beide Grids. Siehe "Identitätsföderation verwenden".
2. Optional kann eine föderierte Gruppe anfängliche Root-Zugriffsberechtigungen sowohl für das Quell- als auch für das Ziel-Tenant-Konto "Dieselbe Administratorgruppe erstellen" auf beiden Grids erhalten, indem dieselbe föderierte Gruppe importiert wird.

   Wenn einer föderierten Gruppe, die auf beiden Grids nicht existiert, die Berechtigung zum Root-Zugriff zugewiesen wird, wird der Mandant nicht auf das Ziel-Grid repliziert.

3. Wenn Sie nicht möchten, dass eine Verbundgruppe anfänglich 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 Identitätsföderation führt ein Grid-Administrator diese Schritte durch, um zu ermitteln, welche Mandanten Bucket-Objekte auf andere StorageGRID Systeme replizieren können.

Schritte

1. Bestimmen Sie, welches Grid das Quell-Grid des Mandanten für Kontoklonvorgänge ist.

   Das Grid, in dem der Mandant ursprünglich erstellt wurde, ist als *Quellgrid* des Mandanten bekannt. Das Grid, in dem der Mandant repliziert wird, ist als *Zielgrid* des Mandanten bekannt.

2. In diesem Grid ein neues S3-Mandantenkonto erstellen oder ein bestehendes Konto bearbeiten.
3. Die Berechtigung **Grid-Federation-Verbindung verwenden** zuweisen.
4. Wenn das Mandantenkonto seine eigenen Verbundbenutzer verwaltet, ist die Berechtigung **Eigene Identitätsquelle verwenden** zuzuweisen.

   Wenn diese Berechtigung zugewiesen ist, müssen sowohl das Quell- als auch das Zielmandantenkonto dieselbe Identitätsquelle konfigurieren, bevor föderierte Gruppen erstellt werden können. Föderierte Gruppen, die dem Quellmandanten hinzugefügt wurden, können nicht in den Zielmandanten geklont werden, es sei denn, beide Grids verwenden dieselbe Identitätsquelle.

5. Eine bestimmte Grid Federation-Verbindung auswählen.
6. ${post_edited_translations.segment}

   Wenn ein neuer Mandant mit der Berechtigung **Grid-Federationsverbindung verwenden** gespeichert wird, erstellt StorageGRID automatisch eine Replik dieses Mandanten im anderen Grid, wie folgt:

   - Beide Mandantenkonten haben die gleiche Konto-ID, den gleichen Namen, das gleiche Speicherkontingent und die gleichen zugewiesenen Berechtigungen.

- Wenn eine Verbundgruppe für Root-Zugriffsberechtigungen des Mandanten ausgewählt wurde, wird diese Gruppe in den Zielmandanten geklont.
- Wenn Sie einen lokalen Benutzer ausgewählt haben, der über die Root-Zugriffsberechtigung für den Mandanten verfügen soll, wird dieser Benutzer auf den Zielmandanten geklont. Das Kennwort für diesen Benutzer wird jedoch nicht geklont.

Weitere Informationen finden sich unter "Zulässige Mandanten für die Grid Federation verwalten".

Zulässiger Workflow für Mieterkonten

${post_edited_translations.segment}

Schritte

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}

   Wenn neue Gruppen oder Benutzer im Quellmandanten erstellt werden, klont StorageGRID diese automatisch in den Zielmandanten, aber es findet kein Klonen vom Ziel zurück zum Quellmandanten statt.

4. S3-Zugriffsschlüssel erstellen.
5. ${post_edited_translations.segment}

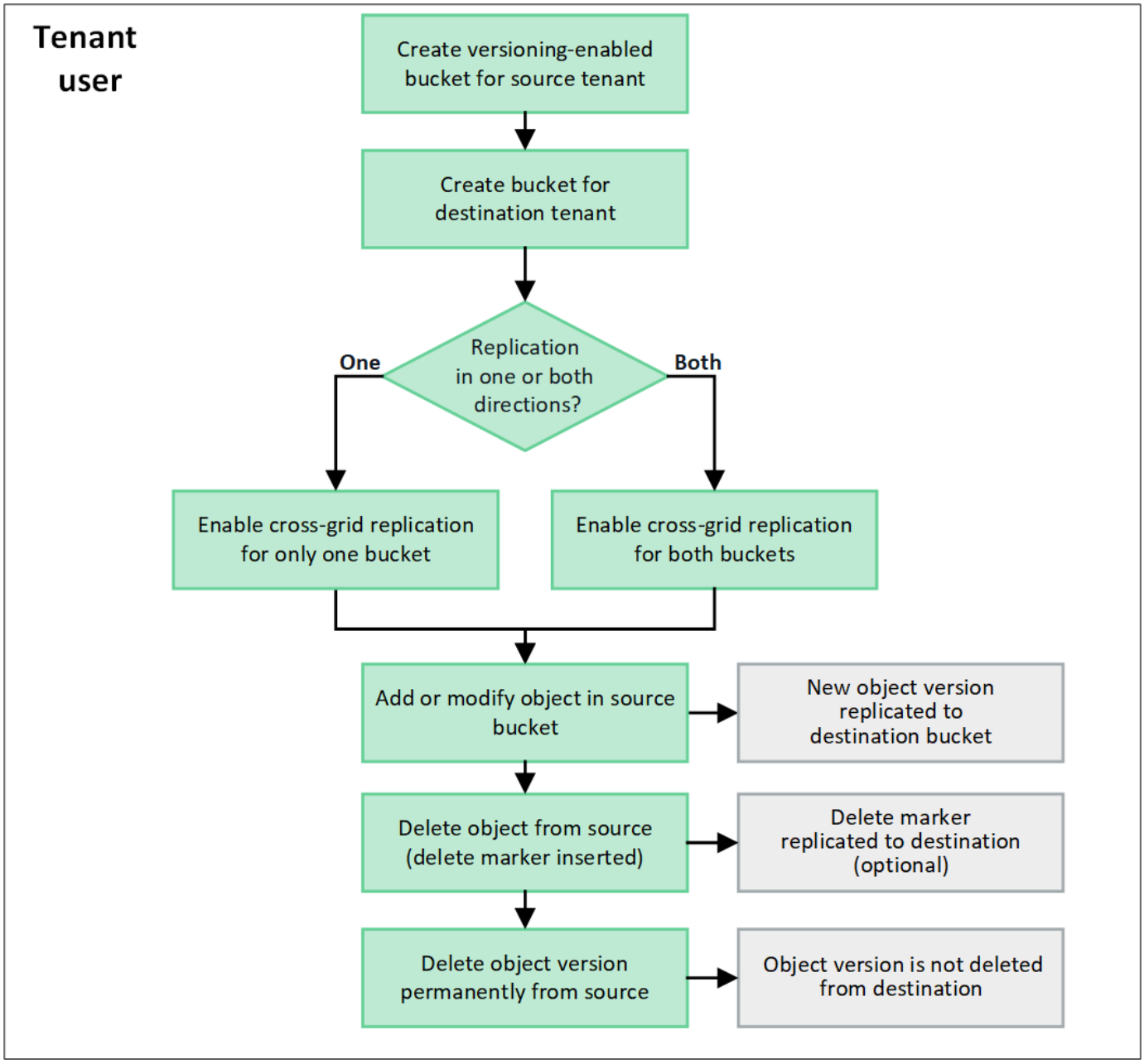
Details zum zulässigen Mandantenkonto-Workflow und Informationen zum Klonen von Gruppen, Benutzern und S3-Zugriffsschlüsseln finden Sie unter "Mandantengruppen und Benutzer klonen" und "Klonen von S3-Zugriffsschlüsseln mithilfe der API".

Erfahren Sie mehr über die gitterübergreifende Replikation in StorageGRID

Die Grid-übergreifende Replikation ist die automatische Replikation von Objekten zwischen ausgewählten S3 Buckets in zwei StorageGRID Systemen, die in einer "Grid Federation Verbindung" verbunden sind. Für die Grid-übergreifende Replikation ist "${post_edited_translations.segment}" erforderlich.

Workflow für die gridübergreifende Replikation

${post_edited_translations.segment}



Anforderungen an die netzübergreifende Replikation

Besitzt ein Mandantenkonto die Berechtigung **Grid-Federationsverbindung verwenden** zur Nutzung einer oder mehrerer "${post_edited_translations.segment}" Grid-Federationsverbindungen, kann ein Mandantenbenutzer mit Root-Zugriffsberechtigung Buckets in den entsprechenden Mandantenkonten auf jedem Grid erstellen. Diese Buckets:

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- Versionierung muss aktiviert sein
- ${post_edited_translations.segment}

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

Mehr erfahren

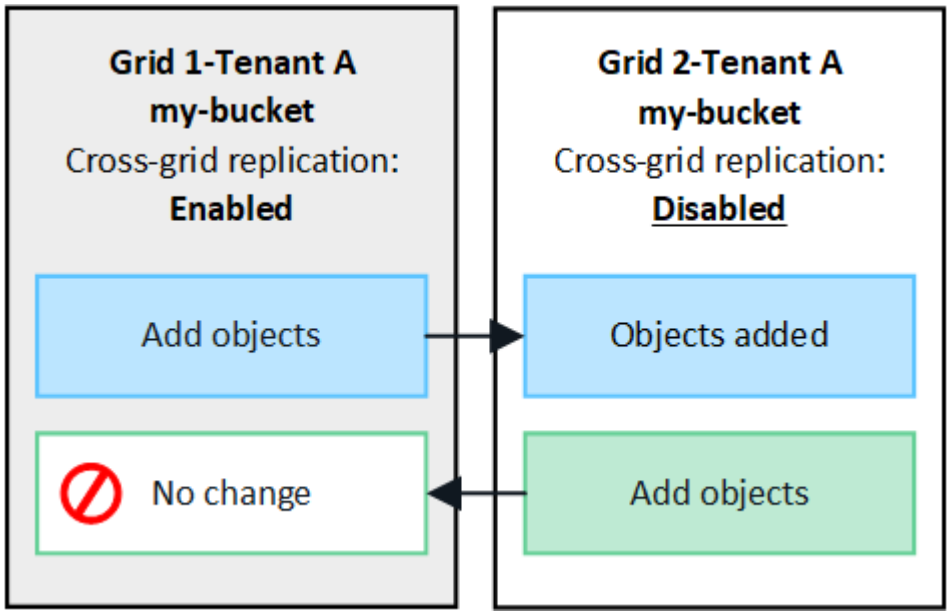
"Verwaltung der gridübergreifenden Replikation"

Funktionsweise der gridübergreifenden Replikation

Sie können die netzübergreifende Replikation so konfigurieren, dass sie in eine Richtung oder in beide Richtungen erfolgt.

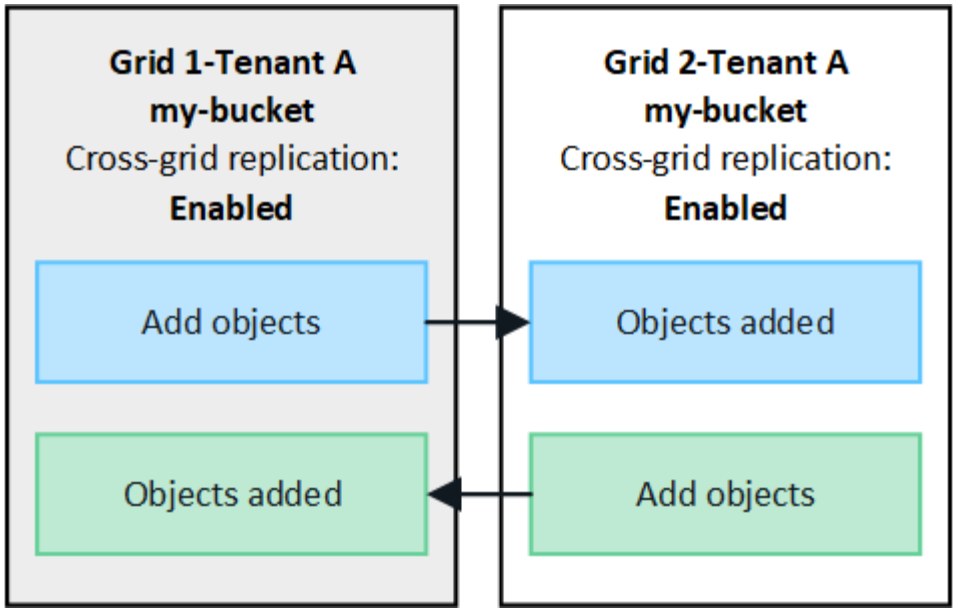
Replikation in eine Richtung

Wenn Sie die netzübergreifende Replikation für einen Bucket nur in einem Grid aktivieren, werden Objekte, die diesem Bucket (dem Quell-Bucket) hinzugefügt werden, in den entsprechenden Bucket im anderen Grid (dem Ziel-Bucket) repliziert. Objekte, die dem Ziel-Bucket hinzugefügt werden, werden jedoch nicht zurück in den Quell-Bucket repliziert. In der Abbildung ist die netzübergreifende Replikation von `my-bucket` Grid 1 zu Grid 2 aktiviert, jedoch nicht in umgekehrter Richtung.



${post_edited_translations.segment}

Wenn Sie die gitterübergreifende Replikation für denselben Bucket auf beiden Grids aktivieren, werden Objekte, die einem der Buckets hinzugefügt werden, in das jeweils andere Grid repliziert. In der Abbildung ist die gitterübergreifende Replikation für `my-bucket` in beide Richtungen aktiviert.



Was geschieht beim Einlesen von Objekten?

Wenn ein S3-Client ein Objekt zu einem Bucket hinzufügt, für den die gridübergreifende Replikation aktiviert ist, geschieht Folgendes:

1. StorageGRID repliziert das Objekt automatisch vom Quell-Bucket in den Ziel-Bucket. Die Zeit für die Ausführung dieses Hintergrundreplikationsvorgangs hängt von mehreren Faktoren ab, unter anderem von der Anzahl anderer ausstehender Replikationsvorgänge.

   Der S3-Client kann den Replikationsstatus eines Objekts durch Ausführen einer GetObject- oder HeadObject-Anforderung überprüfen. Die Antwort enthält einen StorageGRID spezifischen `x-ntap-sg-cgr-replication-status` Antwort-Header, der einen der folgenden Werte aufweist:

Grid	Replikationsstatus
Quelle	• ${post_edited_translations.segment} • **AUSSTEHEND**: Das Objekt wurde noch nicht auf mindestens eine Grid Verbindung repliziert. • **FEHLER**: Die Replikation ist für keine Grid-Verbindung ausstehend und mindestens eine Verbindung ist dauerhaft ausgefallen. Ein Benutzer muss den Fehler beheben.
Ziel	**REPLICA**: Das Objekt wurde aus dem Quellgrid repliziert.

   StorageGRID unterstützt den `x-amz-replication-status` Header nicht.

2. StorageGRID verwendet die aktiven ILM-Richtlinien des jeweiligen Grids, um die Objekte zu verwalten, genau wie jedes andere Objekt. Beispielsweise könnte Objekt A auf Grid 1 als zwei replizierte Kopien gespeichert und dauerhaft aufbewahrt werden, während die auf Grid 2 replizierte Kopie von Objekt A unter Verwendung von 2+1 Erasure Coding gespeichert und nach drei Jahren gelöscht werden könnte.

Was passiert, wenn Objekte gelöscht werden?

Wie in "Datenfluss löschen" beschrieben, kann StorageGRID ein Objekt aus folgenden Gründen löschen:

- Der S3 Client sendet eine Löschanforderung.
- Ein Tenant Manager Benutzer wählt die Option "Objekte im Bucket löschen", um alle Objekte aus einem Bucket zu entfernen.
- 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 einer „Objekte im Bucket löschen“-Operation, des Ablaufs des Bucket-Lebenszyklus oder des Ablaufs der ILM-Platzierung löscht, wird das replizierte Objekt niemals aus dem anderen Grid in einer Grid-Federation-Verbindung gelöscht. Löschmarkierungen, die dem Quell-Bucket durch Löschungen von S3-Clients hinzugefügt wurden, können jedoch optional in den Ziel-Bucket repliziert werden.

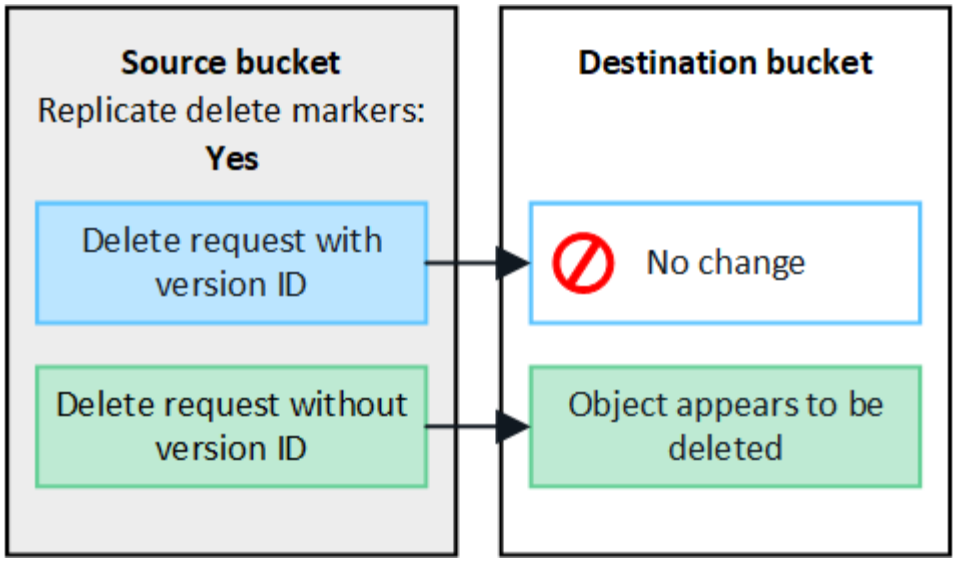
${post_edited_translations.segment}

- Wenn ein S3-Client eine Löschanforderung sendet, die eine Versions-ID enthält, wird diese Version des Objekts dauerhaft entfernt. Dem Bucket wird kein Löschmarker hinzugefügt.
- Wenn ein S3 Client eine Löschanforderung sendet, die keine Versions-ID enthält, löscht StorageGRID keine Objektversionen. Stattdessen fügt es dem Bucket einen Löschmarker hinzu. Der Löschmarker bewirkt, dass sich StorageGRID so verhält, 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 Cross-Grid-Replikation aktiviert ist, ermittelt StorageGRID, ob die Löschanforderung an das Ziel repliziert wird, wie folgt:

- Enthält die Löschanforderung eine Versions-ID, wird die entsprechende Objektversion dauerhaft aus dem Quell-Grid entfernt. StorageGRID repliziert jedoch keine Löschanforderungen mit Versions-ID, sodass dieselbe Objektversion nicht aus dem Ziel-Grid gelöscht wird.
- Wenn die Löschanforderung keine Versions-ID enthält, kann StorageGRID optional die Löschmarkierung replizieren, abhängig davon, wie die netzübergreifende Replikation für den Bucket konfiguriert ist:
  - Wenn Sie sich für die Replikation von Löschmarkierungen entscheiden (Standard), wird dem Quell-Bucket eine Löschmarkierung hinzugefügt und in den Ziel-Bucket repliziert. Dies hat zur Folge, dass das Objekt auf beiden Grids als gelöscht erscheint.
  - Wenn Sie die Replikation von Löschmarkierungen deaktivieren, wird zwar eine Löschmarkierung im Quell-Bucket hinzugefügt, aber nicht in den Ziel-Bucket repliziert. Dadurch werden Objekte, die im Quell-Grid gelöscht werden, im Ziel-Grid nicht gelöscht.

In der Abbildung wurde **Replicate delete markers** auf **Yes** gesetzt, als "${post_edited_translations.segment}". 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 Grids synchron halten möchten, erstellen Sie entsprechende "S3 Lifecycle-Konfigurationen" für die Buckets auf beiden Grids.

${post_edited_translations.segment}

Wenn Sie die Cross-Grid-Replikation verwenden, um Objekte zwischen Grids zu replizieren, können Sie einzelne Objekte verschlüsseln, die Standard-Bucket-Verschlüsselung verwenden oder eine Grid-weite Verschlüsselung konfigurieren. Sie können Einstellungen für die Standard-Bucket-Verschlüsselung oder die Grid-weite Verschlüsselung hinzufügen, ändern oder entfernen, bevor oder nachdem Sie die Cross-Grid-Replikation für einen Bucket aktivieren.

Um einzelne Objekte zu verschlüsseln, kann SSE (serverseitige Verschlüsselung mit von StorageGRID verwalteten Schlüsseln) beim Hinzufügen der Objekte zum Quell-Bucket verwendet werden. Dazu kann der Anforderungs-Header `x-amz-server-side-encryption` verwendet und `AES256` angegeben werden. Siehe "Serverseitige Verschlüsselung verwenden".

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

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

Zur Verwendung der Verschlüsselung auf Grid-Ebene muss die Option **Stored object encryption** auf **AES-256** festgelegt werden. Die Verschlüsselung auf Grid-Ebene gilt für alle Objekte, die nicht auf Bucket-Ebene verschlüsselt sind oder die ohne den Anforderungs-Header `x-amz-server-side-encryption` aufgenommen werden. Siehe "${post_edited_translations.segment}".

SSE unterstützt kein AES-128. Wenn die Option **Verschlüsselung gespeicherter Objekte** für das Quell-Grid 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-Verschlüsselungseinstellung des Ziels, sofern verfügbar.

${post_edited_translations.segment}

1. Den `x-amz-server-side-encryption` Ingest-Header verwenden, falls vorhanden.
2. ${post_edited_translations.segment}
3. Wenn keine Bucket-Einstellung konfiguriert ist, wird die gridweite Verschlüsselungseinstellung verwendet, sofern diese konfiguriert ist.
4. ${post_edited_translations.segment}

${post_edited_translations.segment}

1. ${post_edited_translations.segment}
2. Wenn das Quellobjekt nicht verschlüsselt ist oder AES-128 verwendet, wird die Standardverschlüsselungseinstellung des Ziel-Buckets verwendet, sofern diese konfiguriert ist.
3. Wenn der Ziel-Bucket keine Verschlüsselungseinstellung hat, wird die gridweite Verschlüsselungseinstellung des Ziels verwendet, sofern diese konfiguriert ist.
4. Wenn keine gridweite Einstellung vorhanden ist, das Zielobjekt nicht verschlüsseln.

${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}	Und S3 Object Lock für den Ziel-Bucket ist…
Aktiviert	Aktiviert
Deaktiviert	Aktiviert

${post_edited_translations.segment}

- Die Objekte werden am Zielort in dieser Reihenfolge mit Aufbewahrungseinstellungen gesperrt:

  a. Die Werte des Aufbewahrungsheaders des Quellobjekts für:

  `x-amz-object-lock-mode`

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

  b. Die standardmäßige Aufbewahrungsdauer des Quell-Buckets, falls festgelegt.

  c. Die standardmäßige Aufbewahrungsdauer des Zielbuckets, falls festgelegt.

  Die Standardaufbewahrungsdauer 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 verwenden.
- Ein Fehler tritt auf, wenn der Ziel-Tenant oder Bucket die S3 Object Lock-Einstellungen des Quellobjekts nicht unterstützt. Siehe "Warnungen und Fehler bei der gridübergreifenden Replikation."

Wenn S3 Object Lock für den Quell-Bucket deaktiviert ist:

- ${post_edited_translations.segment}

- Das Zielobjekt kann keinen rechtlichen Sperrstatus festlegen.

PutObjectTagging und DeleteObjectTagging werden nicht unterstützt

PutObjectTagging und DeleteObjectTagging-Anfragen für Objekte in Buckets, bei denen die Cross-Grid-Replikation aktiviert ist, werden nicht unterstützt.

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

PutObjectRetention und PutObjectLegalHold werden nicht unterstützt

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

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

Wie segmentierte Objekte repliziert werden

Die maximale Segmentgröße des Quell-Grids gilt für Objekte, die in das Ziel-Grid repliziert werden. Wenn Objekte in ein anderes Grid repliziert werden, wird die Einstellung **Maximale Segmentgröße** (**Konfiguration** > **System** > **Speicheroptionen**) des Quell-Grids auf beiden Grids verwendet. Angenommen, die maximale Segmentgröße des Quell-Grids beträgt 1 GB, während die maximale Segmentgröße des Ziel-Grids 50 MB beträgt. Wird ein 2-GB-Objekt im Quell-Grid aufgenommen, wird dieses Objekt als zwei 1-GB-Segmente gespeichert. Es wird auch in das Ziel-Grid als zwei 1-GB-Segmente repliziert, obwohl die maximale Segmentgröße dieses Grids 50 MB beträgt.

Vergleichen Sie die netzübergreifende Replikation und CloudMirror-Replikation in StorageGRID

Zu Beginn der Nutzung von Grid Federation empfiehlt sich ein Vergleich der Gemeinsamkeiten und Unterschiede zwischen "gridübergreifende Replikation" und der "StorageGRID CloudMirror Replikationsdienst".

> Sie können CloudMirror nicht für einen Bucket verwenden, der durch Cross-Grid-Replikation repliziert wurde, und umgekehrt.

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

	Gridübergreifende Replikation	CloudMirror Replikationsdienst
Wie ist es aufgebaut?	1. Eine Grid Federation-Verbindung zwischen zwei Grids konfigurieren. 2. Neue Mandantenkonten hinzufügen, die automatisch in das andere Grid geklont werden. 3. Neue Mandantengruppen und Benutzer werden hinzugefügt, die ebenfalls geklont werden. 4. Entsprechende Buckets auf jedem Grid erstellen und die gridübergreifende Replikation in eine oder beide Richtungen ermöglichen.	1. Ein Mandantenbenutzer konfiguriert die CloudMirror-Replikation, indem er einen CloudMirror-Endpunkt (IP-Adresse, Anmeldeinformationen usw.) mithilfe des Tenant Managers oder der S3-API definiert. 2. Jeder Bucket, der diesem Mandantenkonto gehört, kann so konfiguriert werden, dass er auf den CloudMirror Endpoint verweist.
Wer ist für die Einrichtung verantwortlich?	• Ein Grid-Administrator konfiguriert die Verbindung und die Mandanten. • Die Mandantenbenutzer konfigurieren die Gruppen, Benutzer, Schlüssel und Buckets.	Typischerweise ein Mandantenbenutzer.
Was ist das Ziel?	Ein entsprechender und identischer S3-Bucket auf dem anderen StorageGRID System in der Grid-Federation-Verbindung.	• Jede kompatible S3-Infrastruktur (einschließlich Amazon S3). • Google Cloud Platform (GCP)
Ist eine Objektversionierung erforderlich?	Ja, sowohl der Quell- als auch der Ziel-Bucket muss die Objektversionierung aktiviert haben.	Nein, die CloudMirror Replikation unterstützt jede Kombination aus nicht versionierten und versionierten Buckets sowohl auf der Quell- als auch auf der Zielseite.
Was führt dazu, dass Objekte an das Ziel verschoben werden?	Objekte werden automatisch repliziert, wenn sie einem Bucket hinzugefügt werden, für den die Cross-Grid-Replikation aktiviert ist.	Objekte werden automatisch repliziert, wenn sie einem Bucket hinzugefügt werden, der mit einem CloudMirror Endpoint konfiguriert wurde. Objekte, die bereits im Quell-Bucket vorhanden waren, bevor der Bucket mit dem CloudMirror Endpoint konfiguriert wurde, werden nicht repliziert, es sei denn, sie werden geändert.
Wie werden Objekte repliziert?	Die gitterübergreifende Replikation erzeugt versionierte Objekte und repliziert die Versions-ID vom Quell-Bucket zum Ziel-Bucket. Dadurch bleibt die Versionsreihenfolge in beiden Grids erhalten.	CloudMirror Replikation benötigt keine Buckets mit Versionsverwaltung, daher kann CloudMirror die Reihenfolge für einen Schlüssel nur innerhalb eines Standorts beibehalten. Es gibt keine Garantie dafür, dass die Reihenfolge bei Anfragen an ein Objekt an einem anderen Standort erhalten bleibt.

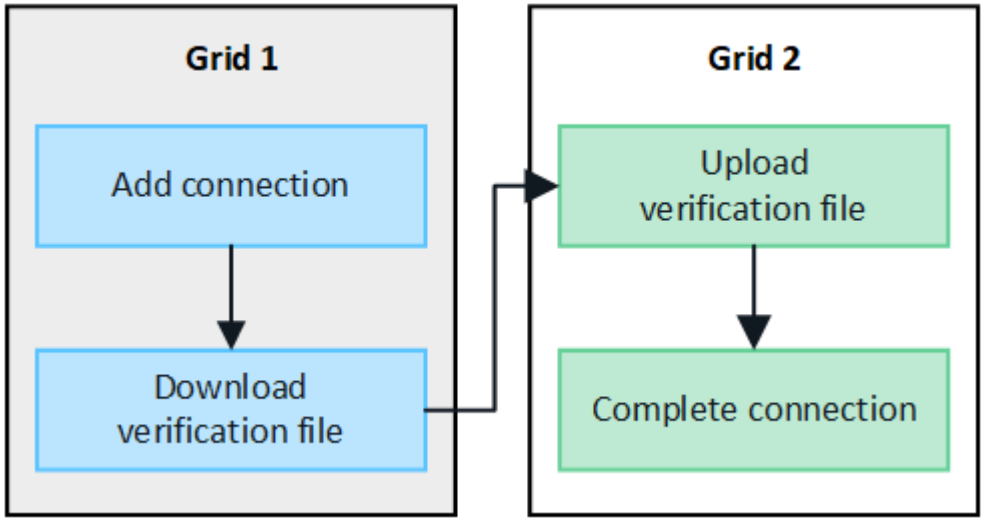
	Gridübergreifende Replikation	CloudMirror Replikationsdienst
Was passiert, wenn ein Objekt nicht repliziert werden kann?	Das Objekt wird zur Replikation in die Warteschlange gestellt, wobei die Speichergrenzen für Metadaten gelten.	Das Objekt wird zur Replikation in die Warteschlange gestellt, vorbehaltlich der Beschränkungen der Plattformdienste (siehe "Empfehlungen für die Nutzung von Plattformdiensten").
Werden die Systemmetadaten des Objekts repliziert?	Ja, wenn ein Objekt in das andere Grid repliziert wird, werden auch seine Systemmetadaten repliziert. Die Metadaten sind in beiden Grids identisch.	Nein, wenn ein Objekt in den externen Bucket repliziert wird, werden seine Systemmetadaten aktualisiert. Die Metadaten unterscheiden sich je nach Speicherort, abhängig vom Zeitpunkt der Aufnahme und dem Verhalten der unabhängigen S3-Infrastruktur.
Wie werden Objekte abgerufen?	Anwendungen können Objekte abrufen oder lesen, indem sie eine Anfrage an den Bucket in einem der beiden Grids stellen.	Anwendungen können Objekte abrufen oder lesen, indem sie eine Anfrage entweder an StorageGRID oder an das S3-Ziel senden. Beispielsweise kann CloudMirror Replikation verwendet werden, um Objekte an eine Partnerorganisation zu spiegeln. Die Partnerorganisation kann mit eigenen Anwendungen Objekte direkt vom S3-Ziel lesen oder aktualisieren. Die Nutzung von StorageGRID ist nicht erforderlich.
Was passiert, wenn ein Objekt gelöscht wird?	• Löschanforderungen, die eine Versions-ID enthalten, werden niemals in das Zielgrid repliziert. • Löschanforderungen, die keine Versions-ID enthalten, fügen dem Quell-Bucket eine Löschmarkierung hinzu, die optional auf das Ziel-Grid repliziert werden kann. • Wenn die netzübergreifende Replikation nur in eine Richtung konfiguriert ist, können Objekte im Ziel-Bucket gelöscht werden, ohne dass dies Auswirkungen auf die Quelle hat.	Die Ergebnisse variieren je nach Versionsstatus der Quell- und Ziel-Buckets (die nicht identisch sein müssen): • Wenn beide Buckets versioniert sind, wird durch eine Löschanforderung an beiden Stellen eine Löschmarkierung hinzugefügt. • Wenn nur der Quell-Bucket versioniert ist, fügt eine Löschanforderung einen Löschmarker zum Quell-Bucket, aber nicht zum Ziel-Bucket hinzu. • Wenn keiner der beiden Buckets versioniert ist, wird eine Löschanforderung das Objekt aus der Quelle, aber nicht aus dem Ziel löschen. In ähnlicher Weise können Objekte im Ziel-Bucket gelöscht werden, ohne die Quelle zu beeinträchtigen.

StorageGRID Grid-Federationsverbindungen erstellen

Sie können eine Grid Federation Verbindung zwischen zwei StorageGRID Systemen

erstellen, wenn Mandantendetails geklont und Objektdaten repliziert werden sollen.

Wie in der Abbildung dargestellt, umfasst das Erstellen einer Grid Federation Verbindung Schritte auf beiden Grids. Sie fügen die Verbindung auf einem Grid hinzu und schließen sie auf dem anderen Grid ab. Es kann von jedem der beiden Grids aus begonnen werden.



Bevor Sie beginnen

- Sie haben die "Überlegungen und Anforderungen" für die Konfiguration von Grid Federation-Verbindungen überprüft.
- Wenn Sie planen, für jedes Grid vollqualifizierte Domainnamen (FQDNs) anstelle von IP- oder VIP-Adressen zu verwenden, wissen Sie, welche Namen zu verwenden sind, und Sie haben bestätigt, dass der DNS-Server für jedes Grid die entsprechenden Einträge enthält.
- Sie verwenden ein "unterstützte Webbrowser".
- Sie besitzen die Root-Zugriffsberechtigung und die Bereitstellungspassphrase für beide Grids.

Verbindung hinzufügen

Diese Schritte sind auf einem der beiden StorageGRID Systeme auszuführen.

Schritte

1. Melden Sie sich beim Grid Manager vom primären Admin-Node eines der beiden Grids an.
2. Wählen Sie **Konfiguration** > **System** > **Grid federation**.
3. ${post_edited_translations.segment}
4. Geben Sie die Verbindungsdetails ein.

Feld	Beschreibung
Verbindungsname	Ein eindeutiger Name, der Ihnen hilft, diese Verbindung zu erkennen, zum Beispiel „Grid 1 Grid 2“.

Feld	Beschreibung
FQDN oder IP für dieses Grid	Eine der folgenden Optionen: • Der FQDN des Grids, bei dem Sie derzeit angemeldet sind • Eine VIP-Adresse einer HA-Gruppe in diesem Grid • Die IP-Adresse eines Admin-Knotens oder Gateway-Knotens in diesem Grid. Die IP-Adresse kann sich in einem beliebigen Netzwerk befinden, das vom Ziel-Grid erreicht werden kann.
Port	Der Port, den Sie für diese Verbindung verwenden möchten. Sie können eine beliebige ungenutzte Portnummer von 23000 bis 23999 eingeben. Beide Grids in dieser Verbindung verwenden denselben Port. Es muss sichergestellt sein, dass kein Node in einem der beiden Grids diesen Port für andere Verbindungen nutzt.
Gültigkeitstage des Zertifikats für dieses Grid	Die Anzahl der Tage, für die die Sicherheitszertifikate dieses Grids in der Verbindung gültig sein sollen. Der Standardwert beträgt 730 Tage (2 Jahre), aber Sie können jeden Wert von 1 bis 762 Tagen eingeben. StorageGRID generiert beim Speichern der Verbindung automatisch Client- und Serverzertifikate für jedes Grid.
Bereitstellungspassphrase für dieses Grid	Die Bereitstellungs-Passphrase für das Grid, bei dem Sie angemeldet sind.
FQDN oder IP für das andere Grid	Eine der folgenden Optionen: • Der FQDN des Grids, zu dem Sie eine Verbindung herstellen möchten • Eine VIP-Adresse einer HA-Gruppe im anderen Grid • Die IP-Adresse eines Admin-Knotens oder Gateway-Knotens im anderen Grid. Die IP-Adresse kann sich in einem beliebigen Netzwerk befinden, das vom Quell-Grid erreichbar ist.

5. **Speichern und fortfahren** auswählen.
6. Für den Schritt „Verifizierungsdatei herunterladen“ ist **Verifizierungsdatei herunterladen** auszuwählen.

   Sobald die Verbindung im anderen Grid hergestellt ist, kann die Verifizierungsdatei von keinem der beiden Grids mehr heruntergeladen werden.

7. Die heruntergeladene Datei (`*connection-name*.grid-federation`finden und an einem sicheren Ort speichern.

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

8. **Schließen** auswählen, um zur Grid federation-Seite zurückzukehren.
9. Bestätigen Sie, dass die neue Verbindung angezeigt wird und dass ihr **Verbindungsstatus** auf **Warten auf Verbindung** steht.
10. Die *connection-name*`.grid-federation` Datei dem Grid-Administrator für das andere Grid bereitstellen.

Vollständige Verbindung

Diese Schritte sind auf dem StorageGRID System auszuführen, zu dem die Verbindung hergestellt wird (dem anderen Grid).

Schritte

1. Melden Sie sich beim Grid Manager vom primären Admin-Knoten aus an.
2. Wählen Sie **Konfiguration** > **System** > **Grid federation**.
3. Wählen Sie **Bestätigungsdatei hochladen**, um auf die Upload-Seite zuzugreifen.
4. Wählen Sie **Verifizierungsdatei hochladen** aus. Suchen Sie anschließend nach der Datei, die vom ersten Grid heruntergeladen wurde, und wählen Sie diese aus (*connection-name*`.grid-federation`).

   Die Verbindungsdetails werden angezeigt.

5. Optional können Sie für dieses Grid eine andere Anzahl gültiger Tage für die Sicherheitszertifikate eingeben. Der Eintrag **Certificate valid days** ist standardmäßig auf den Wert eingestellt, den Sie beim ersten Grid eingegeben haben, aber jedes Grid kann unterschiedliche Ablaufdaten verwenden.

   ${post_edited_translations.segment}

   > Wenn die Zertifikate an einem der beiden Enden der Verbindung ablaufen, funktioniert die Verbindung nicht mehr und die Replikationen bleiben ausstehend, bis die Zertifikate aktualisiert werden.

6. Geben Sie die Bereitstellungs-Passphrase für das Grid ein, bei dem Sie aktuell angemeldet sind.
7. **Speichern und testen** auswählen.

   Die Zertifikate werden generiert und die Verbindung wird getestet. Wenn die Verbindung gültig ist, erscheint eine Erfolgsmeldung und die neue Verbindung wird auf der Grid federation-Seite aufgeführt. Der **Connection status** ist **Connected**.

   Wenn eine Fehlermeldung angezeigt wird, sollten etwaige Probleme behoben werden. Siehe "Fehler in der Grid-Federation beheben".

8. Öffnen Sie die Grid federation-Seite im ersten Grid und aktualisieren Sie den Browser. Es wird bestätigt, dass der **Connection status** jetzt **Connected** ist.
9. Nachdem die Verbindung hergestellt wurde, sind alle Kopien der Verifizierungsdatei sicher zu löschen.

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

Nachdem Sie fertig sind

- Zu berücksichtigende Punkte für "Verwaltung zulässiger Mandanten" werden dargestellt.

- "Ein oder mehrere neue Mandantenkonten erstellen", die Berechtigung **Grid-Federation-Verbindung verwenden** zuweisen und die neue Verbindung auswählen.
- "Verbindung verwalten" nach Bedarf. Sie können Verbindungswerte bearbeiten, eine Verbindung testen, Verbindungszertifikate rotieren oder eine Verbindung entfernen.
- "Verbindung überwachen" als Teil Ihrer normalen StorageGRID Überwachungsaktivitäten.
- "Verbindung beheben", einschließlich der Behebung von Warnungen und Fehlern im Zusammenhang mit dem Klonen von Konten und der netzübergreifenden Replikation.

StorageGRID Grid-Federationsverbindungen verwalten

${post_edited_translations.segment}

Bevor Sie beginnen

- Sie sind beim Grid Manager auf einem der beiden Grids mit einem "unterstützte Webbrowser" angemeldet.
- Sie haben die "Root-Zugriffsberechtigung" für das Grid, bei dem Sie angemeldet sind.

Eine Grid Federation Verbindung bearbeiten

Sie können eine Grid Federation-Verbindung bearbeiten, indem Sie sich am primären Admin Node auf einem der beiden Grids in der Verbindung anmelden. Nachdem Änderungen am ersten Grid vorgenommen wurden, ist eine neue Verifizierungsdatei herunterzuladen und in das andere Grid hochzuladen.

> ⓘ Während die Verbindung bearbeitet wird, verwenden Anfragen zum Klonen von Konten oder zur gridübergreifenden Replikation weiterhin die bestehenden Verbindungseinstellungen. Alle Änderungen, die Sie am ersten Grid vornehmen, werden lokal gespeichert, aber erst nach dem Hochladen in das zweite Grid, dem Speichern und dem Testen verwendet.

Bearbeitung der Verbindung starten

Schritte

1. Melden Sie sich beim Grid Manager vom primären Admin-Node eines der beiden Grids an.
2. Wählen Sie **Knoten** aus und bestätigen Sie, dass alle anderen Admin Nodes in Ihrem System online sind.

> ⓘ Wenn Sie eine Grid-Federation-Verbindung bearbeiten, versucht StorageGRID, eine „Kandidatenkonfigurationsdatei“ auf allen Admin-Knoten des ersten Grids zu speichern. Kann diese Datei nicht auf allen Admin-Knoten gespeichert werden, erscheint beim Auswählen von **Speichern und testen** eine Warnmeldung.

3. Wählen Sie **Konfiguration** > **System** > **Grid federation**.
4. Die Verbindungsdetails können über das Menü **Aktionen** auf der Grid federation-Seite oder auf der Detailseite einer bestimmten Verbindung bearbeitet werden. Siehe "Grid Federation Verbindungen erstellen" für die erforderlichen Eingaben.

Aktionsmenü

a. Das Optionsfeld für die Verbindung auswählen.
b. **Aktionen** > **Bearbeiten** auswählen.
c. Geben Sie die neuen Informationen ein.

Detailseite

a. Ein Verbindungsname kann ausgewählt werden, um die zugehörigen Details anzuzeigen.
b. **Bearbeiten** auswählen.
c. Geben Sie die neuen Informationen ein.

5. Geben Sie die Bereitstellungs-Passphrase für das Grid ein, bei dem Sie angemeldet sind.
6. **Speichern und fortfahren** auswählen.

   Die neuen Werte werden gespeichert, aber sie werden erst auf die Verbindung angewendet, nachdem die neue Verifizierungsdatei im anderen Grid hochgeladen wurde.

7. **Bestätigungsdatei herunterladen** auswählen.

   Um diese Datei zu einem späteren Zeitpunkt herunterzuladen, kann die Detailseite der Verbindung aufgerufen werden.

8. Die heruntergeladene Datei (`*connection-name*.grid-federation`finden und an einem sicheren Ort speichern.

   Die Verifizierungsdatei enthält Geheimnisse und muss sicher aufbewahrt und übertragen werden.

9. **Schließen** auswählen, um zur Grid federation-Seite zurückzukehren.
10. Bestätigen Sie, dass der **Verbindungsstatus** auf **Bearbeitung ausstehend** steht.

    Wenn der Verbindungsstatus beim Beginn der Bearbeitung nicht **Verbunden** war, ändert er sich nicht zu **Bearbeitung ausstehend**.

11. Die `*connection-name*.grid-federation` Datei dem Grid-Administrator für das andere Grid bereitstellen.

Die Bearbeitung der Verbindung abschließen

Die Bearbeitung der Verbindung wird abgeschlossen, indem die Verifizierungsdatei auf dem anderen Grid hochgeladen wird.

Schritte

1. Melden Sie sich beim Grid Manager vom primären Admin-Knoten aus an.
2. Wählen Sie **Konfiguration** > **System** > **Grid federation**.
3. **Bestätigungsdatei hochladen** auswählen, um auf die Upload-Seite zuzugreifen.
4. Wählen Sie **Bestätigungsdatei hochladen**. Anschließend zu der Datei navigieren, die vom ersten Grid heruntergeladen wurde, und diese auswählen.

5. Geben Sie die Bereitstellungs-Passphrase für das Grid ein, bei dem Sie aktuell angemeldet sind.
6. **Speichern und testen** auswählen.

   Wenn die Verbindung mit den bearbeiteten Werten hergestellt werden kann, erscheint eine Erfolgsmeldung. Andernfalls erscheint eine Fehlermeldung. Die Meldung sollte überprüft und etwaige Probleme behoben werden.

7. Schließen Sie den Assistenten, um zur Grid federation-Seite zurückzukehren.
8. Bestätigen Sie, dass der **Verbindungsstatus** auf **Verbunden** steht.
9. Öffnen Sie die Grid federation-Seite im ersten Grid und aktualisieren Sie den Browser. Es wird bestätigt, dass der **Connection status** jetzt **Connected** ist.
10. Nachdem die Verbindung hergestellt wurde, sind alle Kopien der Verifizierungsdatei sicher zu löschen.

Test einer Grid Federation Verbindung

Schritte

1. Melden Sie sich beim Grid Manager vom primären Admin-Knoten aus an.
2. Wählen Sie **Konfiguration** > **System** > **Grid federation**.
3. Die Verbindung kann über das Menü **Aktionen** auf der Grid-Federationsseite oder auf der Detailseite einer bestimmten Verbindung getestet werden.

   Aktionsmenü

   a. Das Optionsfeld für die Verbindung auswählen.

   b. **Aktionen** > **Test** auswählen.

   Detailseite

   a. Ein Verbindungsname kann ausgewählt werden, um die zugehörigen Details anzuzeigen.

   b. **Verbindung testen** auswählen.

4. Verbindungsstatus überprüfen:

Verbindungsstatus	Beschreibung
Verbunden	Beide Grids sind verbunden und kommunizieren normal.
Fehler	Die Verbindung befindet sich im Fehlerzustand. Beispielsweise ist ein Zertifikat abgelaufen oder ein Konfigurationswert nicht mehr gültig.
Bearbeitung ausstehend	Sie haben die Verbindung in diesem Grid bearbeitet, aber die Verbindung verwendet weiterhin die bestehende Konfiguration. Zum Abschluss der Bearbeitung muss die neue Bestätigungsdatei in das andere Grid hochgeladen werden.

Verbindungsstatus	Beschreibung
Warten auf Verbindung	Sie haben die Verbindung in diesem Grid konfiguriert, aber die Verbindung im anderen Grid ist noch nicht hergestellt. Die Verifizierungsdatei kann von diesem Grid heruntergeladen und in das andere Grid hochgeladen werden.
Unbekannt	Die Verbindung befindet sich in einem unbekannten Zustand, möglicherweise aufgrund eines Netzwerkproblems oder eines Offline-Knotens.

5. Wenn der Verbindungsstatus **Fehler** ist, sollten etwaige Probleme behoben werden. Anschließend kann **Verbindung testen** erneut ausgewählt werden, um zu bestätigen, dass das Problem behoben wurde.

Verbindungszertifikate austauschen

Jede Grid Federation-Verbindung nutzt vier automatisch generierte SSL-Zertifikate zur Sicherung der Verbindung. Wenn die beiden Zertifikate für jedes Grid kurz vor ihrem Ablaufdatum stehen, weist die Warnung **Ablauf des Grid Federation-Zertifikats** darauf hin, dass die Zertifikate erneuert werden sollten.

> Wenn die Zertifikate an einem der beiden Enden der Verbindung ablaufen, funktioniert die Verbindung nicht mehr und die Replikationen bleiben ausstehend, bis die Zertifikate aktualisiert werden.

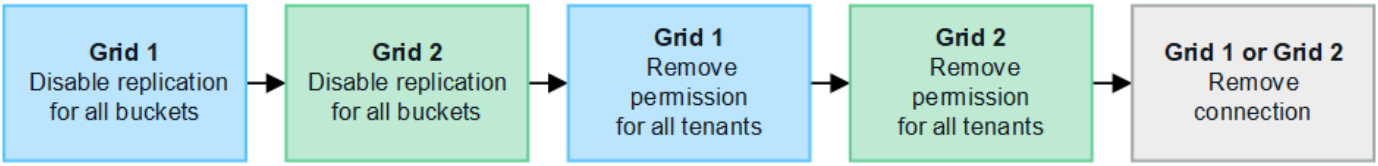
Schritte

1. Melden Sie sich beim Grid Manager vom primären Admin-Node eines der beiden Grids an.
2. Wählen Sie **Konfiguration** > **System** > **Grid federation**.
3. Auf der Seite „Grid-Federation“ kann auf beiden Tabs der Verbindungsname ausgewählt werden, um die Details anzuzeigen.
4. Die Registerkarte **Zertifikate** auswählen.
5. **Zertifikate rotieren** auswählen.
6. Geben Sie an, wie viele Tage die neuen Zertifikate gültig sein sollen.
7. Geben Sie die Bereitstellungs-Passphrase für das Grid ein, bei dem Sie angemeldet sind.
8. **Zertifikate rotieren** auswählen.
9. Wiederholen Sie diese Schritte gegebenenfalls auf dem anderen Grid in der Verbindung.

${post_edited_translations.segment}

Entfernung einer Grid-Federation-Verbindung

Sie können eine Grid Federation-Verbindung von jedem der beiden Grids entfernen. Wie in der Abbildung gezeigt, müssen auf beiden Grids die erforderlichen Schritte durchgeführt werden, um zu bestätigen, dass die Verbindung von keinem Mandanten auf einem der beiden Grids verwendet wird.



Vor der Entfernung einer Verbindung ist Folgendes zu beachten:

- Das Entfernen einer Verbindung löscht keine Elemente, die bereits zwischen den Grids kopiert wurden. Beispielsweise werden Mandantenbenutzer, -gruppen und -objekte, die in beiden Grids vorhanden sind, nicht aus einem der beiden Grids gelöscht, wenn die Berechtigung des Mandanten entfernt wird. Um diese Elemente zu löschen, ist eine manuelle Entfernung aus beiden Grids erforderlich.
- Wenn eine Verbindung entfernt wird, schlägt die Replikation aller Objekte, deren Replikation noch aussteht (aufgenommen, aber noch nicht in das andere Grid repliziert), dauerhaft fehl.

Replikation für alle Mandanten Buckets deaktivieren

Schritte

1. Von einem der beiden Grids aus erfolgt die Anmeldung beim Grid Manager über den primären Admin-Knoten.
2. Wählen Sie **Konfiguration** > **System** > **Grid federation**.
3. Wählen Sie den Verbindungsnamen aus, um die Details anzuzeigen.
4. Auf der Registerkarte **Zulässige Mandanten** lässt sich feststellen, ob die Verbindung von einem Mandanten verwendet wird.
5. Falls Mieter aufgelistet sind, alle Mieter anweisen, "Grid-übergreifende Replikation deaktivieren"für alle ihre Buckets auf beiden Grids in der Verbindung.

> Die Berechtigung **Use grid federation connection** kann nicht entfernt werden, wenn für Mandanten-Buckets die grid-übergreifende Replikation aktiviert ist. Jedes Mandantenkonto muss die grid-übergreifende Replikation für seine Buckets in beiden Grids deaktivieren.

Berechtigung für jeden Mandanten entfernen

Nachdem die Cross-Grid-Replikation für alle Mandanten-Buckets deaktiviert wurde, ist die **Berechtigung *Grid-Federation verwenden** von allen Mandanten auf beiden Grids zu entfernen.

Schritte

1. Wählen Sie **Konfiguration** > **System** > **Grid federation**.
2. Wählen Sie den Verbindungsnamen aus, um die Details anzuzeigen.
3. Für jeden Mandanten auf der Registerkarte **Zulässige Mandanten** ist die Berechtigung **Grid-Federationsverbindung verwenden** von jedem Mandanten zu entfernen. Siehe "Zugelassene Mieter verwalten".
4. Wiederholen Sie diese Schritte für die zugelassenen Mandanten im anderen Grid.

Verbindung entfernen

Schritte

1. Wenn in keinem der beiden Grids ein Mandant die Verbindung verwendet, **Entfernen** auswählen.
2. Die Bestätigungsmeldung prüfen und **Entfernen** auswählen.

- Wenn die Verbindung entfernt werden kann, wird eine Erfolgsmeldung angezeigt. Die Grid Federation Verbindung ist nun aus beiden Grids entfernt.
- Wenn die Verbindung nicht entfernt werden kann (beispielsweise weil sie noch verwendet wird oder ein Verbindungsfehler vorliegt), wird eine Fehlermeldung angezeigt. Es bestehen folgende Möglichkeiten:
  - Der Fehler sollte behoben werden (empfohlen). Weitere Informationen unter "Fehler in der Grid-Federation beheben".
  - Die Verbindung wird zwangsweise entfernt. Im nächsten Abschnitt finden Sie weitere Informationen.

Entfernung einer Grid-Federation-Verbindung durch Erzwingen

Bei Bedarf kann die Entfernung einer Verbindung erzwungen werden, die nicht den Status **Verbunden** aufweist.

Die erzwungene Entfernung löscht die Verbindung nur aus dem lokalen Grid. Um die Verbindung vollständig zu entfernen, sind die gleichen Schritte auf beiden Grids erforderlich.

Schritte

1. Im Bestätigungsdialogfeld die Option **Entfernung erzwingen** auswählen.

   Es erscheint eine Erfolgsmeldung. Diese Grid Federation Verbindung kann nicht mehr verwendet werden. Allerdings könnte die Cross-Grid-Replikation für Mandanten-Buckets weiterhin aktiviert sein und einige Objektkopien wurden möglicherweise bereits zwischen den Grids in der Verbindung repliziert.

2. Vom anderen Grid in der Verbindung erfolgt die Anmeldung beim Grid Manager vom primären Admin-Knoten.
3. Wählen Sie **Konfiguration** > **System** > **Grid federation**.
4. Wählen Sie den Verbindungsnamen aus, um die Details anzuzeigen.
5. **Entfernen** und **Ja** auswählen.
6. **Entfernen erzwingen** auswählen, um die Verbindung aus diesem Grid zu entfernen.

Verwalten Sie die zulässigen Mandanten für StorageGRID Grid-Föderation

Sie können S3-Mandantenkonten die Nutzung einer Grid Federation-Verbindung zwischen zwei StorageGRID Systemen gestatten. Wenn Mandanten die Nutzung einer Verbindung gestattet wird, sind spezielle Schritte erforderlich, um Mandantendetails zu bearbeiten oder die Berechtigung eines Mandanten zur Nutzung der Verbindung dauerhaft zu entfernen.

Bevor Sie beginnen

- Sie sind beim Grid Manager auf einem der beiden Grids mit einem "unterstützte Webbrowser" angemeldet.
- Sie haben die "Root-Zugriffsberechtigung" für das Grid, bei dem Sie angemeldet sind.
- Sie haben "Eine Grid Federation-Verbindung wurde erstellt." zwischen zwei Grids.
- Sie haben die Arbeitsabläufe für "Konto klonen" und "gridübergreifende Replikation" überprüft.
- Wie erforderlich, haben Sie Single Sign-On (SSO) oder die Identifikationsföderation für beide Grids in der Verbindung bereits konfiguriert. Siehe "Was ist Account Clone".

${post_edited_translations.segment}

Wenn Sie einem neuen oder bestehenden Mandantenkonto die Nutzung einer Grid-Federation-Verbindung für die Kontoklonung und die gridübergreifende Replikation ermöglichen möchten, sind die allgemeinen Anweisungen zu "Erstellen eines neuen S3-Mandanten" oder "ein Mandantenkonto bearbeiten" zu beachten:

- Sie können den Mandanten aus jedem Grid in der Verbindung erstellen. Das Grid, in dem ein Mandant erstellt wird, ist das Quell-Grid des Mandanten.
- Der Status der Verbindung muss **Verbunden** sein.
- Wenn der Mandant erstellt oder bearbeitet wird, um die Berechtigung **Grid-Verbundverbindung verwenden** zu aktivieren, und dann auf dem ersten Grid gespeichert wird, wird ein identischer Mandant automatisch auf das andere Grid repliziert. Das Grid, auf das der Mandant repliziert wird, ist das *Ziel-Grid des Mandanten*.
- Die Mandanten in beiden Grids haben dieselbe 20-stellige Konto-ID, denselben Namen, dieselbe Beschreibung, dasselbe Kontingent und dieselben Berechtigungen. Optional kann das Feld **Beschreibung** verwendet werden, um zu erkennen, welcher der Quellmandant und welcher der Zielmandant ist. Beispielsweise erscheint diese Beschreibung für einen Mandanten, der in Grid 1 erstellt wurde, auch für den auf Grid 2 replizierten Mandanten: „Dieser Mandant wurde in Grid 1 erstellt.“
- Aus Sicherheitsgründen wird das Passwort eines lokalen Root-Benutzers nicht in das Ziel-Grid kopiert.

> Bevor sich ein lokaler Root-Benutzer beim replizierten Mandanten auf dem Ziel-Grid anmelden kann, muss ein Grid-Administrator für dieses Grid "das Passwort für den lokalen Root-Benutzer ändern".

- Nachdem der neue oder bearbeitete Mandant in beiden Grids verfügbar ist, können Mandantenbenutzer diese Vorgänge ausführen:
  - Aus dem Quell-Grid des Mandanten Gruppen und lokale Benutzer erstellen, die automatisch in das Ziel-Grid des Mandanten geklont werden. Siehe "Mandantengruppen und Benutzer klonen".
  - Neue S3-Zugriffsschlüssel erstellen, die optional in das Ziel-Grid des Mandanten geklont werden können. Siehe "Klonen von S3-Zugriffsschlüsseln mithilfe der API".
  - Identische Buckets auf beiden Grids in der Verbindung erstellen und die Grid-übergreifende Replikation in eine oder beide Richtungen aktivieren. Siehe "Verwaltung der gridübergreifenden Replikation".

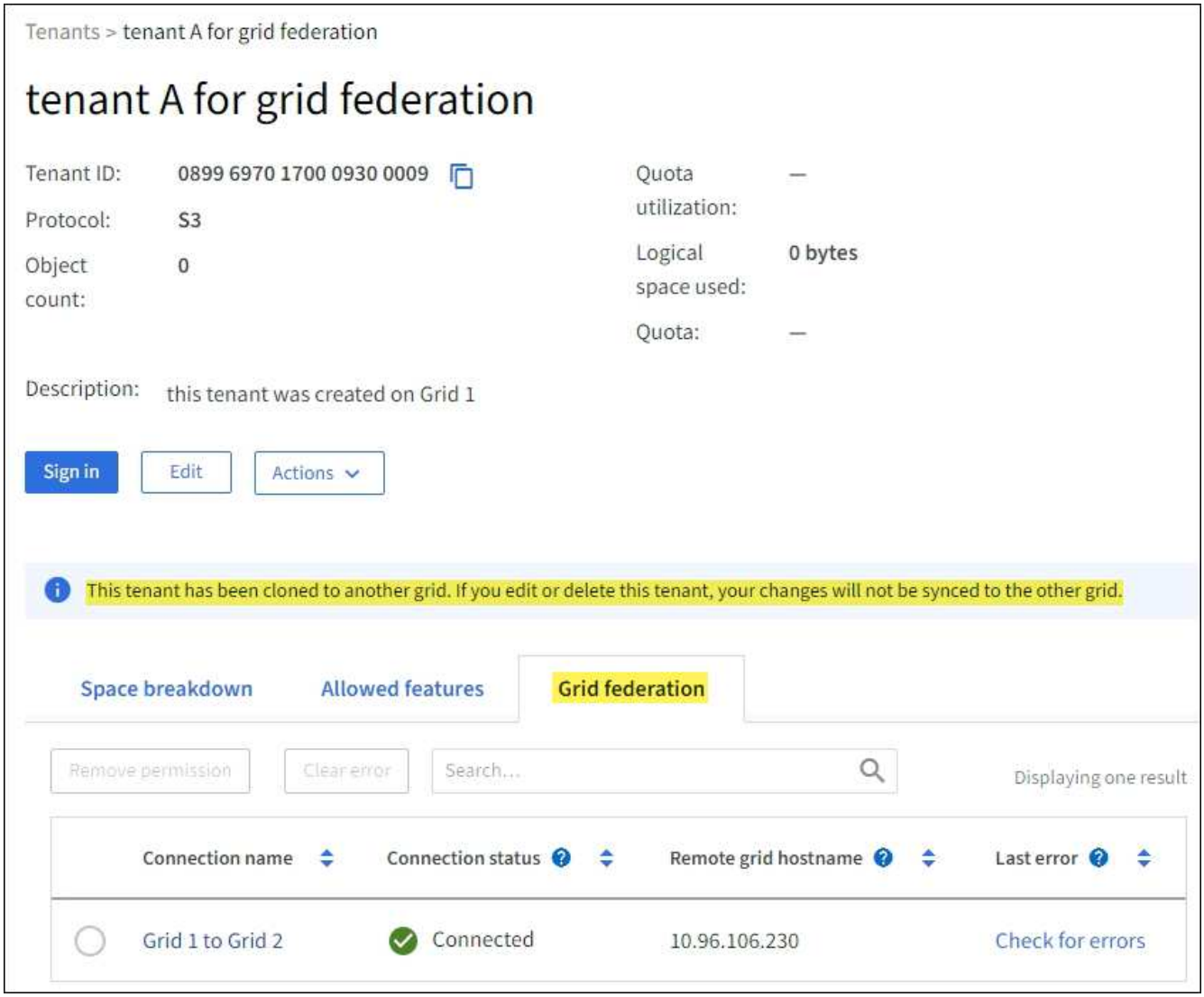
Einen zugelassenen Mandanten anzeigen

Es sind Details zu einem Mandanten verfügbar, der zur Nutzung einer Grid Federation Verbindung berechtigt ist.

Schritte

1. **Tenants** auswählen.
2. Auf der Seite „Mieter“ den Namen des Mieters auswählen, um die Seite mit den Mieterdetails anzuzeigen.

   Wenn dies das Quell-Grid für den Mandanten ist (das heißt, wenn der Mandant in diesem Grid erstellt wurde), erscheint ein Banner, das daran erinnert, dass der Mandant in ein anderes Grid geklont wurde. Wenn dieser Mandant bearbeitet oder gelöscht wird, werden die Änderungen nicht mit dem anderen Grid synchronisiert.



3. Optional kann die Registerkarte **Grid federation** ausgewählt werden, um "die Verbindung zum Grid Federation überwachen".

Einen zulässigen Mandanten bearbeiten

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

- Verfügt ein Mandant über die Berechtigung **Grid-Federationsverbindung verwenden**, können Mandantendetails in beiden Grids der Verbindung bearbeitet werden. Allerdings werden Änderungen nicht in das andere Grid kopiert. Wenn die Mandantendetails zwischen den Grids synchron gehalten werden sollen, sind die gleichen Änderungen auf beiden Grids vorzunehmen.
- Die Berechtigung **Grid-Federationsverbindung verwenden** kann beim Bearbeiten eines Mandanten nicht entfernt werden.
- Beim Bearbeiten eines Mandanten kann keine andere Grid Federation-Verbindung ausgewählt werden.

Einen zulässigen Mandanten löschen

Wenn Sie einen Mandanten entfernen müssen, der über die Berechtigung **Grid-Federationsverbindung verwenden** verfügt, befolgen Sie die allgemeinen Anweisungen für "Löschen eines Mandantenkontos" und

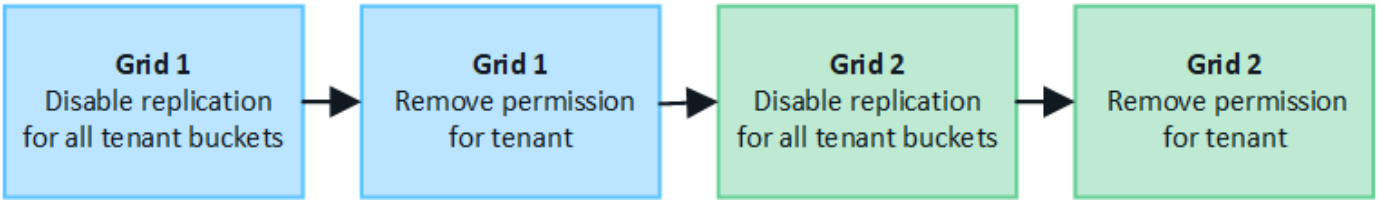
beachten Sie Folgendes:

- Bevor der ursprüngliche Mandant im Quell-Grid entfernt werden kann, müssen alle Buckets für das Konto im Quell-Grid entfernt werden.
- Bevor der geklonte Mandant im Ziel-Grid entfernt werden kann, müssen zuvor alle Buckets für das Konto im Ziel-Grid entfernt werden.
- Wenn entweder der ursprüngliche oder der geklonte Mandant entfernt wird, kann das Konto nicht mehr für die gridübergreifende Replikation verwendet werden.
- Wenn Sie den ursprünglichen Mandanten im Quell-Grid entfernen, bleiben alle Mandantengruppen, Benutzer oder Schlüssel, die in das Ziel-Grid geklont wurden, unberührt. Es besteht die Möglichkeit, den geklonten Mandanten zu löschen oder ihm die Verwaltung seiner eigenen Gruppen, Benutzer, Zugriffsschlüssel und Buckets zu überlassen.
- Wenn Sie den geklonten Mandanten im Zielnetz entfernen, treten Klonfehler auf, wenn dem ursprünglichen Mandanten neue Gruppen oder Benutzer hinzugefügt werden.

  Um diese Fehler zu vermeiden, sollte die Berechtigung des Mandanten zur Nutzung der Grid-Federation-Verbindung entfernt werden, bevor der Mandant aus diesem Grid gelöscht wird.

Berechtigung „Grid Federation-Verbindung nutzen“ entfernen

Um zu verhindern, dass ein Mandant eine Grid-Federation-Verbindung nutzt, muss die Berechtigung **Grid-Federation-Verbindung nutzen** entfernt werden.



Vor der Entfernung der Berechtigung eines Mandanten zur Nutzung einer Grid Federation Verbindung ist Folgendes zu beachten:

- Die Berechtigung **Grid-Federationsverbindung verwenden** kann nicht entfernt werden, wenn für einen der Buckets des Mandanten die grid-übergreifende Replikation aktiviert ist. Das Mandantenkonto muss die grid-übergreifende Replikation zunächst für alle seine Buckets deaktivieren.
- Das Entfernen der Berechtigung „Use grid federation connection“ löscht keine Elemente, die bereits zwischen den Grids repliziert wurden. Beispielsweise werden Mandantenbenutzer, -gruppen und -objekte, die in beiden Grids vorhanden sind, beim Entfernen der Berechtigung des Mandanten nicht aus einem der Grids gelöscht. Um diese Elemente zu löschen, ist eine manuelle Entfernung aus beiden Grids erforderlich.
- Wenn Sie diese Berechtigung mit derselben Grid Federation-Verbindung wieder aktivieren möchten, löschen Sie zuerst diesen Mandanten im Ziel-Grid, andernfalls führt die erneute Aktivierung dieser Berechtigung zu einem Fehler.

> Durch erneutes Aktivieren der Berechtigung **Grid-Federationsverbindung verwenden** wird das lokale Grid zum Quell-Grid und das Klonen in das durch die ausgewählte Grid-Federationsverbindung angegebene Remote-Grid ausgelöst. Existiert das Mandantenkonto bereits im Remote-Grid, führt das Klonen zu einem Konfliktfehler.

Bevor Sie beginnen

- Sie verwenden ein "unterstützte Webbrowser".

- Sie haben die "Root-Zugriffsberechtigung" für beide Grids.

Replikation für Mandanten Buckets deaktivieren

Als erster Schritt besteht darin, die netzübergreifende Replikation für alle Mandanten-Buckets zu deaktivieren.

Schritte

1. Von einem der beiden Grids aus erfolgt die Anmeldung beim Grid Manager über den primären Admin-Knoten.
2. Wählen Sie **Konfiguration** > **System** > **Grid federation**.
3. Wählen Sie den Verbindungsnamen aus, um die Details anzuzeigen.
4. Auf der Registerkarte **Zulässige Mandanten** lässt sich feststellen, ob der Mandant die Verbindung verwendet.
5. Wenn der Mandant aufgeführt ist, sollte er "Grid-übergreifende Replikation deaktivieren" für alle seine Buckets auf beiden Grids in der Verbindung durchführen.

Die Berechtigung **Grid-Federationsverbindung verwenden** kann nicht entfernt werden, wenn für einen Mandanten-Bucket die Grid-übergreifende Replikation aktiviert ist. Der Mandant muss die Grid-übergreifende Replikation für seine Buckets in beiden Grids deaktivieren.

Berechtigung für Mandanten entfernen

Nachdem die netzübergreifende Replikation für Mandanten-Buckets deaktiviert wurde, kann die Berechtigung des Mandanten zur Nutzung der Grid-Federationsverbindung entfernt werden.

Schritte

1. Melden Sie sich beim Grid Manager vom primären Admin-Knoten aus an.
2. Die Berechtigung kann auf der Grid federation-Seite oder der Tenants-Seite entfernt werden.

Grid Federation-Seite

a. Wählen Sie **Konfiguration** > **System** > **Grid federation**.
b. Der Verbindungsname kann ausgewählt werden, um die zugehörige Detailseite anzuzeigen.
c. Auf der Registerkarte **Zulässige Mieter** die Optionsschaltfläche für den Mieter auswählen.
d. **Berechtigung entfernen** auswählen.

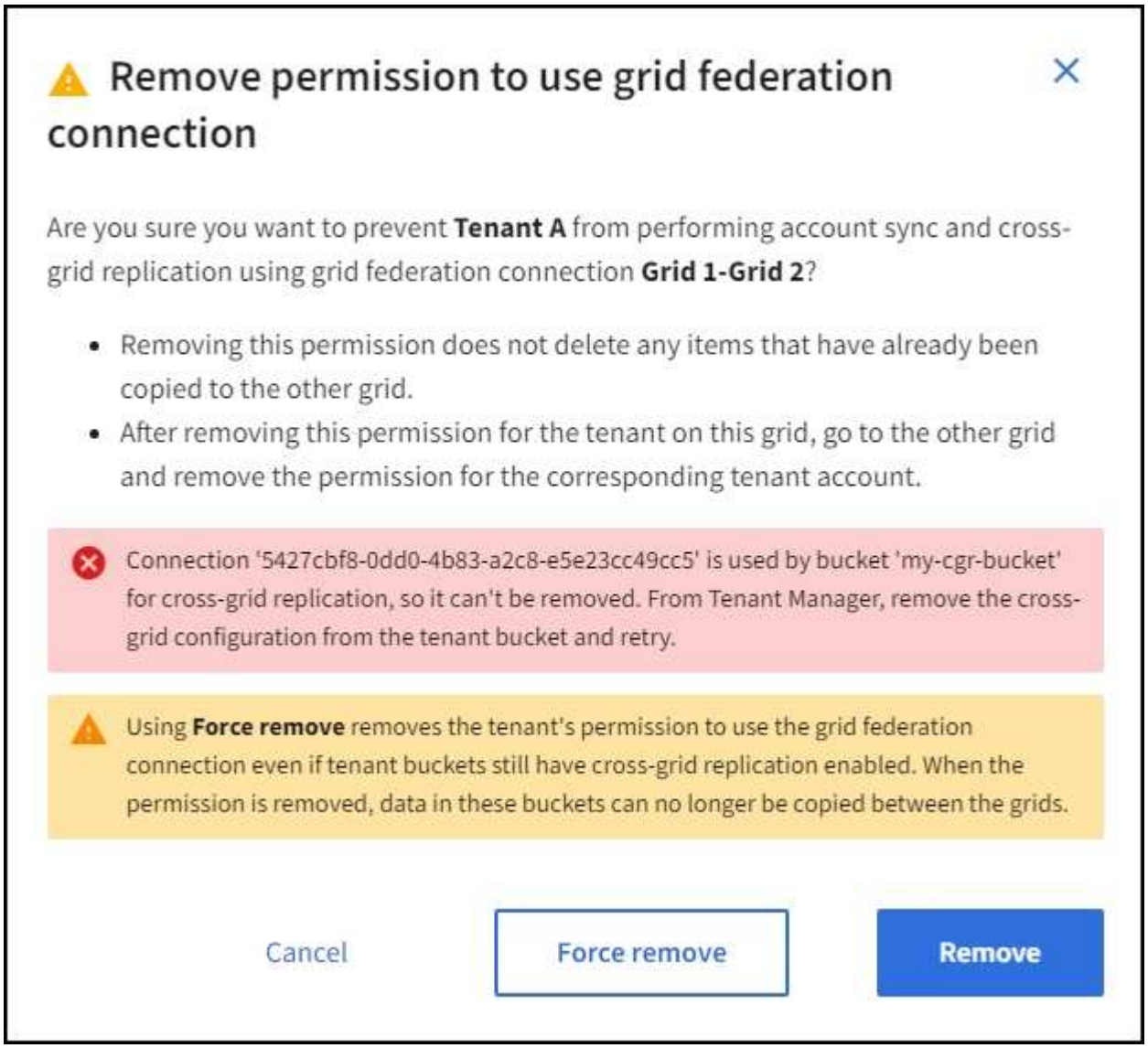
Mandantenseite

a. **Tenants** auswählen.
b. Der Name des Mieters auswählen, damit die Detailseite angezeigt wird.
c. Auf der Registerkarte **Grid federation** die Optionsschaltfläche für die Verbindung auswählen.
d. **Berechtigung entfernen** auswählen.

3. Die Warnungen im Bestätigungsdialogfeld sollten überprüft werden, danach ist **Entfernen** auszuwählen.
   - Wenn die Berechtigung entfernt werden kann, erfolgt eine Rückkehr zur Detailseite und eine Erfolgsmeldung wird angezeigt. Dieser Mandant kann die Grid Federation Verbindung nicht mehr

nutzen.

- Wenn für einen oder mehrere Mandanten-Buckets noch die Cross-Grid-Replikation aktiviert ist, wird eine Fehlermeldung angezeigt.



Es stehen folgende Optionen zur Verfügung:

- (Empfohlen.) Im Tenant Manager anmelden und die Replikation für jeden Bucket des Tenants deaktivieren. Siehe "Verwaltung der gridübergreifenden Replikation". Anschließend die Schritte zur Entfernung der Berechtigung **Use grid connection** wiederholen.
- Die Berechtigung wird zwangsweise entfernt. Im nächsten Abschnitt finden sich weitere Informationen.

4. Zum anderen Grid wechseln und diese Schritte wiederholen, um die Berechtigung für denselben Mandanten im anderen Grid zu entfernen.

Die Berechtigung zwangsweise entfernen

Bei Bedarf kann die Entfernung der Berechtigung eines Mandanten zur Nutzung einer Grid-Federation-Verbindung erzwungen werden, selbst wenn für die Mandanten-Buckets die gridübergreifende Replikation aktiviert ist.

Vor der erzwungenen Entfernung einer Berechtigung eines Mandanten sind die allgemeinen Überlegungen zu die Entfernung der Berechtigung sowie die folgenden zusätzlichen Aspekte zu beachten:

- Wenn Sie die Berechtigung **Use grid federation connection** mit Gewalt entfernen, werden alle Objekte, deren Replikation in das andere Grid noch aussteht (eingelesen, aber noch nicht repliziert), weiterhin repliziert. Um zu verhindern, dass diese Objekte im Replikationsprozess den Ziel-Bucket erreichen, muss die Berechtigung des Mandanten auch für das andere Grid entfernt werden.
- Alle Objekte, die nach der Entfernung der Berechtigung **Use grid federation connection** in den Quell-Bucket aufgenommen werden, werden niemals in den Ziel-Bucket repliziert.

Schritte

1. Melden Sie sich beim Grid Manager vom primären Admin-Knoten aus an.
2. Wählen Sie **Konfiguration** > **System** > **Grid federation**.
3. Der Verbindungsname kann ausgewählt werden, um die zugehörige Detailseite anzuzeigen.
4. Auf der Registerkarte **Zulässige Mieter** die Optionsschaltfläche für den Mieter auswählen.
5. **Berechtigung entfernen** auswählen.
6. Die Warnungen im Bestätigungsdialogfeld sollten überprüft werden, anschließend ist **Entfernung erzwingen** auszuwählen.

   Es erscheint eine Erfolgsmeldung. Dieser Mandant kann die Grid Federation Verbindung nicht mehr nutzen.

7. Gegebenenfalls zum anderen Grid wechseln und diese Schritte wiederholen, um die Berechtigung für dasselbe Mandantenkonto im anderen Grid zwangsweise zu entfernen. Zum Beispiel empfiehlt es sich, diese Schritte im anderen Grid zu wiederholen, um zu verhindern, dass Objekte im Verarbeitungsprozess den Ziel-Bucket erreichen.

Beheben von Grid-Federation-Fehlern in StorageGRID

Möglicherweise treten Warnmeldungen und Fehler im Zusammenhang mit Grid-Federation-Verbindungen, Kontoklon und gridübergreifender Replikation auf, die behoben werden müssen.

Warnungen und Fehler bei der Grid federation Verbindung

Möglicherweise erhalten Sie Warnmeldungen oder es treten Fehler bei Ihren Grid Federation Verbindungen auf.

Nachdem Änderungen zur Behebung eines Verbindungsproblems vorgenommen wurden, sollte die Verbindung getestet werden, um sicherzustellen, dass der Verbindungsstatus wieder auf **Verbunden** steht. Anleitungen finden sich unter "Grid Federation-Verbindungen verwalten".

Warnung vor Verbindungsfehler im Grid Federation-Verbund

Problem

Die Warnung **Fehler bei der Grid-Federation-Verbindung** wurde ausgelöst.

Details

Diese Warnmeldung weist darauf hin, dass die Grid Federation Verbindung zwischen den Grids nicht funktioniert.

Empfohlene Maßnahmen

1. Die Einstellungen auf der Seite Grid Federation für beide Grids überprüfen. Bestätigen, dass alle Werte korrekt sind. Siehe "Grid Federation-Verbindungen verwalten".
2. Die für die Verbindung verwendeten Zertifikate sollten überprüft werden. Es sollte sichergestellt sein, dass keine Warnungen zu abgelaufenen Grid Federation-Zertifikaten vorliegen und die Angaben zu jedem Zertifikat gültig sind. Anweisungen zum Rotieren von Verbindungszertifikaten finden sich in "Grid Federation-Verbindungen verwalten".
3. Bestätigen Sie, dass alle Admin- und Gateway-Knoten in beiden Grids online und verfügbar sind. Alle Warnmeldungen, die diese Knoten möglicherweise beeinträchtigen, sollten behoben werden, bevor ein erneuter Versuch unternommen wird.
4. Wenn ein vollqualifizierter Domainname (FQDN) für das lokale oder Remote-Grid angegeben wurde, sollte überprüft werden, ob der DNS-Server online und verfügbar ist. Siehe "Was ist Grid Federation?" zu Netzwerk-, IP-Adress- und DNS-Anforderungen.

Warnung zum Ablauf des Grid Federation-Zertifikats

Problem

Die Warnung **Ablauf des Grid Federation-Zertifikats** wurde ausgelöst.

Details

Diese Warnung weist darauf hin, dass ein oder mehrere Grid Federation-Zertifikate demnächst ablaufen.

Empfohlene Maßnahmen

Die Anweisungen zum Rotieren von Verbindungszertifikaten befinden sich in "Grid Federation-Verbindungen verwalten".

Fehler beim Bearbeiten einer Grid Federation Verbindung

Problem

Beim Bearbeiten einer Grid-Federation-Verbindung wird beim Auswählen von **Speichern und Testen** die folgende Warnmeldung angezeigt: „Fehler beim Erstellen einer Kandidaten-Konfigurationsdatei auf einem oder mehreren Knoten.“

Details

Wenn eine Grid-Federation-Verbindung bearbeitet wird, versucht StorageGRID, eine „Kandidaten-Konfigurationsdatei“ auf allen Admin-Knoten des ersten Grids zu speichern. Eine Warnmeldung erscheint, wenn diese Datei nicht auf allen Admin-Knoten gespeichert werden kann, beispielsweise weil ein Admin-Knoten offline ist.

Empfohlene Maßnahmen

1. Im Raster, das zum Bearbeiten der Verbindung verwendet wird, die Option **Knoten** auswählen.
2. Bestätigt wird, dass alle Admin-Knoten für dieses Grid online sind.
3. Falls einzelne Knoten offline sind, müssen diese wieder online geschaltet werden, danach kann die Verbindung erneut bearbeitet werden.

Fehler beim Klonen von Konten

Anmeldung bei einem geklonten Mandantenkonto nicht möglich

Problem

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

Details

Aus Sicherheitsgründen wird beim Klonen eines Mandantenkontos vom Quell-Grid zum Ziel-Grid das Passwort, das Sie für den lokalen Root-Benutzer des Mandanten festlegen, nicht geklont. Ebenso werden beim Erstellen lokaler Benutzer durch einen Mandanten im Quell-Grid die lokalen Benutzerpasswörter nicht auf das Ziel-Grid geklont.

Empfohlene Maßnahmen

Bevor sich der Root-Benutzer im Ziel-Grid des Mandanten anmelden kann, muss ein Grid-Administrator zuerst "das Passwort für den lokalen Root-Benutzer ändern" im Ziel-Grid.

Bevor sich ein geklonter lokaler Benutzer an der Ziel-Grid des Mandanten anmelden kann, muss der Root-Benutzer des geklonten Mandanten ein Passwort für den Benutzer auf der Ziel-Grid hinzufügen. Anweisungen finden sich unter "Benutzer verwalten" in der Anleitung zur Verwendung des Tenant Manager.

Mandant ohne Klon erstellt

Problem

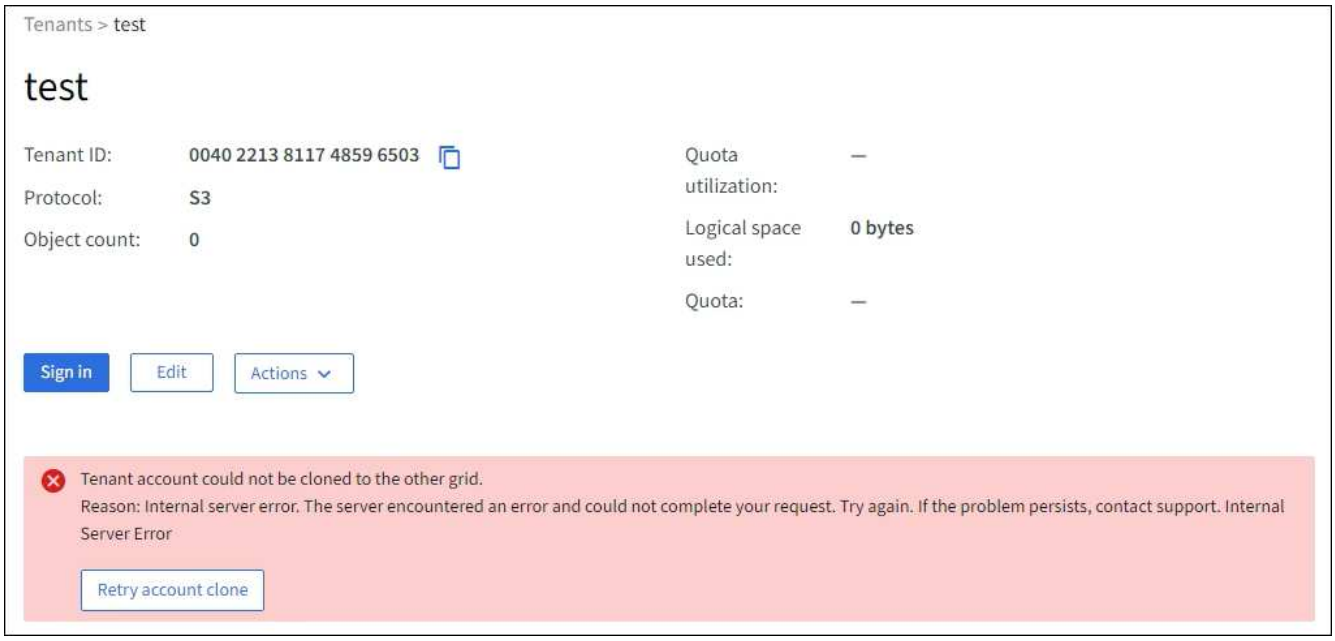
Nach dem Erstellen eines neuen Mandanten mit der Berechtigung **Grid-Federation-Verbindung verwenden** erscheint die Meldung „Mandant ohne Klon erstellt“.

Details

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

Empfohlene Maßnahmen

1. Den in der Fehlermeldung angegebenen Grund prüfen und etwaige Netzwerkprobleme oder andere Schwierigkeiten beheben, die die Verbindung möglicherweise verhindern. Siehe Benachrichtigungen und Fehler bei der Grid Federation Verbindung.
2. Den Anweisungen zum Testen einer Grid Federation Verbindung in "Grid Federation-Verbindungen verwalten" folgen, um zu bestätigen, dass das Problem behoben wurde.
3. Im Quell-Grid des Mandanten die Option **Tenants** auswählen.
4. Das Mandantenkonto ermitteln, das nicht geklont werden konnte.
5. Der Name des Mandanten auswählen, damit die Detailseite angezeigt wird.
6. **Kontoklonierung wiederholen** auswählen.



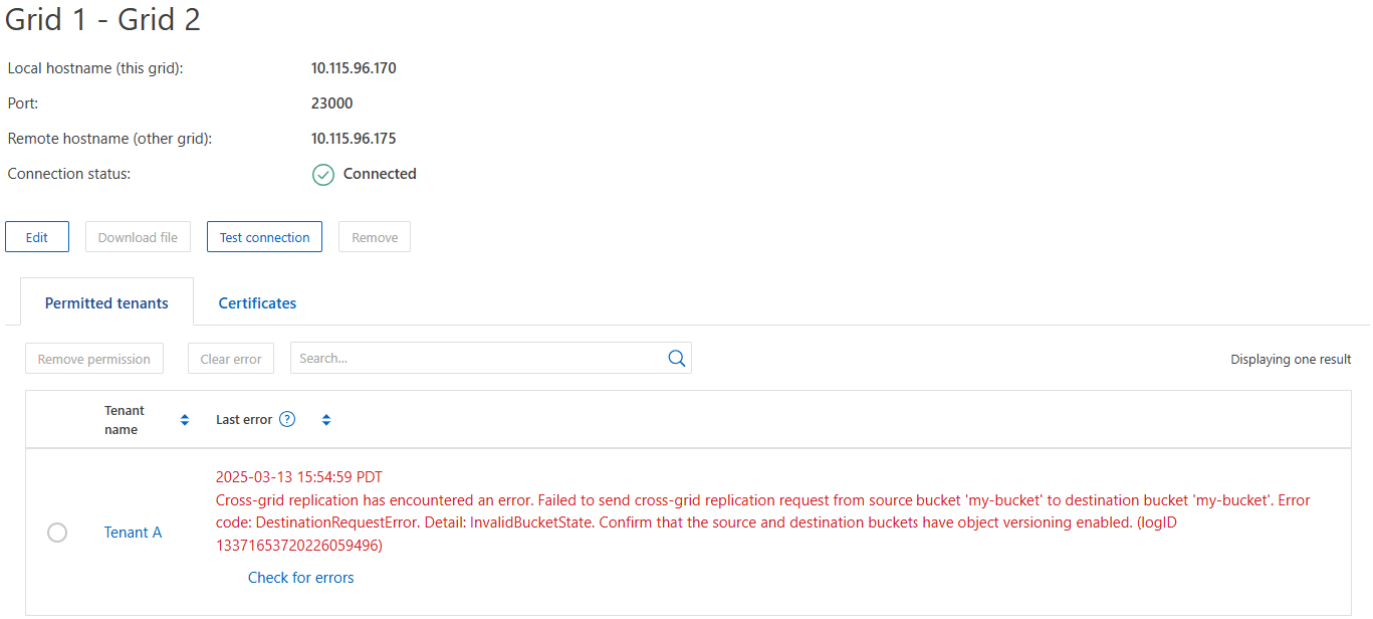
Wenn der Fehler behoben wurde, wird das Mandantenkonto nun in das andere Grid geklont.

Warnungen und Fehler bei der gridübergreifenden Replikation

${post_edited_translations.segment}

Problem

Wenn "Anzeigen einer Grid Federation Verbindung" (oder wenn "Verwaltung der zugelassenen Mandanten" für eine Verbindung) ein Fehler in der Spalte **Letzter Fehler** auf der Seite mit den Verbindungsdetails angezeigt wird. Zum Beispiel:



Details

Für jede Grid-Federation-Verbindung zeigt die Spalte **Letzter Fehler** den neuesten Fehler an, der ggf. bei der Replikation der Daten eines Mandanten in das andere Grid aufgetreten ist. In dieser Spalte wird nur der letzte Grid-übergreifende Replikationsfehler angezeigt; vorherige Fehler, die möglicherweise aufgetreten sind, 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.
- Die Versionierung des Ziel-Buckets ist ausgesetzt.
- Der Ziel-Bucket wurde vom selben Konto neu erstellt, ist jetzt jedoch nicht versioniert.
- ${post_edited_translations.segment}
- Das Quellobjekt verfügt über S3 Object Lock-Einstellungen, und S3 Object Lock ist im Ziel-Bucket deaktiviert.

Empfohlene Maßnahmen

Wenn in der Spalte **Letzter Fehler** eine Fehlermeldung angezeigt wird, sind folgende Schritte auszuführen:

1. ${post_edited_translations.segment}
2. Führen Sie alle empfohlenen Aktionen durch. Wenn beispielsweise die Versionierung für den Ziel-Bucket aufgrund der netzübergreifenden Replikation ausgesetzt wurde, sollte die Versionierung für diesen Bucket wieder aktiviert werden.
3. Die Verbindung oder das Mandantenkonto aus der Tabelle auswählen.
4. ${post_edited_translations.segment}
5. **Ja** auswählen, um die Meldung zu löschen und den Systemstatus zu aktualisieren.
6. Warten Sie 5–6 Minuten und geben Sie dann ein neues Objekt in den Bucket ein. Es sollte bestätigt werden, dass die Fehlermeldung nicht erneut erscheint.

   Um sicherzustellen, dass die Fehlermeldung verschwindet, sollte mindestens 5 Minuten nach dem Zeitstempel in der Meldung abgewartet werden, bevor ein neues Objekt eingelesen wird.

   ${post_edited_translations.segment}

7. Um festzustellen, ob Objekte aufgrund eines Bucket-Fehlers nicht repliziert werden konnten, siehe "Fehlgeschlagene Replikationsvorgänge identifizieren und erneut versuchen".

Warnung vor permanentem Fehler bei der Cross-grid-Replikation

Problem

Die Warnung **Permanenter Fehler bei der Cross-grid replication** wurde ausgelöst.

Details

Diese Warnung weist darauf hin, dass Mandantenobjekte aus einem Grund, der ein Eingreifen des Benutzers erfordert, nicht zwischen den Buckets auf zwei Grids repliziert werden können. Diese Warnung wird typischerweise durch eine Änderung am Quell- oder Ziel-Bucket verursacht.

Empfohlene Maßnahmen

1. Melden Sie sich bei dem Grid an, in dem die Warnung ausgelöst wurde.
2. Navigieren Sie zu **Konfiguration** > **System** > **Grid federation** und suchen Sie den in der Warnmeldung aufgeführten Verbindungsnamen.

3. Auf der Registerkarte „Zulässige Mandanten“ gibt die Spalte **Letzter Fehler** an, bei welchen Mandantenkonten Fehler vorliegen.
4. Weitere Informationen zum Fehler finden Sie in den Anweisungen in "Verbindungen zum Grid-Verbund überwachen" zur Überprüfung der Cross-Grid-Replikationsmetriken.
5. Für jedes betroffene Mandantenkonto:
   a. Siehe die Anweisungen in "Mieteraktivitäten überwachen", um zu bestätigen, dass der Mandant sein Kontingent für die netzübergreifende Replikation im Zielnetz nicht überschritten hat.
   b. Erforderlichenfalls das Kontingent des Mandanten im Ziel-Grid erhöhen, damit neue Objekte gespeichert werden können.
6. Für jeden betroffenen Mandanten bei beiden Grids im Tenant Manager anmelden, um die Liste der Buckets vergleichen zu können.
7. Für jeden Bucket, für den die netzübergreifende Replikation aktiviert ist, Folgendes bestätigen:
   - Für denselben Mandanten existiert ein entsprechender Bucket im anderen Grid (es muss exakt derselbe Name verwendet werden).
   - Bei beiden Buckets ist die Objektversionierung aktiviert (die Versionierung kann in keinem der Grids ausgesetzt werden).
   - Keiner der Buckets befindet sich im Zustand **Objekte werden gelöscht: schreibgeschützt**.
8. Zur Bestätigung, dass das Problem behoben wurde, siehe die Anweisungen in "Verbindungen zum Grid-Verbund überwachen" zur Überprüfung der Cross-Grid-Replikationsmetriken oder führen Sie diese Schritte aus:
   a. Zurück zur Grid Federation-Seite.
   b. ${post_edited_translations.segment}
   c. **Ja** auswählen, um die Meldung zu löschen und den Systemstatus zu aktualisieren.
   d. Warten Sie 5–6 Minuten und geben Sie dann ein neues Objekt in den Bucket ein. Es sollte bestätigt werden, dass die Fehlermeldung nicht erneut erscheint.

   > Um sicherzustellen, dass die Fehlermeldung verschwindet, sollte mindestens 5 Minuten nach dem Zeitstempel in der Meldung abgewartet werden, bevor ein neues Objekt eingelesen wird.

   > Es kann bis zu einem Tag dauern, bis die Warnmeldung nach der Behebung des Problems verschwindet.

   a. Wechseln Sie zu "Fehlgeschlagene Replikationsvorgänge identifizieren und erneut versuchen", um Objekte oder Löschmarkierungen zu identifizieren, die nicht in das andere Grid repliziert werden konnten, und um die Replikation bei Bedarf erneut zu versuchen.

${post_edited_translations.segment}

Problem

Die Warnung **Cross-grid replication resource unavailable** wurde ausgelöst.

Details

Diese Warnmeldung weist darauf hin, dass netzübergreifende Replikationsanforderungen ausstehen, weil eine Ressource nicht verfügbar ist. Beispielsweise könnte ein Netzwerkfehler vorliegen.

Empfohlene Maßnahmen

1. ${post_edited_translations.segment}
2. Wenn das Problem weiterhin besteht, ist zu prüfen, ob für eines der Grids ein Alarm wegen eines **Grid-Federierungs-Verbindungsfehlers** für dieselbe Verbindung oder ein Alarm wegen **Kommunikation mit Node nicht möglich** für einen Node vorliegt. Dieser Alarm wird möglicherweise behoben, wenn diese Alarme gelöst werden.
3. Weitere Informationen zum Fehler finden Sie in den Anweisungen in "Verbindungen zum Grid-Verbund überwachen" zur Überprüfung der Cross-Grid-Replikationsmetriken.
4. ${post_edited_translations.segment}

Die netzübergreifende Replikation läuft nach Behebung des Problems wie gewohnt weiter.

Fehlgeschlagene StorageGRID Replikationsvorgänge identifizieren und wiederholen

Nachdem die Warnung „Permanenter Fehler bei der Cross-grid replication“ behoben wurde, sollte festgestellt werden, ob Objekte oder Löschmarkierungen nicht in das andere Grid repliziert werden konnten. Anschließend können diese Objekte erneut importiert oder die Grid Management API verwendet werden, um die Replikation erneut zu versuchen.

Die Warnung „Permanenter Fehler bei der netzübergreifenden Replikation“ weist darauf hin, dass Mandantenobjekte aus einem Grund, der ein Eingreifen des Benutzers erfordert, nicht zwischen den Buckets auf zwei Grids repliziert werden können. Diese Warnung wird typischerweise durch eine Änderung am Quell- oder Ziel-Bucket verursacht. Weitere Informationen finden sich unter "Fehler in der Grid-Federation beheben".

Feststellen, ob Objekte nicht repliziert wurden.

Um festzustellen, ob Objekte oder Löschmarkierungen nicht in das andere Grid repliziert wurden, kann das Revisionsprotokoll nach "CGRR (Cross-Grid-Replikationsanforderung)" Meldungen durchsucht werden. Diese Meldung wird dem Protokoll hinzugefügt, wenn StorageGRID ein Objekt, ein Multipart-Objekt oder eine Löschmarkierung nicht in den Ziel-Bucket replizieren kann.

Sie können das "audit-explain Tool" verwenden, um die Ergebnisse in ein leichter lesbares Format zu übersetzen.

Bevor Sie beginnen

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

Schritte

1. ${post_edited_translations.segment}
   a. Geben Sie den folgenden Befehl ein: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.
   c. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
   d. Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.

Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` zu `#`.

2. Im Revisionsprotokoll nach CGRR-Meldungen suchen und das Tool audit-explain verwenden, um die Ergebnisse zu formatieren.

   Beispielsweise durchsucht dieser Befehl alle CGRR-Meldungen der letzten 30 Minuten und verwendet das Tool audit-explain.

   ```
   # 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 Cross-Grid-Replikationsanforderungen einen allgemeinen Fehler zurück, da das Objekt nicht repliziert werden konnte. Die ersten drei Fehler beziehen sich auf „replicate object“-Operationen, die letzten drei auf „replicate delete marker“-Operationen.

   ```
   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 die folgenden Informationen:

Feld	Beschreibung
CGRR Cross-Grid Replikationsanfrage	Der Name der Anfrage
Mandant	Die Konto-ID des Mandanten
Verbindung	Die ID der Grid Federation Verbindung

Feld	Beschreibung
Betrieb	Die Art des Replikationsvorgangs, der versucht wurde: • Objekt replizieren • Löschmarkierung replizieren • mehrteiliges Objekt replizieren
Bucket	Der Bucket Name
Objekt	Der Objektname
Version	Die Versions-ID für das Objekt
Fehler	Die Art des Fehlers. Wenn die netzübergreifende Replikation fehlgeschlagen ist, lautet die Fehlermeldung „Allgemeiner Fehler“.

Fehlgeschlagene Replikationen wiederholen

Nachdem eine Liste der Objekte und Löschmarkierungen erstellt wurde, die nicht in den Ziel-Bucket repliziert wurden, und die zugrunde liegenden Probleme behoben sind, besteht die Möglichkeit, die Replikation auf eine der beiden folgenden Arten erneut durchzuführen:

- Jedes Objekt wird erneut in den Quell-Bucket reingestellt.
- Die private Grid Management API wird wie beschrieben verwendet.

Schritte

1. Oben im Grid Manager das Hilfesymbol auswählen und anschließend **API documentation** wählen.
2. **Zur privaten API-Dokumentation** auswählen.

   Die als „Privat“ gekennzeichneten StorageGRID API-Endpunkte können ohne Vorankündigung geändert werden. StorageGRID private Endpunkte ignorieren außerdem die API-Version der Anfrage.

3. Im Abschnitt **cross-grid-replication-advanced** ist der folgende Endpunkt auszuwählen:

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

4. **Ausprobieren** auswählen.
5. Im Textfeld **body** ist der Beispiel-Eintrag für **versionID** durch eine Versions-ID aus dem Revisionsprotokoll audit.log zu ersetzen, die einer fehlgeschlagenen Cross-Grid-Replikationsanforderung entspricht.

   ${post_edited_translations.segment}

6. **Ausführen** auswählen.
7. Bestätigt wird, dass der Server-Antwortcode **204** ist, was darauf hinweist, dass das Objekt oder die Löschmarkierung als ausstehend für die gridübergreifende Replikation in das andere Grid markiert wurde.

„Ausstehend“ bedeutet, dass die Cross-Grid-Replikationsanfrage zur Bearbeitung in die interne Warteschlange aufgenommen wurde.

Replikationswiederholungen überwachen

Es empfiehlt sich, die Replikationswiederholungsvorgänge zu überwachen, um sicherzustellen, dass sie abgeschlossen werden.

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

Wiederholungsvorgänge lassen sich auf zwei Arten überwachen:

- Eine S3 "HeadObject"- oder "GetObject"-Anfrage kann verwendet werden. Die Antwort enthält den StorageGRID-spezifischen `x-ntap-sg-cgr-replication-status`-Antwortheader, der einen der folgenden Werte aufweist:

Grid	Replikationsstatus
Quelle	• **ABGESCHLOSSEN**: Die Replikation war erfolgreich. • **AUSSTEHEND**: Das Objekt ist noch nicht repliziert worden. • **FEHLER**: Die Replikation ist dauerhaft fehlgeschlagen. Ein Benutzer muss den Fehler beheben.
Ziel	**REPLICA**: Das Objekt wurde aus dem Quellgrid repliziert.

- Die private Grid Management API wird wie beschrieben verwendet.

Schritte

1. Im Abschnitt **cross-grid-replication-advanced** der privaten API-Dokumentation ist der folgende Endpunkt auszuwählen:

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

2. **Ausprobieren** auswählen.
3. Im Abschnitt „Parameter“ die Versions-ID eingeben, die in der `cross-grid-replication-retry-failed`Anfrage verwendet wurde.
4. **Ausführen** auswählen.
5. Es wird bestätigt, dass der Server-Antwortcode **200** ist.
6. Der Replikationsstatus ist einer der folgenden:
   - **AUSSTEHEND**: Das Objekt ist noch nicht repliziert worden.
   - **ABGESCHLOSSEN**: Die Replikation war erfolgreich.
   - **FEHLGESCHLAGEN**: Die Replikation ist dauerhaft fehlgeschlagen. Ein Benutzer muss den Fehler beheben.

Sicherheit verwalten

Sicherheit in StorageGRID verwalten

Verschiedene Sicherheitseinstellungen lassen sich über den Grid Manager konfigurieren, um das StorageGRID System zu schützen.

Verschlüsselung verwalten

StorageGRID bietet verschiedene Optionen zur Datenverschlüsselung. Es empfiehlt sich, "Die verfügbaren Verschlüsselungsmethoden werden dargestellt" zu prüfen, welche davon Ihren Datenschutzanforderungen entsprechen.

Zertifikate verwalten

Sie können "die Serverzertifikate konfigurieren und verwalten" für HTTP-Verbindungen oder die Clientzertifikate verwenden, die zur Authentifizierung einer Client- oder Benutzeridentität gegenüber dem Server dienen.

Schlüsselverwaltungsserver konfigurieren

Die Verwendung eines "Schlüsselverwaltungsserver" ermöglicht den Schutz von StorageGRID Daten selbst dann, wenn ein Gerät aus dem Rechenzentrum entfernt wird. Nachdem die Gerätevolumes verschlüsselt wurden, ist ein Zugriff auf Daten auf dem Gerät nur möglich, wenn der Node mit dem KMS kommunizieren kann.

${post_edited_translations.segment}

Proxy-Einstellungen verwalten

Wenn Sie S3-Plattformservices oder Cloud Storage Pools verwenden, können Sie einen "${post_edited_translations.segment}" zwischen Storage Nodes und den externen S3-Endpunkten konfigurieren. Wenn Sie AutoSupport Pakete über HTTPS oder HTTP senden, können Sie einen "Admin Proxyserver" zwischen Admin Nodes und dem technischen Support konfigurieren.

Firewalls kontrollieren

Um die Sicherheit Ihres Systems zu erhöhen, kann der Zugriff auf StorageGRID Admin Nodes gesteuert werden, indem bestimmte Ports am "externe Firewall" geöffnet oder geschlossen werden. Auch der Netzwerkzugriff auf jeden Knoten kann durch die Konfiguration seines "interne Firewall" gesteuert werden. Der Zugriff auf alle Ports außer denen, die für Ihre Bereitstellung benötigt werden, kann verhindert werden.

Überblick über StorageGRID Verschlüsselungsmethoden

StorageGRID bietet verschiedene Optionen zur Datenverschlüsselung. Die verfügbaren Methoden sollten geprüft werden, um festzustellen, welche den Anforderungen an den Datenschutz entsprechen.

Die Tabelle bietet eine Übersicht auf hoher Ebene über die in StorageGRID verfügbaren Verschlüsselungsmethoden.

Verschlüsselungsoption	So funktioniert es	Gilt für
Schlüsselverwaltungsserver (KMS) im Grid Manager	Sie "einen Schlüsselverwaltungsserver konfigurieren" für die StorageGRID Site und "Die Knotenverschlüsselung für das Gerät aktivieren". Anschließend stellt ein Appliance-Knoten eine Verbindung zum KMS her, um einen Key Encryption Key (KEK) anzufordern. Dieser Schlüssel verschlüsselt und entschlüsselt den Data Encryption Key (DEK) auf jedem Volume.	Appliance-Nodes, bei denen die **Node Encryption** während der Installation aktiviert wurde. Alle Daten auf der Appliance sind vor physischem Verlust oder der Entfernung aus dem Rechenzentrum geschützt. ${post_edited_translations.segment}
${post_edited_translations.segment}	Wenn die Appliance Laufwerke enthält, die eine Hardwareverschlüsselung unterstützen, können Sie während der Installation eine Laufwerks-Passphrase festlegen. Wenn Sie eine Laufwerks-Passphrase festlegen, ist es unmöglich, gültige Daten von aus dem System entfernten Laufwerken wiederherzustellen, es sei denn, die Passphrase ist bekannt. Vor dem Start der Installation navigieren Sie zu **Hardware konfigurieren** > **Laufwerksverschlüsselung**, um eine Laufwerks-Passphrase festzulegen, die für alle von StorageGRID verwalteten, selbstverschlüsselnden Laufwerke in einem Node gilt.	Geräte mit selbstverschlüsselnden Laufwerken. Alle Daten auf den gesicherten Laufwerken sind vor physischem Verlust oder Entfernung aus dem Rechenzentrum geschützt. Die Laufwerksverschlüsselung gilt nicht für von SANtricity verwaltete Laufwerke. Bei einem Storage-Appliance mit selbstverschlüsselnden Laufwerken und SANtricity Controllern kann die Laufwerkssicherheit in SANtricity aktiviert werden.
Laufwerkssicherheit im SANtricity System Manager	Wenn die Funktion „Laufwerkssicherheit“ für Ihre StorageGRID Appliance aktiviert ist, kann "SANtricity System Manager" zur Erstellung und Verwaltung des Sicherheitsschlüssels verwendet werden. Der Schlüssel ist erforderlich, um auf die Daten auf den gesicherten Laufwerken zuzugreifen.	Storage Appliances mit Full Disk Encryption (FDE) Laufwerken oder selbstverschlüsselnden Laufwerken. Alle Daten auf den gesicherten Laufwerken sind gegen physischen Verlust oder die Entfernung aus dem Rechenzentrum geschützt. Kann mit einigen Storage Appliances oder mit beliebigen Services Appliances nicht 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 weder auf Bucket-Ebene noch auf Objektebene verschlüsselt sind, während der Aufnahme verschlüsselt.	Neu importierte S3 Objektdaten. Vorhandene gespeicherte Objekte sind nicht verschlüsselt. Objektmetadaten und andere sensible Daten sind nicht verschlüsselt.
S3 Bucket Verschlüsselung	Sie senden eine PutBucketEncryption-Anforderung, um die Verschlüsselung für den Bucket zu aktivieren. Alle neuen Objekte, die nicht auf Objektebene verschlüsselt sind, werden beim Ingest verschlüsselt.	Nur neu ingestierte S3-Objektdaten. Die Verschlüsselung muss für den Bucket angegeben werden. Vorhandene Bucket-Objekte sind nicht verschlüsselt. Objektmetadaten und andere sensible Daten sind nicht verschlüsselt. "Operationen an Buckets"
S3-Objekt Server-seitige Verschlüsselung (SSE)	Sie senden eine S3-Anfrage zum Speichern eines Objekts und fügen den `x-amz-server-side-encryption` Request-Header hinzu.	Nur neu ingestierte S3-Objektdaten. Die Verschlüsselung muss für das Objekt angegeben werden. Objektmetadaten und andere sensible Daten werden nicht verschlüsselt. ${post_edited_translations.segment} "Serverseitige Verschlüsselung verwenden"
${post_edited_translations.segment}	Sie senden eine S3-Anfrage zum Speichern eines Objekts und fügen drei Anfrage-Header hinzu. • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	Nur neu ingestierte S3-Objektdaten. Die Verschlüsselung muss für das Objekt angegeben werden. Objektmetadaten und andere sensible Daten werden nicht verschlüsselt. ${post_edited_translations.segment} "Serverseitige Verschlüsselung verwenden"

Verschlüsselungsoption	So funktioniert es	Gilt für
Externe Volume- oder Datastore-Verschlüsselung	Eine Verschlüsselungsmethode außerhalb von StorageGRID wird verwendet, um ein gesamtes Volume oder einen Datenspeicher zu verschlüsseln, sofern Ihre Bereitstellungsplattform dies unterstützt.	Alle Objektdaten, Metadaten und Systemkonfigurationsdaten, vorausgesetzt, jedes Volume bzw. jeder Datenspeicher ist verschlüsselt. Eine externe Verschlüsselungsmethode ermöglicht eine präzisere Kontrolle über Verschlüsselungsalgorithmen und -schlüssel. Kann mit den anderen aufgeführten Methoden kombiniert werden.
Objektverschlüsselung außerhalb von StorageGRID	${post_edited_translations.segment}	Nur Objektdaten und Metadaten (Systemkonfigurationsdaten sind nicht verschlüsselt). Eine externe Verschlüsselungsmethode ermöglicht eine präzisere Kontrolle über Verschlüsselungsalgorithmen und -schlüssel. Kann mit den anderen aufgeführten Methoden kombiniert werden. "${post_edited_translations.segment}"

Mehrere Verschlüsselungsmethoden verwenden

Abhängig von Ihren Anforderungen können Sie mehr als eine Verschlüsselungsmethode gleichzeitig verwenden. Beispielsweise:

- ${post_edited_translations.segment}
- Sie können ein KMS verwenden, um Daten auf Appliance Knoten zu sichern, und außerdem die Option "Gespeicherte Objektverschlüsselung" verwenden, um alle Objekte beim Einlesen zu verschlüsseln.

Wenn nur ein kleiner Teil Ihrer Objekte eine Verschlüsselung erfordert, sollten Sie stattdessen in Betracht ziehen, die Verschlüsselung auf Bucket- oder einzelner Objektebene zu steuern. Die Aktivierung mehrerer Verschlüsselungsebenen verursacht zusätzliche Performance-Kosten.

Verwandte Informationen

"Informationen zu den FIPS-zertifizierten Verschlüsselungsoptionen"

Zertifikate verwalten

Sicherheitszertifikate in StorageGRID verwalten

Sicherheitszertifikate sind kleine Datendateien, die verwendet werden, um sichere und

vertrauenswürdige Verbindungen zwischen StorageGRID Komponenten sowie zwischen StorageGRID Komponenten und externen Systemen zu schaffen.

StorageGRID verwendet zwei Arten von Sicherheitszertifikaten:

- **Serverzertifikate** sind erforderlich, wenn HTTPS-Verbindungen verwendet werden. Serverzertifikate werden verwendet, um sichere Verbindungen zwischen Clients und Servern herzustellen, die Identität eines Servers gegenüber seinen Clients zu authentifizieren und einen sicheren Kommunikationsweg für Daten bereitzustellen. Der Server und der Client besitzen jeweils eine Kopie des Zertifikats.
- **Clientzertifikate** authentifizieren die Identität eines Clients oder Benutzers gegenüber dem Server und bieten damit 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 seiner Zertifikatskopie. Stimmen die Signaturen überein, beginnt der Client eine Sitzung mit dem Server unter Verwendung desselben öffentlichen Schlüssels.

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

Standardmäßiges 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 Datenverkehr zu sichern. Eine externe Zertifizierungsstelle (CA) kann benutzerdefinierte Zertifikate ausstellen, die den Informationssicherheitsrichtlinien Ihrer Organisation vollständig entsprechen.

Das Grid-CA-Zertifikat eignet sich für Nicht-Produktionsumgebungen. Für Produktionsumgebungen sind benutzerdefinierte Zertifikate zu verwenden, die von einer externen Zertifizierungsstelle signiert wurden. Ungesicherte Verbindungen ohne Zertifikat werden unterstützt, sind jedoch nicht empfehlenswert.

- Benutzerdefinierte CA-Zertifikate entfernen die internen Zertifikate nicht, jedoch sollten die benutzerdefinierten Zertifikate diejenigen sein, die zur Überprüfung von Serververbindungen angegeben werden.
- Alle kundenspezifischen Zertifikate müssen die "Richtlinien zur Systemhärtung für Serverzertifikate" erfüllen.
- StorageGRID unterstützt das Bündeln von Zertifikaten einer Zertifizierungsstelle in einer einzigen Datei (bekannt als CA-Zertifikatsbündel).

> StorageGRID enthält auch Betriebssystem-CA-Zertifikate, die auf allen Grids identisch sind. In Produktionsumgebungen ist sicherzustellen, dass anstelle des Betriebssystem-CA-Zertifikats ein von einer externen Zertifizierungsstelle signiertes benutzerdefiniertes Zertifikat angegeben wird.

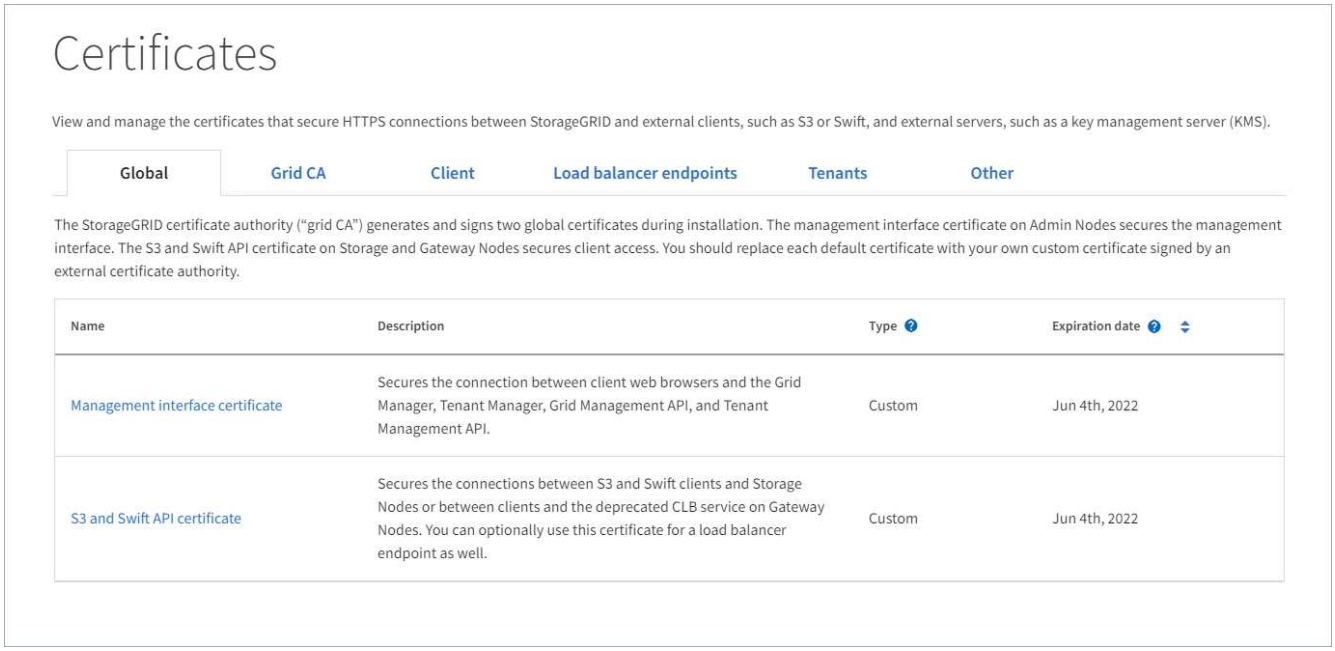
Varianten der Server- und Clientzertifikattypen werden auf verschiedene Weisen implementiert. Alle für Ihre spezifische StorageGRID Konfiguration benötigten Zertifikate sollten vor der Systemkonfiguration bereitliegen.

${post_edited_translations.segment}

Informationen zu allen StorageGRID Zertifikaten stehen an einem zentralen Ort zur Verfügung, zusammen mit Links zum Konfigurationsworkflow für jedes Zertifikat.

Schritte

1. ${post_edited_translations.segment}



2. Durch Auswahl einer Registerkarte auf der Seite „Certificates“ erhalten Sie Informationen zu den einzelnen Zertifikatskategorien und können auf die Zertifikatseinstellungen zugreifen. Sie können auf eine Registerkarte zugreifen, wenn Sie über die "${post_edited_translations.segment}" verfügen.

   - **Global**: Sichert den Zugriff auf StorageGRID von Webbrowsern und externen API-Clients.
   - **Grid CA**: Schützt den internen StorageGRID Datenverkehr.
   - ${post_edited_translations.segment}
   - **Load Balancer Endpunkte**: Sichert Verbindungen zwischen S3 Clients und dem StorageGRID Load Balancer.
   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}

   Die einzelnen Registerkarten werden im Folgenden beschrieben, mit Links zu weiteren Zertifikatsdetails.

Global

Die globalen Zertifikate sichern den Zugriff auf StorageGRID von Webbrowsern und externen S3-API-Clients. Zwei globale Zertifikate werden zu Beginn von der StorageGRID-Zertifizierungsstelle während der Installation generiert. Die empfohlene Vorgehensweise für eine Produktionsumgebung ist die Verwendung benutzerdefinierter Zertifikate, die von einer externen Zertifizierungsstelle signiert sind.

- Managementoberflächenzertifikat: Sichert die Webbrowser-Verbindungen der Clients zu den Managementoberflächen von StorageGRID.
- S3 API-Zertifikat: Sichert Client-API-Verbindungen zu Storage Nodes, Admin Nodes und Gateway Nodes, die von S3-Client-Anwendungen zum Hoch- und Herunterladen von Objektdaten verwendet werden.

Informationen zu den installierten globalen Zertifikaten sind enthalten:

- **Name**: Zertifikatsname mit Link zur Verwaltung des Zertifikats.
- **Beschreibung**
- **Typ**: Benutzerdefiniert oder Standard. + Ein benutzerdefiniertes Zertifikat bietet eine verbesserte Grid-Sicherheit.
- **Ablaufdatum**: Bei Verwendung des Standardzertifikats wird kein Ablaufdatum angezeigt.

${post_edited_translations.segment}

- ${post_edited_translations.segment}
  - "${post_edited_translations.segment}" wird für Verbindungen mit dem Grid Manager und Tenant Manager verwendet.
  - "Das S3-API-Zertifikat ersetzen" Wird für Verbindungen zum Storage Node und zum Load-Balancer-Endpunkt (optional) verwendet.
- "Das Standardzertifikat der Managementoberfläche wiederherstellen".
- "Das Standard-S3-API-Zertifikat wiederherstellen".
- "Ein Skript kann verwendet werden, um ein neues selbstsigniertes Managementoberfläche-Zertifikat zu generieren.".
- Kopieren oder laden Sie die "Managementoberfläche Zertifikat" oder "S3 API-Zertifikat" herunter.

Grid CA

Die von der StorageGRID-Zertifizierungsstelle während der StorageGRID Installation generierte Grid CA-Zertifikat sichert den gesamten internen StorageGRID Datenverkehr.

Die Zertifikatsinformationen umfassen das Ablaufdatum des Zertifikats und dessen Inhalt.

Sie können "Grid CA-Zertifikat kopieren oder herunterladen", aber Sie können es nicht ändern.

Client

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

${post_edited_translations.segment}

${post_edited_translations.segment}

- "${post_edited_translations.segment}"
- Wählen Sie einen Zertifikatsnamen aus, um die Zertifikatsdetails anzuzeigen, wo Sie Folgendes tun können:
  - "Der Name des Clientzertifikats wird geändert."
  - "Die Prometheus-Zugriffsberechtigung wird festgelegt."
  - "Das Clientzertifikat wird hochgeladen und ersetzt."
  - "Kopieren oder laden Sie das Client-Zertifikat herunter."
  - "Das Clientzertifikat entfernen."
- Über **Aktionen** können Sie ein Client-Zertifikat schnell "bearbeiten", "befestigen" oder "${post_edited_translations.segment}". Sie können bis zu 10 Client-Zertifikate auswählen und diese gleichzeitig über **Aktionen** > **Entfernen** entfernen.

Load Balancer Endpunkte

Load Balancer EndpunktzertifikateDie Verbindungen zwischen S3-Clients und dem StorageGRID Load Balancer Service auf Gateway Nodes und Admin Nodes werden gesichert.

Die Tabelle der Load-Balancer-Endpunkte enthält für jeden konfigurierten Load-Balancer-Endpunkt eine Zeile und gibt an, ob für den jeweiligen Endpunkt das globale S3 API-Zertifikat oder ein benutzerdefiniertes Load-Balancer-Endpunktzertifikat verwendet wird. Das Ablaufdatum jedes Zertifikats wird ebenfalls angezeigt.

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

${post_edited_translations.segment}

- "Einen Load Balancer-Endpunkt anzeigen", einschließlich seiner Zertifikatsdetails.
- "Ein Load-Balancer-Endpunktzertifikat für FabricPool angeben."
- "Das globale S3-API-Zertifikat verwenden" anstatt ein neues Load-Balancer-Endpunktzertifikat zu generieren.

${post_edited_translations.segment}

Mieter können ${post_edited_translations.segment} oder ${post_edited_translations.segment} verwenden, um ihre Verbindungen mit StorageGRID abzusichern.

${post_edited_translations.segment}

${post_edited_translations.segment}

- "${post_edited_translations.segment}"
- "${post_edited_translations.segment}"
- "Ein Mandantenname kann ausgewählt werden, um Details zu den Mandantenplattformdiensten anzuzeigen."
- "${post_edited_translations.segment}"

Sonstige

StorageGRID verwendet weitere Sicherheitszertifikate für spezifische Zwecke. Diese Zertifikate sind nach ihrem Funktionsnamen aufgelistet. Zu den weiteren Sicherheitszertifikaten gehören:

- Cloud Storage Pool-Zertifikate
- E-Mail-Benachrichtigungszertifikate
- Externe Syslog-Serverzertifikate
- Grid Federation Verbindungszertifikate
- Zertifikate für Identitätsföderation
- ${post_edited_translations.segment}
- Single Sign-On Zertifikate

Die Informationen geben Auskunft über den Typ des Zertifikats, den eine Funktion verwendet, sowie über das Ablaufdatum des Server- und Clientzertifikats, sofern zutreffend. Die Auswahl eines Funktionsnamens öffnet einen Browser-Tab, in dem die Zertifikatsdetails angezeigt und bearbeitet werden können.

> Informationen zu anderen Zertifikaten können Sie nur einsehen und darauf zugreifen, wenn Sie die "${post_edited_translations.segment}" haben.

${post_edited_translations.segment}

- "Ein Cloud Storage Pool-Zertifikat für S3, C2S S3 oder Azure angeben"
- "Ein Zertifikat für E-Mail-Benachrichtigungen bei Warnmeldungen angeben"
- "Ein Zertifikat für einen externen Syslog Server verwenden"
- "Grid Federation-Verbindungszertifikate rotieren"
- "Ein Identitätsföderationszertifikat anzeigen und bearbeiten"
- "Server- und Clientzertifikate des Key Management Servers (KMS) hochladen"
- "Manuelles Festlegen eines SSO-Zertifikats für eine Relying-Party-Vertrauensstellung"

Details zum Sicherheitszertifikat

Nachfolgend sind die verschiedenen Arten von Sicherheitszertifikaten beschrieben, mit Links zu den Implementierungsanweisungen.

Managementoberflächenzertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server	Authentifiziert die Verbindung zwischen Client-Webbrowsern und der StorageGRID Managementoberfläche, sodass Benutzer auf den Grid Manager und den Tenant Manager ohne Sicherheitswarnungen zugreifen können. Dieses Zertifikat authentifiziert auch Verbindungen zur Grid Management API und zur Tenant Management API. Sie können das während der Installation erstellte Standardzertifikat verwenden oder ein benutzerdefiniertes Zertifikat hochladen.	**Konfiguration** > **Sicherheit** > **Zertifikate**, die Registerkarte **Global** auswählen und dann **Managementoberfläche nzertifikat** auswählen	"Zertifikate für die Managementoberfläche konfigurieren"

S3 API-Zertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server	Authentifiziert sichere S3-Clientverbindungen zu einem Storage Node und zu Load-Balancer-Endpunkten (optional).	**Konfiguration** > **Sicherheit** > **Zertifikate**, die Registerkarte **Global** auswählen und dann **S3 API-Zertifikat** auswählen	"S3 API-Zertifikate konfigurieren"

Grid CA-Zertifikat

Siehe Standardbeschreibung des Grid-CA-Zertifikats.

Administrator Clientzertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Client	Auf jedem Client installiert, ermöglicht StorageGRID die Authentifizierung des externen Clientzugriffs. • Ermöglicht autorisierten externen Clients den Zugriff auf die StorageGRID Prometheus Datenbank. • Ermöglicht die sichere Überwachung von StorageGRID mithilfe externer Tools.	**Konfiguration** > **Sicherheit** > **Zertifikate** und anschließend die Registerkarte **Client** auswählen	"Clientzertifikate konfigurieren"

Load Balancer Endpunktzertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server	Authentifiziert die Verbindung zwischen S3-Clients und dem StorageGRID Load Balancer Service auf Gateway Nodes und Admin Nodes. Ein Load Balancer-Zertifikat kann hochgeladen oder generiert werden, wenn ein Load Balancer-Endpunkt konfiguriert wird. Clientanwendungen 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 S3 API-Zertifikat Zertifikats verwenden, um Verbindungen zum Load Balancer Service zu authentifizieren. Wenn das globale Zertifikat zur Authentifizierung von Load Balancer Verbindungen verwendet wird, ist es nicht erforderlich, ein separates Zertifikat für jeden Load Balancer Endpunkt hochzuladen oder zu generieren. **Hinweis:** Das für die Load-Balancer-Authentifizierung verwendete Zertifikat ist das am häufigsten genutzte Zertifikat während des normalen StorageGRID Betriebs.	**Konfiguration** > **Netzwerk** > **Load Balancer Endpunkte**	• "Load Balancer-Endpunkte konfigurieren" • "Einen Load Balancer-Endpunkt für FabricPool erstellen"

Cloud Storage Pool Endpunktzertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server	Authentifiziert die Verbindung von einem StorageGRID Cloud Storage Pool zu einem externen Speicherort, wie S3 Glacier oder Microsoft Azure Blob storage. Für jeden Cloud-Anbietertyp ist ein separates Zertifikat erforderlich.	**ILM** > **Speicherpools**	"Einen Cloud Storage Pool erstellen"

E-Mail-Benachrichtigungszertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server und Client	Authentifiziert die Verbindung zwischen einem SMTP-E-Mail-Server und StorageGRID, das für Alarmbenachrichtigungen verwendet wird. • Wenn die Kommunikation mit dem SMTP-Server Transport Layer Security (TLS) erfordert, ist das CA-Zertifikat des E-Mail-Servers anzugeben. • Ein Clientzertifikat ist nur anzugeben, wenn der SMTP-E-Mail-Server Clientzertifikate zur Authentifizierung verlangt.	**Benachrichtigungen** > **E-Mail-Einrichtung**	"E-Mail-Benachrichtigungen für Warnmeldungen einrichten"

Externes Syslog-Server-Zertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	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**	"Einen externen Syslog Server verwenden"

Grid Federation Verbindungszertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server und Client	Informationen, die zwischen dem aktuellen StorageGRID System und einem anderen Grid in einer Grid-Federation-Verbindung übertragen werden, werden authentifiziert und verschlüsselt.	**Konfiguration** > **System** > **Grid federation**	• "Grid Federation Verbindungen erstellen" • "Verbindungszertifikate austauschen"

Identitätsföderationszertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server	Authentifiziert die Verbindung zwischen StorageGRID und einem externen Identitätsanbieter wie Active Directory, OpenLDAP oder Oracle Directory Server. Wird für die Identitätsföderation verwendet, wodurch Administratorgruppen und Benutzer von einem externen System verwaltet werden können.	**Konfiguration** > **Zugriffskontrolle** > **Identitätsföderation**	"Identitätsföderation verwenden"

Schlüsselverwaltungsserver (KMS) Zertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server und Client	Authentifiziert die Verbindung zwischen StorageGRID und einem externen Schlüsselverwaltungsserver (KMS), der Verschlüsselungsschlüssel für StorageGRID Appliance-Knoten bereitstellt.	**Konfiguration** > **Sicherheit** > **Schlüsselverwaltungsserver**	"Schlüsselverwaltungsserver (KMS) hinzufügen"

Plattformdienste Endpunktzertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server	Authentifiziert die Verbindung vom StorageGRID Plattformdienst zu einer S3 Speicherressource.	**Tenant Manager** > **SPEICHER (S3)** > **Plattformdienste Endpunkte**	"Plattform Services Endpunkt erstellen" "Plattformdienste-Endpunkt bearbeiten"

Single Sign-On (SSO) Zertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server	Authentifiziert die Verbindung zwischen Identitätsverbunddiensten wie Active Directory Federation Services (AD FS) und StorageGRID, die für Single Sign-On (SSO)-Anfragen verwendet werden.	**Konfiguration** > **Zugriffskontrolle** > **Single sign-on**	"Einmalanmeldung konfigurieren"

Zertifikatsbeispiele

Beispiel 1: Load Balancer Dienst

In diesem Beispiel fungiert StorageGRID als Server.

1. Ein Load-Balancer-Endpunkt wird konfiguriert und ein Serverzertifikat in StorageGRID hochgeladen oder generiert.
2. Eine S3-Clientverbindung wird zum Load-Balancer-Endpunkt konfiguriert und dasselbe Zertifikat auf den Client hochgeladen.
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, sowie mit einer auf dem privaten Schlüssel basierenden Signatur.
5. Der Client vergleicht die Serversignatur mit der Signatur seiner Zertifikatskopie. Wenn die Signaturen übereinstimmen, beginnt der Client eine Sitzung mit demselben öffentlichen Schlüssel.
6. ${post_edited_translations.segment}

${post_edited_translations.segment}

In diesem Beispiel fungiert StorageGRID als Client.

1. Mit externer Key Management Server-Software wird StorageGRID als KMS-Client konfiguriert und ein von einer Zertifizierungsstelle signiertes Serverzertifikat, ein öffentliches Clientzertifikat sowie der private Schlüssel für das Clientzertifikat bezogen.
2. Mit dem Grid Manager wird ein KMS-Server konfiguriert und die Server- und Clientzertifikate sowie der private Clientschlüssel hochgeladen.
3. Wenn ein StorageGRID-Knoten einen Verschlüsselungsschlüssel benötigt, sendet er eine Anfrage an den KMS-Server, die Daten aus dem Zertifikat und eine auf dem privaten Schlüssel basierende Signatur enthält.
4. Der KMS-Server prüft die Zertifikatssignatur und entscheidet, dass er StorageGRID vertrauen kann.
5. Der KMS Server antwortet über die validierte Verbindung.

Unterstützte Serverzertifikatstypen in StorageGRID

Das StorageGRID System unterstützt benutzerdefinierte Zertifikate, die mit RSA oder ECDSA (Elliptic Curve Digital Signature Algorithm) verschlüsselt sind.

> Der Verschlüsselungstyp der Sicherheitsrichtlinie muss mit dem Serverzertifikatstyp übereinstimmen. Beispielsweise erfordern RSA-Cipher RSA-Zertifikate und ECDSA-Cipher ECDSA-Zertifikate. Siehe "Sicherheitszertifikate verwalten". Wenn eine benutzerdefinierte Sicherheitsrichtlinie konfiguriert wird, die nicht mit dem Serverzertifikat kompatibel ist, kann "vorübergehend zur Standard-Sicherheitsrichtlinie zurückkehren".

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

Konfigurieren Sie Managementoberflächenzertifikate in StorageGRID

Sie können das standardmäßige Zertifikat der Managementoberfläche durch ein einzelnes benutzerdefiniertes Zertifikat ersetzen, das Benutzern den Zugriff auf den Grid Manager und den Tenant Manager ohne Sicherheitswarnungen ermöglicht. Sie können auch zum standardmäßigen Zertifikat der Managementoberfläche zurückkehren oder ein neues generieren.

Über diese Aufgabe

Standardmäßig erhält jeder Admin-Knoten ein von der Grid-CA signiertes Zertifikat. Diese von der CA signierten Zertifikate können durch ein einziges gemeinsames benutzerdefiniertes Managementoberflächenzertifikat und den entsprechenden privaten Schlüssel ersetzt werden.

Da ein einziges benutzerdefiniertes Zertifikat für die Managementoberfläche für alle Admin Nodes verwendet

wird, müssen Sie das Zertifikat als Wildcard- oder Multi-Domain-Zertifikat angeben, wenn Clients den Hostnamen bei der Verbindung mit dem Grid Manager und Tenant Manager verifizieren müssen. Das benutzerdefinierte Zertifikat muss so definiert werden, dass es mit allen Admin Nodes im Grid übereinstimmt.

${post_edited_translations.segment}

Um sicherzustellen, dass der Betrieb nicht durch ein fehlerhaftes Serverzertifikat beeinträchtigt wird, löst das System den Alarm **Ablauf des Serverzertifikats für die Managementoberfläche** aus, wenn dieses Serverzertifikat bald abläuft. Bei Bedarf können Sie einsehen, wann das aktuelle Zertifikat abläuft, indem Sie **Konfiguration** > **Sicherheit** > **Zertifikate** auswählen und das Ablaufdatum für das Zertifikat der Managementoberfläche auf der Registerkarte „Global“ prüfen.

Wenn Sie über einen Domänennamen anstatt über eine IP-Adresse auf den Grid Manager oder Tenant Manager zugreifen, zeigt der Browser eine Zertifikatsfehlermeldung ohne Möglichkeit zur Umgehung an, wenn einer der folgenden Fälle eintritt:

- Ihr benutzerdefiniertes Managementoberfläche-Zertifikat läuft ab.
- Sie ${post_edited_translations.segment}.

Ein benutzerdefiniertes Managementoberfläche-Zertifikat hinzufügen

${post_edited_translations.segment}

Schritte

1. **Konfiguration** > **Sicherheit** > **Zertifikate** auswählen.
2. Auf der Registerkarte **Global** die Option **Managementoberfläche-Zertifikat** auswählen.
3. **Benutzerdefiniertes Zertifikat verwenden** auswählen.
4. Das Zertifikat kann hochgeladen oder generiert werden.

Zertifikat hochladen

Die erforderlichen Serverzertifikatsdateien werden hochgeladen.

a. **Zertifikat hochladen** auswählen.

b. ${post_edited_translations.segment}

   - ${post_edited_translations.segment}
   - **Privater Zertifikatsschlüssel**: Die benutzerdefinierte private Schlüsseldatei des Serverzertifikats (`.key`).

     Private EC-Schlüssel müssen mindestens 224 Bit groß sein. Private RSA-Schlüssel müssen mindestens 2048 Bit groß sein.

   - **CA bundle**: Eine einzelne optionale Datei, die die Zertifikate aller zwischengeschalteten Zertifizierungsstellen (CAs) enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatsdateien, in der Reihenfolge der Zertifikatskette zusammengefügt, enthalten.

c. **Zertifikatsdetails** kann erweitert werden, um die Metadaten jedes hochgeladenen Zertifikats anzuzeigen. Wenn ein optionales CA-Bundle hochgeladen wurde, wird jedes Zertifikat auf einem eigenen Tab angezeigt.

   - ${post_edited_translations.segment}

     Geben Sie den Namen der Zertifikatsdatei und den Speicherort für den Download an. Die Datei wird mit der Erweiterung `.pem` gespeichert.

   Zum Beispiel: `storagegrid_certificate.pem`

   - ${post_edited_translations.segment}

d. **Speichern** auswählen. + Das benutzerdefinierte Managementoberflächenzertifikat wird für alle nachfolgenden neuen Verbindungen zum Grid Manager, Tenant Manager, Grid Manager API oder Tenant Manager API verwendet.

Zertifikat generieren

Die Serverzertifikatsdateien werden generiert.

${post_edited_translations.segment}

a. **Zertifikat generieren** auswählen.

b. ${post_edited_translations.segment}

Feld	Beschreibung
Domainname	Ein oder mehrere vollqualifizierte Domain-Namen, die in das Zertifikat aufgenommen werden sollen. Ein * kann als Platzhalter verwendet werden, um mehrere Domain-Namen darzustellen.
${post_edited_translations.segment}	${post_edited_translations.segment}

Feld	Beschreibung
Thema (optional)	${post_edited_translations.segment} Wird in diesem Feld kein Wert eingegeben, verwendet das generierte Zertifikat den ersten Domänennamen oder die erste IP-Adresse als allgemeinen Subjektnamen (CN).
Gültigkeitstage	Anzahl der Tage nach der Erstellung, nach denen das Zertifikat abläuft.
Schlüsselverwendungserweiterungen hinzufügen	Wenn diese Option ausgewählt ist (Standard und empfohlen), werden die Schlüsselverwendungs- und erweiterten Schlüsselverwendungs-Erweiterungen dem generierten Zertifikat hinzugefügt. Diese Erweiterungen definieren den Zweck des im Zertifikat enthaltenen Schlüssels. **Hinweis**: Dieses Kontrollkästchen sollte aktiviert bleiben, es sei denn, bei älteren Clients treten Verbindungsprobleme auf, wenn die Zertifikate diese Erweiterungen enthalten.

c. Wählen Sie **Generieren**.

d. **Zertifikatdetails** zeigt die Metadaten des generierten Zertifikats an.

   - **Zertifikat herunterladen** auswählen, um die Zertifikatsdatei zu speichern.

     Geben Sie den Namen der Zertifikatsdatei und den Speicherort für den Download an. Die Datei wird mit der Erweiterung `.pem` gespeichert.

   Zum Beispiel: `storagegrid_certificate.pem`

   - **Zertifikat PEM kopieren** auswählen, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.

e. **Speichern** auswählen. + Das benutzerdefinierte Managementoberflächenzertifikat wird für alle nachfolgenden neuen Verbindungen zum Grid Manager, Tenant Manager, Grid Manager API oder Tenant Manager API verwendet.

5. ${post_edited_translations.segment}

   Nach dem Hochladen oder Generieren eines neuen Zertifikats kann es bis zu einem Tag dauern, bis etwaige Benachrichtigungen über das Ablaufdatum des Zertifikats entfernt werden.

6. Nach dem Hinzufügen eines benutzerdefinierten Managementoberfläche-Zertifikats zeigt die Seite „Managementoberfläche-Zertifikat“ detaillierte Zertifikatsinformationen zu den verwendeten Zertifikaten an. + Das Zertifikat-PEM kann bei Bedarf heruntergeladen oder kopiert werden.

Das Standardzertifikat der Managementoberfläche wiederherstellen

Es ist möglich, wieder das Standardzertifikat der Managementoberfläche für Verbindungen mit Grid Manager und Tenant Manager zu verwenden.

Schritte

1. **Konfiguration** > **Sicherheit** > **Zertifikate** auswählen.
2. Auf der Registerkarte **Global** die Option **Managementoberfläche-Zertifikat** auswählen.
3. ${post_edited_translations.segment}

   Wenn Sie das Standardzertifikat für die Managementoberfläche wiederherstellen, werden die von Ihnen konfigurierten benutzerdefinierten Serverzertifikatsdateien gelöscht und können nicht mehr vom System wiederhergestellt werden. Das Standardzertifikat für die Managementoberfläche wird für alle nachfolgenden neuen Client-Verbindungen verwendet.

4. ${post_edited_translations.segment}

Ein Skript kann verwendet werden, um ein neues selbstsigniertes Managementoberfläche-Zertifikat zu generieren.

${post_edited_translations.segment}

Bevor Sie beginnen

- Du hast "spezifische Zugriffsberechtigungen".
- Sie haben die `Passwords.txt` Datei.

Über diese Aufgabe

Die empfohlene Vorgehensweise für eine Produktionsumgebung ist die Verwendung eines von einer externen Zertifizierungsstelle signierten Zertifikats.

Schritte

1. Den vollqualifizierten Domainnamen (FQDN) jedes Admin-Knotens ermitteln.
2. ${post_edited_translations.segment}
   a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
   b. Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.
   c. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
   d. Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.

      Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` zu `#`.

3. ${post_edited_translations.segment}

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

   - Für `--domains` sind Platzhalter zu verwenden, um die vollqualifizierten Domain-Namen aller Admin-Nodes darzustellen. Beispielsweise verwendet `*.ui.storagegrid.example.com` den Platzhalter *, um `admin1.ui.storagegrid.example.com` und `admin2.ui.storagegrid.example.com` darzustellen.
   - Setzen von `--type` auf `management` zur Konfiguration des Zertifikats für die Managementoberfläche, das vom Grid Manager und Tenant Manager verwendet wird.
   - Standardmäßig sind generierte Zertifikate ein Jahr (365 Tage) gültig und müssen vor Ablauf neu erstellt werden. Mit dem `--days` Argument lässt sich die Standardgültigkeitsdauer überschreiben.

Die Gültigkeitsdauer eines Zertifikats beginnt, wenn `make-certificate` ausgeführt wird. Sie müssen sicherstellen, dass der Management-Client mit derselben Zeitquelle wie StorageGRID synchronisiert ist, da der Client das Zertifikat andernfalls möglicherweise ablehnt.

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

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

4. Das Zertifikat auswählen und kopieren.

   ${post_edited_translations.segment}

5. Melden Sie sich von der Befehlsshell ab. `$ exit`
6. ${post_edited_translations.segment}
   a. Auf den Grid Manager zugreifen.
   b. **Konfiguration** > **Sicherheit** > **Zertifikate** auswählen
   c. Auf der Registerkarte **Global** die Option **Managementoberfläche-Zertifikat** auswählen.
7. Konfigurieren Sie Ihren Management-Client so, dass das kopierte öffentliche Zertifikat verwendet wird. Die BEGIN- und END-Tags sind einzuschließen.

${post_edited_translations.segment}

${post_edited_translations.segment}

Schritte

1. **Konfiguration** > **Sicherheit** > **Zertifikate** auswählen.
2. Auf der Registerkarte **Global** die Option **Managementoberfläche-Zertifikat** auswählen.
3. ${post_edited_translations.segment}

${post_edited_translations.segment}

Die Zertifikats- oder CA-Bundle-Datei `.pem` herunterladen. Bei Verwendung eines optionalen CA-Bundles wird jedes Zertifikat im Bundle auf einer eigenen Unterregisterkarte angezeigt.

a. **Zertifikat herunterladen** oder **CA-Bundle herunterladen** auswählen.

   ${post_edited_translations.segment}

b. Geben Sie den Namen der Zertifikatsdatei und den Speicherort für den Download an. Die Datei wird mit der Erweiterung `.pem` gespeichert.

   Zum Beispiel: `storagegrid_certificate.pem`

${post_edited_translations.segment}

Kopieren Sie den Zertifikatstext, um ihn an anderer Stelle einzufügen. Wenn ein optionales CA-Bundle verwendet wird, wird jedes Zertifikat im Bundle auf einem eigenen Unterreiter angezeigt.

a. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

b. Das kopierte Zertifikat in einen Texteditor einfügen.

c. Die Textdatei mit der Erweiterung `.pem` speichern.

   Zum Beispiel: `storagegrid_certificate.pem`

Konfigurieren Sie S3-API-Zertifikate in StorageGRID

Sie können das Serverzertifikat, das für S3-Clientverbindungen zu Storage Nodes oder zu Load-Balancer-Endpunkten verwendet wird, ersetzen oder wiederherstellen. Das Ersatz-Serverzertifikat ist spezifisch für Ihre Organisation.

Swift-Details wurden aus dieser Version der Dokumentationsseite entfernt. Siehe "StorageGRID 11.8: S3 und Swift API-Zertifikate konfigurieren".

Über diese Aufgabe

Standardmäßig erhält jeder Storage Node ein vom Grid-CA signiertes X.509-Serverzertifikat. Diese von der CA signierten Zertifikate können durch ein einzelnes, gemeinsames benutzerdefiniertes Serverzertifikat und den entsprechenden privaten Schlüssel ersetzt werden.

Für alle Storage Nodes wird ein einzelnes benutzerdefiniertes Serverzertifikat verwendet, daher muss das Zertifikat als Wildcard- oder Multi-Domain-Zertifikat angegeben werden, wenn Clients den Hostnamen beim Verbinden mit dem Storage Endpoint überprüfen müssen. Das benutzerdefinierte Zertifikat ist so zu definieren, dass es mit allen Storage Nodes im Grid übereinstimmt.

Nach Abschluss der Konfiguration auf dem Server müssen Sie möglicherweise auch das Grid CA-Zertifikat im S3 API-Client installieren, den Sie für den Zugriff auf das System verwenden, abhängig von der verwendeten Stammzertifizierungsstelle (CA).

Um sicherzustellen, dass der Betrieb durch ein fehlerhaftes Serverzertifikat nicht beeinträchtigt wird, wird die Warnung **Ablauf des globalen Serverzertifikats für S3 API** ausgelöst, wenn das Stammserverzertifikat kurz vor dem Ablauf steht. Wie erforderlich, kann eingesehen werden, wann das aktuelle Zertifikat abläuft, indem **Konfiguration** > **Sicherheit** > **Zertifikate** ausgewählt und auf der Registerkarte „Global“ das Ablaufdatum des S3 API-Zertifikats betrachtet wird.

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

Ein benutzerdefiniertes S3 API-Zertifikat hinzufügen

Schritte

1. **Konfiguration** > **Sicherheit** > **Zertifikate** auswählen.
2. Auf der Registerkarte **Global** die Option **S3 API certificate** auswählen.
3. **Benutzerdefiniertes Zertifikat verwenden** auswählen.
4. Das Zertifikat kann hochgeladen oder generiert werden.

Zertifikat hochladen

Die erforderlichen Serverzertifikatsdateien werden hochgeladen.

a. **Zertifikat hochladen** auswählen.

b. ${post_edited_translations.segment}

   - ${post_edited_translations.segment}
   - **Privater Zertifikatsschlüssel**: Die benutzerdefinierte private Schlüsseldatei des Serverzertifikats (`.key`).

     Private EC-Schlüssel müssen mindestens 224 Bit groß sein. Private RSA-Schlüssel müssen mindestens 2048 Bit groß sein.

   - **CA bundle**: Eine optionale Datei, die die Zertifikate aller ausstellenden Zwischenzertifizierungsstellen enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatsdateien in der Reihenfolge der Zertifikatskette enthalten.

c. Wählen Sie die Zertifikatsdetails aus, um die Metadaten und die PEM für jedes hochgeladene benutzerdefinierte S3 API-Zertifikat anzuzeigen. Wenn ein optionales CA-Bundle hochgeladen wurde, erscheint jedes Zertifikat auf einer eigenen Registerkarte.

   - ${post_edited_translations.segment}

     Geben Sie den Namen der Zertifikatsdatei und den Speicherort für den Download an. Die Datei wird mit der Erweiterung `.pem` gespeichert.

   Zum Beispiel: `storagegrid_certificate.pem`

   - ${post_edited_translations.segment}

d. **Speichern** auswählen.

   Das benutzerdefinierte Serverzertifikat wird für nachfolgende neue S3-Clientverbindungen verwendet.

Zertifikat generieren

Die Serverzertifikatsdateien werden generiert.

a. **Zertifikat generieren** auswählen.

b. ${post_edited_translations.segment}

Feld	Beschreibung
Domainname	Ein oder mehrere vollqualifizierte Domain-Namen, die in das Zertifikat aufgenommen werden sollen. Ein * kann als Platzhalter verwendet werden, um mehrere Domain-Namen darzustellen.
${post_edited_translations.segment}	${post_edited_translations.segment}

Feld	Beschreibung
Thema (optional)	${post_edited_translations.segment} Wird in diesem Feld kein Wert eingegeben, verwendet das generierte Zertifikat den ersten Domänennamen oder die erste IP-Adresse als allgemeinen Subjektnamen (CN).
Gültigkeitstage	Anzahl der Tage nach der Erstellung, nach denen das Zertifikat abläuft.
Schlüsselverwendungserweiterungen hinzufügen	Wenn diese Option ausgewählt ist (Standard und empfohlen), werden die Schlüsselverwendungs- und erweiterten Schlüsselverwendungs-Erweiterungen dem generierten Zertifikat hinzugefügt. Diese Erweiterungen definieren den Zweck des im Zertifikat enthaltenen Schlüssels. **Hinweis**: Dieses Kontrollkästchen sollte aktiviert bleiben, es sei denn, bei älteren Clients treten Verbindungsprobleme auf, wenn die Zertifikate diese Erweiterungen enthalten.

c. Wählen Sie **Generieren**.

d. **Zertifikatdetails** auswählen, um die Metadaten und die PEM für das generierte benutzerdefinierte S3-API-Zertifikat anzuzeigen.

   - **Zertifikat herunterladen** auswählen, um die Zertifikatsdatei zu speichern.

     Geben Sie den Namen der Zertifikatsdatei und den Speicherort für den Download an. Die Datei wird mit der Erweiterung `.pem` gespeichert.

   Zum Beispiel: `storagegrid_certificate.pem`

   - **Zertifikat PEM kopieren** auswählen, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.

e. **Speichern** auswählen.

   Das benutzerdefinierte Serverzertifikat wird für nachfolgende neue S3-Clientverbindungen verwendet.

5. Wählen Sie eine Registerkarte aus, um Metadaten für das Standard StorageGRID Serverzertifikat, ein hochgeladenes, von einer Zertifizierungsstelle signiertes Zertifikat oder ein generiertes benutzerdefiniertes Zertifikat anzuzeigen.

   Nach dem Hochladen oder Generieren eines neuen Zertifikats kann es bis zu einem Tag dauern, bis etwaige Benachrichtigungen über das Ablaufdatum des Zertifikats entfernt werden.

6. ${post_edited_translations.segment}

7. Nachdem Sie ein benutzerdefiniertes S3 API-Zertifikat hinzugefügt haben, zeigt die Seite S3 API-Zertifikat detaillierte Zertifikatsinformationen für das verwendete benutzerdefinierte S3 API-Zertifikat an. + Das

Zertifikat-PEM kann bei Bedarf heruntergeladen oder kopiert werden.

Das Standard-S3-API-Zertifikat wiederherstellen

Sie können für S3-Clientverbindungen zu Storage Nodes wieder das Standard-S3-API-Zertifikat verwenden. Das Standard-S3-API-Zertifikat kann jedoch nicht für einen Load Balancer Endpoint verwendet werden.

Schritte

1. **Konfiguration** > **Sicherheit** > **Zertifikate** auswählen.
2. Auf der Registerkarte **Global** die Option **S3 API certificate** auswählen.
3. ${post_edited_translations.segment}

   Wenn die Standardversion des globalen S3-API-Zertifikats wiederhergestellt wird, werden die von Ihnen konfigurierten benutzerdefinierten Serverzertifikatsdateien gelöscht und können nicht aus dem System wiederhergestellt werden. Das Standard-S3-API-Zertifikat wird für nachfolgende neue S3-Clientverbindungen zu Storage Nodes verwendet.

4. **OK** auswählen bestätigt die Warnung und stellt das Standard-S3-API-Zertifikat wieder her.

   Wenn Sie über Root-Zugriffsberechtigung verfügen und das benutzerdefinierte S3-API-Zertifikat für Load-Balancer-Endpunktverbindungen verwendet wurde, wird eine Liste der Load-Balancer-Endpunkte angezeigt, die mit dem Standard-S3-API-Zertifikat nicht mehr zugänglich sind. Zur Bearbeitung oder Entfernung der betroffenen Endpunkte zu "Load Balancer-Endpunkte konfigurieren" wechseln.

5. ${post_edited_translations.segment}

Das S3 API-Zertifikat herunterladen oder kopieren

Sie können den Inhalt des S3 API-Zertifikats speichern oder kopieren, um ihn an anderer Stelle zu verwenden.

Schritte

1. **Konfiguration** > **Sicherheit** > **Zertifikate** auswählen.
2. Auf der Registerkarte **Global** die Option **S3 API certificate** auswählen.
3. ${post_edited_translations.segment}

${post_edited_translations.segment}

Die Zertifikats- oder CA-Bundle-Datei `.pem` herunterladen. Bei Verwendung eines optionalen CA-Bundles wird jedes Zertifikat im Bundle auf einer eigenen Unterregisterkarte angezeigt.

a. **Zertifikat herunterladen** oder **CA-Bundle herunterladen** auswählen.

   ${post_edited_translations.segment}

b. Geben Sie den Namen der Zertifikatsdatei und den Speicherort für den Download an. Die Datei wird mit der Erweiterung `.pem` gespeichert.

   Zum Beispiel: `storagegrid_certificate.pem`

${post_edited_translations.segment}

Kopieren Sie den Zertifikatstext, um ihn an anderer Stelle einzufügen. Wenn ein optionales CA-Bundle verwendet wird, wird jedes Zertifikat im Bundle auf einem eigenen Unterreiter angezeigt.

a. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

b. Das kopierte Zertifikat in einen Texteditor einfügen.

c. Die Textdatei mit der Erweiterung `.pem` speichern.

   Zum Beispiel: `storagegrid_certificate.pem`

Verwandte Informationen

- "S3 REST-API verwenden"
- "S3-Endpunkt-Domänennamen konfigurieren"

Kopieren Sie das StorageGRID Grid CA-Zertifikat

StorageGRID verwendet eine interne Zertifizierungsstelle (CA), um den internen Datenverkehr zu sichern. Dieses Zertifikat ändert sich nicht, wenn Sie eigene Zertifikate hochladen.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Du hast "spezifische Zugriffsberechtigungen".

Über diese Aufgabe

Wenn ein benutzerdefiniertes Serverzertifikat konfiguriert wurde, sollten Clientanwendungen den Server mithilfe des benutzerdefinierten Serverzertifikats verifizieren. Sie sollten das CA-Zertifikat nicht vom StorageGRID System kopieren.

Schritte

1. ${post_edited_translations.segment}

2. Im Abschnitt **Certificate PEM** das Zertifikat herunterladen oder kopieren.

Zertifikatsdatei herunterladen

Laden Sie die Zertifikatsdatei `.pem` herunter.

a. **Zertifikat herunterladen** auswählen.

b. Geben Sie den Namen der Zertifikatsdatei und den Speicherort für den Download an. Die Datei wird mit der Erweiterung `.pem` gespeichert.

   Zum Beispiel: `storagegrid_certificate.pem`

Zertifikat-PEM kopieren

Den Zertifikatstext kopieren, um ihn an anderer Stelle einzufügen.

a. **Zertifikat PEM kopieren** auswählen.

b. Das kopierte Zertifikat in einen Texteditor einfügen.

c. Die Textdatei mit der Erweiterung `.pem` speichern.

   Zum Beispiel: `storagegrid_certificate.pem`

StorageGRID Zertifikate für FabricPool konfigurieren

Für S3-Clients, die eine strikte Hostnamenvalidierung durchführen und die Deaktivierung der strikten Hostnamenvalidierung nicht unterstützen, wie ONTAP-Clients mit FabricPool, besteht die Möglichkeit, beim Konfigurieren des Load Balancer-Endpunkts ein Serverzertifikat zu generieren oder hochzuladen.

Bevor Sie beginnen

- Du hast "spezifische Zugriffsberechtigungen".
- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.

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 (CA) signiert ist. In Produktionsumgebungen sollten Sie ein Zertifikat verwenden, das von einer bekannten CA signiert ist. Von einer CA signierte Zertifikate lassen sich unterbrechungsfrei austauschen. Sie sind außerdem sicherer, da sie einen besseren Schutz vor Man-in-the-Middle-Angriffen bieten.

Die folgenden Schritte bieten allgemeine Richtlinien für S3-Clients, die FabricPool verwenden. Ausführlichere Informationen und Verfahren finden sich unter "StorageGRID für FabricPool konfigurieren".

Schritte

1. Optional kann eine Hochverfügbarkeitsgruppe (HA-Gruppe) für FabricPool konfiguriert werden.
2. Ein S3 Load Balancer-Endpunkt für die Verwendung mit FabricPool wird erstellt.

   Beim Erstellen eines HTTPS Load-Balancer-Endpunkts werden Sie aufgefordert, Ihr Serverzertifikat, den privaten Zertifikatsschlüssel und optional das CA-Bundle hochzuladen.

3. StorageGRID als Cloud-Tier in ONTAP anbinden.

   Geben Sie den Port des Load-Balancer-Endpunkts und die vollqualifizierte Domain an, die im hochgeladenen CA-Zertifikat verwendet wird. Anschließend ist das CA-Zertifikat bereitzustellen.

> Wenn das StorageGRID-Zertifikat von einer Zwischenzertifizierungsstelle ausgestellt wurde, muss das Zertifikat dieser Zwischenzertifizierungsstelle bereitgestellt werden. Wenn das StorageGRID-Zertifikat direkt von der Stammzertifizierungsstelle ausgestellt wurde, muss das Stammzertifizierungsstellenzertifikat bereitgestellt werden.

Clientzertifikate in StorageGRID konfigurieren

Clientzertifikate ermöglichen autorisierten externen Clients den Zugriff auf die StorageGRID Prometheus Datenbank und bieten eine sichere Möglichkeit für externe Tools, StorageGRID zu überwachen.

Wenn Sie mit einem externen Überwachungstool auf StorageGRID zugreifen müssen, ist es erforderlich, ein Clientzertifikat mit dem Grid Manager hochzuladen oder zu generieren und die Zertifikatsinformationen in das externe Tool zu kopieren.

Siehe "Sicherheitszertifikate verwalten" und "Benutzerdefinierte Serverzertifikate konfigurieren".

> Um sicherzustellen, dass der Betrieb nicht durch ein fehlerhaftes Serverzertifikat unterbrochen wird, wird der Alarm **Ablauf von auf der Seite „Zertifikate“ konfigurierten Client-Zertifikaten** ausgelöst, wenn dieses Serverzertifikat bald abläuft. Bei Bedarf können Sie einsehen, wann das aktuelle Zertifikat abläuft, indem Sie **Konfiguration** > **Sicherheit** > **Zertifikate** auswählen und das Ablaufdatum für das Client-Zertifikat auf der Registerkarte „Client“ prüfen.

> Wenn ein Key Management Server (KMS) zum Schutz der Daten auf speziell konfigurierten Appliance-Knoten verwendet wird, finden sich spezifische Informationen zu "Hochladen eines KMS Clientzertifikats".

Bevor Sie beginnen

- Sie verfügen über Root-Zugriffsberechtigung.
- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Zum Konfigurieren eines Clientzertifikats:
  - Sie haben die IP-Adresse oder den Domainnamen des Admin-Knotens.
  - Wenn das StorageGRID Managementoberflächenzertifikat konfiguriert wurde, stehen die Zertifizierungsstelle, das Clientzertifikat und der private Schlüssel zur Verfügung, die für die Konfiguration des Managementoberflächenzertifikats verwendet wurden.
  - Um Ihr eigenes Zertifikat hochzuladen, ist der private Schlüssel für das Zertifikat auf Ihrem lokalen Computer verfügbar.
  - Der private Schlüssel muss bei seiner Erstellung gespeichert oder aufgezeichnet worden sein. Wenn der ursprüngliche private Schlüssel nicht vorhanden ist, muss ein neuer erstellt werden.
- Ein Clientzertifikat kann wie folgt bearbeitet werden:
  - Sie haben die IP-Adresse oder den Domainnamen des Admin-Knotens.
  - Zum Hochladen Ihres eigenen Zertifikats oder eines neuen Zertifikats sind der private Schlüssel, das

Clientzertifikat und die CA (falls verwendet) auf Ihrem lokalen Computer verfügbar.

Clientzertifikate hinzufügen

Um das Clientzertifikat hinzuzufügen, kann eines der folgenden Verfahren verwendet werden:

- Zertifikat für die Managementoberfläche bereits konfiguriert
- Vom CA ausgestelltes Client-Zertifikat
- Vom Grid Manager generiertes Zertifikat

Zertifikat für die Managementoberfläche bereits konfiguriert

Dieses Verfahren dient dazu, ein Clientzertifikat hinzuzufügen, wenn für die Managementoberfläche bereits ein Zertifikat der Managementoberfläche mit einer vom Kunden bereitgestellten Zertifizierungsstelle, einem Clientzertifikat und einem privaten Schlüssel konfiguriert ist.

Schritte

1. Im Grid Manager **Konfiguration** > **Sicherheit** > **Zertifikate** auswählen und dann die Registerkarte **Client** wählen.
2. Wählen Sie **Add**.
3. Geben Sie einen Zertifikatsnamen ein.
4. Um mit Ihrem externen Überwachungstool auf Prometheus-Metriken zuzugreifen, **Prometheus zulassen** auswählen.
5. Wählen Sie **Weiter**.
6. Für den Schritt **Zertifikate anhängen** ist das Zertifikat der Managementoberfläche hochzuladen.
   a. **Zertifikat hochladen** auswählen.
   b. **Durchsuchen** auswählen und die Zertifikatsdatei der Managementoberfläche auswählen (`.pem`).
      - **Client certificate details** auswählen, um die Zertifikat-Metadaten und das Zertifikat-PEM anzuzeigen.
      - **Zertifikat PEM kopieren** auswählen, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.
   c. **Erstellen** auswählen, um das Zertifikat im Grid Manager zu speichern.

   ${post_edited_translations.segment}
7. Ein externes Überwachungstool konfigurieren, wie beispielsweise Grafana.

Vom CA ausgestelltes Client-Zertifikat

Dieses Verfahren dient dazu, ein Administrator-Clientzertifikat hinzuzufügen, wenn kein Managementoberfläche-Zertifikat konfiguriert wurde und geplant ist, ein Clientzertifikat für Prometheus hinzuzufügen, das ein von einer Zertifizierungsstelle ausgestelltes Clientzertifikat und einen privaten Schlüssel verwendet.

Schritte

1. Führen Sie die Schritte aus, um "ein Managementoberfläche-Zertifikat konfigurieren".
2. Im Grid Manager **Konfiguration** > **Sicherheit** > **Zertifikate** auswählen und dann die Registerkarte **Client** wählen.

3. Wählen Sie **Add**.
4. Geben Sie einen Zertifikatsnamen ein.
5. Um mit Ihrem externen Überwachungstool auf Prometheus-Metriken zuzugreifen, **Prometheus zulassen** auswählen.
6. Wählen Sie **Weiter**.
7. Für den Schritt **Zertifikate anhängen** die Dateien für das Clientzertifikat, den privaten Schlüssel und das CA-Bundle hochladen:
   a. **Zertifikat hochladen** auswählen.
   b. **Durchsuchen** auswählen und die Clientzertifikat-, Privatschlüssel- und CA-Bundle-Dateien (`.pem` auswählen.
      - **Client certificate details** auswählen, um die Zertifikat-Metadaten und das Zertifikat-PEM anzuzeigen.
      - **Zertifikat PEM kopieren** auswählen, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.
   c. **Erstellen** auswählen, um das Zertifikat im Grid Manager zu speichern.

      Die neuen Zertifikate erscheinen auf der Registerkarte „Client“.
8. Ein externes Überwachungstool konfigurieren, wie beispielsweise Grafana.

Vom Grid Manager generiertes Zertifikat

${post_edited_translations.segment}

Schritte

1. Im Grid Manager **Konfiguration** > **Sicherheit** > **Zertifikate** auswählen und dann die Registerkarte **Client** wählen.
2. Wählen Sie **Add**.
3. Geben Sie einen Zertifikatsnamen ein.
4. Um mit Ihrem externen Überwachungstool auf Prometheus-Metriken zuzugreifen, **Prometheus zulassen** auswählen.
5. Wählen Sie **Weiter**.
6. Für den Schritt **Zertifikate anhängen** wird **Zertifikat generieren** ausgewählt.
7. ${post_edited_translations.segment}
   - **Subjekt** (optional): X.509-Subjekt oder individueller Name (DN) des Zertifikatsinhabers.
   - **Gültigkeitstage**: Die Anzahl der Tage, für die das generierte Zertifikat gültig ist, beginnend ab dem Zeitpunkt seiner Generierung.
   - **Schlüsselverwendungserweiterungen hinzufügen**: Wenn diese Option ausgewählt ist (Standard und empfohlen), werden Schlüsselverwendungs- und erweiterte Schlüsselverwendungserweiterungen zum generierten Zertifikat hinzugefügt.

     Diese Erweiterungen definieren den Zweck des im Zertifikat enthaltenen Schlüssels.

     Dieses Kontrollkästchen sollte aktiviert bleiben, es sei denn, bei älteren Clients treten Verbindungsprobleme auf, wenn die Zertifikate diese Erweiterungen enthalten.

8. Wählen Sie **Generieren**.
9. **Client certificate details** auswählen, um die Zertifikat-Metadaten und die Zertifikat-PEM anzuzeigen.

   Nach dem Schließen des Dialogfelds kann der private Schlüssel des Zertifikats nicht mehr eingesehen werden. Der Schlüssel sollte an einem sicheren Ort gespeichert oder heruntergeladen werden.

   - **Zertifikat PEM kopieren** auswählen, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.
   - **Zertifikat herunterladen** auswählen, um die Zertifikatsdatei zu speichern.

     Geben Sie den Namen der Zertifikatsdatei und den Speicherort für den Download an. Die Datei wird mit der Erweiterung `.pem` gespeichert.

     Zum Beispiel: `storagegrid_certificate.pem`

   - **Privaten Schlüssel kopieren** auswählen, um den privaten Schlüssel des Zertifikats zum Einfügen an anderer Stelle zu kopieren.
   - **Privaten Schlüssel herunterladen** auswählen, um den privaten Schlüssel als Datei zu speichern.

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

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

    ${post_edited_translations.segment}

11. Im Grid Manager **Konfiguration** > **Sicherheit** > **Zertifikate** auswählen und dann die Registerkarte **Global** wählen.
12. **Management Interface certificate** auswählen.
13. **Benutzerdefiniertes Zertifikat verwenden** auswählen.
14. Laden Sie die Dateien certificate.pem und private_key.pem aus dem Details zum Client-Zertifikat Schritt hoch. Das CA-Bundle muss nicht hochgeladen werden.
    a. Wählen Sie **Zertifikat hochladen** und dann **Weiter**.
    b. Jede Zertifikatsdatei (`.pem` hochladen.
    c. **Speichern** auswählen, um das Zertifikat im Grid Manager zu speichern.

       Das neue Zertifikat erscheint auf der Zertifikatsseite der Managementoberfläche.

15. Ein externes Überwachungstool konfigurieren, wie beispielsweise Grafana.

Ein externes Überwachungstool konfigurieren

Schritte

1. Die folgenden Einstellungen werden im externen Überwachungstool, wie zum Beispiel Grafana, konfiguriert.
   a. **Name**: Geben Sie einen Namen für die Verbindung ein.

      StorageGRID benötigt diese Informationen nicht, aber ein Name ist erforderlich, um die Verbindung zu testen.

b. **URL**: Geben Sie den Domänennamen oder die IP-Adresse für den Admin Node ein. HTTPS und Port 9091 sind anzugeben.

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

c. **TLS Client Auth** und **With CA Cert** aktivieren.

d. Unter „TLS/SSL Auth Details“ kopieren und einfügen:
   - Das Managementoberfläche-CA-Zertifikat zu **CA Cert**
   - Das Client-Zertifikat auf **Client Cert**
   - Der private Schlüssel zu **Client Key**

e. **ServerName**: Der Domänenname des Admin-Knotens ist einzugeben.

   ServerName muss mit dem Domänennamen übereinstimmen, wie er im Zertifikat der Managementoberfläche erscheint.

2. Das Zertifikat und den privaten Schlüssel, die aus StorageGRID oder einer lokalen Datei kopiert wurden, speichern und testen.

   Sie können nun mit Ihrem externen Überwachungstool auf die Prometheus-Metriken von StorageGRID zugreifen.

   Informationen zu den Kennzahlen finden sich unter "Anleitung zur Überwachung von StorageGRID".

Clientzertifikate bearbeiten

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

Schritte

1. **Konfiguration** > **Sicherheit** > **Zertifikate** auswählen und dann die Registerkarte **Client** wählen.

   Die Tabelle listet die Ablaufdaten der Zertifikate und die Prometheus-Zugriffsberechtigungen auf. Wenn ein Zertifikat demnächst abläuft oder bereits abgelaufen ist, erscheint eine Meldung in der Tabelle und eine Warnung wird ausgelöst.

2. Wählen Sie das Zertifikat aus, das Sie bearbeiten möchten.
3. **Bearbeiten** auswählen und dann **Name und Berechtigungen bearbeiten** auswählen
4. Geben Sie einen Zertifikatsnamen ein.
5. Um mit Ihrem externen Überwachungstool auf Prometheus-Metriken zuzugreifen, **Prometheus zulassen** auswählen.
6. **Weiter** auswählen, um das Zertifikat im Grid Manager zu speichern.

   Das aktualisierte Zertifikat wird auf der Registerkarte „Client“ angezeigt.

Neues Client-Zertifikat anhängen

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

Schritte

1. **Konfiguration** > **Sicherheit** > **Zertifikate** auswählen und dann die Registerkarte **Client** wählen.

   Die Tabelle listet die Ablaufdaten der Zertifikate und die Prometheus-Zugriffsberechtigungen auf. Wenn ein Zertifikat demnächst abläuft oder bereits abgelaufen ist, erscheint eine Meldung in der Tabelle und eine Warnung wird ausgelöst.

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

Zertifikat hochladen

Den Zertifikatstext kopieren, um ihn an anderer Stelle einzufügen.

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

b. Den Namen des Clientzertifikats hochladen (`.pem`).

   Client certificate details auswählen, um die Zertifikat-Metadaten und das Zertifikat-PEM anzuzeigen.

   - **Zertifikat herunterladen** auswählen, um die Zertifikatsdatei zu speichern.

     Geben Sie den Namen der Zertifikatsdatei und den Speicherort für den Download an. Die Datei wird mit der Erweiterung `.pem` gespeichert.

   Zum Beispiel: `storagegrid_certificate.pem`

   - **Zertifikat PEM kopieren** auswählen, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.

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

   Das aktualisierte Zertifikat wird auf der Registerkarte „Client“ angezeigt.

Zertifikat generieren

Den Zertifikatstext zum Einfügen an anderer Stelle generieren.

a. **Zertifikat generieren** auswählen.

b. ${post_edited_translations.segment}

   - **Subjekt** (optional): X.509-Subjekt oder individueller Name (DN) des Zertifikatsinhabers.
   - **Gültigkeitstage**: Die Anzahl der Tage, für die das generierte Zertifikat gültig ist, beginnend ab dem Zeitpunkt seiner Generierung.
   - **Schlüsselverwendungserweiterungen hinzufügen**: Wenn diese Option ausgewählt ist (Standard und empfohlen), werden Schlüsselverwendungs- und erweiterte Schlüsselverwendungserweiterungen zum generierten Zertifikat hinzugefügt.

     Diese Erweiterungen definieren den Zweck des im Zertifikat enthaltenen Schlüssels.

     Dieses Kontrollkästchen sollte aktiviert bleiben, es sei denn, bei älteren Clients treten Verbindungsprobleme auf, wenn die Zertifikate diese Erweiterungen enthalten.

c. Wählen Sie **Generieren**.

d. **Client certificate details** auswählen, um die Zertifikat-Metadaten und das Zertifikat-PEM anzuzeigen.

   Nach dem Schließen des Dialogfelds kann der private Schlüssel des Zertifikats nicht mehr eingesehen werden. Der Schlüssel sollte an einem sicheren Ort gespeichert oder heruntergeladen werden.

- **Zertifikat PEM kopieren** auswählen, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.
- **Zertifikat herunterladen** auswählen, um die Zertifikatsdatei zu speichern.

  Geben Sie den Namen der Zertifikatsdatei und den Speicherort für den Download an. Die Datei wird mit der Erweiterung `.pem` gespeichert.

  Zum Beispiel: `storagegrid_certificate.pem`

- **Privaten Schlüssel kopieren** auswählen, um den privaten Schlüssel des Zertifikats zum Einfügen an anderer Stelle zu kopieren.
- **Privaten Schlüssel herunterladen** auswählen, um den privaten Schlüssel als Datei zu speichern.

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

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

${post_edited_translations.segment}

Clientzertifikate herunterladen oder kopieren

Sie können ein Clientzertifikat herunterladen oder kopieren, um es anderweitig zu verwenden.

Schritte

1. **Konfiguration** > **Sicherheit** > **Zertifikate** auswählen und dann die Registerkarte **Client** wählen.
2. Wählen Sie das Zertifikat aus, das Sie kopieren oder herunterladen möchten.
3. Zertifikat herunterladen oder kopieren.

Zertifikatsdatei herunterladen

Laden Sie die Zertifikatsdatei `.pem` herunter.

a. **Zertifikat herunterladen** auswählen.

b. Geben Sie den Namen der Zertifikatsdatei und den Speicherort für den Download an. Die Datei wird mit der Erweiterung `.pem` gespeichert.

   Zum Beispiel: `storagegrid_certificate.pem`

Zertifikat kopieren

Den Zertifikatstext kopieren, um ihn an anderer Stelle einzufügen.

a. **Zertifikat PEM kopieren** auswählen.

b. Das kopierte Zertifikat in einen Texteditor einfügen.

c. Die Textdatei mit der Erweiterung `.pem` speichern.

   Zum Beispiel: `storagegrid_certificate.pem`

Clientzertifikate entfernen

Wenn ein Administrator-Clientzertifikat nicht mehr benötigt wird, kann es entfernt werden.

Schritte

1. **Konfiguration** > **Sicherheit** > **Zertifikate** auswählen und dann die Registerkarte **Client** wählen.
2. Wählen Sie das Zertifikat aus, das Sie entfernen möchten.
3. **Löschen** auswählen und anschließend bestätigen.

> Um bis zu 10 Zertifikate zu entfernen, jedes zu entfernende Zertifikat auf der Registerkarte „Client“ auswählen und anschließend **Aktionen** > **Löschen** wählen.

Nach der Entfernung eines Zertifikats müssen Clients, die dieses Zertifikat verwendet haben, ein neues Clientzertifikat angeben, um auf die StorageGRID Prometheus Datenbank zuzugreifen.

Sicherheitseinstellungen konfigurieren

Verwalten Sie die TLS- und SSH-Richtlinie in StorageGRID

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

Die Sicherheitsrichtlinie steuert, wie TLS und SSH Daten während der Übertragung verschlüsseln. Im Allgemeinen empfiehlt sich die Verwendung der Kompatibilitätsrichtlinie „Modern“ (Standard), es sei denn, das System muss Common Criteria-konform sein oder es werden andere Verschlüsselungsverfahren benötigt.

Einige StorageGRID Dienste wurden noch nicht aktualisiert, um die in diesen Richtlinien enthaltenen Verschlüsselungsverfahren zu verwenden.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Root-Zugriffsberechtigung".

Eine Sicherheitsrichtlinie auswählen

Schritte

1. **Konfiguration** > **Sicherheit** > **Sicherheitseinstellungen** auswählen.

   Die Registerkarte **TLS und SSH Richtlinien** zeigt die verfügbaren Richtlinien an. Die aktuell aktive Richtlinie ist durch ein grünes Häkchen auf der Richtlinienkachel gekennzeichnet.

2. In den Registerkarten finden sich Informationen zu den verfügbaren Richtlinien.

Moderne Kompatibilität (Standard)

Die Standardrichtlinie eignet sich, wenn eine starke Verschlüsselung erforderlich ist und keine besonderen Anforderungen bestehen. Diese Richtlinie ist mit den meisten TLS- und SSH-Clients kompatibel.

Kompatibilität mit älteren Systemen

Die Legacy-Kompatibilitätsrichtlinie bietet zusätzliche Kompatibilitätsoptionen für ältere Clients. Die zusätzlichen Optionen in dieser Richtlinie können sie weniger sicher machen als die Modern-Kompatibilitätsrichtlinie.

Gemeinsame Kriterien

Die Common Criteria-Richtlinie ist zu verwenden, wenn eine Common Criteria Zertifizierung erforderlich ist.

FIPS strict

Die FIPS-Richtlinie „Streng“ ist zu verwenden, wenn eine Common Criteria Zertifizierung erforderlich ist 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 benötigt wird. Die Verwendung dieser Richtlinie kann die Leistung verringern.

Das NCSM 3.0.8 und das NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 Modul werden in den folgenden Operationen 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 Service (Load-Balancer-Endpunkte)
  - TLS-Verbindungen zwischen Clients und dem LDR-Service
  - Objektinhaltsverschlüsselung für SSE-S3, SSE-C und die Einstellung für die Verschlüsselung gespeicherter Objekte
  - SSH-Verbindungen

  Weitere Informationen bietet das 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.

  - Entropiesammlung
  - Knotenverschlüsselung

  Weitere Informationen bietet das NIST Cryptographic Algorithm Validation Program "Zertifikate Nr. A6242 bis Nr. A6257" und "Entropiezertifikat Nr. E223".

Hinweis: Nachdem Sie diese Richtlinie ausgewählt haben, "Einen rollierenden Neustart durchführen" für alle Knoten, um den NCSM zu aktivieren. **Wartung** > **Rollierender Neustart** dient zum Initiieren und Überwachen von Neustarts.

Benutzerdefiniert

Eine benutzerdefinierte Richtlinie ist erforderlich, wenn eigene Verschlüsselungsverfahren angewendet werden sollen.

Optional, falls Ihr StorageGRID FIPS 140-Kryptografieanforderungen hat, kann die FIPS-Modus-Funktion aktiviert werden, um das NCSM 3.0.8 und das NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 Modul zu verwenden:

a. Den `fipsMode`Parameter auf `true` festlegen.
b. Wenn Sie dazu aufgefordert werden, "Einen rollierenden Neustart durchführen" für alle Nodes die Kryptografie-Module aktivieren. **Wartung** > **Rollierender Neustart** dient zum Initiieren und Überwachen der Neustarts.
c. **Support** > **Diagnostik** auswählen, um die aktiven FIPS-Modulversionen anzuzeigen.

3. Einzelheiten zu den Verschlüsselungsverfahren, Protokollen und Algorithmen der einzelnen Richtlinien sind unter **Details anzeigen** zu finden.
4. ${post_edited_translations.segment}

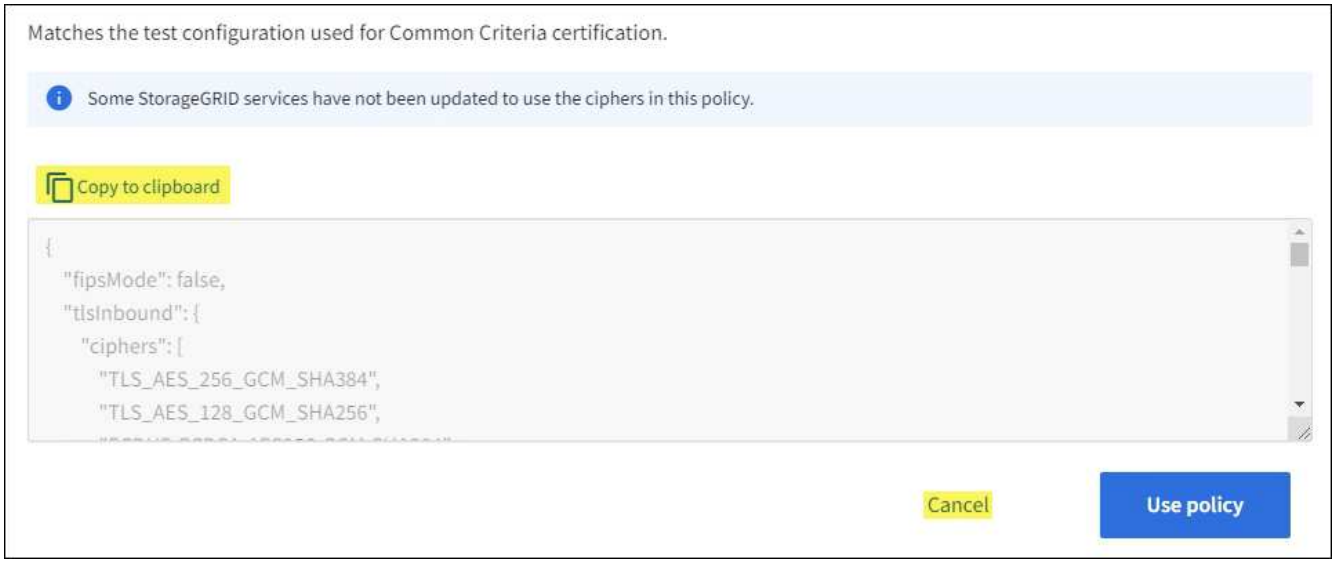
   Neben **Aktuelle Richtlinie** auf der Richtlinienkachel erscheint ein grünes Häkchen.

${post_edited_translations.segment}

Sie können eine benutzerdefinierte Richtlinie erstellen, wenn Sie eigene Verschlüsselungsverfahren anwenden müssen.

Schritte

1. Wählen Sie in der Kachel der Richtlinie, die der von Ihnen zu erstellenden benutzerdefinierten Richtlinie am ähnlichsten ist, **Details anzeigen** aus.
2. ${post_edited_translations.segment}



3. Im Feld **Benutzerdefinierte Richtlinie** die Option **Konfigurieren und verwenden** auswählen.
4. ${post_edited_translations.segment}

5. **Nutzungsrichtlinie** auswählen.

   ${post_edited_translations.segment}

6. ${post_edited_translations.segment}

Vorübergehend zur Standard-Sicherheitsrichtlinie zurückkehren

Wenn Sie eine benutzerdefinierte Sicherheitsrichtlinie konfiguriert haben, können Sie sich möglicherweise nicht beim Grid Manager anmelden, wenn die konfigurierte TLS-Richtlinie nicht mit dem "${post_edited_translations.segment}" kompatibel ist.

Sie können vorübergehend zur Standard-Sicherheitsrichtlinie zurückkehren.

Schritte

1. ${post_edited_translations.segment}
   a. Geben Sie den folgenden Befehl ein: `ssh admin@Admin_Node_IP`
   b. Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.
   c. Geben Sie den folgenden Befehl ein, um zu root zu wechseln: `su -`
   d. Geben Sie das in der `Passwords.txt` Datei aufgeführte Passwort ein.

      Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` zu `#`.

2. Führen Sie den folgenden Befehl aus:

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

3. ${post_edited_translations.segment}
4. Führen Sie die Schritte in Eine Sicherheitsrichtlinie auswählen aus, um die Richtlinie erneut zu konfigurieren.

Konfigurieren Sie die StorageGRID Netzwerk- und Objektsicherheit

Es besteht die Möglichkeit, die Netzwerk- und Objektsicherheit so zu konfigurieren, dass gespeicherte Objekte verschlüsselt werden, bestimmte S3-Anfragen verhindert werden oder Clientverbindungen zu Storage Nodes HTTP anstelle von HTTPS verwenden.

Verschlüsselung gespeicherter Objekte

Die Verschlüsselung gespeicherter Objekte ermöglicht die Verschlüsselung aller Objektdaten beim Import über S3. Standardmäßig werden gespeicherte Objekte nicht verschlüsselt, es besteht jedoch die Möglichkeit, Objekte mit dem AES-128- oder AES-256-Algorithmus zu verschlüsseln. Bei aktivierter Einstellung werden alle neu importierten Objekte verschlüsselt, während bereits gespeicherte Objekte unverändert bleiben. Bei deaktivierter Verschlüsselung bleiben aktuell verschlüsselte Objekte verschlüsselt, neu importierte Objekte jedoch unverschlüsselt.

Die Einstellung „Gespeicherte Objektverschlüsselung“ gilt nur für S3-Objekte, die nicht durch Verschlüsselung auf Bucket-Ebene oder Objekt-Ebene verschlüsselt wurden.

Weitere Details zu StorageGRID Verschlüsselungsmethoden sind unter "Überblick über StorageGRID Verschlüsselungsmethoden" zu finden.

Verhindern der Client-Änderung

Die Einstellung „Clientänderungen verhindern“ ist systemweit. Wenn die Option „Clientänderungen verhindern“ ausgewählt ist, werden die folgenden Anfragen abgelehnt.

S3 REST API

- DeleteBucket-Anfragen
- Anfragen zur Änderung der Daten eines bestehenden Objekts, der benutzerdefinierten Metadaten oder der S3-Objektkennzeichnung

HTTP für Storage Node-Verbindungen aktivieren

Standardmäßig verwenden Clientanwendungen das HTTPS Netzwerkprotokoll für alle direkten Verbindungen zu Storage Nodes. Optional kann HTTP für diese Verbindungen aktiviert werden, beispielsweise beim Testen eines nicht produktiven Grids.

HTTP sollte für Speicherknotenverbindungen nur verwendet werden, wenn S3-Clients direkte HTTP-Verbindungen zu Speicherknoten herstellen müssen. Für Clients, die ausschließlich HTTPS-Verbindungen nutzen oder sich mit dem Load Balancer Service verbinden, ist diese Option nicht erforderlich (da "Jeden Load Balancer-Endpunkt konfigurieren" entweder HTTP oder HTTPS verwendet werden kann).

Siehe "Zusammenfassung: IP-Adressen und Ports für Clientverbindungen", um zu erfahren, welche Ports S3-Clients verwenden, wenn sie über HTTP oder HTTPS eine Verbindung zu Storage Nodes herstellen.

Optionen auswählen

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie verfügen über Root-Zugriffsberechtigung.

Schritte

1. **Konfiguration** > **Sicherheit** > **Sicherheitseinstellungen** auswählen.
2. Die Registerkarte **Netzwerk und Objekte** auswählen.
3. Für die Verschlüsselung gespeicherter Objekte die Einstellung **Keine** (Standard) verwenden, wenn gespeicherte Objekte nicht verschlüsselt werden sollen, oder **AES-128** bzw. **AES-256** auswählen, um gespeicherte Objekte zu verschlüsseln.
4. Optional **Clientänderungen verhindern** auswählen, um zu verhindern, dass S3-Clients bestimmte Anfragen stellen.

   Wenn diese Einstellung geändert wird, dauert es etwa eine Minute, bis die neue Einstellung wirksam wird. Der konfigurierte Wert wird aus Performance- und Skalierungsgründen zwischengespeichert.

5. Optional kann **HTTP für Storage Node-Verbindungen aktivieren** ausgewählt werden, wenn Clients sich direkt mit Storage Nodes verbinden und HTTP-Verbindungen verwendet werden sollen.

   Vorsicht ist geboten bei der Aktivierung von HTTP für ein Produktions-Grid, da Anfragen unverschlüsselt übertragen werden.

6. **Speichern** auswählen.

Ändern Sie die Sicherheitseinstellungen der StorageGRID-Schnittstelle

Über die Sicherheitseinstellungen der Schnittstelle lässt sich steuern, ob Benutzer abgemeldet werden, wenn sie länger als die angegebene Zeit inaktiv sind, und ob ein Stacktrace in API-Fehlerantworten enthalten ist.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Du hast "Root-Zugriffsberechtigung".

Über diese Aufgabe

Die Seite **Sicherheitseinstellungen** enthält die Einstellungen **Browser-Inaktivitäts-Zeitüberschreitung** und **Management-API-Stacktrace**.

Browser-Inaktivitätszeitüberschreitung

Gibt an, wie lange der Browser eines Benutzers inaktiv sein kann, bevor der Benutzer abgemeldet wird. Der Standardwert beträgt 15 Minuten.

Die Zeitüberschreitung bei Browser-Inaktivität wird außerdem durch Folgendes gesteuert:

- Ein separater, nicht konfigurierbarer StorageGRID Timer, der der Systemsicherheit dient. Das Authentifizierungs-Token jedes Benutzers läuft 16 Stunden nach der Anmeldung ab. Wenn die Authentifizierung eines Benutzers abläuft, wird dieser Benutzer automatisch abgemeldet, selbst wenn die Zeitüberschreitung für die Browser-Inaktivität deaktiviert ist oder der Wert für die Browser-Zeitüberschreitung noch nicht erreicht wurde. Um das Token zu erneuern, muss sich der Benutzer erneut anmelden.
- Timeout-Einstellungen für den Identitätsanbieter, vorausgesetzt, Single Sign-On (SSO) ist für StorageGRID aktiviert.

  Wenn SSO aktiviert ist und der Browser eines Benutzers eine Zeitüberschreitung aufweist, müssen die SSO-Anmeldeinformationen erneut eingegeben werden, um wieder auf StorageGRID zugreifen zu können. Siehe "Funktionsweise von SSO".

Stacktrace der Management API

Steuert, ob in den Fehlerantworten der Grid Manager und Tenant Manager API ein Stacktrace zurückgegeben wird.

Diese Option ist standardmäßig deaktiviert, aber es kann sinnvoll sein, diese Funktionalität für eine Testumgebung zu aktivieren. In der Regel sollte die Stack-Trace-Funktion in Produktionsumgebungen deaktiviert bleiben, um bei API-Fehlern keine internen Softwaredetails preiszugeben.

Schritte

1. **Konfiguration** > **Sicherheit** > **Sicherheitseinstellungen** auswählen.
2. Die Registerkarte **Interface** auswählen.
3. Die Einstellung für die Zeitüberschreitung bei Browser-Inaktivität kann wie folgt geändert werden:
   a. Das Akkordeon aufklappen.
   b. Um den Zeitraum für die Zeitüberschreitung zu ändern, ist ein Wert zwischen 60 Sekunden und 7 Tagen anzugeben. Die Standard-Zeitüberschreitung beträgt 15 Minuten.
   c. Zum Deaktivieren dieser Funktion das Häkchen aus der Checkbox entfernen.

d. **Speichern** auswählen.

   Die neue Einstellung betrifft keine Benutzer, die aktuell angemeldet sind. Benutzer müssen sich erneut anmelden oder ihren Browser aktualisieren, damit die neue Zeitüberschreitungseinstellung wirksam wird.

4. Die Einstellung für den Management API Stacktrace kann wie folgt geändert werden:
   a. Das Akkordeon aufklappen.
   b. Das Kontrollkästchen ermöglicht die Rückgabe eines Stacktraces in den API-Fehlerantworten von Grid Manager und Tenant Manager.

      ${post_edited_translations.segment}

   c. **Speichern** auswählen.

Externen SSH-Zugriff in StorageGRID verwalten

Der SSH-Zugriff für eingehenden Datenverkehr in das Grid kann durch Blockieren oder Zulassen des externen Zugriffs verwaltet werden. Die Verwaltung des externen SSH-Zugriffs hat keine Auswirkungen auf den Datenverkehr zwischen den Knoten im Grid.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Du hast "Root-Zugriffsberechtigung".

Über diese Aufgabe

Zur Erhöhung der Systemsicherheit ist der externe SSH-Zugriff standardmäßig blockiert. Wenn Aufgaben ausgeführt werden müssen, die einen eingehenden SSH-Zugriff erfordern, wie etwa zur Fehlerbehebung, sollte der externe Zugriff vorübergehend erlaubt werden. Nach Abschluss der Aufgabe ist der externe Zugriff wieder zu blockieren.

Schritte

1. **Konfiguration** > **Sicherheit** > **Sicherheitseinstellungen** auswählen.
2. Die Registerkarte **SSH blockieren** auswählen.
3. Die Option **Eingehenden SSH-Zugriff blockieren** dient zur Verwaltung des externen SSH-Zugriffs:
   a. Das Kontrollkästchen zum Blockieren des Zugriffs (Standardeinstellung) auswählen.
   b. Deaktivieren Sie das Kontrollkästchen, um den Zugriff zu erlauben.

      Erfordert Zugriff auf Port 22 zwischen dem Service-Laptop und allen anderen Grid-Knoten. Der Zugriff auf Port 22 sollte nach Abschluss der Wartungsaufgabe entfernt werden.

4. **Speichern** auswählen.

Schlüsselverwaltungsserver konfigurieren

Erfahren Sie mehr über Schlüsselverwaltungsserver in StorageGRID

Ein Key Management Server (KMS) ist ein externes System eines Drittanbieters, das Verschlüsselungsschlüssel für StorageGRID Appliance-Knoten am zugehörigen StorageGRID Standort mithilfe des Key Management Interoperability Protocol (KMIP) bereitstellt.

StorageGRID unterstützt nur bestimmte Schlüsselverwaltungsserver. Eine Liste der unterstützten Produkte und Versionen ist über das "NetApp Interoperabilitätsmatrix Tool (IMT)" verfügbar.

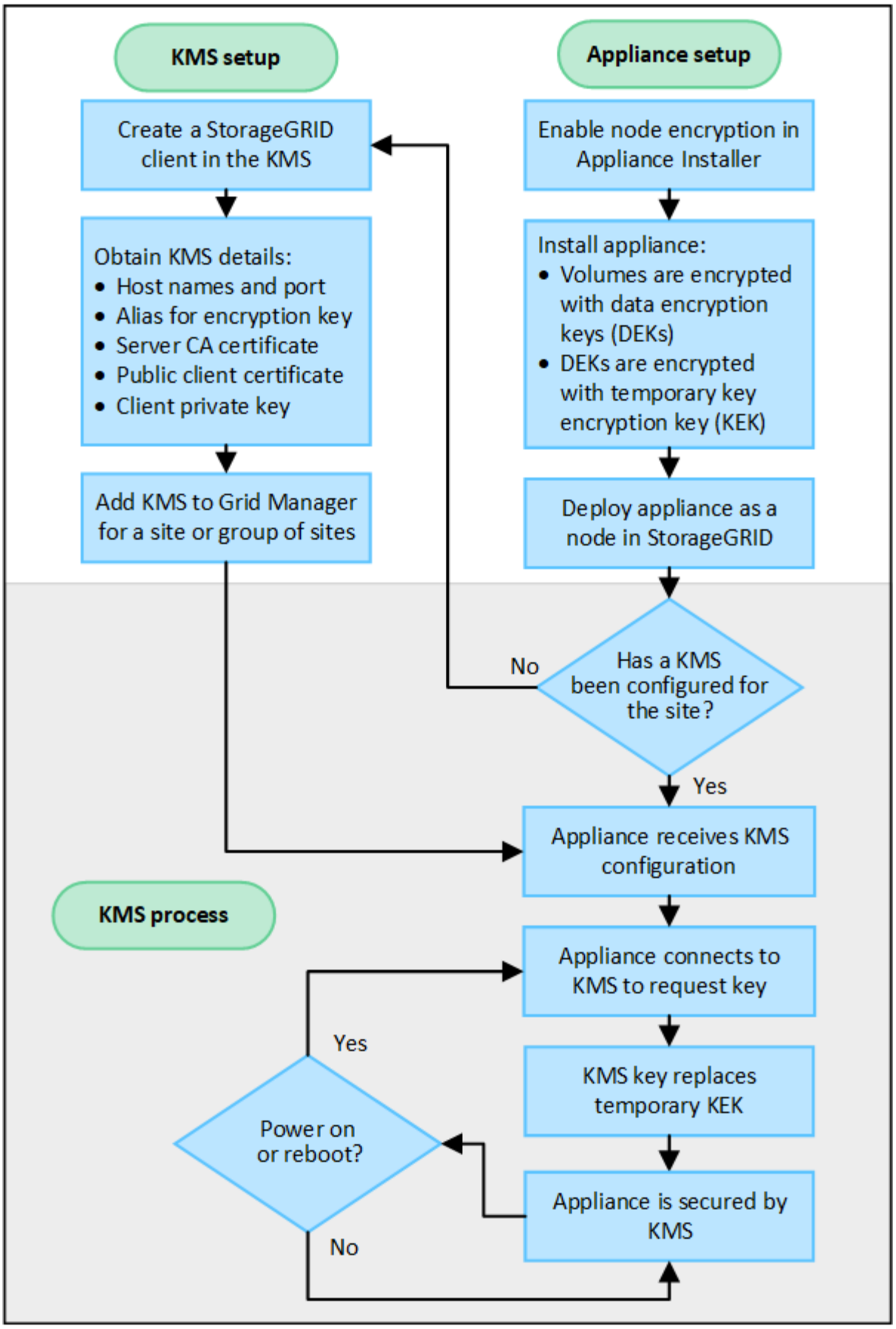
Sie können einen oder mehrere Schlüsselverwaltungsserver verwenden, um die Knotenverschlüsselungsschlüssel für alle StorageGRID Appliance-Knoten zu verwalten, bei denen die Einstellung **Knotenverschlüsselung** während der Installation aktiviert wurde. Die Verwendung von Schlüsselverwaltungsservern mit diesen Appliance-Knoten ermöglicht den Schutz Ihrer Daten, selbst wenn eine Appliance aus dem Rechenzentrum entfernt wird. Nachdem die Appliance-Volumes verschlüsselt wurden, ist ein Zugriff auf die Daten auf der Appliance nur möglich, wenn der Knoten mit dem KMS kommunizieren kann.

> StorageGRID erstellt oder verwaltet keine externen Schlüssel, die zum Verschlüsseln und Entschlüsseln von Appliance-Knoten verwendet werden. Wenn ein externer Schlüsselverwaltungsserver zum Schutz von StorageGRID Daten verwendet werden soll, ist es erforderlich, die Einrichtung dieses Servers sowie die Verwaltung der Verschlüsselungsschlüssel zu verstehen. Die Ausführung von Aufgaben im Zusammenhang mit der Schlüsselverwaltung fällt nicht in den Geltungsbereich dieser Anleitung. Bei Bedarf bietet die Dokumentation Ihres Schlüsselverwaltungsservers Unterstützung, alternativ kann der technische Support kontaktiert werden.

StorageGRID Schlüsselverwaltungsserver und Appliance-Konfiguration

Bevor Sie einen Key-Management-Server (KMS) zum Schutz von StorageGRID Daten auf Appliance-Knoten verwenden können, müssen zwei Konfigurationsaufgaben abgeschlossen werden: die Einrichtung eines oder mehrerer KMS-Server und die Aktivierung der Knotenverschlüsselung für die Appliance-Knoten. Wenn diese beiden Konfigurationsaufgaben abgeschlossen sind, erfolgt der Schlüsselverwaltungsprozess automatisch.

Das Flussdiagramm zeigt die wichtigsten Schritte für die Verwendung eines KMS zur Sicherung von StorageGRID Daten auf Appliance-Knoten.



Das Flussdiagramm zeigt, dass die Einrichtung des KMS und die Einrichtung der Appliance parallel erfolgen;

jedoch können Sie die Key-Management-Server je nach Ihren Anforderungen vor oder nach der Aktivierung der Knotenverschlüsselung für neue Appliance-Knoten einrichten.

Einrichtung des Schlüsselverwaltungsservers (KMS)

Die Einrichtung eines Schlüsselverwaltungsservers umfasst die folgenden übergeordneten Schritte.

Schritt	Siehe
Auf die KMS-Software zugreifen und für StorageGRID bei jedem KMS oder KMS-Cluster einen Client hinzufügen.	"StorageGRID als Client im KMS konfigurieren"
Die erforderlichen Informationen für den StorageGRID Client auf dem KMS erhalten.	"StorageGRID als Client im KMS konfigurieren"
Den KMS zum Grid Manager hinzufügen, einem einzelnen Standort oder einer Standardgruppe von Standorten zuweisen, die erforderlichen Zertifikate hochladen und die KMS Konfiguration speichern.	"${post_edited_translations.segment}"

Das Gerät einrichten

Die Einrichtung eines Appliance-Knotens für die KMS-Nutzung umfasst die folgenden Schritte auf hoher Ebene.

1. Während der Hardwarekonfigurationsphase der Appliance-Installation wird mithilfe des StorageGRID Appliance Installers die Einstellung **Knotenverschlüsselung** für die Appliance aktiviert.

   > Die Einstellung **Knotenverschlüsselung** kann nach dem Hinzufügen eines Geräts zum Grid nicht aktiviert werden, und die externe Schlüsselverwaltung kann nicht für Geräte verwendet werden, bei denen die Knotenverschlüsselung nicht aktiviert ist.

2. Führen Sie das StorageGRID Appliance Installer aus. Während der Installation wird jedem Appliance Volume ein zufälliger Datenverschlüsselungsschlüssel (DEK) wie folgt zugewiesen:
   - Die DEKs dienen der Verschlüsselung der Daten auf jedem Volume. Diese Schlüssel werden mithilfe der Linux Unified Key Setup (LUKS) Festplattenverschlüsselung im Appliance-Betriebssystem generiert und können nicht geändert werden.
   - Jeder einzelne DEK wird durch einen Master Key Encryption Key (KEK) verschlüsselt. Der anfängliche KEK ist ein temporärer Schlüssel, der die DEKs verschlüsselt, bis das Gerät eine Verbindung zum KMS herstellen kann.
3. Den Appliance-Knoten zu StorageGRID hinzufügen.

Siehe "Knotenverschlüsselung aktivieren" für Einzelheiten.

Schlüsselmanagement Verschlüsselungsprozess (erfolgt automatisch)

Die Schlüsselverwaltungsverschlüsselung umfasst die folgenden Schritte auf hoher Ebene, die automatisch durchgeführt werden.

1. Wenn ein Gerät mit aktivierter Knotenverschlüsselung in das Grid eingebunden wird, prüft StorageGRID, ob für den Standort, der den neuen Knoten enthält, eine KMS-Konfiguration vorhanden ist.

- Wenn für den Standort bereits ein KMS konfiguriert wurde, erhält das Gerät die KMS-Konfiguration.
- Wenn für den Standort noch kein KMS konfiguriert wurde, bleiben die Daten auf dem Gerät weiterhin durch den temporären KEK verschlüsselt, bis ein KMS für den Standort konfiguriert ist und das Gerät die KMS-Konfiguration erhält.

2. Das Gerät nutzt die KMS-Konfiguration, um eine Verbindung zum KMS herzustellen und einen Verschlüsselungsschlüssel anzufordern.
3. Der KMS sendet einen Verschlüsselungsschlüssel an das Appliance. Der neue Schlüssel vom KMS ersetzt den temporären KEK und wird nun zum Verschlüsseln und Entschlüsseln der DEKs für die Appliance-Volumes verwendet.

> Alle Daten, die vor der Verbindung des verschlüsselten Appliance-Knotens mit dem konfigurierten KMS vorhanden sind, werden mit einem temporären Schlüssel verschlüsselt. Die Appliance-Volumes sollten jedoch nicht als vor Entfernung aus dem Rechenzentrum geschützt betrachtet werden, bis der temporäre Schlüssel durch den KMS-Verschlüsselungsschlüssel ersetzt wurde.

4. Wird das Gerät eingeschaltet oder neu gestartet, stellt es eine erneute Verbindung zum KMS her, um den Schlüssel anzufordern. Der im flüchtigen Speicher gespeicherte Schlüssel kann einen Stromausfall oder Neustart nicht überstehen.

Anforderungen und Überlegungen zum StorageGRID-Schlüsselverwaltungsserver

Bevor ein externer Key Management Server (KMS) konfiguriert wird, sind die zu berücksichtigenden Aspekte und Anforderungen zu verstehen.

Welche Version von KMIP wird unterstützt?

StorageGRID unterstützt KMIP Version 1.4.

"${post_edited_translations.segment}"

${post_edited_translations.segment}

Die Firewall-Einstellungen des Netzwerks müssen es jedem Geräteknoten ermöglichen, über den für das Key Management Interoperability Protocol (KMIP) verwendeten Port zu kommunizieren. Der Standardport für KMIP ist 5696.

Es ist sicherzustellen, dass jeder Appliance-Knoten, der Knotenverschlüsselung verwendet, Netzwerkzugriff auf den KMS oder KMS-Cluster hat, den Sie für den Standort konfiguriert haben.

Welche TLS-Versionen werden unterstützt?

Die Kommunikation zwischen den Appliance-Knoten und dem konfigurierten KMS erfolgt über sichere TLS-Verbindungen. StorageGRID kann entweder das Protokoll TLS 1.2 oder TLS 1.3 unterstützen, wenn KMIP-Verbindungen zu einem KMS oder KMS-Cluster hergestellt werden, abhängig davon, was vom KMS unterstützt wird und welches "TLS und SSH-Richtlinie" Sie verwenden.

StorageGRID handelt beim Herstellen der Verbindung das Protokoll und die Verschlüsselung (TLS 1.2) oder die Cipher Suite (TLS 1.3) mit dem KMS aus. Um zu sehen, welche Protokollversionen und Verschlüsselungen/Cipher Suites verfügbar sind, ist der Abschnitt `tlsOutbound` der aktiven TLS- und SSH-Richtlinie des Grids (**Konfiguration** > **Sicherheit Sicherheitseinstellungen**) zu prüfen.

${post_edited_translations.segment}

Sie können einen Key Management Server (KMS) verwenden, um Verschlüsselungsschlüssel für jede StorageGRID Appliance in Ihrem Grid zu verwalten, bei der die Einstellung **Node Encryption** aktiviert ist. Diese Einstellung kann nur während der Hardwarekonfigurationsphase der Appliance-Installation über den StorageGRID Appliance Installer aktiviert werden.

> Die Knotenverschlüsselung kann nach dem Hinzufügen eines Geräts zum Grid nicht aktiviert werden, und externe Schlüsselverwaltung kann für Geräte, bei denen die Knotenverschlüsselung nicht aktiviert ist, nicht verwendet werden.

${post_edited_translations.segment}

${post_edited_translations.segment}

- Als virtuelle Maschinen (VMs) bereitgestellte Nodes
- ${post_edited_translations.segment}

${post_edited_translations.segment}

Wann sollten die Schlüsselverwaltungsserver konfiguriert werden?

Bei einer Neuinstallation wird in der Regel empfohlen, einen oder mehrere Key Management Server im Grid Manager einzurichten, bevor Mandanten erstellt werden. Diese Reihenfolge stellt sicher, dass die Knoten geschützt sind, bevor Objektdaten darauf gespeichert werden.

${post_edited_translations.segment}

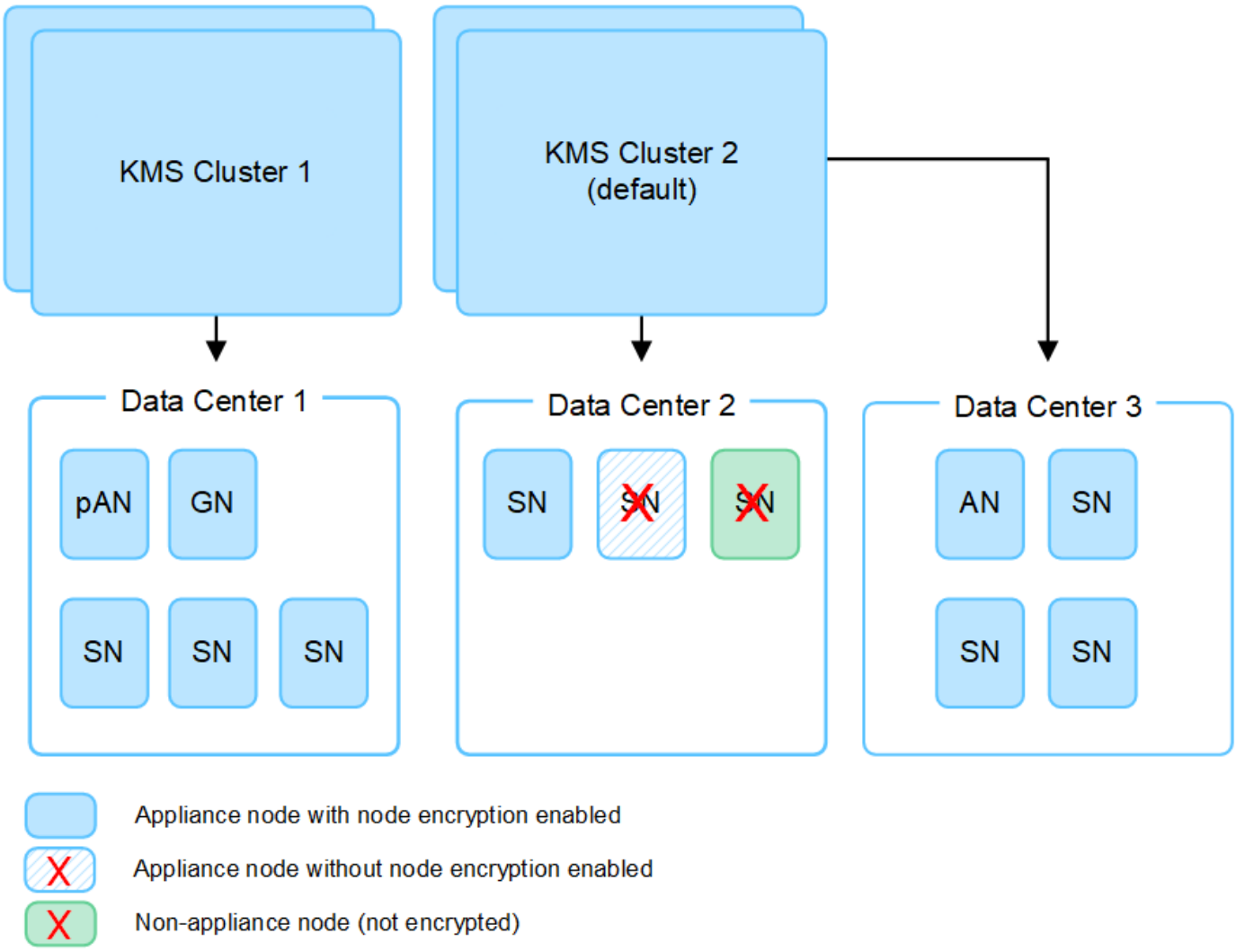
Wie viele Key-Management-Server werden benötigt?

Sie können einen oder mehrere externe Schlüsselverwaltungsserver (KMS) konfigurieren, die den Appliance-Knoten in Ihrem StorageGRID System Verschlüsselungsschlüssel bereitstellen. Jeder KMS stellt den StorageGRID Appliance-Knoten an einem einzelnen Standort oder an einer Gruppe von Standorten einen einzelnen Verschlüsselungsschlüssel zur Verfügung.

StorageGRID unterstützt die Verwendung von KMS Clustern. Jeder KMS Cluster enthält mehrere replizierte Schlüsselverwaltungsserver, die Konfigurationseinstellungen und Verschlüsselungsschlüssel gemeinsam nutzen. Die Verwendung von KMS Clustern für die Schlüsselverwaltung wird empfohlen, da sie die Failover-Fähigkeiten einer Hochverfügbarkeitskonfiguration verbessert.

Angenommen, Ihr StorageGRID System verfügt beispielsweise über drei Rechenzentrumsstandorte. Sie können einen KMS-Cluster so konfigurieren, dass er einen Schlüssel für alle Appliance-Nodes in Rechenzentrum 1 bereitstellt, und einen zweiten KMS-Cluster, um einen Schlüssel für alle Appliance-Nodes an allen anderen Standorten bereitzustellen. Wenn Sie den zweiten KMS-Cluster hinzufügen, können Sie einen Standard-KMS für Rechenzentrum 2 und Rechenzentrum 3 konfigurieren.

${post_edited_translations.segment}



${post_edited_translations.segment}

Als Best Practice für die Sicherheit sollten Sie die von jedem konfigurierten KMS verwendeten "den Verschlüsselungsschlüssel rotieren" regelmäßig wechseln.

${post_edited_translations.segment}

- Sie wird automatisch an die verschlüsselten Appliance-Knoten an dem bzw. den Standorten verteilt, die mit dem KMS verbunden sind. Die Verteilung sollte innerhalb einer Stunde nach der Schlüsselrotation erfolgen.
- Wenn der verschlüsselte Appliance-Knoten offline ist, wenn die neue Schlüsselversion verteilt wird, erhält der Knoten den neuen Schlüssel, sobald er neu startet.
- Kann die neue Schlüsselversion aus irgendeinem Grund nicht zur Verschlüsselung der Appliance-Volumes verwendet werden, wird für den Appliance-Knoten die Warnung **KMS encryption key rotation failed** ausgelöst. Möglicherweise ist es erforderlich, den technischen Support zu kontaktieren, um bei der Behebung dieser Warnung Unterstützung zu erhalten.

${post_edited_translations.segment}

Wenn Sie eine verschlüsselte Appliance in ein anderes StorageGRID-System einbinden müssen, muss der Grid-Knoten zunächst außer Betrieb genommen werden, damit die Objektdaten auf einen anderen Knoten

verschoben werden können. Anschließend kann der StorageGRID Appliance Installer verwendet werden, um "KMS Konfiguration löschen". Durch das Löschen der KMS-Konfiguration wird die Einstellung **Knotenverschlüsselung** deaktiviert und die Verknüpfung zwischen dem Appliance-Knoten und der KMS-Konfiguration für den StorageGRID-Standort entfernt.

> Ohne Zugriff auf den KMS-Verschlüsselungsschlüssel kann auf alle auf dem Gerät verbleibenden Daten nicht mehr zugegriffen werden und sie sind dauerhaft gesperrt.

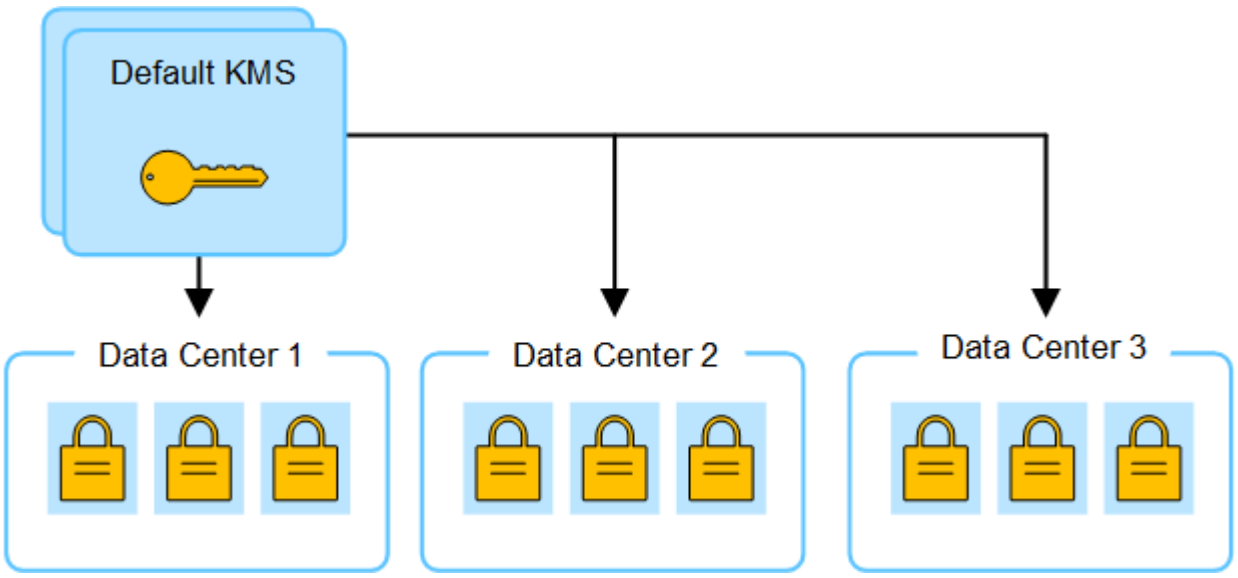
Überlegungen zum Wechsel des KMS für einen StorageGRID Standort

Jeder Key-Management-Server (KMS) oder KMS-Cluster stellt einen Verschlüsselungsschlüssel für alle Appliance-Knoten an einem einzelnen Standort oder an einer Gruppe von Standorten bereit. Falls der für einen Standort verwendete KMS geändert werden soll, kann es erforderlich sein, den Verschlüsselungsschlüssel von einem KMS auf einen anderen zu kopieren.

Wenn Sie das für einen Standort verwendete KMS ändern, müssen Sie sicherstellen, dass die zuvor verschlüsselten Appliance-Knoten an diesem Standort mit dem auf dem neuen KMS gespeicherten Schlüssel entschlüsselt werden können. In manchen Fällen ist es erforderlich, die aktuelle Version des Verschlüsselungsschlüssels vom ursprünglichen KMS auf das neue KMS zu kopieren. Es muss sichergestellt werden, dass das KMS über den korrekten Schlüssel zum Entschlüsseln der verschlüsselten Appliance-Knoten am Standort verfügt.

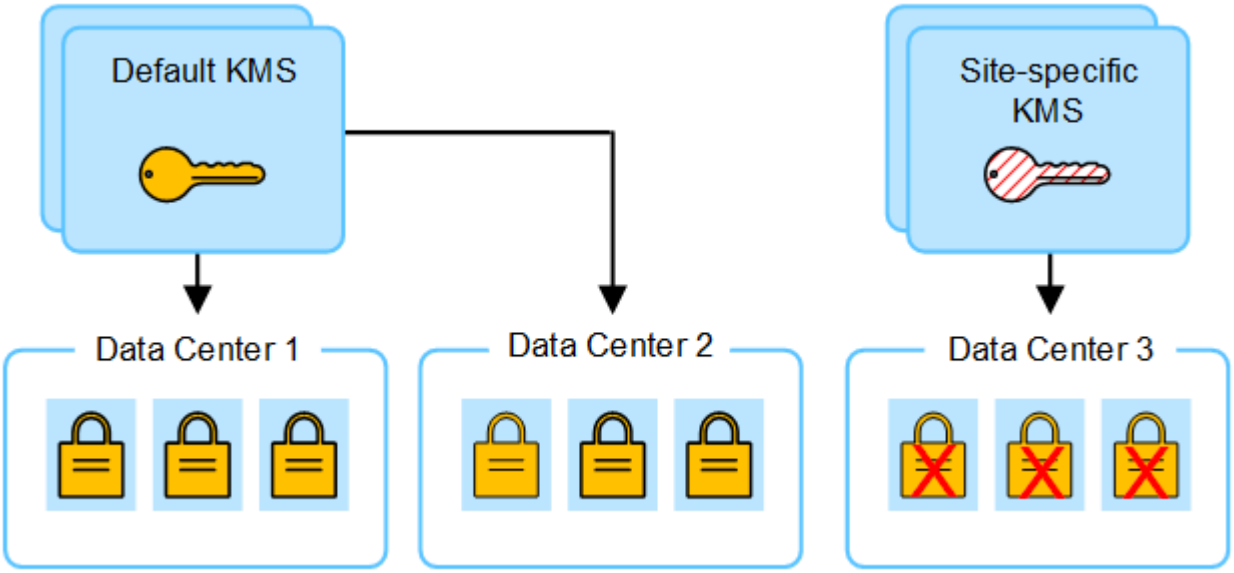
Beispiel:

1. Zunächst wird ein Standard-KMS konfiguriert, das für alle Standorte gilt, die kein dediziertes KMS haben.
2. Nach dem Speichern des KMS verbinden sich alle Appliance-Knoten, auf denen die Einstellung **Knotenverschlüsselung** aktiviert ist, mit dem KMS und fordern den Verschlüsselungsschlüssel an. Dieser Schlüssel dient zur Verschlüsselung der Appliance-Knoten an allen Standorten. Derselbe Schlüssel muss auch zum Entschlüsseln dieser Appliances verwendet werden.

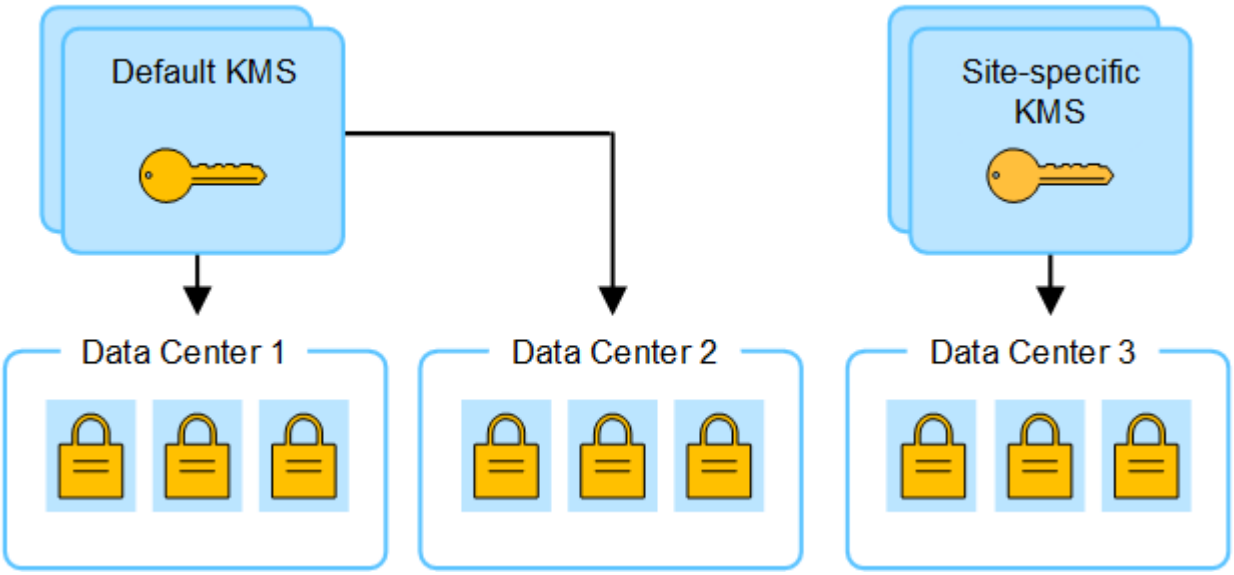


3. Sie entscheiden sich, für einen Standort (Data Center 3 in der Abbildung) ein standortspezifisches KMS hinzuzufügen. Da die Appliance-Knoten jedoch bereits verschlüsselt sind, tritt beim Speichern der Konfiguration für das standortspezifische KMS ein Validierungsfehler auf. Der Fehler entsteht, weil das standortspezifische KMS nicht über den korrekten Schlüssel zum Entschlüsseln der Knoten an diesem

Standort verfügt.



4. Um das Problem zu beheben, kopieren Sie die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS in das neue KMS. (Technisch gesehen kopieren Sie den ursprünglichen Schlüssel in einen neuen Schlüssel mit demselben Alias. Der ursprüngliche Schlüssel wird zu einer vorherigen Version des neuen Schlüssels.) Das standortspezifische KMS verfügt nun über den richtigen Schlüssel, um die Appliance-Knoten in Data Center 3 zu entschlüsseln, sodass es in StorageGRID gespeichert werden kann.



${post_edited_translations.segment}

${post_edited_translations.segment}

Anwendungsfall für die Änderung des KMS einer Site	Erforderliche Schritte
${post_edited_translations.segment}	Den standortspezifischen KMS bearbeiten. Im Feld **Verwaltet Schlüssel für** die Option **Standorte, die nicht von einem anderen KMS verwaltet werden (Standard KMS)** auswählen. Der standortspezifische KMS wird nun als Standard KMS verwendet. Dies gilt für alle Standorte, die keinen dedizierten KMS haben. "${post_edited_translations.segment}"
Sie verfügen über einen Standard-KMS und fügen im Rahmen einer Erweiterung einen neuen Standort hinzu. Sie möchten den Standard-KMS nicht für den neuen Standort verwenden.	1. Falls die Appliance-Knoten am neuen Standort bereits vom Standard-KMS verschlüsselt wurden, kann die KMS-Software verwendet werden, um die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS auf einen neuen KMS zu kopieren. 2. Mit dem Grid Manager den neuen KMS hinzufügen und den Standort auswählen. "${post_edited_translations.segment}"
Sie möchten, dass der KMS für einen Standort einen anderen Server verwendet.	1. ${post_edited_translations.segment} 2. Im Grid Manager kann die bestehende KMS Konfiguration bearbeitet und der neue Hostname oder die neue IP-Adresse eingegeben werden. "${post_edited_translations.segment}"

StorageGRID als Client im KMS konfigurieren

StorageGRID muss als Client für jeden externen Schlüsselverwaltungsserver oder KMS-Cluster konfiguriert werden, bevor der KMS zu StorageGRID hinzugefügt werden kann.

Diese Anweisungen gelten für Thales CipherTrust Manager und Hashicorp Vault. Eine Liste der unterstützten Produkte und Versionen ist über "NetApp Interoperabilitätsmatrix Tool (IMT)" verfügbar.

Schritte

1. Aus der KMS-Software heraus einen StorageGRID Client für jeden KMS oder KMS-Cluster erstellen, der verwendet werden soll.

   Jeder KMS verwaltet einen einzigen Verschlüsselungsschlüssel für die StorageGRID Appliance-Knoten an einem einzelnen Standort oder an einer Gruppe von Standorten.

2. Ein Schlüssel kann mit einer der folgenden beiden Methoden erstellt werden:
   - Verwenden Sie die Schlüsselverwaltungsseite Ihres KMS-Produkts. Ein AES-Verschlüsselungsschlüssel ist für jeden KMS oder KMS-Cluster zu erstellen.

     Der Verschlüsselungsschlüssel muss mindestens 2.048 Bit lang und exportierbar sein.

- Lassen Sie StorageGRID den Schlüssel erstellen. Sie werden beim Testen und Speichern nach "Hochladen von Client-Zertifikaten" dazu aufgefordert.

3. Für jeden KMS oder KMS-Cluster die folgenden Informationen notieren.

   Diese Informationen werden benötigt, wenn der KMS zu StorageGRID hinzugefügt wird:

   - Hostname oder IP-Adresse für jeden Server.
   - KMIP-Port, der vom KMS verwendet wird.
   - Schlüsselalias für den Verschlüsselungsschlüssel im KMS.

4. Für jeden KMS oder KMS Cluster ist ein Serverzertifikat zu beschaffen, das von einer Zertifizierungsstelle (CA) signiert ist, oder ein Zertifikatspaket, das alle PEM-kodierten CA-Zertifikatsdateien in der Reihenfolge der Zertifikatskette enthält.

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

   - Das Zertifikat muss das Privacy Enhanced Mail (PEM) Base-64-kodierte X.509-Format verwenden.
   - Das Feld „Subject Alternative Name (SAN)“ in jedem Serverzertifikat muss den vollqualifizierten Domainnamen (FQDN) oder die IP-Adresse enthalten, zu der StorageGRID eine Verbindung herstellt.

     > Bei der Konfiguration des KMS in StorageGRID sind im Feld **Hostname** die gleichen vollqualifizierten Domains (FQDNs) oder IP-Adressen einzugeben.

   - ${post_edited_translations.segment}

5. ${post_edited_translations.segment}

   Das Clientzertifikat ermöglicht StorageGRID, sich gegenüber dem KMS zu authentifizieren.

Fügen Sie einen Schlüsselverwaltungsserver in StorageGRID hinzu

Sie verwenden den StorageGRID Key Management Server Assistenten, um jeden KMS oder jedes KMS Cluster hinzuzufügen.

Bevor Sie beginnen

- Sie haben die "Überlegungen und Anforderungen für die Verwendung eines Schlüsselverwaltungsservers" überprüft.
- Sie haben "StorageGRID als Client im KMS konfiguriert" und verfügen über die erforderlichen Informationen für jeden KMS oder KMS-Cluster.
- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Root-Zugriffsberechtigung".

Über diese Aufgabe

Wenn möglich, sollten standortspezifische Schlüsselverwaltungsserver (KMS) konfiguriert werden, bevor ein Standard-KMS konfiguriert wird, der für alle Standorte gilt, die nicht von einem anderen KMS verwaltet werden. Wenn zuerst der Standard-KMS erstellt wird, werden alle knotenverschlüsselten Appliances im Grid vom Standard-KMS verschlüsselt. Wenn später ein standortspezifischer KMS erstellt werden soll, muss zunächst die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS in den neuen KMS kopiert werden. Siehe "Überlegungen zum Wechsel des KMS für einen Standort" für Details.

Schritt 1: KMS Details

Im ersten Schritt (KMS-Details) des Assistenten zum Hinzufügen eines Key Management Servers werden Details zum KMS oder KMS-Cluster angegeben.

Schritte

1. **Konfiguration** > **Sicherheit** > **Schlüsselverwaltungsserver** auswählen.

   Die Seite des Schlüsselverwaltungsservers wird mit der ausgewählten Registerkarte „Konfigurationsdetails“ angezeigt.

2. Wählen Sie **Create**.

   Schritt 1 (KMS-Details) des Assistenten zum Hinzufügen eines Key Management Servers erscheint.

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

Feld	Beschreibung
KMS-Name	Ein beschreibender Name, der Ihnen hilft, dieses KMS zu identifizieren. Muss zwischen 1 und 64 Zeichen lang sein.
Schlüsselname	Der exakte Schlüsselalias für den StorageGRID Client im KMS. Muss zwischen 1 und 255 Zeichen lang sein. **Hinweis**: Falls Sie mit Ihrem KMS-Produkt noch keinen Schlüssel erstellt haben, werden Sie aufgefordert, StorageGRID den Schlüssel zu erstellen.
Verwaltet Schlüssel für	Die StorageGRID Site, die diesem KMS zugeordnet wird. Wenn möglich, sollten standortspezifische Schlüsselverwaltungsserver konfiguriert werden, bevor ein Standard-KMS konfiguriert wird, der für alle Sites gilt, die nicht von einem anderen KMS verwaltet werden. • Wählen Sie einen Standort aus, wenn dieses KMS die Verschlüsselungsschlüssel für die Appliance-Knoten an einem bestimmten Standort verwaltet. • **Standorte, die nicht von einem anderen KMS verwaltet werden (Standard-KMS)** kann ausgewählt werden, um einen Standard-KMS zu konfigurieren, der für alle Standorte gilt, die keinen dedizierten KMS haben, sowie für alle Standorte, die in späteren Erweiterungen hinzugefügt werden. **Hinweis:** Ein Validierungsfehler tritt auf, wenn die KMS-Konfiguration gespeichert wird und eine Site ausgewählt wird, die zuvor vom Standard-KMS verschlüsselt wurde, aber dem neuen KMS nicht die aktuelle Version des ursprünglichen Verschlüsselungsschlüssels bereitgestellt wurde.

Feld	Beschreibung
Port	Der Port, den der KMS-Server für das Key Management Interoperability Protocol (KMIP) verwendet. Standardmäßig 5696, der KMIP-Standardport.
Hostname	Der vollqualifizierte Domainname oder die IP-Adresse für den KMS. **Hinweis:** Das Feld „Subject Alternative Name“ (SAN) des Serverzertifikats muss den hier eingegebenen vollqualifizierten Domainnamen (FQDN) oder die IP-Adresse enthalten. Andernfalls kann StorageGRID keine Verbindung zum KMS oder zu allen Servern in einem KMS-Cluster herstellen.

4. Wenn Sie einen KMS Cluster konfigurieren, kann mit **Weiteren Hostnamen hinzufügen** für jeden Server im Cluster ein Hostname hinzugefügt werden.
5. Wählen Sie **Weiter**.

Schritt 2: Serverzertifikat hochladen

Im zweiten Schritt (Serverzertifikat hochladen) des Assistenten zum Hinzufügen eines Schlüsselverwaltungsservers wird das Serverzertifikat (oder Zertifikatspaket) für den KMS hochgeladen. Das Serverzertifikat ermöglicht dem externen KMS, sich gegenüber StorageGRID zu authentifizieren.

Schritte

1. Ab **Schritt 2 (Serverzertifikat hochladen)** zum Speicherort des gespeicherten Serverzertifikats oder Zertifikatspakets navigieren.
2. Die Zertifikatsdatei hochladen.

   Die Metadaten des Serverzertifikats werden angezeigt.

   Wenn Sie ein Zertifikatspaket hochgeladen haben, erscheinen die Metadaten für jedes Zertifikat auf einem eigenen Tab.

3. Wählen Sie **Weiter**.

Schritt 3: Clientzertifikate hochladen

Im dritten Schritt (Clientzertifikate hochladen) des Assistenten zum Hinzufügen eines Schlüsselverwaltungsservers werden das Clientzertifikat und der private Schlüssel des Clientzertifikats hochgeladen. Das Clientzertifikat ermöglicht es StorageGRID, sich beim KMS zu authentifizieren.

Schritte

1. Ab **Schritt 3 (Clientzertifikate hochladen)** zum Speicherort des Clientzertifikats navigieren.
2. Die Clientzertifikatsdatei hochladen.

   Die Metadaten des Client-Zertifikats werden angezeigt.

3. Navigieren Sie zum Speicherort des privaten Schlüssels für das Clientzertifikat.
4. Die private Schlüsseldatei hochladen.

5. **Testen und speichern** auswählen.

   Falls kein Schlüssel existiert, werden Sie aufgefordert, dass StorageGRID einen erstellt.

   Die Verbindungen zwischen dem Schlüsselverwaltungsserver und den Appliance-Knoten werden geprüft. Sind alle Verbindungen gültig und wird der korrekte Schlüssel im KMS gefunden, wird der neue Schlüsselverwaltungsserver der Tabelle auf der Seite „Schlüsselverwaltungsserver“ hinzugefügt.

   > Unmittelbar nach dem Hinzufügen eines KMS wird der Zertifikatsstatus auf der Seite „Key Management Server“ als Unbekannt angezeigt. Es kann bis zu 30 Minuten dauern, bis StorageGRID den tatsächlichen Status jedes Zertifikats ermittelt. Der aktuelle Status wird erst nach Aktualisierung des Webbrowsers angezeigt.

6. Wenn beim Auswählen von **Testen und speichern** eine Fehlermeldung erscheint, die Details der Meldung können überprüft und anschließend **OK** ausgewählt werden.

   Beispielsweise kann die Fehlermeldung 422: Unprocessable Entity auftreten, wenn ein Verbindungstest fehlschlägt.

7. Wenn die aktuelle Konfiguration gespeichert werden soll, ohne die externe Verbindung zu testen, ist **Speichern erzwingen** auszuwählen.

   > Durch Auswahl von **Speichern erzwingen** wird die KMS-Konfiguration gespeichert, jedoch wird die externe Verbindung jeder Appliance zu diesem KMS nicht getestet. Wenn es ein Problem mit der Konfiguration gibt, ist es möglicherweise nicht möglich, Appliance-Knoten mit aktivierter Knotenverschlüsselung am betroffenen Standort neu zu starten. Der Zugriff auf Ihre Daten kann bis zur Behebung der Probleme verloren gehen.

8. ${post_edited_translations.segment}

   Die KMS Konfiguration ist gespeichert, aber die Verbindung zum KMS wird nicht getestet.

Verwalten eines Schlüsselverwaltungsservers in StorageGRID

${post_edited_translations.segment}

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Erforderliche Zugriffsberechtigung".

${post_edited_translations.segment}

${post_edited_translations.segment}

Schritte

1. **Konfiguration** > **Sicherheit** > **Schlüsselverwaltungsserver** auswählen.

   Die Seite des Schlüsselverwaltungsservers wird angezeigt und zeigt die folgenden Informationen an:

   - ${post_edited_translations.segment}
   - ${post_edited_translations.segment}

2. Um die Details für einen bestimmten KMS anzuzeigen und Aktionen für diesen KMS auszuführen, wählen Sie den Namen des KMS aus. Die Detailseite für den KMS listet die folgenden Informationen auf:

Feld	Beschreibung
Verwaltet Schlüssel für	Die mit dem KMS verknüpfte StorageGRID Site. ${post_edited_translations.segment}
Hostname	Der vollqualifizierte Domainname oder die IP-Adresse des KMS. Wenn ein Cluster aus zwei Key-Management-Servern besteht, werden der vollqualifizierte Domain-Name oder die IP-Adresse beider Server aufgeführt. Wenn mehr als zwei Key-Management-Server in einem Cluster vorhanden sind, werden der vollqualifizierte Domain-Name oder die IP-Adresse des ersten KMS zusammen mit der Anzahl der zusätzlichen Key-Management-Server im Cluster aufgeführt. Zum Beispiel: `10.10.10.10 and 10.10.10.11` oder `10.10.10.10 and 2 others`. Alle Hostnamen in einem Cluster werden angezeigt, wenn ein KMS ausgewählt und **Bearbeiten** oder **Aktionen** > **Bearbeiten** gewählt wird.

3. Auf der KMS-Detailseite sind auf den einzelnen Tabs die folgenden Informationen ersichtlich:

Tab	Feld	Beschreibung
Wichtige Details	Schlüsselname	${post_edited_translations.segment}
Schlüssel-UID	${post_edited_translations.segment}	${post_edited_translations.segment}
${post_edited_translations.segment}	Serverzertifikat	Metadaten
${post_edited_translations.segment}	Zertifikat PEM	${post_edited_translations.segment}
Client-Zertifikat	Metadaten	${post_edited_translations.segment}

4. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

Wenn Sie den Verschlüsselungsschlüssel mithilfe der KMS-Software rotieren, sollte die Rotation von der zuletzt verwendeten Version des Schlüssels zu einer neuen Version desselben Schlüssels erfolgen. Es sollte keine Rotation zu einem völlig anderen Schlüssel durchgeführt werden.

Versuchen Sie niemals, einen Schlüssel zu rotieren, indem Sie den Schlüsselnamen (Alias) für den KMS ändern. StorageGRID benötigt, dass alle zuvor verwendeten Schlüsselversionen (sowie alle zukünftigen) mit demselben Schlüsselalias über den KMS zugänglich sind. Wenn der Schlüsselalias für einen konfigurierten KMS geändert wird, kann StorageGRID Ihre Daten möglicherweise nicht entschlüsseln.

Zertifikate verwalten

Alle Probleme mit Server- oder Clientzertifikaten sollten umgehend behoben werden. Zertifikate sollten nach Möglichkeit vor deren Ablauf ersetzt werden.

${post_edited_translations.segment}

Schritte

1. **Konfiguration** > **Sicherheit** > **Schlüsselverwaltungsserver** auswählen.
2. ${post_edited_translations.segment}
3. Wenn das Ablaufdatum eines Zertifikats für ein KMS unbekannt ist, bis zu 30 Minuten abwarten und anschließend den Webbrowser aktualisieren.
4. Wenn in der Spalte „Zertifikatablauf“ angezeigt wird, dass ein Zertifikat abgelaufen ist oder demnächst abläuft, kann der KMS ausgewählt werden, um zur KMS-Detailseite zu gelangen.
   a. ${post_edited_translations.segment}
   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}
5. ${post_edited_translations.segment}

   Es kann bis zu 30 Minuten dauern, bis StorageGRID die Aktualisierungen zum Ablaufdatum des Zertifikats erhält. Durch Aktualisieren des Webbrowsers werden die aktuellen Werte angezeigt.

Wenn der Status **Serverzertifikatstatus unbekannt** angezeigt wird, sollte sichergestellt sein, dass Ihr KMS das Abrufen eines Serverzertifikats ohne ein Clientzertifikat zulässt.

Verschlüsselte Knoten anzeigen

Sie können Informationen über die Appliance-Knoten in Ihrem StorageGRID System anzeigen, bei denen die Einstellung **Knotenverschlüsselung** aktiviert ist.

Schritte

1. **Konfiguration** > **Sicherheit** > **Schlüsselverwaltungsserver** auswählen.

   Die Seite „Schlüsselverwaltungsserver“ wird angezeigt. Die Registerkarte „Konfigurationsdetails“ zeigt alle konfigurierten Schlüsselverwaltungsserver an.

2. Oben auf der Seite die Registerkarte **Verschlüsselte Knoten** auswählen.

Auf der Registerkarte „Verschlüsselte Knoten“ werden die Appliance-Knoten in Ihrem StorageGRID System aufgelistet, bei denen die Einstellung **Knotenverschlüsselung** aktiviert ist.

3. Die Informationen in der Tabelle für jeden Geräteknoten werden angezeigt.

Spalte	Beschreibung
Knotenname	Der Name des Geräteknotens.
Knotentyp	Der Knotentyp: Storage, Admin oder Gateway.
Standort	Der Name des StorageGRID Standorts, an dem der Knoten installiert ist.
KMS-Name	Der beschreibende Name des für den Node verwendeten KMS. Falls kein KMS aufgeführt ist, kann auf der Registerkarte „Konfigurationsdetails“ ein KMS hinzugefügt werden. "${post_edited_translations.segment}"
Schlüssel-UID	Die eindeutige ID des Verschlüsselungsschlüssels, der zum Verschlüsseln und Entschlüsseln von Daten auf dem Geräteknoten verwendet wird. Die vollständige Schlüssel-UID wird angezeigt, wenn der Text markiert wird. Ein Bindestrich (--) zeigt an, dass die Schlüssel-UID unbekannt ist, möglicherweise aufgrund eines Verbindungsproblems zwischen dem Appliance-Knoten und dem KMS.
Status	Der Status der Verbindung zwischen dem KMS und dem Appliance-Knoten. Wenn der Knoten verbunden ist, wird der Zeitstempel alle 30 Minuten aktualisiert. Es kann mehrere Minuten dauern, bis der Verbindungsstatus nach Änderungen der KMS-Konfiguration aktualisiert wird. **Hinweis:** Aktualisieren Sie Ihren Webbrowser, um die neuen Werte zu sehen.

4. Wenn die Spalte „Status“ auf ein KMS-Problem hinweist, sollte das Problem umgehend behoben werden.

   Im Normalbetrieb des KMS wird der Status als **Mit KMS verbunden** angezeigt. Wenn ein Knoten vom Grid getrennt ist, wird der Verbindungsstatus des Knotens angezeigt (Administrativ getrennt oder Unbekannt).

   Andere Statusmeldungen entsprechen StorageGRID Warnungen mit denselben Namen:

   - Die KMS Konfiguration konnte nicht geladen werden.
   - KMS-Verbindungsfehler
   - KMS-Verschlüsselungsschlüsselname nicht gefunden
   - KMS-Verschlüsselungsschlüsselrotation fehlgeschlagen
   - Der KMS-Schlüssel konnte ein Appliance-Volume nicht entschlüsseln.
   - KMS ist nicht konfiguriert

   Empfohlene Maßnahmen für diese Warnmeldungen ausführen.

Etwaige Probleme sind umgehend zu beheben, damit Ihre Daten vollständig geschützt sind.

Bearbeiten einer KMS

Möglicherweise ist eine Bearbeitung der Konfiguration eines Schlüsselverwaltungsservers erforderlich, beispielsweise wenn ein Zertifikat demnächst abläuft.

Bevor Sie beginnen

- Wenn Sie planen, die für ein KMS ausgewählte Website zu aktualisieren, wurde die "Überlegungen zum Wechsel des KMS für einen Standort" überprüft.
- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Root-Zugriffsberechtigung".

Schritte

1. **Konfiguration** > **Sicherheit** > **Schlüsselverwaltungsserver** auswählen.

   Die Seite „Schlüsselverwaltungsserver“ wird angezeigt und zeigt alle konfigurierten Schlüsselverwaltungsserver.

2. Wählen Sie den KMS aus, den Sie bearbeiten möchten, und wählen Sie **Aktionen** > **Bearbeiten**.

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

3. Optional können die Details in **Schritt 1 (KMS-Details)** des Assistenten zum Bearbeiten eines Key Management Servers aktualisiert werden.

Feld	Beschreibung
KMS-Name	Ein beschreibender Name, der Ihnen hilft, dieses KMS zu identifizieren. Muss zwischen 1 und 64 Zeichen lang sein.
Schlüsselname	Der exakte Schlüsselalias für den StorageGRID Client im KMS. Muss zwischen 1 und 255 Zeichen lang sein. Sie müssen den Schlüsselnamen nur in seltenen Fällen bearbeiten. Beispielsweise ist eine Bearbeitung des Schlüsselnamens erforderlich, wenn der Alias im KMS umbenannt wird oder wenn alle Versionen des vorherigen Schlüssels in den Versionsverlauf des neuen Alias kopiert wurden.
Verwaltet Schlüssel für	Wenn Sie ein standortspezifisches KMS bearbeiten und noch kein Standard-KMS eingerichtet haben, kann optional **Standorte, die nicht von einem anderen KMS verwaltet werden (Standard-KMS)** ausgewählt werden. Diese Auswahl wandelt das standortspezifische KMS in das Standard-KMS um, das für alle Standorte gilt, die kein dediziertes KMS haben, sowie für alle Standorte, die im Rahmen einer Erweiterung hinzugefügt werden. **Hinweis:** Wenn Sie ein standortspezifisches KMS bearbeiten, kann kein anderer Standort ausgewählt werden. Wenn das Standard-KMS bearbeitet wird, kann kein bestimmter Standort ausgewählt werden.

Feld	Beschreibung
Port	Der Port, den der KMS-Server für das Key Management Interoperability Protocol (KMIP) verwendet. Standardmäßig 5696, der KMIP-Standardport.
Hostname	Der vollqualifizierte Domainname oder die IP-Adresse für den KMS. **Hinweis:** Das Feld „Subject Alternative Name“ (SAN) des Serverzertifikats muss den hier eingegebenen vollqualifizierten Domainnamen (FQDN) oder die IP-Adresse enthalten. Andernfalls kann StorageGRID keine Verbindung zum KMS oder zu allen Servern in einem KMS-Cluster herstellen.

4. Wenn Sie einen KMS Cluster konfigurieren, kann mit **Weiteren Hostnamen hinzufügen** für jeden Server im Cluster ein Hostname hinzugefügt werden.
5. Wählen Sie **Weiter**.

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

6. Falls das Serverzertifikat ersetzt werden muss, **Durchsuchen** auswählen und die neue Datei hochladen.
7. Wählen Sie **Weiter**.

   Schritt 3 (Clientzertifikate hochladen) des Assistenten zum Bearbeiten eines Key Management Server wird angezeigt.

8. Falls das Clientzertifikat und der private Schlüssel des Clientzertifikats ersetzt werden müssen, kann **Durchsuchen** ausgewählt und die neuen Dateien hochgeladen werden.
9. **Testen und speichern** auswählen.

   Die Verbindungen zwischen dem Schlüsselverwaltungsserver und allen node-verschlüsselten Appliance-Knoten an den betroffenen Standorten werden geprüft. Wenn alle Knotenverbindungen gültig sind und der korrekte Schlüssel auf dem KMS gefunden wird, wird der Schlüsselverwaltungsserver der Tabelle auf der Seite „Key Management Server“ hinzugefügt.

10. Wenn eine Fehlermeldung angezeigt wird, die Details der Meldung prüfen und **OK** auswählen.

    Beispielsweise kann die Fehlermeldung 422: Unprocessable Entity auftreten, wenn die für diesen KMS ausgewählte Site bereits von einem anderen KMS verwaltet wird oder wenn ein Verbindungstest fehlgeschlagen ist.

11. Falls die aktuelle Konfiguration vor der Behebung der Verbindungsfehler gespeichert werden muss, kann **Speichern erzwingen** ausgewählt werden.

    > Durch Auswahl von **Speichern erzwingen** wird die KMS-Konfiguration gespeichert, jedoch wird die externe Verbindung jeder Appliance zu diesem KMS nicht getestet. Wenn es ein Problem mit der Konfiguration gibt, ist es möglicherweise nicht möglich, Appliance-Knoten mit aktivierter Knotenverschlüsselung am betroffenen Standort neu zu starten. Der Zugriff auf Ihre Daten kann bis zur Behebung der Probleme verloren gehen.

    Die KMS Konfiguration ist gespeichert.

12. ${post_edited_translations.segment}

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

Entfernen eines Key Management Servers (KMS)

In manchen Fällen möchten Sie möglicherweise einen Schlüsselverwaltungsserver entfernen. Beispielsweise kann ein standortspezifischer KMS entfernt werden, wenn der Standort außer Betrieb genommen wurde.

Bevor Sie beginnen

- Sie haben die "Überlegungen und Anforderungen für die Verwendung eines Schlüsselverwaltungsservers" überprüft.
- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Root-Zugriffsberechtigung".

Über diese Aufgabe

In diesen Fällen kann ein KMS entfernt werden:

- Sie können einen standortspezifischen KMS entfernen, wenn der Standort außer Betrieb genommen wurde oder wenn der Standort keine Appliance-Knoten mit aktivierter Knotenverschlüsselung enthält.
- Der Standard-KMS kann entfernt werden, wenn für jeden Standort, der Appliance-Knoten mit aktivierter Knotenverschlüsselung besitzt, bereits ein standortspezifischer KMS vorhanden ist.

Schritte

1. **Konfiguration** > **Sicherheit** > **Schlüsselverwaltungsserver** auswählen.

   Die Seite „Schlüsselverwaltungsserver“ wird angezeigt und zeigt alle konfigurierten Schlüsselverwaltungsserver.

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

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

3. Folgendes trifft zu:
   - Sie entfernen einen standortspezifischen KMS für einen Standort, der keinen Appliance-Knoten mit aktivierter Knotenverschlüsselung hat.
   - Sie entfernen den Standard-KMS, aber für jeden Standort mit Knotenverschlüsselung existiert bereits ein standortspezifischer KMS.
4. **Ja** auswählen.

   Die KMS Konfiguration wird entfernt.

Proxy-Einstellungen verwalten

Konfigurieren Sie einen StorageGRID-Speicherproxy

Wenn Sie Plattformdienste oder Cloud Storage Pools verwenden, kann ein nicht-transparenter Proxy zwischen Storage Nodes und den externen S3-Endpunkten konfiguriert werden. Zum Beispiel kann ein nicht-transparenter Proxy erforderlich sein, damit Plattformdienste-Nachrichten an externe Endpunkte, wie etwa einen Endpunkt im

Internet, gesendet werden können.

${post_edited_translations.segment}

Bevor Sie beginnen

- Du hast "spezifische Zugriffsberechtigungen".
- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.

Über diese Aufgabe

${post_edited_translations.segment}

Schritte

1. **Konfiguration** > **Sicherheit** > **Proxy-Einstellungen** auswählen.
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
4. Den Hostnamen oder die IP-Adresse des Proxyserver eingeben.
5. Optional kann der Port eingegeben werden, der für die Verbindung zum Proxyserver verwendet wird.

   Dieses Feld bleibt leer, um den Standardport für das Protokoll zu verwenden: 80 für HTTP oder 1080 für SOCKS5.

6. **Speichern** auswählen.

   ${post_edited_translations.segment}

   Es kann bis zu 10 Minuten dauern, bis Proxy-Änderungen wirksam werden.

7. ${post_edited_translations.segment}
8. ${post_edited_translations.segment}

Konfigurieren Sie die Admin-Proxy-Einstellungen in StorageGRID

Wenn Sie AutoSupport-Pakete über HTTP oder HTTPS versenden, kann ein nicht transparenter Proxyserver zwischen Admin-Nodes und dem technischen Support (AutoSupport) konfiguriert werden.

Weitere Informationen zu AutoSupport sind unter "Konfiguration von AutoSupport" verfügbar.

Bevor Sie beginnen

- Du hast "spezifische Zugriffsberechtigungen".
- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.

Über diese Aufgabe

Die Einstellungen für einen einzelnen Admin-Proxy können konfiguriert werden.

Schritte

1. **Konfiguration** > **Sicherheit** > **Proxy-Einstellungen** auswählen.

   Die Seite „Proxy-Einstellungen“ wird angezeigt. Standardmäßig ist im Tab-Menü Storage ausgewählt.

2. Die Registerkarte **Admin** auswählen.
3. Das Kontrollkästchen **Admin Proxy aktivieren** auswählen.
4. Den Hostnamen oder die IP-Adresse des Proxyserver eingeben.
5. Geben Sie den Port ein, der für die Verbindung zum Proxyserver verwendet wird.
6. Optional kann ein Benutzername und ein Passwort für den Proxyserver eingegeben werden.

   Lassen Sie diese Felder leer, wenn Ihr Proxyserver keinen Benutzernamen oder kein Passwort benötigt.

7. Wählen Sie eine der folgenden Optionen aus:

   - Wenn die Verbindung zum Admin-Proxy gesichert werden soll, ist **Proxy-Zertifikat überprüfen** auszuwählen. Ein CA-Bundle kann hochgeladen werden, um die Authentizität der vom Admin Proxyserver präsentierten SSL-Zertifikate zu überprüfen.

     AutoSupport on Demand, E-Series AutoSupport durch StorageGRID und die Update Path-Bestimmung auf der StorageGRID Upgrade-Seite funktionieren nicht, wenn ein Proxy-Zertifikat verifiziert wird.

   Nach dem Hochladen des CA-Bundle werden dessen Metadaten angezeigt.

   - Wenn keine Zertifikate bei der Kommunikation mit dem Admin Proxyserver validiert werden sollen, ist **Proxy-Zertifikat nicht überprüfen** auszuwählen.
8. **Speichern** auswählen.

   Nachdem der Admin-Proxy gespeichert wurde, wird der Proxyserver zwischen den Admin-Knoten und dem technischen Support konfiguriert.

   Es kann bis zu 10 Minuten dauern, bis Proxy-Änderungen wirksam werden.

9. Falls der Admin-Proxy deaktiviert werden soll, das Kontrollkästchen **Admin-Proxy aktivieren** deaktivieren und anschließend **Speichern** auswählen.

Firewalls kontrollieren

StorageGRID-Zugriff an einer externen Firewall steuern

Es besteht die Möglichkeit, bestimmte Ports an der externen Firewall zu öffnen oder zu schließen.

Sie können den Zugriff auf die Benutzeroberflächen und APIs auf StorageGRID Admin Nodes steuern, indem Sie bestimmte Ports an der externen Firewall öffnen oder schließen. Beispielsweise kann verhindert werden, dass Mandanten sich über die Firewall mit dem Grid Manager verbinden, zusätzlich zu anderen Methoden zur Steuerung des Systemzugriffs.

Wenn die StorageGRID interne Firewall konfiguriert werden soll, siehe "${post_edited_translations.segment}".

Port	Beschreibung	${post_edited_translations.segment}
443	${post_edited_translations.segment}	Webbrowser und Management-API-Clients können auf den Grid Manager, die Grid Management API, den Tenant Manager und die Tenant Management API zugreifen. ${post_edited_translations.segment}
8443	Eingeschränkter Grid Manager Port auf Admin-Knoten	• Webbrowser und Management-API-Clients können über HTTPS auf den Grid Manager und die Grid Management API zugreifen. • Webbrowser und Management-API-Clients haben keinen Zugriff auf den Tenant Manager oder die Tenant Management API. • Anfragen für interne Inhalte werden abgelehnt.
9443	Eingeschränkter Mandantenmanager-Port auf Admin-Knoten	• Webbrowser und Management-API-Clients können über HTTPS auf den Tenant Manager und die Tenant Management API zugreifen. • Webbrowser und Management-API-Clients können nicht auf den Grid Manager oder die Grid Management API zugreifen. • Anfragen für interne Inhalte werden abgelehnt.

Single sign-on (SSO) ist auf den eingeschränkten Ports von Grid Manager oder Tenant Manager nicht verfügbar. Der Standard-HTTPS-Port (443) muss verwendet werden, wenn Benutzer sich mit Single sign-on authentifizieren sollen.

Verwandte Informationen

- "Anmeldung beim Grid Manager"
- "Mandantenkonto erstellen"
- "${post_edited_translations.segment}"

Interne Firewall-Steuerungen in StorageGRID verwalten

StorageGRID umfasst auf jedem Knoten eine interne Firewall, die die Sicherheit Ihres Grids erhöht, indem sie die Kontrolle über den Netzwerkzugriff auf den Knoten ermöglicht. Mit der Firewall lässt sich der Netzwerkzugriff auf alle Ports außer denen, die für Ihre spezifische Grid-Bereitstellung erforderlich sind, verhindern. Die auf der Firewall-Steuerungsseite vorgenommenen Konfigurationsänderungen werden auf jeden Knoten angewendet.

Auf der Firewall-Steuerungsseite stehen drei Registerkarten zur Verfügung, mit denen der benötigte Zugriff für Ihr Grid angepasst werden kann.

- **Liste privilegierter Adressen**: Diese Registerkarte ermöglicht ausgewählten Zugriff auf geschlossene Ports. IP-Adressen oder Subnetze in CIDR-Notation können hinzugefügt werden, die auf Ports zugreifen

dürfen, die über die Registerkarte „Externen Zugriff verwalten“ geschlossen wurden.

- **Externen Zugriff verwalten**: Diese Registerkarte dient dazu, standardmäßig geöffnete Ports zu schließen oder zuvor geschlossene Ports wieder zu öffnen.
- **Nicht vertrauenswürdiges Client-Netzwerk**: In diesem Tab kann angegeben werden, ob ein Knoten eingehenden Datenverkehr aus dem Client-Netzwerk vertraut.

  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 an Load-Balancer-Endpunktports, die auf diesem Knoten konfiguriert sind (globale, Knoteninterface- und Knotentyp-gebundene Endpunkte).
  - Die Endpunktports des Load Balancers sind die einzigen offenen Ports in nicht vertrauenswürdigen Client-Netzwerken, unabhängig von den Einstellungen auf der Registerkarte „Externe Netzwerke verwalten“.
  - Wenn die Verbindung als vertrauenswürdig eingestuft ist, sind alle unter der Registerkarte „Externen Zugriff verwalten“ geöffneten Ports sowie alle auf dem Client Network geöffneten Load-Balancer-Endpunkte zugänglich.

> Die Einstellungen, die Sie auf einem Tab vornehmen, können sich auf die Zugriffsänderungen auswirken, die Sie auf einem anderen Tab vornehmen. Es empfiehlt sich, die Einstellungen auf allen Tabs zu überprüfen, damit Ihr Netzwerk wie erwartet funktioniert.

Informationen zur Konfiguration der internen Firewall-Steuerung sind unter "Firewall-Steuerung konfigurieren" zu finden.

Weitere Informationen zu externen Firewalls und Netzwerksicherheit sind unter "Zugriffskontrolle an der externen Firewall" zu finden.

Registerkarten „Liste privilegierter Adressen“ und „Externen Zugriff verwalten“

Die Registerkarte „Privilegierte Adressenliste“ ermöglicht die Registrierung einer oder mehrerer IP-Adressen, denen Zugriff auf geschlossene Grid-Ports gewährt wird. Die Registerkarte „Externen Zugriff verwalten“ ermöglicht das Schließen des externen Zugriffs auf ausgewählte externe Ports oder alle offenen externen Ports (externe Ports sind Ports, die standardmäßig für Nicht-Grid-Knoten zugänglich sind). Diese beiden Registerkarten können häufig zusammen verwendet werden, um den genauen Netzwerkzugriff zu definieren, der für Ihr Grid zulässig sein soll.

> Privilegierte IP-Adressen haben standardmäßig keinen Zugriff auf interne Grid-Ports.

Beispiel 1: Nutzung eines Jump-Hosts für Wartungsaufgaben

Angenommen, Sie möchten einen Jump-Host (einen sicherheitsgehärteten Host) für die Netzwerkadministration verwenden. Dazu könnten folgende allgemeine Schritte genutzt werden:

1. ${post_edited_translations.segment}
2. Auf der Registerkarte „Externen Zugriff verwalten“ lassen sich alle Ports blockieren.

Fügen Sie die privilegierte IP-Adresse hinzu, bevor Sie die Ports 443 und 8443 blockieren. Alle Benutzer, die derzeit über einen 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.

Nach dem Speichern Ihrer Konfiguration werden alle externen Ports auf dem Admin Node in Ihrem Grid für alle Hosts außer dem Jump Host blockiert. Anschließend kann der Jump Host genutzt werden, um Wartungsaufgaben in Ihrem Grid sicherer durchzuführen.

Beispiel 2: Sensible Ports sperren

Angenommen, Sie möchten sensible Ports und den Dienst auf diesem Port absichern. Dazu könnten die folgenden allgemeinen Schritte genutzt werden:

1. Die Registerkarte „Liste privilegierter Adressen“ ermöglicht den Zugriff ausschließlich für die Hosts, die Zugriff auf den Dienst benötigen.
2. Auf der Registerkarte „Externen Zugriff verwalten“ lassen sich alle Ports blockieren.

Fügen Sie die privilegierte IP-Adresse hinzu, bevor der Zugriff auf die Ports blockiert wird, die für den Zugriff auf Grid Manager und Tenant Manager zugewiesen sind (voreingestellte Ports sind 443 und 8443). Alle Benutzer, die derzeit über einen blockierten Port verbunden sind, einschließlich Ihnen, verlieren den Zugriff auf Grid Manager, sofern ihre IP-Adresse nicht der Liste der privilegierten Adressen hinzugefügt wurde.

Nach dem Speichern Ihrer Konfiguration stehen der sensible Port und der darauf befindliche Dienst Hosts auf der Liste privilegierter Adressen zur Verfügung. Allen anderen Hosts wird der Zugriff auf den Dienst verweigert, unabhängig davon, über welche Schnittstelle die Anfrage erfolgt.

Beispiel 3: Deaktivieren des Zugriffs auf nicht verwendete Dienste

Auf Netzwerkebene könnten einige Dienste deaktiviert werden, die Sie nicht zu verwenden beabsichtigen. Beispielsweise lässt sich HTTP S3-Client-Datenverkehr blockieren, indem auf der Registerkarte „Externen Zugriff verwalten“ der Schalter zum Sperren von Port 18084 verwendet wird.

Registerkarte „Nicht vertrauenswürdige Clientnetzwerke“

Wenn Sie ein Client-Netzwerk verwenden, kann StorageGRID vor feindlichen Angriffen geschützt werden, indem eingehender Client-Datenverkehr nur an explizit konfigurierten Endpunkten akzeptiert wird.

Standardmäßig ist das Client-Netzwerk auf jedem Grid-Knoten *vertrauenswürdig*. Das heißt, StorageGRID vertraut standardmäßig eingehenden Verbindungen zu jedem Grid-Knoten auf allen "verfügbare externe Anschlüsse".

Sie können die Bedrohung durch Angriffe auf Ihr StorageGRID System verringern, indem Sie das Client-Netzwerk jedes Knotens als *nicht vertrauenswürdig* festlegen. Ist das Client-Netzwerk eines Knotens nicht vertrauenswürdig, akzeptiert der Knoten eingehende Verbindungen nur auf Ports, die explizit als Load Balancer-Endpunkte konfiguriert sind. Siehe "Load Balancer-Endpunkte konfigurieren" und "Firewall-Steuerung konfigurieren".

Beispiel 1: Der Gateway-Knoten akzeptiert nur HTTPS S3-Anfragen.

Angenommen, Sie möchten, dass ein Gateway Node den gesamten eingehenden Datenverkehr im Client-Netzwerk mit Ausnahme von HTTPS S3-Anfragen ablehnt. Dazu sind die folgenden allgemeinen Schritte

erforderlich:

1. Auf der "Load Balancer Endpunkte" Seite einen Load-Balancer-Endpunkt für S3 über HTTPS auf Port 443 konfigurieren.
2. Auf der Firewall-Steuerungsseite wird „Nicht vertrauenswürdig“ ausgewählt, um anzugeben, dass das Client-Netzwerk auf dem Gateway-Knoten nicht vertrauenswürdig ist.

Nach dem Speichern Ihrer Konfiguration wird der gesamte eingehende Datenverkehr im Client-Netzwerk des Gateway-Knotens verworfen, mit Ausnahme von HTTPS S3-Anfragen auf Port 443 und ICMP-Echo (Ping)-Anfragen.

Beispiel 2: Der Storage Node sendet S3-Plattformdienste-Anfragen.

Angenommen, Sie möchten ausgehenden S3-Plattformdienste-Datenverkehr von einem Storage Node aktivieren, aber eingehende Verbindungen zu diesem Storage Node im Client-Netzwerk verhindern. Dazu ist folgender allgemeiner Schritt erforderlich:

- Auf der Registerkarte „Nicht vertrauenswürdige Clientnetzwerke“ der Firewall-Steuerungsseite wird angegeben, dass das Clientnetzwerk auf dem Storage Node nicht vertrauenswürdig ist.

Nach dem Speichern Ihrer Konfiguration akzeptiert der Storage Node keinen eingehenden Datenverkehr mehr im Client Network, lässt aber weiterhin ausgehende Anfragen an konfigurierte Plattformdienstziele zu.

Beispiel 3: Beschränkung des Zugriffs auf Grid Manager auf ein Subnetz

Angenommen, Sie möchten den Zugriff auf Grid Manager nur in einem bestimmten Subnetz zulassen. Dafür sind die folgenden Schritte erforderlich:

1. Das Clientnetzwerk der Admin-Knoten wird mit dem Subnetz verbunden.
2. Die Registerkarte „Nicht vertrauenswürdiges Clientnetzwerk“ dient zur Konfiguration des Clientnetzwerks als nicht vertrauenswürdig.
3. Wenn ein Managementoberfläche Load-Balancer-Endpunkt erstellt wird, ist der Port einzugeben und die Managementoberfläche auszuwählen, auf die der Port zugreift.
4. **Ja** für Nicht vertrauenswürdiges Clientnetzwerk auswählen.
5. Auf der Registerkarte „Externen Zugriff verwalten“ lassen sich alle externen Ports blockieren (mit oder ohne festgelegte privilegierte IP-Adressen für Hosts außerhalb dieses Subnetzes).

Nach dem Speichern Ihrer Konfiguration können nur Hosts im angegebenen Subnetz auf den Grid Manager zugreifen. Alle anderen Hosts sind gesperrt.

Konfigurieren Sie die interne Firewall von StorageGRID

Die StorageGRID Firewall kann so konfiguriert werden, dass der Netzwerkzugriff auf bestimmte Ports Ihrer StorageGRID Knoten gesteuert wird.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Du hast "spezifische Zugriffsberechtigungen".
- Sie haben die Informationen in "Firewall-Steuerung verwalten" und "Netzwerkrichtlinien" überprüft.
- Wenn ein Admin-Knoten oder Gateway-Knoten eingehenden Datenverkehr nur über explizit konfigurierte Endpunkte akzeptieren soll, sind die Load-Balancer-Endpunkte definiert.

Bei einer Änderung der Konfiguration des Client-Netzwerks können bestehende Client-Verbindungen fehlschlagen, wenn Load Balancer-Endpunkte nicht konfiguriert wurden.

Über diese Aufgabe

StorageGRID verfügt über eine interne Firewall auf jedem Knoten, die es ermöglicht, einige der Ports auf den Knoten Ihres Grids zu öffnen oder zu schließen. Mit den Firewall-Steuerungsregisterkarten lassen sich Ports, die im Grid Network, Admin Network und Client Network standardmäßig geöffnet sind, öffnen oder schließen. Es kann außerdem eine Liste privilegierter IP-Adressen erstellt werden, die auf geschlossene Grid-Ports zugreifen können. Bei Verwendung eines Client Network kann festgelegt werden, ob ein Knoten eingehenden Datenverkehr aus dem Client Network vertraut, und der Zugriff auf bestimmte Ports im Client Network kann konfiguriert werden.

Die Beschränkung der für IP-Adressen außerhalb Ihres Grids geöffneten Ports auf das absolut Notwendige erhöht die Sicherheit Ihres Grids. Die Einstellungen auf den drei Registerkarten der Firewall-Steuerung sorgen dafür, dass nur die benötigten Ports geöffnet sind.

Weitere Informationen zur Verwendung von Firewall-Steuerelementen, einschließlich Beispielen, sind unter "Firewall-Steuerung verwalten" zu finden.

Weitere Informationen zu externen Firewalls und Netzwerksicherheit sind unter "Zugriffskontrolle an der externen Firewall" zu finden.

Firewall-Steuerungen für den Zugriff

Schritte

1. **Konfiguration** > **Sicherheit** > **Firewall-Steuerung** auswählen.

   Die drei Registerkarten auf dieser Seite sind in "Firewall-Steuerung verwalten" beschrieben.

2. Jede Registerkarte kann zur Konfiguration der Firewall-Steuerung ausgewählt werden.

   Sie können diese Registerkarten in beliebiger Reihenfolge verwenden. Die Konfigurationen, die Sie auf einer Registerkarte vornehmen, schränken die Möglichkeiten auf den anderen Registerkarten nicht ein, allerdings können Konfigurationsänderungen auf einer Registerkarte das Verhalten von Ports beeinflussen, die auf anderen Registerkarten konfiguriert sind.

Liste privilegierter Adressen

Die Registerkarte „Privilegierte Adressliste“ dient dazu, Hosts den Zugriff auf Ports zu ermöglichen, die standardmäßig geschlossen sind oder durch Einstellungen auf der Registerkarte „Externen Zugriff verwalten“ geschlossen wurden.

Privilegierte IP-Adressen und Subnetze haben standardmäßig keinen internen Grid-Zugriff. Auch Load Balancer-Endpunkte und zusätzliche Ports, die im Tab „Privilegierte Adressenliste“ geöffnet sind, sind zugänglich, selbst wenn sie im Tab „Externen Zugriff verwalten“ blockiert sind.

Die Einstellungen auf der Registerkarte „Privilegierte Adressliste“ können die Einstellungen auf der Registerkarte „Untrusted Client Network“ nicht überschreiben.

Schritte

1. Auf der Registerkarte „Liste privilegierter Adressen“ die Adresse oder das IP-Subnetz eingeben, für das Sie den Zugriff auf geschlossene Ports gewähren möchten.

2. Optional kann **Weitere IP-Adresse oder Subnetz in CIDR-Notation hinzufügen** ausgewählt werden, um zusätzliche privilegierte Clients hinzuzufügen.

   So wenige Adressen wie möglich sollten zur privilegierten Liste hinzugefügt werden.

3. Optional kann **Privilegierten IP-Adressen der Zugriff auf interne StorageGRID-Ports erlaubt werden**. Siehe "StorageGRID interne Ports".

   Diese Option hebt einige Schutzmechanismen für interne Dienste auf. Wenn möglich, sollte sie deaktiviert bleiben.

4. **Speichern** auswählen.

Externen Zugriff verwalten

Wenn ein Port im Tab „Externen Zugriff verwalten“ geschlossen wird, kann auf den Port von keiner Nicht-Grid-IP-Adresse zugegriffen werden, es sei denn, die IP-Adresse wird der Liste der privilegierten Adressen hinzugefügt. Es können nur Ports geschlossen werden, die standardmäßig geöffnet sind, und nur Ports geöffnet werden, die zuvor geschlossen wurden.

Die Einstellungen auf der Registerkarte „Externen Zugriff verwalten“ können die Einstellungen auf der Registerkarte „Nicht vertrauenswürdiges Clientnetzwerk“ nicht überschreiben. Wenn ein Knoten beispielsweise als nicht vertrauenswürdig eingestuft ist, wird Port SSH/22 im Clientnetzwerk blockiert, selbst wenn er auf der Registerkarte „Externen Zugriff verwalten“ geöffnet ist. Die Einstellungen auf der Registerkarte „Nicht vertrauenswürdiges Clientnetzwerk“ überschreiben geschlossene Ports (wie 443, 8443, 9443) im Clientnetzwerk.

Schritte

1. **Externen Zugriff verwalten** auswählen. Die Registerkarte zeigt eine Tabelle mit allen externen Ports (Ports, die standardmäßig von Nicht-Grid-Knoten zugänglich sind) für die Knoten in Ihrem Grid.
2. Die Ports, die geöffnet oder geschlossen sein sollen, lassen sich mit den folgenden Optionen konfigurieren:
   - Der Schalter neben jedem Port öffnet oder schließt den ausgewählten Port.
   - **Alle angezeigten Ports öffnen** öffnet alle in der Tabelle aufgeführten Ports.
   - **Alle angezeigten Ports schließen** schließt alle in der Tabelle aufgeführten Ports.

   Wenn Sie die Grid Manager Ports 443 oder 8443 schließen, verlieren alle Benutzer, die derzeit über einen blockierten Port verbunden sind, einschließlich Ihnen, den Zugriff auf Grid Manager, es sei denn, ihre IP-Adresse wurde der Privileged address list 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 beliebigen externen Port zu finden, indem Sie eine Portnummer eingeben. Es kann auch eine Teil-Portnummer eingegeben werden. Wenn zum Beispiel **2** eingegeben wird, werden alle Ports angezeigt, deren Name die Zeichenfolge „2“ enthält.

3. **Speichern** auswählen

Nicht vertrauenswürdiges Client-Netzwerk

Wenn das Clientnetzwerk eines Knotens nicht vertrauenswürdig ist, akzeptiert der Knoten eingehenden Datenverkehr nur auf Ports, die als Load-Balancer-Endpunkte konfiguriert sind, und optional auf zusätzlichen Ports, die Sie auf dieser Registerkarte auswählen. Auf dieser Registerkarte lässt sich außerdem die Standardeinstellung für neue Knoten festlegen, die bei einer Erweiterung hinzugefügt werden.

> Bestehende Clientverbindungen können fehlschlagen, wenn Load-Balancer-Endpunkte nicht konfiguriert wurden.

Die Konfigurationsänderungen, die Sie auf der Registerkarte **Nicht vertrauenswürdiges Clientnetzwerk** vornehmen, überschreiben die Einstellungen auf der Registerkarte **Externen Zugriff verwalten**.

Schritte

1. **Nicht vertrauenswürdiges Clientnetzwerk** auswählen.
2. Im Abschnitt „Standardeinstellungen für neue Knoten festlegen“ ist anzugeben, welche Standardeinstellung gelten soll, wenn im Rahmen einer Erweiterungsprozedur neue Knoten zum Grid hinzugefügt werden.
   - **Vertrauenswürdig** (Standard): Wenn ein Knoten in einer Erweiterung hinzugefügt wird, ist sein Client-Netzwerk vertrauenswürdig.
   - **Nicht vertrauenswürdig**: Wenn ein Knoten in einer Erweiterung hinzugefügt wird, ist sein Client-Netzwerk nicht vertrauenswürdig.

     Bei Bedarf kann zu diesem Tab zurückgekehrt werden, um die Einstellung für einen bestimmten neuen Knoten zu ändern.

     > Diese Einstellung hat keine Auswirkungen auf die bestehenden Knoten in Ihrem StorageGRID System.

3. Verwenden Sie die folgenden Optionen, um die Knoten auszuwählen, die Clientverbindungen nur an explizit konfigurierten Load Balancer-Endpunkten oder an zusätzlich ausgewählten Ports zulassen:
   - **Angezeigte Knoten als nicht vertrauenswürdig einstufen** auswählen, um alle in der Tabelle angezeigten Knoten zur Liste „Nicht vertrauenswürdiges Clientnetzwerk“ hinzuzufügen.
   - **Angezeigten Knoten vertrauen** auswählen, um alle in der Tabelle angezeigten Knoten aus der Liste „Nicht vertrauenswürdiges Clientnetzwerk“ zu entfernen.
   - Verwenden Sie den Schalter neben jedem Knoten, um das Client-Netzwerk für den ausgewählten Knoten als Trusted oder Untrusted festzulegen.

     Beispielsweise kann **Auf angezeigten Knoten als nicht vertrauenswürdig einstufen** ausgewählt werden, um alle Knoten zur Liste „Nicht vertrauenswürdiges Clientnetzwerk“ hinzuzufügen, und anschließend kann der Schalter neben einem einzelnen Knoten verwendet werden, um diesen einzelnen Knoten zur Liste „Vertrauenswürdiges Clientnetzwerk“ hinzuzufügen.

     > Verwenden Sie die Bildlaufleiste auf der rechten Seite der Tabelle, um sicherzustellen, dass Sie alle verfügbaren Nodes angezeigt haben. Das Suchfeld kann verwendet werden, um die Einstellungen eines beliebigen Nodes durch Eingabe des Node-Namens zu finden. Es kann auch ein Teil des Namens eingegeben werden. Wenn zum Beispiel **GW** eingegeben wird, werden alle Nodes angezeigt, deren Name die Zeichenfolge "GW" enthält.

4. **Speichern** auswählen.

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

Mandanten verwalten

Mandantenkonten in StorageGRID

Ein Mandantenkonto ermöglicht die Nutzung der Simple Storage Service (S3) REST API zum Speichern und Abrufen von Objekten in einem StorageGRID-System.

Swift-Details wurden aus dieser Version der Dokumentationsseite entfernt. Siehe "StorageGRID 11.8: Mandantenverwaltung".

Als Grid-Administrator erstellen und verwalten Sie die Mandantenkonten, die S3-Clients zum Speichern und Abrufen von Objekten verwenden.

Jedes Mandantenkonto verfügt über föderierte oder lokale Gruppen, Benutzer, S3 Buckets und Objekte.

Mandantenkonten können verwendet werden, um gespeicherte Objekte nach verschiedenen Entitäten zu trennen. Beispielsweise können mehrere Mandantenkonten für einen der folgenden Anwendungsfälle verwendet werden:

- **Anwendungsfall im Unternehmensumfeld:** Bei der Administration eines StorageGRID-Systems in einer Unternehmensanwendung kann es sinnvoll sein, den Objektspeicher des Grids nach den verschiedenen Abteilungen Ihrer Organisation zu trennen. In diesem Fall könnten Mandantenkonten für die Marketingabteilung, die Kundensupportabteilung, die Personalabteilung und so weiter erstellt werden.

  Wenn Sie das S3-Client-Protokoll verwenden, können Sie S3-Buckets und Bucket-Richtlinien verwenden, um Objekte zwischen den Abteilungen in einem Unternehmen zu trennen. Sie müssen keine Mandantenkonten verwenden. Siehe die Anweisungen zur Implementierung von "S3 Buckets und Bucket-Richtlinien" für weitere Informationen.

- **Anwendungsfall für Dienstanbieter:** Wenn Sie ein StorageGRID-System als Dienstanbieter verwalten, kann der Objektspeicher des Grids nach den verschiedenen Entitäten getrennt werden, die den Speicherplatz in Ihrem Grid mieten. In diesem Fall werden Mandantenkonten für Company A, Company B, Company C und so weiter erstellt.

Weitere Informationen finden sich unter "Ein Mandantenkonto verwenden".

Wie wird ein Mandantenkonto erstellt?

Verwenden Sie den Grid Manager, um ein Mandantenkonto zu erstellen. Beim Erstellen eines Mandantenkontos werden die folgenden Informationen angegeben:

- Grundlegende Informationen einschließlich Mandantenname, Clienttyp (S3) und optionalem Speicherplatzkontingent.
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

Zusätzlich kann die Einstellung „S3 Object Lock“ für das StorageGRID System aktiviert werden, falls S3-Mandantenkonten regulatorischen Anforderungen entsprechen müssen. Wenn S3 Object Lock aktiviert ist, können alle S3-Mandantenkonten konforme Buckets erstellen und verwalten.

Wofür wird der Tenant Manager verwendet?

${post_edited_translations.segment}

- Identitätsföderation einrichten (sofern die Identitätsquelle nicht mit dem Grid geteilt wird)
- Gruppen und Benutzer verwalten
- Grid Federation für die Kontoklonung und die gridübergreifende Replikation verwenden
- S3-Zugriffsschlüssel verwalten
- S3 Buckets erstellen und verwalten
- S3-Plattformdienste verwenden
- S3 Select nutzen
- Speichernutzung überwachen

S3-Tenant-Benutzer können zwar mit dem Tenant Manager S3-Zugriffsschlüssel und Buckets erstellen und verwalten, sie müssen jedoch eine S3-Clientanwendung verwenden, um Objekte zu importieren und zu verwalten. Weitere Informationen sind unter "S3 REST-API verwenden" zu finden.

Erstellen Sie ein StorageGRID-Tenant-Konto

Sie müssen mindestens ein Mandantenkonto erstellen, um den Zugriff auf den Speicher in Ihrem StorageGRID System zu steuern.

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, einer Administratorgruppe mit der Berechtigung Root-Zugriff angehört.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Root-Zugriff oder Berechtigung für Mandantenkonten".
- Wenn das Mandantenkonto die für den Grid Manager konfigurierte Identitätsquelle verwendet und Sie einer Verbundgruppe Root-Zugriffsberechtigungen für das Mandantenkonto erteilen möchten, wurde diese Verbundgruppe in den Grid Manager importiert. Es ist nicht erforderlich, dieser Administratorgruppe Grid Manager-Berechtigungen zuzuweisen. Siehe "${post_edited_translations.segment}".
- Wenn Sie einem S3-Mandanten ermöglichen möchten, Kontodaten zu klonen und Bucket-Objekte mithilfe einer Grid-Federation-Verbindung in ein anderes Grid zu replizieren:
  - Du hast "Die Grid Federation-Verbindung wurde konfiguriert.".
  - Der Verbindungsstatus ist **Verbunden**.
  - Sie verfügen über Root-Zugriffsberechtigung.
  - Sie haben die Überlegungen zu "Verwaltung der zugelassenen Mandanten für die Grid Federation" überprüft.
  - Wenn das Mandantenkonto die für Grid Manager konfigurierte Identitätsquelle verwendet, wurde

dieselbe föderierte Gruppe in Grid Manager auf beiden Grids importiert.

Wenn der Mandant erstellt wird, wird diese Gruppe ausgewählt, damit sie die anfängliche Root-Zugriffsberechtigung sowohl für das Quell- als auch für das Zielmandantenkonto erhält.

Wenn diese Administratorgruppe auf beiden Grids vor der Erstellung des Mandanten nicht existiert, wird der Mandant nicht an das Ziel repliziert.

Assistenten aufrufen

Schritte

1. **Tenants** auswählen.
2. Wählen Sie **Create**.

Details eingeben

Schritte

1. Details für den Mandanten eingeben.

Feld	Beschreibung
Name	Ein Name für das Mandantenkonto. Mandantennamen müssen nicht eindeutig sein. Bei der Erstellung des Mandantenkontos erhält dieses eine eindeutige, 20-stellige Konto-ID.
Beschreibung (optional)	Eine Beschreibung zur Identifizierung des Tenants. Wenn Sie einen Mandanten erstellen, der eine Grid-Federation-Verbindung verwendet, kann dieses Feld optional genutzt werden, um zu identifizieren, welcher der Quellmandant und welcher der Zielmandant ist. Beispielsweise erscheint diese Beschreibung für einen auf Grid 1 erstellten Mandanten auch bei dem auf Grid 2 replizierten Mandanten: „This tenant was created on Grid 1.“
Clienttyp	Muss **S3** sein.
Speicherkontingent (optional)	Wenn für diesen Mandanten ein Speicherkontingent festgelegt werden soll, sind ein numerischer Wert für das Kontingent und die Einheiten anzugeben.

2. Wählen Sie **Weiter**.

Berechtigungen auswählen

Schritte

1. Optional können die grundlegenden Berechtigungen ausgewählt werden, die dieser Mandant haben soll.

Für einige dieser Berechtigungen gelten zusätzliche Anforderungen. Details dazu erhalten Sie durch Auswahl des Hilfesymbols neben der jeweiligen Berechtigung.

Berechtigung	Falls ausgewählt…
Plattformdienste zulassen	Der Mandant kann S3-Plattformdienste wie CloudMirror nutzen. Siehe "Plattformdienste für S3-Mandantenkonten verwalten".
Eigene Identitätsquelle verwenden	Der Mandant kann seine eigene Identitätsquelle für Verbundgruppen und Benutzer konfigurieren und verwalten. Diese Option ist deaktiviert, wenn Sie "SSO konfiguriert" für Ihr StorageGRID System haben.
S3 Select zulassen	Der Mandant kann S3 SelectObjectContent API-Anfragen stellen, um Objektdaten zu filtern und abzurufen. Siehe "S3 Select für Mandantenkonten verwalten". **Wichtig**: SelectObjectContent-Anfragen können die Leistung des Load-Balancers für alle S3 Clients und alle Mandanten beeinträchtigen. Diese Funktion sollte nur bei Bedarf und nur für vertrauenswürdige Mandanten aktiviert werden.

2. Optional können die erweiterten Berechtigungen ausgewählt werden, die dieser Mandant haben soll.

Berechtigung	Falls ausgewählt…
Grid Federation Verbindung	Der Mieter kann eine Grid-Federation-Verbindung nutzen, die: • Veranlasst, dass dieser Mandant sowie alle dem Konto hinzugefügten Mandantengruppen und Benutzer von diesem Grid (dem *Quell-Grid*) auf das andere Grid in der ausgewählten Verbindung (das *Ziel-Grid*) geklont werden. • Ermöglicht diesem Mandanten die Konfiguration der netzübergreifenden Replikation zwischen entsprechenden Buckets auf jedem Grid. Siehe "Verwaltung der zulässigen Mandanten für die Grid Federation".
S3 Object Lock	Dem Mandanten die Nutzung bestimmter Funktionen von S3 Object Lock ermöglichen: • **Maximale Aufbewahrungsdauer festlegen** definiert, wie lange neue Objekte, die diesem Bucket hinzugefügt werden, ab dem Zeitpunkt ihrer Aufnahme aufbewahrt werden. • **Konformitätsmodus** verhindert, dass Benutzer geschützte Objektversionen während der Aufbewahrungsfrist überschreiben oder löschen.

3. Wählen Sie **Weiter**.

Root-Zugriff definieren und Mandanten erstellen

Schritte

1. Root-Zugriff für das Mandantenkonto wird definiert, abhängig davon, ob Ihr StorageGRID System Identitätsföderation, Single Sign-On (SSO) oder beides verwendet.

Option	Tun Sie Folgendes
Wenn die Identitätsföderation nicht aktiviert ist	Das Passwort, das beim Anmelden beim Mandanten als lokaler Root-Benutzer verwendet wird, angeben.
Wenn die Identitätsföderation aktiviert ist	a. Wählen Sie eine vorhandene Verbundgruppe aus, die die Root-Zugriffsberechtigung für den Mandanten erhält. b. Optional kann das Passwort angegeben werden, das beim Anmelden beim Mandanten als lokaler Root-Benutzer verwendet wird.
Wenn sowohl Identitätsföderation als auch Single Sign-On (SSO) aktiviert sind	Wählen Sie eine vorhandene Verbundgruppe aus, der Root-Zugriff für den Mandanten gewährt wird. Lokale Benutzer können sich nicht anmelden.

2. **Mandant erstellen** auswählen.

   Es erscheint eine Erfolgsmeldung, und der neue Tenant wird auf der Tenants-Seite aufgeführt. Wie Tenant-Details angezeigt und Tenant-Aktivitäten überwacht werden können, ist unter "Mieteraktivitäten überwachen" zu finden.

   > Das Anwenden der Mandanteneinstellungen im gesamten Grid kann abhängig von der Netzwerkverbindung, dem Knotenstatus und den Cassandra-Operationen 15 Minuten oder länger in Anspruch nehmen.

3. Wenn die Berechtigung **Grid-Federationsverbindung verwenden** für den Mandanten ausgewählt wurde:
   a. Bestätigt wird, dass ein identischer Mandant in das andere Grid der Verbindung repliziert wurde. Die Mandanten in beiden Grids verfügen über dieselbe 20-stellige Konto-ID, denselben Namen, dieselbe Beschreibung, dasselbe Kontingent und dieselben Berechtigungen.

      > Wenn die Fehlermeldung „Tenant ohne Klon erstellt“ angezeigt wird, finden sich die Anweisungen in "Fehler in der Grid-Federation beheben".

   b. Wenn bei der Definition von Root-Zugriff ein lokales Root-Benutzerpasswort angegeben wurde, "das Passwort für den lokalen Root-Benutzer ändern" für den replizierten Mandanten.

      > Ein lokaler Root-Benutzer kann sich erst beim Tenant Manager im Zielnetz anmelden, nachdem das Passwort geändert wurde.

Anmeldung beim Tenant (optional)

Bei Bedarf ist eine Anmeldung beim neuen Mandanten jetzt möglich, um die Konfiguration abzuschließen, oder eine spätere Anmeldung beim Mandanten ist möglich. Die Anmeldeschritte hängen davon ab, ob Sie beim Grid Manager über den Standardport (443) oder über einen eingeschränkten Port angemeldet sind. Siehe "Zugriffskontrolle an der externen Firewall".

Jetzt anmelden

Wenn Sie … verwenden	Folgendes ist zu tun…
Port 443 und ein Passwort für den lokalen Root-Benutzer wird festgelegt	1. **Als Root anmelden** auswählen. Nach der Anmeldung erscheinen Links zum Konfigurieren von Buckets, Identitätsföderation, Gruppen und Benutzern. 2. Wählen Sie die Links aus, um das Mandantenkonto zu konfigurieren. Jeder Link öffnet die entsprechende Seite im Tenant Manager. Zum Ausfüllen der Seite siehe "Anleitung zur Verwendung von Mandantenkonten".
Port 443 und es wurde kein Passwort für den lokalen Root-Benutzer festgelegt	**Anmelden** auswählen und die Anmeldeinformationen für einen Benutzer in der Root access föderierten Gruppe eingeben.
Ein eingeschränkter Port	1. **Fertigstellen** auswählen 2. **Restricted** in der Mandantentabelle bietet weitere Informationen zum Zugriff auf dieses Mandantenkonto. Die URL für den Tenant Manager hat folgendes Format: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* ist ein vollqualifizierter Domainname oder die IP-Adresse eines Admin-Knotens ◦ *port* ist der nur für Mieter zugängliche Port ◦ *20-digit-account-id* ist die eindeutige Konto-ID des Mandanten

Später anmelden

Wenn Sie … verwenden	Führen Sie eine der folgenden Aktionen aus…
Port 443	• Im Grid Manager **Mandanten** auswählen und rechts neben dem Mandantennamen **Anmelden** auswählen. • 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 vollqualifizierter Domainname oder die IP-Adresse eines Admin-Knotens ◦ *20-digit-account-id* ist die eindeutige Konto-ID des Mandanten

Wenn Sie … verwenden	Führen Sie eine der folgenden Aktionen aus…
Ein eingeschränkter Port	• Im Grid Manager **Mandanten** auswählen und anschließend **Eingeschränkt** wählen. • 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 vollqualifizierter Domainname oder die IP-Adresse eines Admin-Knotens ◦ *port* ist der nur für Mieter zugängliche beschränkte Port ◦ *20-digit-account-id* ist die eindeutige Konto-ID des Mandanten

Den Mandanten konfigurieren

Die Anweisungen in "Ein Mandantenkonto verwenden" enthalten Informationen zur Verwaltung von Mandantengruppen und Benutzern, S3-Zugriffsschlüsseln, Buckets, Plattformdiensten sowie Kontoklonierung und gridübergreifender Replikation.

Bearbeiten eines StorageGRID-Tenant-Kontos

Sie können ein Mandantenkonto bearbeiten, um den Anzeigenamen, das Speicherkontingent oder die Mandantenberechtigungen zu ändern.

Besitzt ein Mandant die Berechtigung **Grid-Federationsverbindung verwenden**, können Mandantendetails in beiden Grids der Verbindung bearbeitet werden. Änderungen, die in einem Grid der Verbindung vorgenommen werden, werden jedoch nicht in das andere Grid übernommen. Wenn die Mandantendetails in beiden Grids exakt synchron gehalten werden sollen, sind die gleichen Änderungen in beiden Grids vorzunehmen. Siehe "Verwalten der zulässigen Mandanten für die Grid Federation Verbindung".

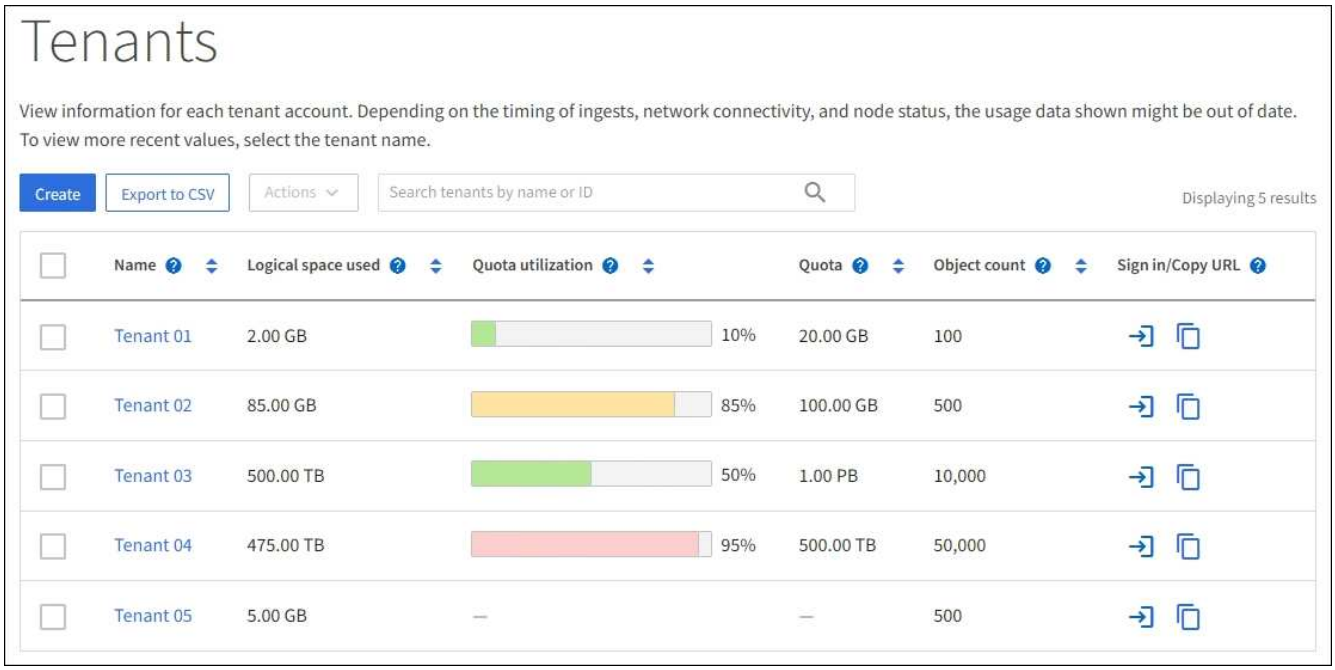
Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Root-Zugriff oder Berechtigung für Mandantenkonten".

Das Anwenden der Mandanteneinstellungen im gesamten Grid kann abhängig von der Netzwerkverbindung, dem Knotenstatus und den Cassandra-Operationen 15 Minuten oder länger in Anspruch nehmen.

Schritte

1. **Tenants** auswählen.



2. Das Mandantenkonto, das bearbeitet werden soll, auswählen.

   Im Suchfeld kann nach einem Mieter anhand des Namens oder der Mieter-ID gesucht werden.

3. Wählen Sie den Mieter aus. Folgende Möglichkeiten stehen zur Verfügung:
   - Aktivieren Sie das Kontrollkästchen für den Mandanten und wählen Sie **Aktionen** > **Bearbeiten**.
   - Wählen Sie den Namen des Mandanten aus, um die Detailseite anzuzeigen, und wählen Sie **Bearbeiten**.
4. Optional können die Werte für diese Felder geändert werden:
   - **Name**
   - **Beschreibung**
   - **Speicherkontingent**
5. Wählen Sie **Weiter**.
6. Wählen Sie die Berechtigungen für das Mandantenkonto aus oder heben Sie die Auswahl auf.
   - Wenn Sie die **Plattformdienste** für einen Mandanten deaktivieren, der diese bereits nutzt, funktionieren die für seine S3-Buckets konfigurierten Dienste nicht mehr. Dem Mandanten wird keine Fehlermeldung angezeigt. Wenn der Mandant beispielsweise die CloudMirror Replikation für einen S3-Bucket konfiguriert hat, kann er weiterhin Objekte im Bucket speichern, aber Kopien dieser Objekte werden nicht mehr im externen S3-Bucket erstellt, den er als Endpunkt konfiguriert hat. Siehe "Plattformdienste für S3-Mandantenkonten verwalten".
   - Die Einstellung **Eigene Identitätsquelle verwenden** legt fest, ob das Mandantenkonto seine eigene Identitätsquelle oder die für den Grid Manager konfigurierte Identitätsquelle verwendet.

     Wenn **Eigene Identitätsquelle verwenden** ausgewählt ist:

     - Deaktiviert und ausgewählt, der Mandant hat 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, ist SSO für das StorageGRID System aktiviert. Der Mandant

muss die für den Grid Manager konfigurierte Identitätsquelle verwenden.

- Aktivieren oder deaktivieren Sie die Berechtigung **S3 Select zulassen** je nach Bedarf. Siehe "S3 Select für Mandantenkonten verwalten".
- Die Berechtigung **Use grid federation connection** kann entfernt werden:
  i. Die Registerkarte **Grid federation** auswählen.
  ii. **Berechtigung entfernen** auswählen.
- Die Berechtigung **Use grid federation connection** kann wie folgt hinzugefügt werden:
  i. Die Registerkarte **Grid federation** auswählen.
  ii. Das Kontrollkästchen **Grid Federation Verbindung verwenden** auswählen.
  iii. Optional kann **Vorhandene lokale Benutzer und Gruppen klonen** ausgewählt werden, um diese in das Remote-Grid zu klonen. Es besteht die Möglichkeit, den laufenden Klonvorgang zu stoppen oder das Klonen erneut zu versuchen, falls nach Abschluss des letzten Klonvorgangs einige lokale Benutzer oder Gruppen nicht geklont werden konnten.
- Eine maximale Aufbewahrungsfrist kann festgelegt oder der Compliance-Modus zugelassen werden:

> Die S3 Object Lock muss im Grid aktiviert sein, bevor Sie diese Einstellungen verwenden können.

  i. Die Registerkarte **S3 Object Lock** auswählen.
  ii. Für **Maximale Aufbewahrungsdauer festlegen** einen Wert eingeben und den Zeitraum aus dem Dropdown-Menü auswählen.
  iii. Für **Konformitätsmodus zulassen** das Kontrollkästchen auswählen.

Passwort für den lokalen Root-Benutzer eines StorageGRID-Mandanten ändern

Möglicherweise muss das Passwort für den lokalen Root-Benutzer eines Mandanten geändert werden, wenn der Root-Benutzer vom Konto ausgesperrt ist.

Bevor Sie beginnen

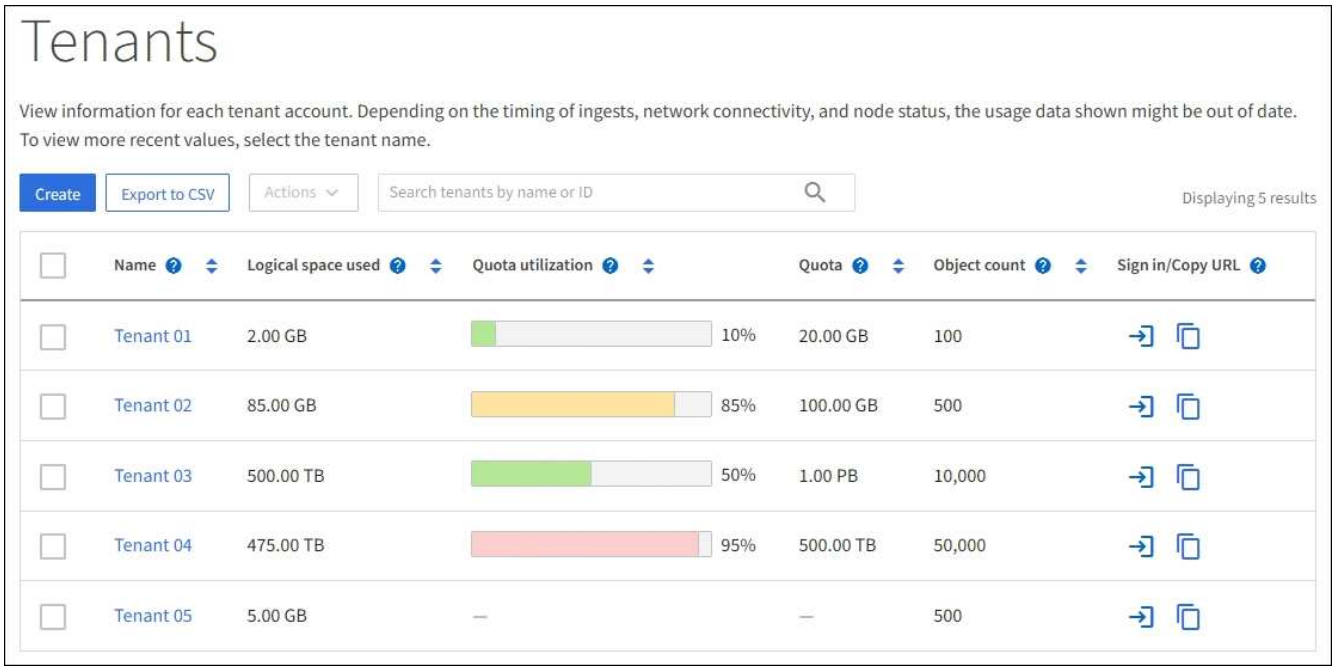
- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Du hast "spezifische Zugriffsberechtigungen".

Über diese Aufgabe

Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, kann sich der lokale Root-Benutzer nicht beim Mandantenkonto anmelden. Um Aufgaben als Root-Benutzer auszuführen, müssen Benutzer einer Verbundgruppe angehören, die über die Root-Zugriffsberechtigung für den Mandanten verfügt.

Schritte

1. **Tenants** auswählen.



2. Wählen Sie das Mandantenkonto aus. Folgende Möglichkeiten stehen zur Verfügung:
   - Aktivieren Sie das Kontrollkästchen für den Mandanten und wählen Sie **Aktionen** > **Root-Passwort ändern**.
   - Wählen Sie den Namen des Mandanten aus, um die Detailseite anzuzeigen, und wählen Sie **Aktionen** > **Root-Passwort ändern**.
3. Geben Sie das neue Passwort für das Mandantenkonto ein.
4. **Speichern** auswählen.

Löschen eines StorageGRID-Tenant-Kontos

Sie können ein Mandantenkonto löschen, wenn Sie den Zugriff des Mandanten auf das System dauerhaft entfernen möchten.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Du hast "spezifische Zugriffsberechtigungen".
- Sie haben alle mit dem Mandantenkonto verknüpften S3 Buckets und Objekte entfernt.
- Wenn dem Mieter die Nutzung einer Grid-Federation-Verbindung gestattet ist, wurden die Überlegungen für "Löschen eines Mandanten mit der Berechtigung „Grid Federation-Verbindung verwenden“" geprüft.

Schritte

1. **Tenants** auswählen.
2. Das oder die Mandantenkonten, die gelöscht werden sollen, ermitteln.

   Im Suchfeld kann nach einem Mieter anhand des Namens oder der Mieter-ID gesucht werden.

3. Mehrere Mandanten können gelöscht werden, indem die entsprechenden Kontrollkästchen ausgewählt und **Aktionen** > **Löschen** gewählt wird.
4. Um einen einzelnen Mandanten zu löschen, kann eine der folgenden Aktionen durchgeführt werden:

- Das Kontrollkästchen auswählen und **Aktionen** > **Löschen** wählen.
- Wählen Sie den Mandantennamen aus, um die Detailseite anzuzeigen, und dann **Aktionen** > **Löschen** auswählen.

5. **Ja** auswählen.

Plattformdienste verwalten

Erfahren Sie mehr über die StorageGRID-Plattformdienste

Zu den Plattformdiensten gehören CloudMirror Replikation, Ereignisbenachrichtigungen und der Suchintegrationsdienst.

Wenn Sie Plattformdienste für S3-Mandantenkonten aktivieren, muss das Grid so konfiguriert werden, dass Mandanten auf die externen Ressourcen zugreifen können, die für die Nutzung dieser Dienste erforderlich sind.

Plattformdienste werden für "Branch Buckets" nicht unterstützt.

CloudMirror Replikation

Der StorageGRID CloudMirror Replikationsdienst wird verwendet, um bestimmte Objekte aus einem StorageGRID Bucket an ein festgelegtes externes Ziel zu spiegeln.

Beispielsweise kann die CloudMirror-Replikation genutzt werden, um bestimmte Kundendatensätze in Amazon S3 zu spiegeln und anschließend AWS-Services für Analysen der Daten zu verwenden.

CloudMirror-Replikation weist einige wichtige Ähnlichkeiten und Unterschiede zur cross-grid Replikationsfunktion auf. Weitere Informationen finden sich unter "Vergleich der netzübergreifenden Replikation und der CloudMirror-Replikation".

> CloudMirror Replikation wird nicht unterstützt, wenn für den Quell-Bucket S3 Object Lock aktiviert ist.

Benachrichtigungen

${post_edited_translations.segment}

Beispielsweise kann konfiguriert werden, dass Benachrichtigungen an Administratoren gesendet werden, wenn ein Objekt zu einem Bucket hinzugefügt wird, wobei die Objekte Protokolldateien darstellen, die mit einem kritischen Systemereignis verbunden sind.

> Obwohl Ereignisbenachrichtigungen für einen Bucket mit aktiviertem S3 Object Lock konfiguriert werden können, werden die S3 Object Lock Metadaten (einschließlich Retain Until Date und Legal Hold Status) der Objekte nicht in die Benachrichtigungsnachrichten aufgenommen.

Suchintegrationsdienst

Der Suchintegrationsdienst wird verwendet, um Metadaten von S3-Objekten an einen bestimmten Elasticsearch-Index zu senden, wo die Metadaten mithilfe des externen Dienstes durchsucht oder analysiert werden können.

Sie könnten beispielsweise Ihre Buckets so konfigurieren, dass sie S3-Objektmetadaten an einen entfernten

Elasticsearch-Dienst senden. Anschließend könnten Sie Elasticsearch verwenden, um Suchen über mehrere Buckets hinweg durchzuführen und anspruchsvolle Analysen der in Ihren Objektmetadaten vorhandenen Muster vorzunehmen.

${post_edited_translations.segment}

Plattformdienste geben Mandanten die Möglichkeit, externe Speicherressourcen, Benachrichtigungsdienste sowie Such- oder Analysedienste mit ihren Daten zu verwenden. Da der Zielort für Plattformdienste typischerweise außerhalb Ihrer StorageGRID Bereitstellung liegt, ist zu entscheiden, ob Mandanten die Nutzung dieser Dienste gestattet werden soll. Wenn dies der Fall ist, muss die Nutzung von Plattformdiensten beim Erstellen oder Bearbeiten von Mandantenkonten aktiviert werden. Das Netzwerk ist außerdem so zu konfigurieren, dass die von Mandanten generierten Plattformdienstnachrichten ihre Ziele erreichen können.

Empfehlungen für die Nutzung von Plattformdiensten

${post_edited_translations.segment}

- Wenn für einen S3-Bucket im StorageGRID System sowohl Versionierung als auch CloudMirror Replikation aktiviert sind, sollte die S3-Bucket-Versionierung auch für den Zielendpunkt aktiviert werden. Dies ermöglicht es der CloudMirror Replikation, ähnliche Objektversionen auf dem Endpunkt zu erzeugen.
- Es sollten nicht mehr als 100 aktive Mandanten mit S3-Anfragen verwendet werden, die CloudMirror Replikation, Benachrichtigungen und Suchintegration erfordern. Mehr als 100 aktive Mandanten können zu einer langsameren S3-Client-Performance führen.
- Anfragen an einen Endpunkt, die nicht abgeschlossen werden können, werden bis zu einem Maximum von 500.000 Anfragen in eine Warteschlange eingereiht. Dieses Limit wird gleichmäßig unter den aktiven Mandanten aufgeteilt. Neuen Mandanten ist es gestattet, dieses Limit von 500.000 vorübergehend zu überschreiten, damit neu erstellte Mandanten nicht ungerechtfertigt benachteiligt werden.

Verwandte Informationen

- "Plattformdienste verwalten"
- "Konfigurieren der Storage Proxy-Einstellungen"
- "StorageGRID überwachen"

Netzwerk und Ports für StorageGRID Plattformdienste

Wenn Sie einem S3-Mandanten die Nutzung von Plattformdiensten gestatten, müssen Sie das Netzwerk für das Grid so konfigurieren, dass Plattformdienstnachrichten an ihre Ziele zugestellt werden können.

Plattformdienste können für ein S3-Mandantenkonto beim Erstellen oder Aktualisieren des Mandantenkontos aktiviert werden. Wenn Plattformdienste aktiviert sind, kann der Mandant Endpunkte erstellen, die als Ziel für CloudMirror-Replikation, Ereignisbenachrichtigungen oder Suchintegrationsnachrichten aus seinen S3-Buckets dienen. Diese Plattformdienstnachrichten werden von Storage Nodes, auf denen der ADC-Dienst ausgeführt wird, an die Zielendpunkte gesendet.

Beispielsweise könnten Mandanten die folgenden Arten von Zielendpunkten konfigurieren:

- Ein lokal gehosteter Elasticsearch Cluster
- 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-Benachrichtigungsanfragen 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
- Ein externer Endpunkt, beispielsweise ein Endpunkt bei Amazon Web Services.

Um sicherzustellen, dass Plattformdienstnachrichten zugestellt werden können, müssen die Netzwerke, die die ADC Storage Nodes enthalten, konfiguriert werden. Es muss sichergestellt sein, dass die folgenden Ports für das Senden von Plattformdienstnachrichten an die Zielendpunkte verwendet werden können.

Standardmäßig werden Plattformdienstnachrichten über 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)
- ${post_edited_translations.segment}

Mandanten können beim Erstellen oder Bearbeiten eines Endpunkts einen anderen Port angeben.

> Wenn eine StorageGRID-Bereitstellung als Ziel für die CloudMirror-Replikation verwendet wird, können Replikationsnachrichten möglicherweise auf einem anderen Port als 80 oder 443 empfangen werden. Es muss sichergestellt sein, dass der von der Ziel StorageGRID Bereitstellung für S3 verwendete Port im Endpunkt angegeben ist.

Wenn Sie einen nicht transparenten Proxyserver verwenden, muss auch "Speicher-Proxy-Einstellungen konfigurieren" zugelassen werden, damit Nachrichten an externe Endpunkte, wie beispielsweise einen Endpunkt im Internet, gesendet werden können.

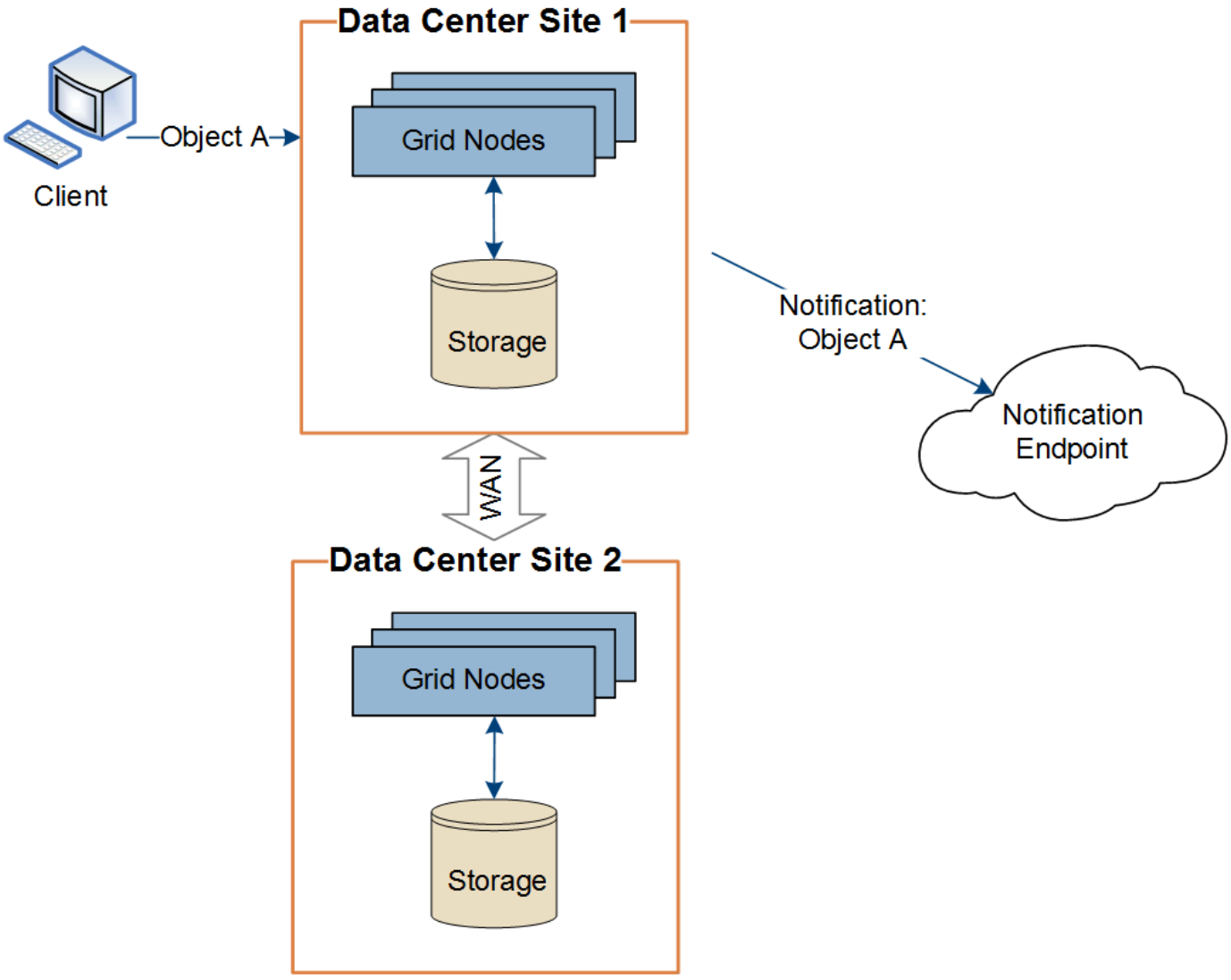
Verwandte Informationen

"Ein Mandantenkonto verwenden"_

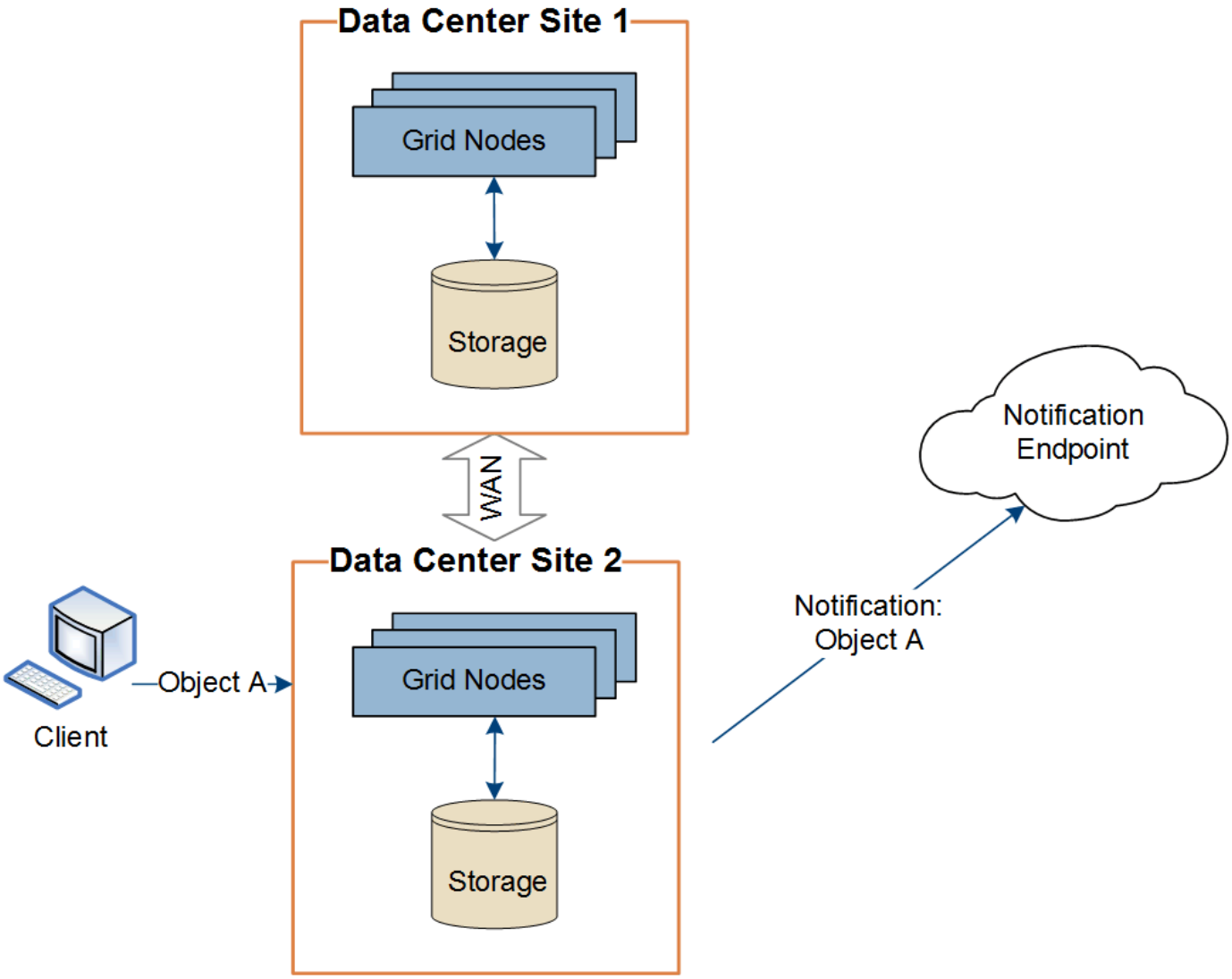
Standortbezogene Zustellung von StorageGRID-Plattformdienste-Nachrichten

Alle Plattformdienste-Operationen werden standortbezogen ausgeführt.

Das bedeutet: Wenn ein Mandant einen Client verwendet, um eine S3-API-Erstellungsoperation für ein Objekt durchzuführen, indem er eine Verbindung zu einem Gateway-Knoten am Rechenzentrumsstandort 1 herstellt, wird die Benachrichtigung über diese Aktion ausgelöst und vom Rechenzentrumsstandort 1 gesendet.



${post_edited_translations.segment}



${post_edited_translations.segment}

Fehlerbehebung bei StorageGRID-Plattformdiensten

Die in den Plattformdiensten verwendeten Endpunkte werden von Mandantenbenutzern im Tenant Manager erstellt und verwaltet. Wenn ein Mandant jedoch Probleme bei der Konfiguration oder Nutzung von Plattformdiensten hat, kann der Grid Manager möglicherweise zur Lösung des Problems beitragen.

Probleme mit neuen Endpunkten

Bevor ein Mandant Plattformdienste nutzen kann, muss er mit dem Tenant Manager einen oder mehrere Endpunkte erstellen. Jeder Endpunkt repräsentiert ein externes Ziel für einen Plattformdienst, wie zum Beispiel einen StorageGRID S3 Bucket, einen Amazon Web Services Bucket, ein Amazon Simple Notification Service Topic, ein Kafka Topic oder einen lokal oder auf AWS gehosteten Elasticsearch Cluster. Jeder Endpunkt enthält sowohl den Speicherort der externen Ressource als auch die für den Zugriff auf diese Ressource erforderlichen Anmeldeinformationen.

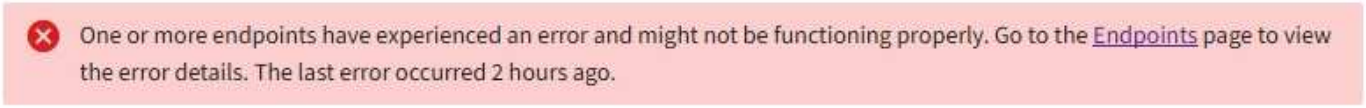
Wenn ein Mandant einen Endpunkt erstellt, prüft das StorageGRID-System, ob dieser Endpunkt existiert und mit den angegebenen Anmeldeinformationen erreichbar ist. Die Verbindung zum Endpunkt wird von einem Knoten an jedem Standort validiert.

Schlägt die Endpunktvalidierung fehl, erläutert eine Fehlermeldung, warum die Endpunktvalidierung fehlgeschlagen ist. Der Mandantenbenutzer sollte das Problem beheben und dann versuchen, den Endpunkt erneut zu erstellen.

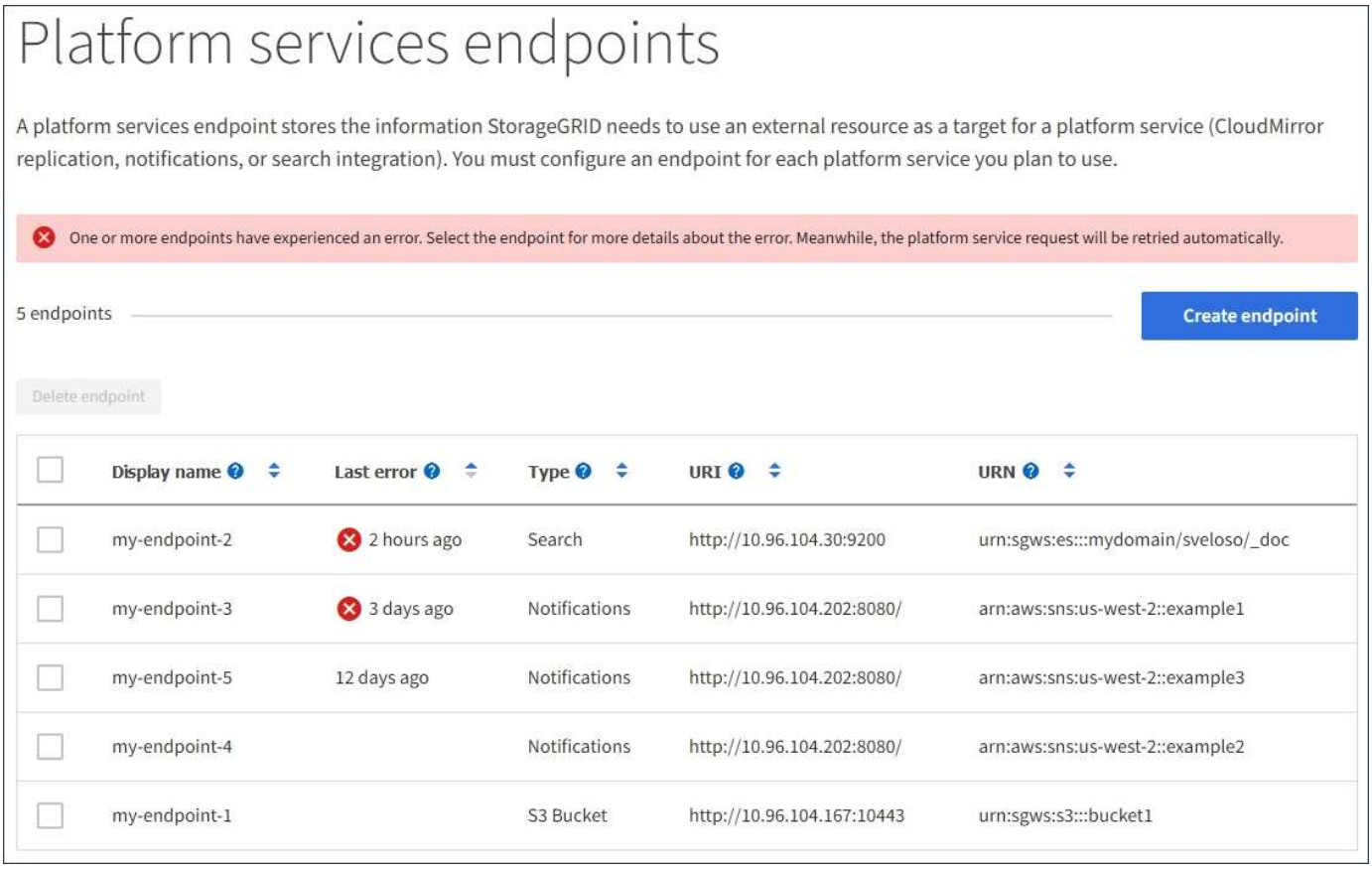
Die Erstellung eines Endpunkts schlägt fehl, wenn die Plattformdienste für das Mandantenkonto nicht aktiviert sind.

Probleme mit bestehenden Endpunkten

Wenn beim Versuch von StorageGRID, einen vorhandenen Endpunkt zu erreichen, ein Fehler auftritt, wird eine Meldung im Dashboard des Tenant Managers angezeigt.



Benutzer können auf der Seite „Endpunkte“ die jeweils aktuellste Fehlermeldung für jeden Endpunkt einsehen und feststellen, wie lange der Fehler zurückliegt. Die Spalte „Letzter Fehler“ zeigt die letzte Fehlermeldung für jeden Endpunkt an und gibt an, wie lange der Fehler zurückliegt. Fehler, die mit dem Symbol gekennzeichnet sind, sind innerhalb der letzten 7 Tage aufgetreten.



Einige Fehlermeldungen in der Spalte **Letzter Fehler** enthalten möglicherweise eine logID in Klammern. Ein Grid-Administrator oder der technische Support kann diese ID verwenden, um detailliertere Informationen zum Fehler in der bycast.log zu finden.

Probleme im Zusammenhang mit Proxyservern

Wenn Sie eine "Storage Proxy" zwischen Storage Nodes und Plattformdienst-Endpunkten konfiguriert haben, können Fehler auftreten, wenn Ihr Proxyservice keine Nachrichten von StorageGRID zulässt. Zur Behebung dieser Probleme sollten die Einstellungen Ihres Proxyservers überprüft werden, um sicherzustellen, dass plattformdienstbezogene Nachrichten nicht blockiert werden.

Feststellen, ob ein Fehler aufgetreten ist

Wenn in den letzten 7 Tagen Endpunktfehler aufgetreten sind, zeigt das Dashboard im Tenant Manager eine Warnmeldung an. Auf der Seite Endpunkte sind weitere Details zum Fehler zu sehen.

Client-Operationen schlagen fehl

Bestimmte Probleme mit Plattformdiensten können dazu führen, dass Clientoperationen im S3-Bucket fehlschlagen. Beispielsweise schlagen S3-Clientoperationen fehl, wenn der interne Replicated State Machine (RSM) Service ausfällt oder wenn zu viele Plattformdienste-Nachrichten zur Zustellung in der Warteschlange stehen.

Status der Dienste prüfen:

1. Wählen Sie **Nodes** > ***site*** > ***Storage Node*** > **Overview**.
2. In der Tabelle „Warnungen“ auf aktive Warnungen prüfen.
3. Alle aktiven Warnmeldungen beheben. Bei Bedarf den technischen Support kontaktieren.

Behebbare und nicht behebbare Endpunktfehler

Nach der Erstellung von Endpunkten können aus verschiedenen Gründen Fehler bei Plattformdienstanfragen auftreten. Einige Fehler lassen sich durch Benutzereingriff beheben. Beispielsweise können behebbare Fehler aus folgenden Gründen auftreten:

- Die Zugangsdaten des Benutzers wurden gelöscht oder sind abgelaufen.
- Der Ziel Bucket existiert nicht.
- Die Benachrichtigung kann nicht zugestellt werden.

Wenn StorageGRID auf einen behebbaren Fehler stößt, wird die Anfrage an den Plattformdienst so lange wiederholt, bis sie erfolgreich ist.

Andere Fehler sind nicht behebbar. Beispielsweise können nicht behebbare Fehler aus folgenden Gründen auftreten:

- Der Endpunkt wurde gelöscht.
- Ein Webhook-Endpunkt-Ziel antwortet auf eine Benachrichtigungsanfrage mit einem `400 Bad Request` Fehler.

Wenn StorageGRID auf einen nicht behebbaren Endpunktfehler stößt:

- Im Grid Manager unter **Support** > **Tools** > **Metrics** > **Grafana** > **Platform Services Overview** sind Fehlerdetails einsehbar.
- Im Tenant Manager unter **STORAGE (S3)** > **Platform Services Endpoints** sind die Fehlerdetails einsehbar.
- Prüfen Sie `/var/local/log/bycast-err.log` auf zugehörige Fehler. Speicherknoten, die den ADC-

Service enthalten, verfügen über diese Protokolldatei.

Plattformdienstnachrichten können nicht zugestellt werden

Tritt beim Ziel ein Problem auf, das den Empfang von Plattformdienstnachrichten verhindert, wird die Clientoperation für den Bucket zwar erfolgreich ausgeführt, die Plattformdienstnachricht jedoch nicht zugestellt. Dieser Fehler kann beispielsweise auftreten, wenn die Anmeldeinformationen beim Ziel aktualisiert werden, sodass StorageGRID sich nicht mehr beim Zieldienst authentifizieren kann.

Es wird geprüft, ob entsprechende Warnmeldungen vorliegen.

Langsamere Leistung bei Plattformdienstanfragen

StorageGRID Software kann eingehende S3-Anfragen für einen Bucket drosseln, wenn die Rate, mit der die Anfragen gesendet werden, die Rate übersteigt, mit der der Zielendpunkt die Anfragen empfangen kann. Eine Drosselung tritt nur auf, wenn ein Rückstau an Anfragen besteht, die auf die Übermittlung an den Zielendpunkt warten.

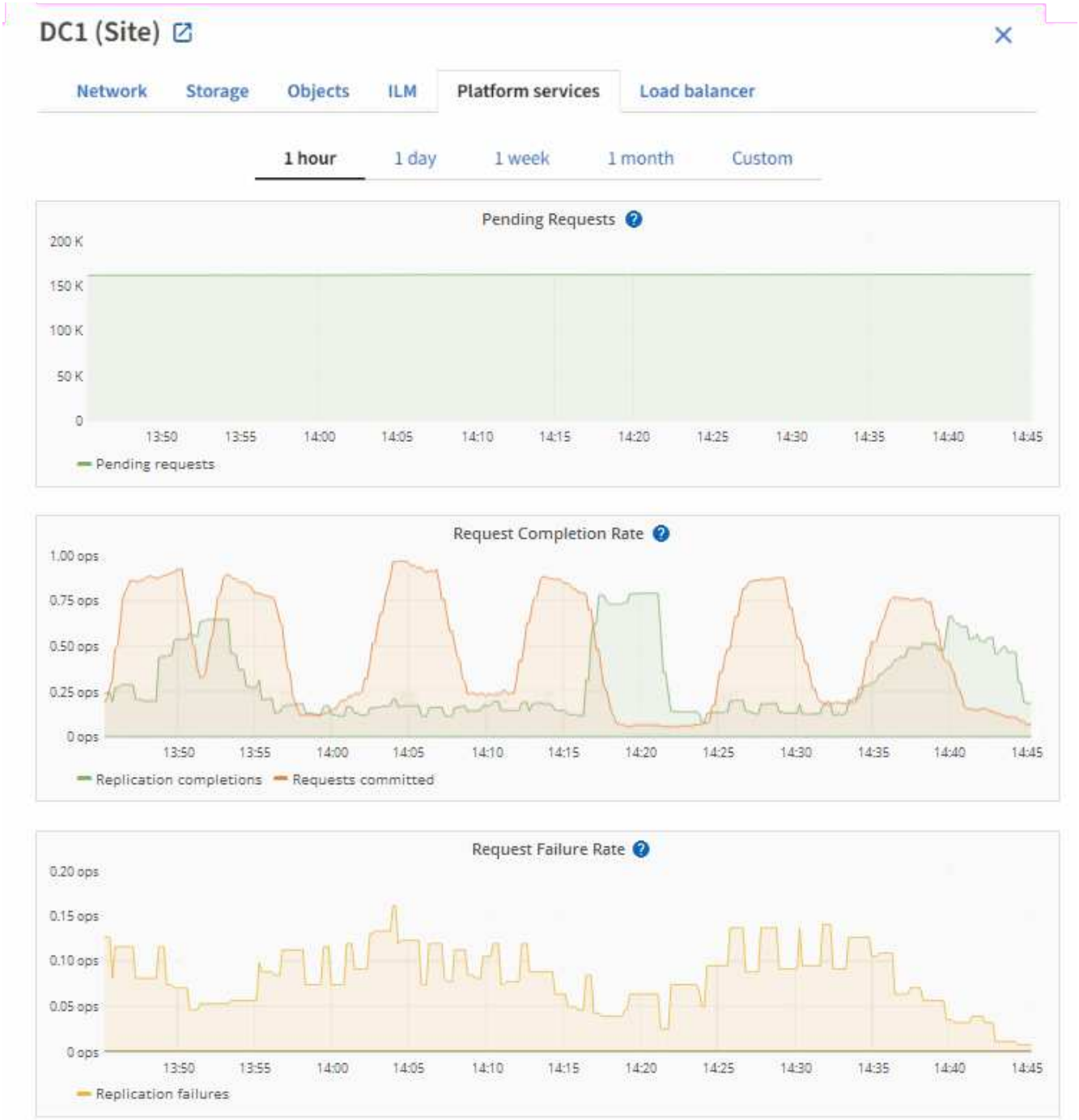
Der einzige sichtbare Effekt ist, dass die Ausführung eingehender S3-Anfragen länger dauert. Bei deutlich langsamerer Performance empfiehlt sich eine Reduzierung der Aufnahmerate oder die Nutzung eines Endpunkts mit höherer Kapazität. Wenn der Rückstand an Anfragen weiter zunimmt, schlagen Client-S3-Operationen (wie PUT-Anfragen) schließlich fehl.

CloudMirror-Anfragen werden eher von der Leistung des Zielendpunkts beeinflusst, da diese Anfragen typischerweise einen größeren Datentransfer als Suchintegrations- oder Ereignisbenachrichtigungsanfragen umfassen.

Plattformdienstanfragen schlagen fehl

Die Fehlerrate bei Anfragen an Plattformdienste anzeigen:

1. Wählen Sie **Knoten**.
2. ***site*** > **Plattformdienste** auswählen.
3. Das Diagramm zur Fehlerrate der Anfragen wird angezeigt.



Warnung: Plattform-Services nicht verfügbar

Die Warnung **Plattformdienste nicht verfügbar** bedeutet, dass an einem Standort keine Plattformdienstoperationen durchgeführt werden können, da zu wenige Speicherknoten mit dem RSM-Dienst ausgeführt werden oder verfügbar sind.

Der RSM Service stellt sicher, dass Plattform-Serviceanfragen an ihre jeweiligen Endpunkte gesendet werden.

Um diese Warnung zu beheben, bestimmen Sie, welche Storage Nodes am Standort den RSM Service enthalten. (Der RSM Service ist auf Storage Nodes vorhanden, die auch den ADC Service enthalten.) Anschließend ist sicherzustellen, dass die einfache Mehrheit dieser Storage Nodes ausgeführt wird und verfügbar ist.

Wenn an einem Standort mehr als ein Storage Node, der den RSM-Dienst enthält, ausfällt, gehen alle ausstehenden Plattformdienstanforderungen für diesen Standort verloren.

Zusätzliche Hinweise zur Fehlerbehebung für Plattformdienste-Endpunkte

Weitere Informationen finden Sie unter "${post_edited_translations.segment}".

Verwandte Informationen

"Fehlerbehebung im StorageGRID System"

Verwalten Sie S3 Select für Mandantenkonten in StorageGRID

Bestimmten S3-Mandanten kann die Nutzung von S3 Select ermöglicht werden, um SelectObjectContent-Anfragen für einzelne Objekte zu stellen.

S3 Select bietet eine effiziente Möglichkeit, große Datenmengen zu durchsuchen, ohne eine Datenbank und zugehörige Ressourcen für Suchvorgänge bereitstellen zu müssen. Auch die Kosten und die Latenz beim Abrufen von Daten werden verringert.

Was ist S3 Select?

S3 Select ermöglicht es S3 Clients, SelectObjectContent-Anfragen zu verwenden, um nur die von einem Objekt benötigten Daten zu filtern und abzurufen. Die StorageGRID Implementierung von S3 Select umfasst eine Teilmenge der Befehle und Funktionen von S3 Select.

${post_edited_translations.segment}

Anforderungen an die Grid-Administration

Der Grid-Administrator muss den Mandanten die S3 Select-Berechtigung erteilen. **S3 Select zulassen** ist auszuwählen, wenn "einen Mandanten erstellen" oder "einen Mandanten bearbeiten".

Anforderungen an das Objektformat

Das abzufragende Objekt muss in einem der folgenden Formate vorliegen:

- **CSV**. Kann unverändert verwendet oder in GZIP- oder BZIP2-Archive komprimiert werden.
- **Parquet**. Zusätzliche Anforderungen für Parquet Objekte:
  - S3 Select unterstützt ausschließlich spaltenorientierte Komprimierung mit GZIP oder Snappy. S3 Select unterstützt keine Komprimierung ganzer Parquet-Objekte.
  - S3 Select unterstützt keine Parquet-Ausgabe. Das Ausgabeformat muss als CSV oder JSON angegeben werden.
  - Die maximale unkomprimierte Zeilengruppengröße beträgt 512 MB.
  - Sie müssen die im Schema des Objekts angegebenen Datentypen verwenden.
  - Die logischen Datentypen INTERVAL, JSON, LIST, TIME und UUID können nicht verwendet werden.

Endpunktanforderungen

Die SelectObjectContent-Anfrage muss an einen "StorageGRID Load Balancer Endpoint" gesendet werden.

Die vom Endpunkt verwendeten Admin- und Gateway-Knoten müssen einer der folgenden sein:

- Ein Services Appliance-Knoten
- Ein VMware basierter Softwareknoten
- Ein Bare Metal-Knoten, auf dem ein Kernel mit aktiviertem cgroup v2 läuft

Allgemeine Überlegungen

Anfragen können nicht direkt an Storage Nodes gesendet werden.

> SelectObjectContent-Anfragen können die Leistung des Load-Balancers für alle S3 Clients und alle Mandanten beeinträchtigen. Diese Funktion sollte nur bei Bedarf und nur für vertrauenswürdige Mandanten aktiviert werden.

Siehe "Anleitung zur Verwendung von S3 Select".

Um "Grafana Diagramme" für S3 Select-Operationen im Zeitverlauf anzuzeigen, in Grid Manager **Support** > **Tools** > **Metrics** auswählen.

Clientverbindungen konfigurieren

Konfigurieren Sie S3-Clientverbindungen zu StorageGRID

Als Grid-Administrator verwalten Sie die Konfigurationsoptionen, die steuern, wie S3-Clientanwendungen eine Verbindung zu Ihrem StorageGRID System herstellen, um Daten zu speichern und abzurufen.

> Die Swift-Details wurden aus dieser Version der Dokumentationsseite entfernt. Siehe "StorageGRID 11.8: S3 und Swift Clientverbindungen konfigurieren".

Konfigurationsaufgaben

1. Führen Sie die erforderlichen Vorbereitungsschritte in StorageGRID durch, abhängig davon, wie die Clientanwendung eine Verbindung zu StorageGRID herstellt.

Erforderliche Aufgaben

Folgendes ist erforderlich:

- IP-Adressen
- Domainnamen
- SSL-Zertifikat

Optionale Aufgaben

Optional kann Folgendes konfiguriert werden:

- Identitätsföderation
- SSO

1. Verwenden Sie StorageGRID, um die Werte zu erhalten, die die Anwendung für die Verbindung zum Grid

benötigt. Sie können entweder den S3-Einrichtungsassistenten verwenden oder jede StorageGRID Entität manuell konfigurieren.

S3-Einrichtungsassistent verwenden

Die Schritte im S3-Einrichtungsassistenten sind zu befolgen.

Manuell konfigurieren

1. Hochverfügbarkeitsgruppe erstellen
2. Load Balancer-Endpunkt erstellen
3. Mandantenkonto erstellen
4. Bucket und Zugriffsschlüssel erstellen
5. ILM-Regel und Richtlinie konfigurieren

1. Verwenden Sie die S3-Anwendung, um die Verbindung zu StorageGRID abzuschließen. DNS-Einträge werden erstellt, um IP-Adressen den geplanten Domänennamen zuzuordnen.

   Bei Bedarf sind zusätzliche Anwendungseinstellungen vorzunehmen.

2. Fortlaufende Aufgaben in der Anwendung und in StorageGRID ermöglichen die Verwaltung und Überwachung des Objektspeichers im Zeitverlauf.

Informationen, die benötigt werden, um StorageGRID an eine Clientanwendung anzubinden

Bevor StorageGRID an eine S3-Clientanwendung angebunden werden kann, sind Konfigurationsschritte in StorageGRID erforderlich und bestimmte Werte müssen abgerufen werden.

Welche Werte werden benötigt?

Die folgende Tabelle zeigt die Werte, die Sie in StorageGRID konfigurieren müssen, und wo diese Werte von der S3-Anwendung und dem DNS-Server verwendet werden.

Wert	Wo der Wert konfiguriert wird	Wo Wert verwendet wird
Virtuelle IP-Adressen (VIP)	StorageGRID > HA-Gruppe	DNS-Eintrag
Port	StorageGRID > Load Balancer Endpoint	Client Anwendung
SSL-Zertifikat	StorageGRID > Load Balancer Endpoint	Client Anwendung
Servername (FQDN)	StorageGRID > Load Balancer Endpoint	• Client Anwendung • DNS-Eintrag
S3-Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel	${post_edited_translations.segment}	Client Anwendung

Wert	Wo der Wert konfiguriert wird	Wo Wert verwendet wird
Bucket/Container-Name	${post_edited_translations.segment}	Client Anwendung

Wie erhalte ich diese Werte?

${post_edited_translations.segment}

- Verwendung des "S3 Einrichtungsassistent". Der S3 Einrichtungsassistent unterstützt Sie bei der schnellen Konfiguration 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 hilft sicherzustellen, dass Ihre Einstellungen den Best Practices von StorageGRID entsprechen.

  ${post_edited_translations.segment}

- **Verwenden von "FabricPool Einrichtungsassistent"**. Ähnlich wie der S3-Einrichtungsassistent hilft Ihnen der FabricPool Einrichtungsassistent dabei, die erforderlichen Werte schnell zu konfigurieren, und gibt eine Datei aus, die Sie bei der Konfiguration einer FabricPool Cloud-Tier in ONTAP verwenden können.

  Wenn StorageGRID als Objektspeichersystem für eine FabricPool Cloud-Tier vorgesehen ist, wird die Verwendung des FabricPool Einrichtungsassistenten empfohlen, es sei denn, es liegen besondere Anforderungen vor oder die Implementierung erfordert umfangreiche 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 durch manuelle Konfiguration ermitteln. Die folgenden Schritte sind auszuführen:
  a. Die gewünschte Hochverfügbarkeitsgruppe (HA-Gruppe) für die S3-Anwendung wird konfiguriert. Weitere Informationen unter "${post_edited_translations.segment}".
  b. Erstellen des Load-Balancer-Endpunkts, den die S3-Anwendung verwenden wird. Siehe "Load Balancer-Endpunkte konfigurieren".
  c. Erstellen des Mandantenkontos, das die S3-Anwendung verwendet. Siehe "Ein Mandantenkonto erstellen".
  d. Für einen S3-Mandanten im Mandantenkonto anmelden und für jeden Benutzer, der auf die Anwendung zugreift, eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel generieren. Siehe "${post_edited_translations.segment}".
  e. Erstellen eines oder mehrerer S3 Buckets im Mandantenkonto. Für S3 siehe "S3 Bucket erstellen".
  f. Um spezifische Platzierungsanweisungen für die Objekte hinzuzufügen, die zum neuen Mandanten oder Bucket/Container gehören, erstellen Sie eine neue ILM-Regel und aktivieren Sie eine neue ILM-Richtlinie, um diese Regel zu verwenden. Siehe "${post_edited_translations.segment}" und "ILM-Richtlinie erstellen".

Sicherheit für S3-Clients in StorageGRID

StorageGRID Mandantenkonten verwenden S3-Client-Anwendungen, um Objektdaten in StorageGRID zu speichern. Sie sollten die für Client-Anwendungen implementierten

Sicherheitsmaßnahmen überprüfen.

Zusammenfassung

${post_edited_translations.segment}

Verbindungssicherheit
TLS

Server-Authentifizierung
${post_edited_translations.segment}

Client-Authentifizierung
S3-Konto-Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel

Client-Autorisierung
Bucket-Eigentum und alle anwendbaren Zugriffskontrollrichtlinien

Wie StorageGRID Sicherheit für Client-Anwendungen bereitstellt

S3 Clientanwendungen können eine Verbindung zum Load Balancer Service auf Gateway Nodes oder Admin Nodes oder direkt zu Storage Nodes herstellen.

- Clients, die sich mit dem Load Balancer Service verbinden, können HTTPS oder HTTP verwenden, abhängig davon, wie Sie "den Load Balancer-Endpunkt konfigurieren".

  HTTPS bietet eine sichere, TLS-verschlüsselte Kommunikation und wird empfohlen. Ein Sicherheitszertifikat muss an den Endpunkt angehängt werden.

  ${post_edited_translations.segment}

- Clients, die eine Verbindung zu Storage Nodes herstellen, können ebenfalls HTTPS oder HTTP verwenden.

  HTTPS ist die Standardeinstellung und wird empfohlen.

  HTTP bietet eine weniger sichere, unverschlüsselte Kommunikation, kann aber optional "aktiviert" für Nicht-Produktions- oder Testnetze verwendet werden.

- Die Kommunikation zwischen StorageGRID und dem Client wird mit TLS verschlüsselt.
- Die Kommunikation zwischen dem Load Balancer Service und den Storage Nodes innerhalb des Grids ist verschlüsselt, unabhängig davon, ob der Load Balancer Endpoint für HTTP- oder HTTPS-Verbindungen konfiguriert ist.
- Clients müssen "HTTP-Authentifizierungsheader" an StorageGRID übermitteln, um REST-API-Operationen auszuführen.

Sicherheitszertifikate und Client-Anwendungen

In allen Fällen können Clientanwendungen TLS-Verbindungen herstellen, indem entweder ein vom Grid-Administrator hochgeladenes benutzerdefiniertes Serverzertifikat oder ein vom StorageGRID System generiertes Zertifikat verwendet wird:

- Wenn Clientanwendungen eine Verbindung zum Load-Balancer-Dienst herstellen, verwenden sie das für

den Load-Balancer-Endpunkt konfigurierte Zertifikat. Jeder Load-Balancer-Endpunkt verfügt über ein eigenes Zertifikat, entweder ein vom Grid-Administrator hochgeladenes benutzerdefiniertes Serverzertifikat oder ein Zertifikat, das der Grid-Administrator bei der Konfiguration des Endpunkts in StorageGRID generiert hat.

Siehe "Überlegungen zum Lastausgleich".

- Wenn Clientanwendungen eine direkte Verbindung zu einem Storage Node herstellen, verwenden sie entweder die systemgenerierten Serverzertifikate, die bei der Installation des StorageGRID Systems für die Storage Nodes erstellt wurden (und von der Systemzertifizierungsstelle signiert sind), oder ein einzelnes benutzerdefiniertes Serverzertifikat, das vom Grid-Administrator für das Grid bereitgestellt wird. Siehe "ein benutzerdefiniertes S3 API-Zertifikat hinzufügen".

Clients sollten so konfiguriert sein, dass sie der Zertifizierungsstelle vertrauen, die das jeweilige Zertifikat signiert hat, das für die Herstellung von TLS-Verbindungen verwendet wird.

Unterstützte Hash- und Verschlüsselungsalgorithmen für TLS-Bibliotheken

Das StorageGRID System unterstützt eine Reihe von Cipher Suites, die Clientanwendungen beim Aufbau einer TLS-Sitzung verwenden können. Zur Konfiguration von Ciphers befindet sich die Option unter **Konfiguration** > **Sicherheit** > **Sicherheitseinstellungen** mit Auswahl von **TLS- und SSH-Richtlinien**.

Unterstützte TLS-Versionen

StorageGRID unterstützt TLS 1.2 und TLS 1.3.

SSLv3 und TLS 1.1 (oder frühere Versionen) werden nicht mehr unterstützt.

S3-Einrichtungsassistent verwenden

Überlegungen und Anforderungen zum StorageGRID S3-Einrichtungsassistenten

${post_edited_translations.segment}

Wann der S3 Setup-Assistent verwendet werden sollte

Der S3-Einrichtungsassistent führt Sie durch jeden Schritt der Konfiguration von StorageGRID für die Verwendung mit einer S3-Anwendung. Im Rahmen des Assistenten werden Dateien heruntergeladen, die zur Eingabe von Werten in die S3-Anwendung verwendet werden können. Mit dem Assistenten lässt sich das System schneller konfigurieren und es wird sichergestellt, dass die Einstellungen den Best Practices von StorageGRID entsprechen.

Wenn Sie über die "Root-Zugriffsberechtigung" verfügen, kann der S3-Einrichtungsassistent beim ersten Start des StorageGRID Grid Managers abgeschlossen werden oder zu einem späteren Zeitpunkt aufgerufen und abgeschlossen werden. Je nach Anforderungen ist es auch möglich, einige oder alle erforderlichen Elemente manuell zu konfigurieren und anschließend mithilfe des Assistenten die Werte zusammenzustellen, die eine S3-Anwendung benötigt.

Bevor der Assistent verwendet wird

Vor der Verwendung des Assistenten sollte bestätigt werden, dass diese Voraussetzungen erfüllt sind.

IP-Adressen beziehen und VLAN-Schnittstellen einrichten

Wenn Sie eine Hochverfügbarkeitsgruppe (HA-Gruppe) konfigurieren, ist bekannt, mit welchen Knoten sich die S3-Anwendung verbindet und welches StorageGRID Netzwerk verwendet wird. Es ist ebenfalls bekannt, welche Werte für die Subnetz-CIDR, die Gateway-IP-Adresse und die virtuellen IP-Adressen (VIP) einzugeben sind.

Wenn geplant ist, ein virtuelles LAN zu verwenden, um den Datenverkehr der S3-Anwendung zu trennen, wurde die VLAN-Schnittstelle bereits konfiguriert. Siehe "${post_edited_translations.segment}".

Identitätsföderation und SSO konfigurieren

Wenn für Ihr StorageGRID System Identitätsföderation oder Single Sign-On (SSO) vorgesehen ist, sind diese Funktionen aktiviert. Es ist außerdem bekannt, welche föderierte Gruppe Root-Zugriff auf das Mandantenkonto erhalten soll, das die S3-Anwendung verwendet. Siehe "Identitätsföderation verwenden" und "Einmalanmeldung konfigurieren".

Domainnamen beziehen und konfigurieren

Es ist bekannt, welcher vollqualifizierte Domainname (FQDN) für StorageGRID zu verwenden ist. Domain Name Server (DNS)-Einträge ordnen diesen FQDN den virtuellen IP-Adressen (VIP) der HA-Gruppe zu, die mit dem Assistenten erstellt wird.

Wenn Sie S3-Anfragen im Virtual Hosted-Style verwenden möchten, sollten Sie "konfigurierte S3 Endpoint-Domänennamen" haben. Die Verwendung von Virtual Hosted-Style-Anfragen wird empfohlen.

Überprüfung der Anforderungen an Load Balancer und Sicherheitszertifikate

Wenn Sie den StorageGRID Load Balancer verwenden möchten, wurden die allgemeinen Überlegungen zum Load Balancing geprüft. Sie verfügen über die Zertifikate, die Sie hochladen werden, oder die Werte, die Sie zum Generieren eines Zertifikats benötigen.

Wenn ein externer (Drittanbieter-)Load-Balancer-Endpunkt verwendet werden soll, sind der vollqualifizierte Domainname (FQDN), der Port und das Zertifikat für diesen Load Balancer vorhanden.

Beliebige Grid Federation-Verbindungen konfigurieren

Wenn Sie 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:

- Du hast "Die Grid Federation-Verbindung wurde konfiguriert.".
- Der Verbindungsstatus ist **Verbunden**.
- Sie verfügen über Root-Zugriffsberechtigung.

Rufen Sie den S3-Einrichtungsassistenten in StorageGRID auf und schließen Sie ihn ab

Sie können den S3-Einrichtungsassistenten verwenden, um StorageGRID für die Verwendung mit einer S3-Anwendung zu konfigurieren. Der Einrichtungsassistent stellt die Werte bereit, die die Anwendung benötigt, um auf einen StorageGRID Bucket zuzugreifen und Objekte zu speichern.

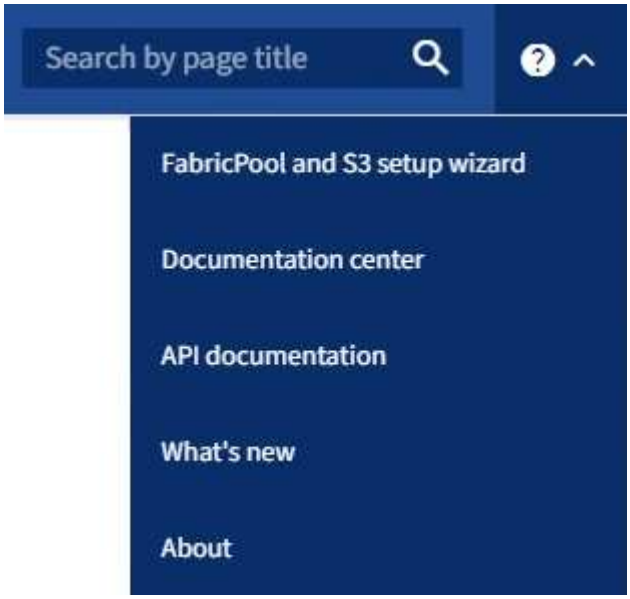
Bevor Sie beginnen

- Sie haben die "Root-Zugriffsberechtigung".
- Sie haben die "Überlegungen und Anforderungen" für die Verwendung des Assistenten überprüft.

Assistenten aufrufen

Schritte

1. Melden Sie sich beim Grid Manager mit einem "unterstützte Webbrowser" an.
2. Wenn das Banner **FabricPool and S3 setup wizard** im Dashboard angezeigt wird, kann der Link im Banner ausgewählt werden. Wenn das Banner nicht mehr angezeigt wird, steht im Grid Manager das Hilfesymbol in der Kopfzeile zur Verfügung, über das **FabricPool and S3 setup wizard** ausgewählt werden kann.



3. Im Abschnitt „S3-Anwendung“ auf der Seite des FabricPool und S3-Setup-Assistenten ist **Jetzt konfigurieren** auszuwählen.

${post_edited_translations.segment}

Eine HA-Gruppe ist eine Sammlung von Nodes, die jeweils den StorageGRID Load-Balancer-Dienst 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 die Workload mit minimalen Auswirkungen auf S3-Vorgänge übernehmen.

Details zu dieser Aufgabe finden Sie unter "Hochverfügbarkeitsgruppen verwalten".

Schritte

1. Wenn Sie die Verwendung eines externen Load Balancers planen, müssen Sie keine HA-Gruppe erstellen. Wählen Sie **Diesen Schritt überspringen** und gehen Sie zu Schritt 2 von 6: Load Balancer Endpunkt konfigurieren.
2. Um den StorageGRID Load Balancer zu nutzen, kann eine neue HA-Gruppe erstellt oder eine bestehende HA-Gruppe verwendet werden.

HA-Gruppe erstellen

a. Zum Erstellen einer neuen HA-Gruppe **HA-Gruppe erstellen** auswählen.

b. Für den Schritt **Details eingeben** sind die folgenden Felder auszufüllen.

Feld	Beschreibung
HA Gruppenname	Ein eindeutiger Anzeigename für diese HA Gruppe.
Beschreibung (optional)	Die Beschreibung dieser HA-Gruppe.

c. Im Schritt **Schnittstellen hinzufügen** werden die Knotenschnittstellen ausgewählt, die in dieser HA-Gruppe verwendet werden sollen.

Mit den Spaltenüberschriften lassen sich die Zeilen sortieren, oder durch Eingabe eines Suchbegriffs können Schnittstellen schneller gefunden werden.

${post_edited_translations.segment}

d. ${post_edited_translations.segment}

${post_edited_translations.segment}

Die erste Schnittstelle in der Liste ist die Primary-Schnittstelle. Die Primary-Schnittstelle ist die aktive Schnittstelle, sofern kein Fehler auftritt.

Wenn die HA-Gruppe mehr als eine Schnittstelle umfasst und die aktive Schnittstelle ausfällt, werden die virtuellen IP-Adressen (VIP-Adressen) auf die erste Backup-Schnittstelle in der Prioritätsreihenfolge verschoben. Wenn diese Schnittstelle ausfällt, werden die VIP-Adressen auf die nächste Backup-Schnittstelle verschoben usw. Nach Behebung der Fehler werden die VIP-Adressen wieder auf die verfügbare Schnittstelle mit der höchsten Priorität verschoben.

e. Für den Schritt **IP-Adressen eingeben** sind die folgenden Felder auszufüllen.

Feld	Beschreibung
Subnetz CIDR	${post_edited_translations.segment} Die Netzwerkadresse darf keine gesetzten Host-Bits aufweisen. Zum Beispiel `192.16.0.0/22`.
Gateway-IP-Adresse (optional)	Wenn sich die für den Zugriff auf StorageGRID verwendeten S3-IP-Adressen nicht im selben Subnetz wie die StorageGRID VIP-Adressen befinden, ist die lokale Gateway-IP-Adresse der StorageGRID VIP einzugeben. Die lokale Gateway-IP-Adresse muss innerhalb des VIP-Subnetzes liegen.

Feld	Beschreibung
Virtuelle IP-Adresse	Geben Sie mindestens eine und höchstens 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 zusätzliche IPv4- und IPv6-Adressen angeben.

f. **HA-Gruppe erstellen** auswählen und anschließend **Fertigstellen**, um zum S3-Setup-Assistenten zurückzukehren.

g. **Weiter** auswählen, um zum Load Balancer Schritt zu gelangen.

Vorhandene HA-Gruppe verwenden

a. Um eine bestehende HA-Gruppe zu verwenden, den Namen der HA-Gruppe unter **HA-Gruppe auswählen** auswählen.

b. **Weiter** auswählen, um zum Load Balancer Schritt zu gelangen.

Schritt 2 von 6: Load Balancer Endpunkt konfigurieren

StorageGRID nutzt einen Load Balancer, um die Arbeitslast von Clientanwendungen zu verwalten. Lastverteilung maximiert Geschwindigkeit und Verbindungskapazität über mehrere Storage Nodes hinweg.

Sie können den StorageGRID Load Balancer Service verwenden, der auf allen Gateway und Admin Nodes verfügbar ist, oder eine Verbindung zu einem externen (Drittanbieter) Load Balancer herstellen. Die Verwendung des StorageGRID Load Balancer wird empfohlen.

Nähere Informationen zu dieser Aufgabe finden sich unter "Überlegungen zum Lastausgleich".

Zur Nutzung des StorageGRID Load Balancer Service die Registerkarte **StorageGRID load balancer** auswählen und anschließend den gewünschten Load Balancer Endpoint erstellen oder auswählen. Für die Verwendung eines externen Load Balancers die Registerkarte **External load balancer** auswählen und Details zu dem bereits konfigurierten System angeben.

${post_edited_translations.segment}

Schritte

1. ${post_edited_translations.segment}
2. Für den Schritt **Endpunktdetails eingeben** sind die folgenden Felder auszufüllen.

Feld	Beschreibung
Name	${post_edited_translations.segment}
Port	Der StorageGRID Port, den Sie für die Lastverteilung verwenden möchten. Dieses Feld ist standardmäßig auf 10433 für den ersten von Ihnen erstellten Endpunkt voreingestellt, Sie können jedoch jeden ungenutzten 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. Siehe "StorageGRID interne Ports".
Clienttyp	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 auf den Endpunkt über eine beliebige IP-Adresse oder über bestimmte IP-Adressen und Netzwerkschnittstellen zugegriffen wird.

Modus	Beschreibung
Global (Standard)	Clients können mit der IP-Adresse eines beliebigen Gateway-Knotens oder Admin-Knotens, der virtuellen IP-Adresse (VIP) einer beliebigen HA-Gruppe in einem beliebigen Netzwerk oder einem entsprechenden FQDN auf den Endpunkt zugreifen. Die Einstellung **Global** (Standard) sollte verwendet werden, es sei denn, die Zugänglichkeit dieses Endpunkts muss eingeschränkt werden.
Virtuelle IPs von HA-Gruppen	Clients müssen eine virtuelle IP-Adresse (oder den entsprechenden FQDN) einer HA-Gruppe verwenden, um auf diesen Endpunkt zuzugreifen. Endpunkte mit diesem Bindungsmodus können alle die gleiche Portnummer verwenden, solange sich die für die Endpunkte ausgewählten HA-Gruppen nicht überschneiden.

Modus	Beschreibung
Knotenschnittstellen	Clients müssen die IP-Adressen (oder die entsprechenden FQDNs) der ausgewählten Knotenschnittstellen verwenden, um auf diesen Endpunkt zuzugreifen.
Knotentyp	${post_edited_translations.segment}

4. ${post_edited_translations.segment}

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 verwenden, um auf ihre Buckets zuzugreifen.
Ausgewählte Mandanten blockieren	Die ausgewählten Mandantenkonten können diesen Endpunkt nicht für den Zugriff auf ihre Buckets verwenden. Alle anderen Mandanten können diesen Endpunkt verwenden.

5. Für den Schritt **Zertifikat anhängen** eine der folgenden Optionen auswählen:

Feld	Beschreibung
${post_edited_translations.segment}	${post_edited_translations.segment}
Zertifikat generieren	Mit dieser Option wird ein selbstsigniertes Zertifikat generiert. Siehe "Load Balancer-Endpunkte konfigurieren" für Details zu den einzugebenden Informationen.
StorageGRID S3-Zertifikat verwenden	Diese Option sollte nur verwendet werden, wenn bereits eine benutzerdefinierte Version des StorageGRID Globalzertifikats hochgeladen oder generiert wurde. Siehe "S3 API-Zertifikate konfigurieren" für Details.

6. **Fertigstellen** auswählen, um zum S3-Setup-Assistenten zurückzukehren.
7. ${post_edited_translations.segment}

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

${post_edited_translations.segment}

Schritte

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}

Externen Load Balancer verwenden

Schritte

1. Zur Verwendung eines externen Load Balancer sind die folgenden Felder auszufüllen.

Feld	Beschreibung
FQDN	Der vollqualifizierte Domainname (FQDN) des externen Load Balancers.
Port	Die Portnummer, die die S3-Anwendung für die Verbindung zum externen Load Balancer verwendet.
Zertifikat	${post_edited_translations.segment}

2. ${post_edited_translations.segment}

${post_edited_translations.segment}

Ein Mandant ist eine Entität, die S3-Anwendungen zum Speichern und Abrufen von Objekten in StorageGRID verwenden kann. Jeder Mandant verfügt über eigene Benutzer, Zugriffsschlüssel, Buckets, Objekte und einen spezifischen Satz von Funktionen.

Ein Bucket ist ein Container, der die Objekte und Objektmetadaten eines Mandanten speichert. Obwohl Mandanten mehrere Buckets haben können, unterstützt der Assistent dabei, einen Mandanten und einen Bucket auf die schnellste und einfachste Weise zu erstellen. Wenn später Buckets hinzugefügt oder Optionen festgelegt werden müssen, kann der Tenant Manager verwendet werden.

Weitere Informationen zu dieser Aufgabe finden Sie unter "Mandantenkonto erstellen" und "S3 Bucket erstellen".

Schritte

1. Geben Sie einen Namen für das Mandantenkonto ein.

   Die Namen der Mandanten müssen nicht eindeutig sein. Bei der Erstellung des Mandantenkontos erhält dieses eine eindeutige, numerische Konto-ID.

2. Der Root-Zugriff für das Mandantenkonto wird basierend darauf definiert, ob Ihr StorageGRID System "Identitätsföderation", "${post_edited_translations.segment}" oder beides verwendet.

Option	Tun Sie Folgendes
Wenn die Identitätsföderation nicht aktiviert ist	Das Passwort, das beim Anmelden beim Mandanten als lokaler Root-Benutzer verwendet wird, angeben.
Wenn die Identitätsföderation aktiviert ist	a. Wählen Sie eine bestehende Verbundgruppe aus, um "Root-Zugriffsberechtigung" für den Mandanten zu haben. b. Optional kann das Passwort angegeben werden, das beim Anmelden beim Mandanten als lokaler Root-Benutzer verwendet wird.

Option	Tun Sie Folgendes
Wenn sowohl Identitätsföderation als auch Single Sign-On (SSO) aktiviert sind	Wählen Sie eine bestehende Verbundgruppe aus, um "Root-Zugriffsberechtigung" für den Mandanten zu haben. Lokale Benutzer können sich nicht anmelden.

3. ${post_edited_translations.segment}

   Diese Option ist auszuwählen, wenn der einzige Benutzer für den Mandanten der Root-Benutzer ist. Wenn andere Benutzer diesen Mandanten verwenden, "Tenant Manager verwenden" können Schlüssel und Berechtigungen konfiguriert werden.

4. Wenn jetzt ein Bucket für diesen Mandanten erstellt werden soll, ist **Bucket für diesen Mandanten erstellen** auszuwählen.

   Wenn S3 Object Lock für das Grid aktiviert ist, ist für den in diesem Schritt erstellten Bucket S3 Object Lock nicht aktiviert. Wenn Sie einen S3 Object Lock Bucket für diese S3-Anwendung benötigen, wählen Sie nicht aus, jetzt einen Bucket zu erstellen. Verwenden Sie stattdessen den Tenant Manager, um später "${post_edited_translations.segment}".

   a. Geben Sie den Namen des Buckets ein, den die S3-Anwendung verwenden wird. Zum Beispiel `s3-bucket`.

      Der Bucket-Name kann nach der Erstellung nicht mehr geändert werden.

   b. Die **Region** für diesen Bucket auswählen.

      Die Standardregion (`us-east-1` sollte verwendet werden, es sei denn, es ist geplant, ILM zukünftig zum Filtern von Objekten basierend auf der Region des Buckets einzusetzen.

5. **Erstellen und fortfahren** auswählen.

Schritt 4 von 6: Daten herunterladen

Im Schritt „Daten herunterladen“ können Sie eine oder zwei Dateien herunterladen, um die Details der soeben vorgenommenen Konfiguration zu speichern.

Schritte

1. Wenn **Root-Benutzer S3-Zugriffsschlüssel automatisch erstellen** ausgewählt wurde, gilt eines oder beides der folgenden Verfahren:
   - Wählen Sie **Zugriffsschlüssel herunterladen**, um eine `.csv` Datei herunterzuladen, die den Mandantenkontonamen, 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. **Konfigurationswerte herunterladen** ermöglicht das Herunterladen einer `.txt` Datei, die die Einstellungen für den Load Balancer Endpoint, den Tenant, den Bucket und den Root-Benutzer enthält.
3. Diese Informationen sollten an einem sicheren Ort gespeichert werden.

Schließen Sie diese Seite erst, nachdem Sie beide Zugriffsschlüssel kopiert haben. Die Schlüssel sind nach dem Schließen der Seite nicht mehr verfügbar. Diese Informationen sollten an einem sicheren Ort gespeichert werden, da sie zum Abrufen von Daten aus Ihrem StorageGRID System verwendet werden können.

4. Falls Sie dazu aufgefordert werden, das Kontrollkästchen auswählen, um zu bestätigen, dass Sie die Schlüssel heruntergeladen oder kopiert haben.
5. **Weiter** auswählen, um zum ILM Regel- und Richtlinienschritt zu gelangen.

Schritt 5 von 6: ILM-Regel und ILM-Richtlinie für S3 überprüfen

Die Regeln des Informationslebenszyklusmanagements (ILM) steuern die Platzierung, Speicherdauer und das Aufnahmeverhalten aller Objekte in Ihrem StorageGRID System. Die mit StorageGRID enthaltene ILM-Richtlinie erstellt zwei replizierte Kopien aller Objekte. Diese Richtlinie bleibt in Kraft, bis mindestens eine neue Richtlinie aktiviert wird.

Schritte

1. Die auf der Seite bereitgestellten Informationen können überprüft werden.
2. Wenn spezifische Anweisungen für die Objekte des neuen Mandanten oder Buckets hinzugefügt werden sollen, ist eine neue Regel und eine neue Richtlinie zu erstellen. Siehe "${post_edited_translations.segment}" und "ILM Richtlinien verwenden".
3. **Ich habe diese Schritte überprüft und verstehe, was ich tun muss** auswählen.
4. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie wissen, was als Nächstes zu tun ist.
5. **Weiter** auswählen, um zu **Zusammenfassung** zu gelangen.

Schritt 6 von 6: Zusammenfassung überprüfen

Schritte

1. Überprüfen Sie die Zusammenfassung.
2. Beachten Sie die Details in den nächsten Schritten, die die möglicherweise erforderliche zusätzliche Konfiguration vor der Verbindung mit dem S3 Client beschreiben. Wenn beispielsweise **Sign in as root** ausgewählt wird, erfolgt eine Weiterleitung zum Tenant Manager, wo Tenant-Benutzer hinzugefügt, zusätzliche Buckets erstellt und Bucket-Einstellungen aktualisiert werden können.
3. Wählen Sie **Fertigstellen**.
4. Die Anwendung wird mit der Datei, die von StorageGRID heruntergeladen wurde, oder mit den manuell ermittelten Werten konfiguriert.

HA-Gruppen verwalten

Erfahren Sie mehr über StorageGRID Hochverfügbarkeitsgruppen

${post_edited_translations.segment}

Sie können die Netzwerkschnittstellen mehrerer Admin- und Gateway-Knoten zu einer hochverfügbaren (HA) Gruppe zusammenfassen. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle die Arbeitslast übernehmen.

Jede HA-Gruppe ermöglicht den Zugriff auf die gemeinsam genutzten Dienste auf den ausgewählten Knoten.

- HA-Gruppen, die Gateway-Knoten, Admin-Knoten oder beides umfassen, bieten hochverfügbare Datenverbindungen für S3-Clients.
- HA-Gruppen, die ausschließlich Admin-Knoten enthalten, bieten hochverfügbare Verbindungen zum Grid Manager und zum Tenant Manager.
- Eine HA-Gruppe, die ausschließlich Service-Appliances und VMware-basierte Softwareknoten umfasst, kann hochverfügbare Verbindungen für "S3-Mandanten, die S3 Select verwenden" bereitstellen. HA-Gruppen werden bei der Verwendung von S3 Select empfohlen, sind aber nicht erforderlich.

Wie wird eine HA Gruppe erstellt?

1. Sie wählen eine Netzwerkschnittstelle für einen oder mehrere Admin Nodes oder Gateway Nodes aus. Sie können eine Grid Network-Schnittstelle (eth0), eine Client Network-Schnittstelle (eth2), eine VLAN-Schnittstelle oder eine Zugriffsschnittstelle verwenden, die Sie dem Node hinzugefügt haben.

   > Sie können einer HA-Gruppe keine Schnittstelle hinzufügen, wenn diese über eine per DHCP zugewiesene IP-Adresse verfügt.

2. Sie definieren eine Schnittstelle als primäre Schnittstelle. Die primäre Schnittstelle ist die aktive Schnittstelle, es sei denn, es tritt ein Ausfall auf.
3. ${post_edited_translations.segment}
4. Sie weisen der Gruppe ein bis zehn virtuelle IP-Adressen (VIP-Adressen) zu. Clientanwendungen können jede dieser VIP-Adressen verwenden, um eine Verbindung zu StorageGRID herzustellen.

Anweisungen dazu finden Sie unter "${post_edited_translations.segment}".

${post_edited_translations.segment}

Im Normalbetrieb werden alle VIP-Adressen der HA-Gruppe der Primary-Schnittstelle hinzugefügt, die an erster Stelle in der Prioritätsreihenfolge steht. Solange die Primary-Schnittstelle verfügbar ist, wird sie verwendet, wenn Clients eine Verbindung zu einer beliebigen VIP-Adresse der Gruppe herstellen. Das heißt, im Normalbetrieb ist die Primary-Schnittstelle die „aktive“ Schnittstelle der Gruppe.

Ebenso fungieren im Normalbetrieb alle Schnittstellen mit niedrigerer Priorität für die HA-Gruppe als "Backup"-Schnittstellen. Diese Backup-Schnittstellen kommen erst dann zum Einsatz, wenn die primäre (derzeit aktive) Schnittstelle nicht mehr verfügbar ist.

Aktueller HA-Gruppenstatus eines Knotens

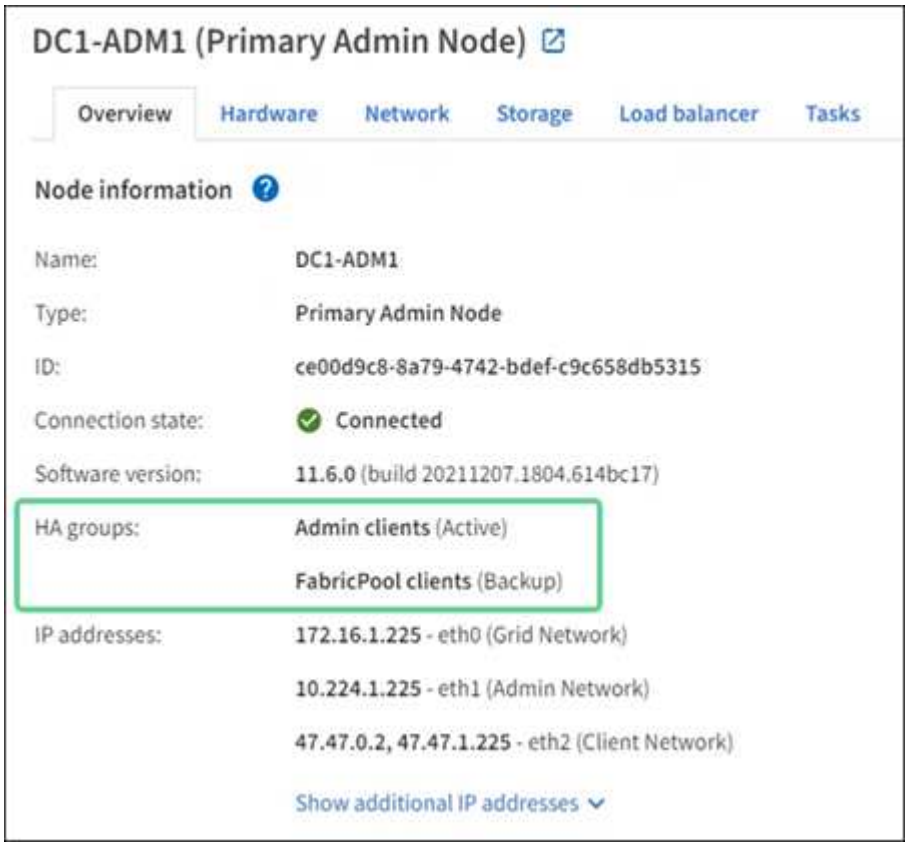
Ob ein Knoten einer HA-Gruppe zugewiesen ist und wie sein aktueller Status ist, wird unter **Knoten** > ***node*** angezeigt.

Wenn die Registerkarte **Übersicht** einen Eintrag für **HA groups** enthält, wird der Knoten den aufgeführten **HA groups** zugeordnet. Der Wert nach dem Gruppennamen gibt den aktuellen Status des Knotens in der **HA group** an:

- **Aktiv**: Die HA-Gruppe wird aktuell auf diesem Knoten ausgeführt.
- **Backup**: Die HA-Gruppe verwendet diesen Knoten derzeit nicht, dies ist eine Backup-Schnittstelle.
- **Angehalten**: Die HA-Gruppe kann auf diesem Knoten nicht gehostet werden, da der Hochverfügbarkeitsdienst (keepalived) manuell gestoppt wurde.
- **Fehler**: Die HA-Gruppe kann auf diesem Knoten aufgrund eines oder mehrerer der folgenden Gründe nicht gehostet werden:

- Der Load Balancer (nginx-gw) Dienst läuft nicht auf dem Knoten.
- Die eth0 oder VIP-Schnittstelle des Knotens ist ausgefallen.
- Der Knoten ist ausgefallen.

In diesem Beispiel wurde der primäre Admin-Knoten zu zwei HA-Gruppen hinzugefügt. Dieser Knoten ist aktuell die aktive Schnittstelle für die Admin-Clients-Gruppe und eine Backup-Schnittstelle für die FabricPool Clients-Gruppe.



Was passiert, wenn die aktive Schnittstelle ausfällt?

Die Schnittstelle, die aktuell die VIP-Adressen hostet, ist die aktive Schnittstelle. Wenn die HA-Gruppe aus mehr als einer Schnittstelle besteht und die aktive Schnittstelle ausfällt, werden die VIP-Adressen in der Prioritätsreihenfolge auf die erste verfügbare Backup-Schnittstelle verschoben. Fällt diese Schnittstelle aus, werden die VIP-Adressen auf die nächste verfügbare Backup-Schnittstelle verschoben und so weiter.

Ein Failover kann aus folgenden Gründen ausgelöst werden:

- Der Knoten, auf dem die Schnittstelle konfiguriert ist, fällt aus.
- Der Knoten, auf dem die Schnittstelle konfiguriert ist, verliert für mindestens 2 Minuten die Verbindung zu allen anderen Knoten.
- Die aktive Schnittstelle fällt aus.
- Der Load Balancer Dienst stoppt.
- Der Hochverfügbarkeitsdienst wird angehalten.

Ein Failover wird möglicherweise nicht durch Netzwerkfehler außerhalb des Knotens ausgelöst, der die aktive Schnittstelle hostet. Ebenso wird ein Failover nicht durch die Dienste für den Grid Manager oder den Tenant Manager ausgelöst.

Der Failover-Prozess dauert in der Regel nur wenige Sekunden und ist so schnell, dass Clientanwendungen kaum beeinträchtigt werden und sich auf normale Wiederholungsmechanismen verlassen können, um den Betrieb fortzusetzen.

Sobald der Fehler behoben ist und wieder eine Schnittstelle mit höherer Priorität verfügbar ist, werden die VIP-Adressen automatisch auf die Schnittstelle mit der höchsten verfügbaren Priorität verschoben.

Wie StorageGRID HA-Gruppen Hochverfügbarkeit bereitstellen

Mit Hochverfügbarkeitsgruppen (HA-Gruppen) lassen sich hochverfügbare Verbindungen zu StorageGRID für Objektdaten und für administrative Zwecke bereitstellen.

- Eine HA-Gruppe kann hochverfügbare administrative Verbindungen zum Grid Manager oder zum Tenant Manager bereitstellen.
- Eine HA-Gruppe kann hochverfügbare Datenverbindungen für S3-Clients bereitstellen.
- Eine HA-Gruppe, die nur eine Schnittstelle enthält, ermöglicht die Bereitstellung vieler VIP-Adressen und das explizite Festlegen von IPv6-Adressen.

Eine HA-Gruppe kann nur dann hochverfügbar sein, wenn alle in der Gruppe enthaltenen Knoten dieselben Dienste bereitstellen. Beim Erstellen einer HA-Gruppe werden Schnittstellen von den Knotentypen hinzugefügt, die die benötigten Dienste bereitstellen.

- **Admin-Knoten**: Der Load Balancer Service ist enthalten und ermöglicht den Zugriff auf den Grid Manager oder den Tenant Manager.
- **Gateway-Knoten**: Enthalten den Load Balancer Service.

Zweck der HA Gruppe	Knoten dieses Typs zur HA Gruppe hinzufügen
Zugriff auf Grid Manager	• Primärer Admin Node (**Primary**) • Nicht-primäre Admin Nodes **Hinweis:** Der primäre Admin-Node muss die primäre Schnittstelle sein. Einige Wartungsvorgänge können nur vom primären Admin-Node aus durchgeführt werden.
Zugriff nur auf den Tenant Manager	• Primäre oder nicht-primäre Admin Nodes
S3 Clientzugriff, Load Balancer Service	• Admin-Nodes • Gateway-Nodes
S3 Clientzugriff für "S3 Select"	• Service Appliances • VMware-basierte Software-Nodes **Hinweis**: HA Gruppen werden bei der Verwendung von S3 Select empfohlen, sind aber nicht erforderlich.

Einschränkungen bei der Verwendung von HA-Gruppen mit Grid Manager oder Tenant Manager

Wenn ein Grid Manager oder Tenant Manager Dienst ausfällt, wird kein HA-Gruppen-Failover ausgelöst.

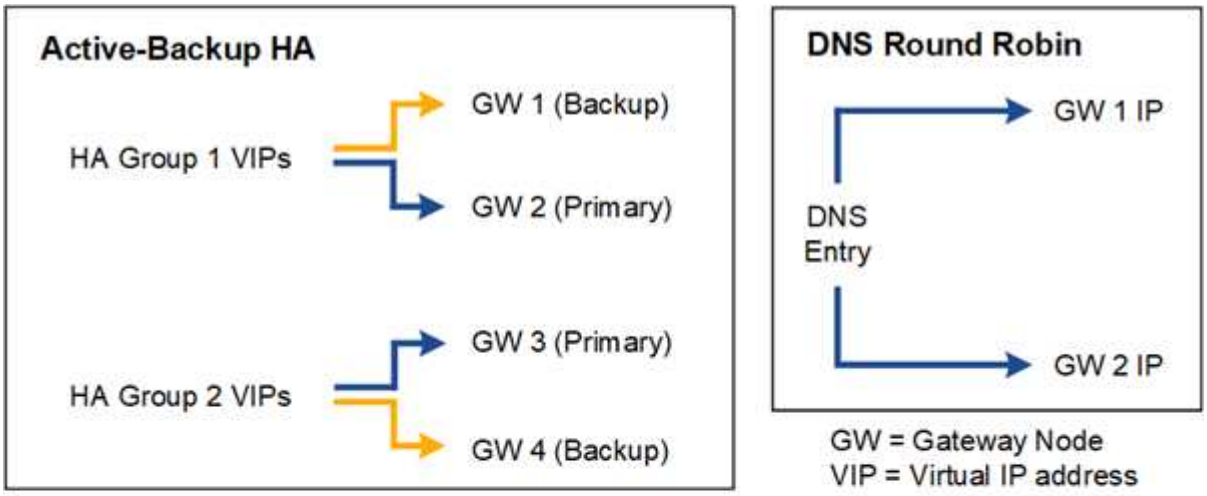
Wenn Sie beim Failover im Grid Manager oder im Tenant Manager angemeldet sind, werden Sie abgemeldet und müssen sich erneut anmelden, um Ihre Aufgabe fortzusetzen.

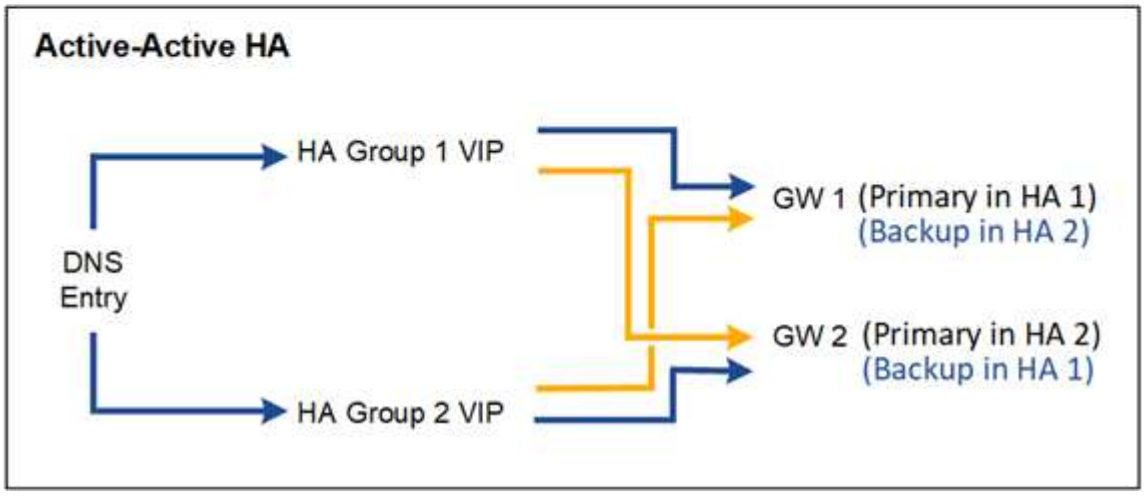
Einige Wartungsarbeiten können nicht durchgeführt werden, wenn der primäre Admin Node nicht verfügbar ist. Während eines Failovers kann der Grid Manager zur Überwachung des StorageGRID Systems verwendet werden.

Konfigurationsoptionen für StorageGRID High-Availability-Gruppen

Die folgenden Diagramme zeigen Beispiele für verschiedene Möglichkeiten, wie Sie Hochverfügbarkeitsgruppen (HA-Gruppen) konfigurieren können. Jede Option hat Vor- und Nachteile.

In den Diagrammen kennzeichnet Blau die primäre Schnittstelle in der HA-Gruppe und Gelb die Backup-Schnittstelle in der HA-Gruppe.





Die Tabelle fasst die Vorteile jeder im Diagramm dargestellten HA Konfiguration zusammen.

Konfiguration	Vorteile	Nachteile
Active-Backup HA	• Verwaltet von StorageGRID ohne externe Abhängigkeiten. • Schnelles Failover.	• Nur ein Knoten in einer HA-Gruppe ist aktiv. Mindestens ein Knoten pro HA-Gruppe ist im Leerlauf.
DNS Round Robin	• Erhöhter Gesamtdurchsatz. • Keine Leerlauf-Hosts.	• Langsames Failover, das vom Verhalten des Clients abhängen kann. • Erfordert die Konfiguration von Hardware außerhalb von StorageGRID. • Erfordert einen vom Kunden implementierten Gesundheitscheck.
Active-Active-HA	• Der Datenverkehr wird auf mehrere HA-Gruppen verteilt. • Hoher Gesamtdurchsatz, der mit der Anzahl der HA-Gruppen skaliert. • Schnelles Failover.	• Komplexer zu konfigurieren. • Erfordert die Konfiguration von Hardware außerhalb von StorageGRID. • Erfordert einen vom Kunden implementierten Gesundheitscheck.

Konfigurieren von Hochverfügbarkeitsgruppen in StorageGRID

Sie können Hochverfügbarkeitsgruppen (HA-Gruppen) konfigurieren, um hochverfügbaren Zugriff auf die Dienste auf Admin-Nodes oder Gateway-Nodes bereitzustellen.

Ein StorageGRID System kann maximal 255 HA Gruppen haben.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Root-Zugriffsberechtigung".
- Wenn Sie eine VLAN-Schnittstelle in einer HA-Gruppe verwenden möchten, haben Sie die VLAN-Schnittstelle erstellt. Siehe "${post_edited_translations.segment}".
- Wenn eine Zugriffsschnittstelle für einen Node in einer HA-Gruppe verwendet werden soll, wurde die Schnittstelle erstellt:
  - **Linux (vor der Installation des Node)**: "Knotenkonfigurationsdateien erstellen"
  - **Linux (nach der Installation des Nodes)**: "Trunk- oder Zugriffsschnittstellen zu einem Node hinzufügen"
  - **VMware (nach der Installation des Knotens)**: "Trunk- oder Zugriffsschnittstellen zu einem Node hinzufügen"

„Linux“ bezieht sich auf eine RHEL-, Ubuntu- oder Debian-Installation. Eine Liste der unterstützten Versionen befindet sich unter "NetApp Interoperabilitätsmatrix Tool (IMT)".

Eine Hochverfügbarkeitsgruppe erstellen

Beim Erstellen einer Hochverfügbarkeitsgruppe werden eine oder mehrere Schnittstellen ausgewählt und in eine Prioritätsreihenfolge gebracht. Danach werden der Gruppe eine oder mehrere VIP-Adressen zugewiesen.

Eine Schnittstelle muss für einen Gateway-Node oder einen Admin-Node vorhanden sein, um in eine HA-Gruppe aufgenommen zu werden. Eine HA-Gruppe kann für einen bestimmten Node nur eine Schnittstelle verwenden, jedoch können andere Schnittstellen desselben Nodes in anderen HA-Gruppen verwendet werden.

Assistenten aufrufen

Schritte

1. **Konfiguration** > **Netzwerk** > **Hochverfügbarkeitsgruppen** auswählen.
2. Wählen Sie **Create**.

Details für die HA-Gruppe eingeben

Schritte

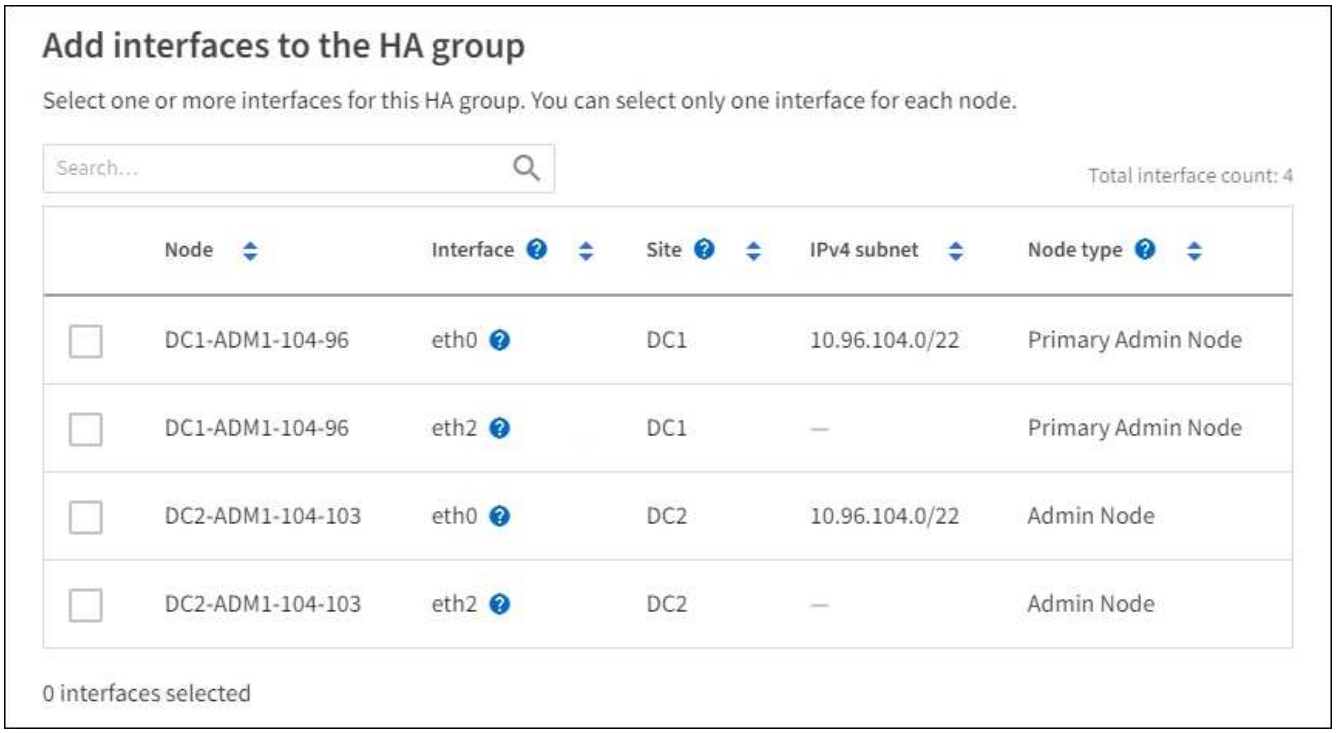
1. Einen eindeutigen Namen für die HA Gruppe angeben.
2. Optional kann eine Beschreibung für die HA Gruppe eingegeben werden.
3. Wählen Sie **Weiter**.

Schnittstellen zur HA-Gruppe hinzufügen

Schritte

1. Wählen Sie eine oder mehrere Schnittstellen aus, die zu dieser HA Gruppe hinzugefügt werden sollen.

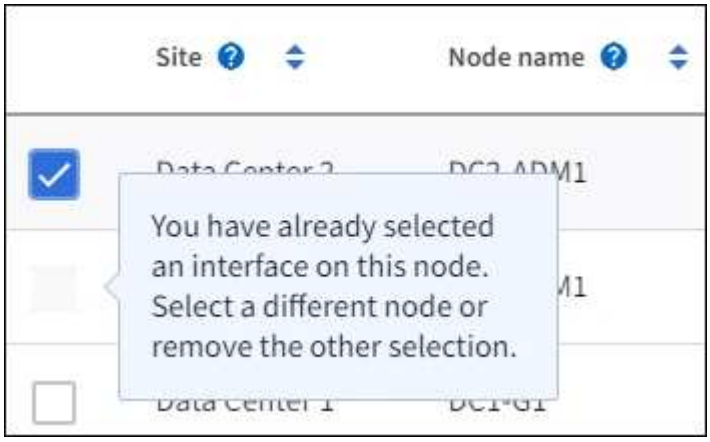
   Mit den Spaltenüberschriften lassen sich die Zeilen sortieren, oder durch Eingabe eines Suchbegriffs können Schnittstellen schneller gefunden werden.



Nach dem Erstellen einer VLAN-Schnittstelle kann es bis zu 5 Minuten dauern, bis die neue Schnittstelle in der Tabelle erscheint.

Richtlinien für die Auswahl von Schnittstellen

- Sie müssen mindestens eine Schnittstelle auswählen.
- Sie können für einen Node nur eine Schnittstelle auswählen.
- Wenn die HA-Gruppe für den HA-Schutz von Admin-Node-Diensten vorgesehen ist, zu denen der Grid Manager und der Tenant Manager gehören, sollten nur Schnittstellen auf Admin-Nodes ausgewählt werden.
- Wenn die HA-Gruppe für den HA-Schutz des S3-Client-Datenverkehrs vorgesehen ist, werden Schnittstellen auf Admin Nodes, Gateway Nodes oder beiden ausgewählt.
- Wenn Sie Schnittstellen auf verschiedenen Knotentypen auswählen, erscheint ein Informationshinweis. Es wird darauf hingewiesen, dass bei einem Failover die vom zuvor aktiven Node bereitgestellten Dienste auf dem neu aktiven Node möglicherweise nicht verfügbar sind. Beispielsweise kann ein Backup Gateway Node keinen HA-Schutz für die Admin Node-Dienste bieten. Ebenso kann ein Backup Admin Node nicht alle Wartungsverfahren ausführen, die der primäre Admin Node bereitstellen kann.
- Wenn Sie keine Schnittstelle auswählen können, ist das entsprechende Kontrollkästchen deaktiviert. Die QuickInfo bietet weitere Informationen.



- Eine Schnittstelle kann nicht ausgewählt werden, wenn deren Subnetzwert oder Gateway mit einer anderen ausgewählten Schnittstelle in Konflikt steht.
- Eine konfigurierte Schnittstelle kann nicht ausgewählt werden, wenn sie keine statische IP-Adresse besitzt.

2. Wählen Sie **Weiter**.

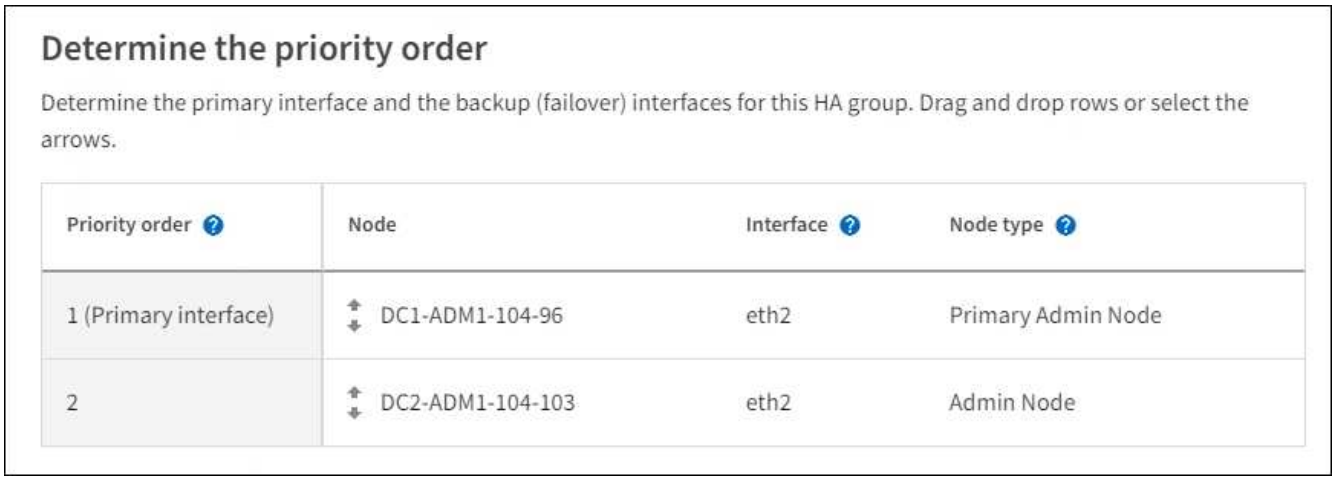
Prioritätsreihenfolge festlegen

Wenn die HA-Gruppe mehr als eine Schnittstelle umfasst, kann bestimmt werden, welche die primäre Schnittstelle ist und welche die Backup- (Failover-) Schnittstellen sind. Wenn die primäre Schnittstelle ausfällt, werden die VIP-Adressen auf die verfügbare Schnittstelle mit der höchsten Priorität verschoben. Fällt diese Schnittstelle aus, werden die VIP-Adressen auf die verfügbare Schnittstelle mit der nächsthöheren Priorität verschoben und so weiter.

Schritte

1. Zeilen in der Spalte **Prioritätsreihenfolge** ziehen, um die primäre Schnittstelle und etwaige Backup-Schnittstellen zu bestimmen.

Die erste Schnittstelle in der Liste ist die Primary-Schnittstelle. Die Primary-Schnittstelle ist die aktive Schnittstelle, sofern kein Fehler auftritt.



Wenn die HA-Gruppe Zugriff auf den Grid Manager gewährt, muss eine Schnittstelle auf dem primären Admin-Node als primäre Schnittstelle ausgewählt werden. Einige Wartungsvorgänge sind nur vom primären Admin-Node aus möglich.

2. Wählen Sie **Weiter**.

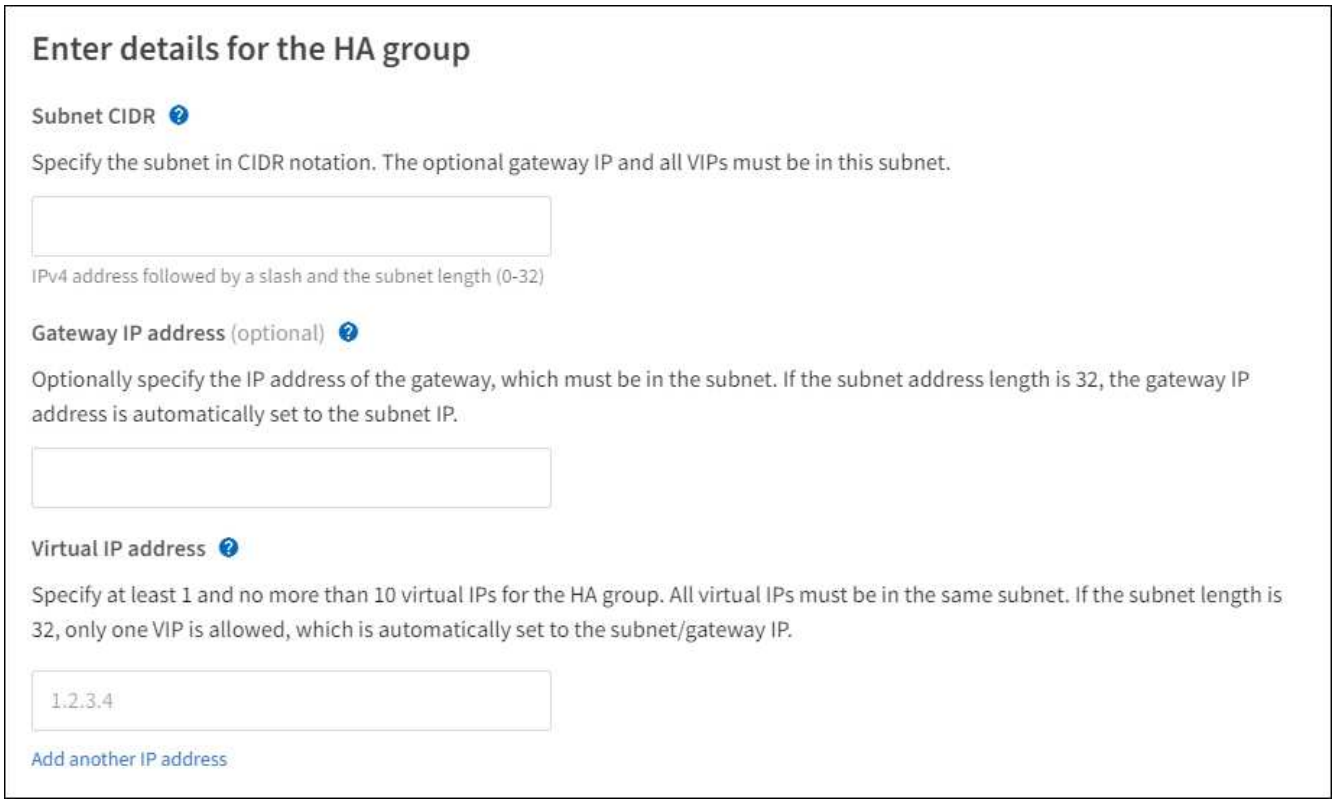
IP-Adressen eingeben

Schritte

1. Im Feld **Subnet CIDR** ist das VIP-Subnetz in CIDR-Notation anzugeben, also eine IPv4-Adresse, gefolgt von einem Schrägstrich und der Subnetzlänge (0-32).

   Die Netzwerkadresse darf keine gesetzten Host-Bits aufweisen. Zum Beispiel `192.16.0.0/22`.

   Bei Verwendung eines 32-Bit-Präfixes dient die VIP-Netzwerkadresse auch als Gateway-Adresse und VIP-Adresse.



2. Optional kann die **Gateway-IP-Adresse** eingegeben werden, falls S3-Administrations- oder Mandantenclients von einem anderen Subnetz auf diese VIP-Adressen zugreifen. Die Gateway-Adresse muss sich innerhalb des VIP-Subnetzes befinden.

   Client- und Administratorbenutzer nutzen dieses Gateway für den Zugriff auf die virtuellen IP-Adressen.

3. Geben Sie mindestens eine und höchstens zehn VIP-Adressen für die aktive Schnittstelle in der HA-Gruppe ein. Alle VIP-Adressen müssen sich innerhalb des VIP-Subnetzes befinden und sind gleichzeitig auf der aktiven Schnittstelle aktiv.

   Sie müssen mindestens eine IPv4-Adresse angeben. Optional können Sie zusätzliche IPv4- und IPv6-Adressen angeben.

4. **HA-Gruppe erstellen** auswählen und **Fertigstellen** wählen.

   Die HA Group ist erstellt, und die konfigurierten virtuellen IP-Adressen können nun verwendet werden.

Nächste Schritte

Wenn diese HA-Gruppe für den Lastausgleich verwendet wird, sollte ein Load-Balancer-Endpunkt erstellt werden, um den Port und das Netzwerkprotokoll zu bestimmen und alle erforderlichen Zertifikate anzuhängen. Siehe "Load Balancer-Endpunkte konfigurieren".

Eine hochverfügbare Gruppe bearbeiten

Sie können eine hochverfügbare (HA) Gruppe 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 kann es erforderlich sein, eine HA-Gruppe zu bearbeiten, wenn der Node entfernt werden soll,

der einer ausgewählten Schnittstelle in einem Standort- oder Node-Decommissioning-Verfahren zugeordnet ist.

Schritte

1. **Konfiguration** > **Netzwerk** > **Hochverfügbarkeitsgruppen** auswählen.

   Die Seite „Hochverfügbarkeitsgruppen“ zeigt alle vorhandenen HA Gruppen.

2. Aktivieren Sie das Kontrollkästchen für die HA Gruppe, die bearbeitet werden soll.
3. Führen Sie je nach gewünschter Aktualisierung eine der folgenden Optionen aus:
   - **Aktionen** > **Virtuelle IP-Adresse bearbeiten** auswählen, um VIP-Adressen hinzuzufügen oder zu entfernen.
   - **Aktionen** > **HA-Gruppe bearbeiten** auswählen, 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. Die virtuellen IP-Adressen für die HA-Gruppe werden aktualisiert.
   b. **Speichern** auswählen.
   c. Wählen Sie **Fertigstellen**.
5. Wenn Sie **HA-Gruppe bearbeiten** ausgewählt haben:
   a. Optional kann der Name oder die Beschreibung der Gruppe aktualisiert werden.
   b. Optional können die Kontrollkästchen aktiviert oder deaktiviert werden, um Schnittstellen hinzuzufügen oder zu entfernen.

      Wenn die HA-Gruppe Zugriff auf den Grid Manager gewährt, ist eine Schnittstelle auf dem primären Admin-Node als primäre Schnittstelle auszuwählen. Einige Wartungsvorgänge sind nur vom primären Admin-Node aus möglich.

   c. Optional lassen sich Zeilen per Drag & Drop verschieben, um die Prioritätsreihenfolge der Primary-Schnittstelle und aller Backup-Schnittstellen für diese HA-Gruppe zu ändern.
   d. Optional können die virtuellen IP-Adressen aktualisiert werden.
   e. **Speichern** auswählen und anschließend **Fertigstellen** auswählen.

Eine Hochverfügbarkeitsgruppe entfernen

Sie können eine oder mehrere Hochverfügbarkeitsgruppen (HA) gleichzeitig entfernen.

Eine HA-Gruppe kann nicht entfernt werden, wenn sie an einen Load-Balancer-Endpunkt gebunden ist. Zum Löschen einer HA-Gruppe muss sie von allen Load-Balancer-Endpunkten entfernt werden, die sie verwenden.

Um Client-Unterbrechungen zu vermeiden, sollten alle betroffenen S3-Clientanwendungen aktualisiert werden, bevor eine HA Gruppe entfernt wird. Jeder Client muss so aktualisiert werden, dass er eine andere IP-Adresse verwendet, zum Beispiel die virtuelle IP-Adresse einer anderen HA Gruppe oder die IP-Adresse, die während der Installation für eine Schnittstelle konfiguriert wurde.

Schritte

1. **Konfiguration** > **Netzwerk** > **Hochverfügbarkeitsgruppen** auswählen.

2. Die Spalte **Load balancer endpoints** für jede HA-Gruppe, die entfernt werden soll, prüfen. Wenn Load balancer endpoints aufgeführt sind:
   a. Zu **Konfiguration** > **Netzwerk** > **Load balancer endpoints** wechseln.
   b. Das Kontrollkästchen für den Endpunkt auswählen.
   c. **Aktionen** > **Endpunktbindungsmodus bearbeiten** auswählen.
   d. Der Bindungsmodus wird aktualisiert, um die HA Gruppe zu entfernen.
   e. Wählen Sie **Save changes**.
3. Wenn keine Load-Balancer-Endpunkte aufgeführt sind, das Kontrollkästchen für jede HA-Gruppe auswählen, die entfernt werden soll.
4. Wählen Sie **Aktionen** > **HA-Gruppe entfernen**.
5. Die Nachricht kann überprüft werden, und mit **HA-Gruppe löschen** wird die Auswahl bestätigt.

   Alle ausgewählten HA-Gruppen werden entfernt. Auf der Seite Hochverfügbarkeitsgruppen erscheint ein grünes Erfolgsbanner.

Lastverteilung verwalten

Erfahren Sie mehr über StorageGRID Load Balancing

Sie können Load Balancing verwenden, um die Arbeitslasten für die Datenaufnahme und die Datenabfrage von S3-Clients zu bewältigen.

Was ist Lastverteilung?

Wenn eine Clientanwendung Daten in einem StorageGRID-System speichert oder abruft, verwendet StorageGRID einen Load Balancer, um die Datenaufnahme und -abfrage zu verwalten. Load Balancing maximiert Geschwindigkeit und Verbindungskapazität, indem die Arbeitslast auf mehrere Storage Nodes verteilt wird.

Der StorageGRID Load Balancer Service ist auf allen Admin Nodes und allen Gateway Nodes installiert und bietet Layer 7 Load Balancing. Er übernimmt die Transport Layer Security (TLS) Terminierung von Clientanfragen, prüft die Anfragen und stellt neue sichere Verbindungen zu den Storage Nodes her.

Der Load Balancer Service auf jedem Knoten arbeitet unabhängig, wenn er Client-Datenverkehr an die Storage Nodes weiterleitet. Durch einen Gewichtungsprozess leitet der Load Balancer Service mehr Anfragen an Storage Nodes mit höherer CPU-Verfügbarkeit weiter.

> Obwohl der StorageGRID Load Balancer-Dienst die empfohlene Methode zum Lastausgleich ist, können Sie alternativ auch einen Load Balancer eines Drittanbieters integrieren. Weitere Informationen erhalten Sie von Ihrem NetApp Account Representative oder unter "Verwenden Sie Load Balancer von Drittanbietern mit StorageGRID".

Wie viele Load-Balancing-Knoten werden benötigt?

Als allgemeine Best Practice sollte jeder Standort in Ihrem StorageGRID System zwei oder mehr Knoten mit dem Load Balancer Service umfassen. Ein Standort kann beispielsweise zwei Gateway Nodes oder sowohl einen Admin Node als auch einen Gateway Node enthalten. Es sollte sichergestellt sein, dass für jeden Load Balancer Knoten eine ausreichende Netzwerk-, Hardware- oder Virtualisierungsinfrastruktur vorhanden ist, unabhängig davon, ob Service Appliances, Bare Metal Nodes oder virtuelle Maschinen (VM) basierte Knoten

verwendet werden.

Was ist ein Load Balancer Endpunkt?

Ein Load Balancer-Endpunkt definiert den Port und das Netzwerkprotokoll (HTTPS oder HTTP), das von eingehenden und ausgehenden Client-Anwendungsanfragen verwendet wird, um auf die Knoten zuzugreifen, die den Load Balancer-Service enthalten. Der Endpunkt definiert außerdem den Clienttyp (S3), den Bindungsmodus und optional eine Liste zulässiger oder gesperrter Mandanten.

Um einen Load-Balancer-Endpunkt zu erstellen, kann entweder der Grid Manager verwendet werden oder die S3-Einrichtung und die FabricPool-Assistenten abgeschlossen werden:

- "Load Balancer-Endpunkte konfigurieren"
- "Den S3 Setup-Assistenten verwenden"
- "Den FabricPool Einrichtungsassistenten verwenden"

Überlegungen zum Load Balancer Caching

Caching verbessert die Performance deutlich, wenn eine Arbeitslast auf eine Teilmenge der Daten zugreift und Objekte mehrfach verwendet. Zudem ermöglicht Caching den Fernzugriff auf den Objektspeicher ohne vollständige Grid-Bereitstellung. Load balancer Caching ist nur für Gateway Nodes verfügbar.

Beim Erstellen von Load Balancer-Endpunkten:

- Caching sollte nur für Workloads aktiviert werden, die in Cache speicherbar sind. Workloads, die häufiger auf nicht zwischengespeicherte Daten als auf zwischengespeicherte Daten zugreifen, weisen eine schlechtere Performance auf als ohne Nutzung des Caches. In einigen Fällen können Workloads mit hohen Überschreibungs- und Löschraten auch die garantierte Schreibausdauer des Laufwerks überschreiten.
- Das Hinzufügen zusätzlicher Endpunkte oder Knoten für das Caching einzelner Workloads, die sich gut für das Caching eignen, kann in Betracht gezogen werden.
- Verwenden Sie separate Endpunkte für in Cache speicherbare und nicht in Cache speicherbare Workloads. Diese Trennung gewährleistet, dass Caching-Mechanismen angemessen angewendet werden und die Verarbeitung nicht in Cache speicherbarer Daten nicht beeinträchtigen.
- Eine potenziell in Cache speicherbare Arbeitslast kann bewertet werden, indem sie an den cachefähigen Endpunkt geleitet wird. Die Cache-Treffer-Rate sollte überwacht und überprüft werden, um die Eignung der Arbeitslast für das Caching zu bestimmen. Diese Bewertung trägt zur Optimierung der Performance und zur effizienten Nutzung der Cache-Ressourcen bei.
- "Audit-Protokolle prüfen"um festzustellen, ob eine bestehende Arbeitslast für Caching geeignet ist. Für einen bestimmten Zeitraum ist zu ermitteln, wie viel Prozent der GET-Anfragen eindeutige Objekte betreffen. Um für Caching geeignet zu sein, sollte dieser Wert unter 50 % liegen.

Beispiele für Arbeitslasten, die sich gut für das Caching eignen könnten

- Datenseen
- Hochleistungsrechnen (HPC)
- KI/ML-Training
- Content-Distribution-Netzwerke (CDN)
- Media Asset Management

- Videoproduktion

> - Es können mehrere Objektversionen zwischengespeichert werden.
> - Bereichsleseoperationen werden unterstützt.

Beispiele für Arbeitslasten, die sich nicht gut für das Caching eignen

- FabricPool
- Backup-Anwendungen
- Storage-Tiering

> Falls für Inhalte, die vom Cache bereitgestellt werden sollen, eine Verschlüsselung im Ruhezustand auf dem Cache-Knoten erforderlich ist, "Knoten- oder Laufwerkverschlüsselung aktivieren".

Arten von Objekten und Anfragen, die nicht im Cache gespeichert 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 Verfahren verschlüsselt wurden:
  - SSE (serverseitige Verschlüsselung mit von StorageGRID verwalteten Schlüsseln)
  - SSE-C (serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln)
  - Verschlüsselung gespeicherter Objekte

Alle Anfragen, die nicht zwischengespeichert sind, werden an einen vorgelagerten LDR weitergeleitet, als wäre der Cache nicht aktiviert.

Verwandte Informationen

- "Fehlerbehebung beim Load Balancer Caching"
- Weitere Informationen zum Load-Balancer-Caching sind beim technischen Support erhältlich.

Überlegungen zum Port

Der Port für einen Load-Balancer-Endpunkt ist standardmäßig 10433 für den ersten Endpunkt, den Sie erstellen, aber Sie können jeden ungenutzten externen Port zwischen 1 und 65535 angeben. Wenn Sie Port 80 oder 443 verwenden, nutzt der Endpunkt den Load Balancer Service nur auf Gateway-Knoten. Diese Ports sind auf Admin-Knoten reserviert. Wenn Sie denselben Port für mehr als einen Endpunkt verwenden, muss für jeden Endpunkt ein anderer Bindungsmodus angegeben werden.

Von anderen Grid-Services verwendete Ports sind nicht zulässig. Siehe "StorageGRID interne Ports".

Überlegungen zum Netzwerkprotokoll

In den meisten Fällen sollten die Verbindungen zwischen Clientanwendungen und StorageGRID die Transport Layer Security (TLS)-Verschlüsselung verwenden. Eine Verbindung zu StorageGRID ohne TLS-Verschlüsselung wird unterstützt, ist jedoch insbesondere in Produktionsumgebungen nicht empfehlenswert. Beim Auswählen des Netzwerkprotokolls für den StorageGRID Load Balancer-Endpunkt sollte **HTTPS** gewählt werden.

Überlegungen zu Load Balancer Endpunktzertifikaten

Wenn Sie **HTTPS** als Netzwerkprotokoll für den Load-Balancer-Endpunkt auswählen, müssen Sie ein Sicherheitszertifikat bereitstellen. Beim Erstellen des Load-Balancer-Endpunkts stehen diese drei Optionen zur Verfügung:

- **Laden Sie ein signiertes Zertifikat hoch (empfohlen)**. Dieses Zertifikat kann von einer öffentlich vertrauenswürdigen oder einer privaten Zertifizierungsstelle (CA) signiert sein. Die Verwendung eines Serverzertifikats einer öffentlich vertrauenswürdigen CA zur Sicherung der Verbindung ist die beste Vorgehensweise. Im Gegensatz zu generierten Zertifikaten können von einer CA signierte Zertifikate ohne Unterbrechung ausgetauscht werden, was dazu beitragen kann, Ablaufprobleme zu vermeiden.

  Sie müssen die folgenden Dateien beschaffen, bevor Sie den Load Balancer Endpunkt erstellen:

  - Die benutzerdefinierte Serverzertifikatsdatei.
  - Die benutzerdefinierte private Schlüsseldatei des Serverzertifikats.
  - Optional ein CA-Bundle der Zertifikate von jeder zwischengeschalteten ausstellenden Zertifizierungsstelle.
- **Ein selbstsigniertes Zertifikat generieren**.
- **Verwenden Sie das globale StorageGRID S3-Zertifikat**. Eine benutzerdefinierte Version dieses Zertifikats muss hochgeladen oder generiert werden, bevor sie für den Load-Balancer-Endpunkt ausgewählt werden kann. Siehe "S3 API-Zertifikate konfigurieren".

Welche Werte werden benötigt?

Um das Zertifikat zu erstellen, müssen Sie alle Domänennamen und IP-Adressen kennen, die S3-Clientanwendungen für den Zugriff auf den Endpunkt verwenden.

Der Eintrag **Subject DN** (Distinguished Name) des Zertifikats muss die vollqualifizierte Domain enthalten, die die Clientanwendung für StorageGRID verwendet. Beispiel:

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

Wie erforderlich, kann das Zertifikat Platzhalter verwenden, um die vollqualifizierten Domainnamen aller Admin-Knoten und Gateway-Knoten darzustellen, auf denen der Load Balancer Service ausgeführt wird. Beispielsweise verwendet `*.storagegrid.example.com` das *-Platzhalterzeichen, um `adm1.storagegrid.example.com` und `gn1.storagegrid.example.com` darzustellen.

Wenn die Verwendung von S3-Anfragen im Virtual Hosted-Style vorgesehen ist, muss das Zertifikat auch einen **Alternative Name**-Eintrag für jede von Ihnen konfigurierte "S3-Endpunkt-Domainname" enthalten, einschließlich aller Platzhalternamen. Beispielsweise:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

Wenn Sie Wildcards für Domainnamen verwenden, ist die "Richtlinien zur Härtung von Serverzertifikaten" zu prüfen.

Für jeden Namen im Sicherheitszertifikat ist außerdem ein DNS-Eintrag zu definieren.

Wie werden ablaufende Zertifikate verwaltet?

Wenn das Zertifikat, das zur Sicherung der Verbindung zwischen der S3-Anwendung und StorageGRID verwendet wird, abläuft, kann die Anwendung vorübergehend den Zugriff auf StorageGRID verlieren.

Um Probleme mit abgelaufenen Zertifikaten zu vermeiden, sind diese bewährten Vorgehensweisen zu beachten:

- Alle Warnmeldungen, die auf bevorstehende Ablaufdaten von Zertifikaten hinweisen, wie zum Beispiel die Warnmeldungen **Expiration of load balancer endpoint certificate** und **Expiration of global server certificate for S3 API**, sollten sorgfältig überwacht werden.
- Die Versionen des Zertifikats von StorageGRID und der S3-Anwendung sollten stets synchron gehalten werden. Wenn das für einen Load-Balancer-Endpunkt verwendete Zertifikat ersetzt oder erneuert wird, muss auch das entsprechende Zertifikat der S3-Anwendung ersetzt oder erneuert werden.
- Verwenden Sie ein öffentlich signiertes CA-Zertifikat. Wenn ein von einer CA signiertes Zertifikat verwendet wird, können Zertifikate, deren Ablauf bevorsteht, ohne Unterbrechung ersetzt werden.
- Wenn Sie ein selbstsigniertes StorageGRID Zertifikat generiert haben und dieses Zertifikat demnächst abläuft, muss das Zertifikat sowohl in StorageGRID als auch in der S3 Anwendung manuell ersetzt werden, bevor das bestehende Zertifikat abläuft.

Überlegungen zum Bindungsmodus

Der Bindungsmodus ermöglicht die Steuerung, welche IP-Adressen für den Zugriff auf einen Load Balancer Endpunkt verwendet werden dürfen. Wenn ein Endpunkt den Bindungsmodus verwendet, können Clientanwendungen nur auf den Endpunkt zugreifen, wenn sie eine zulässige IP-Adresse oder den entsprechenden vollqualifizierten Domainnamen (FQDN) verwenden. Clientanwendungen, die eine andere IP-Adresse oder einen anderen FQDN verwenden, können nicht auf den Endpunkt zugreifen.

Sie können einen der folgenden Bindungsmodi angeben:

- **Global** (Standard): Clientanwendungen 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 Endpoint zugreifen. Diese Einstellung ist zu verwenden, sofern keine Einschränkung der Erreichbarkeit eines Endpunkts erforderlich ist.
- **Virtuelle IPs von HA-Gruppen**. Clientanwendungen müssen eine virtuelle IP-Adresse (oder den entsprechenden FQDN) einer HA-Gruppe verwenden.
- **Knotenschnittstellen**. Clients müssen die IP-Adressen (oder die entsprechenden FQDNs) der ausgewählten Knotenschnittstellen verwenden.
- **Knotentyp**. Abhängig vom gewählten Knotentyp müssen Clients entweder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Admin Node oder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Gateway Node verwenden.

Überlegungen zum Mieterzugang

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 dürfen. Es kann allen Mandanten der Zugriff auf einen Endpunkt erlaubt werden (Standardeinstellung), oder es kann für jeden Endpunkt eine Liste der zulässigen oder gesperrten Mandanten festgelegt werden.

Mit dieser Funktion lässt sich eine bessere Sicherheitsisolation zwischen Mandanten und deren Endpunkten erreichen. So kann beispielsweise sichergestellt werden, dass streng geheime oder hochgradig vertrauliche Materialien eines Mandanten für andere Mandanten vollständig unzugänglich bleiben.

> Zum Zwecke der Zugriffskontrolle wird der Mandant anhand der in der Clientanfrage verwendeten Zugriffsschlüssel ermittelt. Werden keine Zugriffsschlüssel als Teil der Anfrage angegeben (z. B. bei anonymem Zugriff), wird der Bucket-Inhaber zur Ermittlung des Mandanten herangezogen.

Beispiel für den Mandantenzugriff

Um nachvollziehen zu können, wie diese Sicherheitsfunktion arbeitet, dient das folgende Beispiel zur Veranschaulichung:

1. Sie haben zwei Load Balancer Endpunkte erstellt, wie folgt:
   - **Öffentlicher** Endpunkt: Verwendet Port 10443 und ermöglicht den Zugriff für alle Mandanten.
   - **Streng geheim** Endpoint: Verwendet Port 10444 und ermöglicht den Zugriff ausschließlich für den Mandanten **Streng geheim**. Allen anderen Mandanten ist der Zugriff auf diesen Endpoint verwehrt.
2. Das `top-secret.pdf` befindet sich in einem Bucket, der dem **Top secret** Tenant gehört.

Um auf das `top-secret.pdf` zuzugreifen, kann ein Benutzer im Mandanten **Top secret** eine GET-Anfrage an `https://w.x.y.z:10444/top-secret.pdf` stellen. Da dieser Mandant den Endpunkt 10444 verwenden darf, kann der Benutzer auf das Objekt zugreifen. Wenn jedoch ein Benutzer eines anderen Mandanten dieselbe Anfrage an dieselbe URL stellt, erhält er sofort die Meldung „Zugriff verweigert“. Der Zugriff wird auch dann verweigert, wenn die Anmeldeinformationen und die Signatur gültig sind.

CPU-Verfügbarkeit

Der Load Balancer Service auf jedem Admin Node und Gateway Node arbeitet unabhängig, wenn S3-Datenverkehr an die Storage Nodes weitergeleitet wird. Durch einen Gewichtungsprozess leitet der Load Balancer Service mehr Anfragen an Storage Nodes mit höherer CPU-Verfügbarkeit weiter. Die Lastinformation der Node-CPU wird alle paar Minuten aktualisiert, die Gewichtung kann jedoch häufiger aktualisiert werden. Allen Storage Nodes wird ein minimaler Basisgewichtungswert zugewiesen, selbst wenn ein Node eine Auslastung von 100 % meldet oder seine Auslastung nicht meldet.

In einigen Fällen sind Informationen über die CPU-Verfügbarkeit auf den Standort beschränkt, an dem der Load Balancer Service ausgeführt wird.

StorageGRID Load-Balancer-Endpunkte konfigurieren

Die Load Balancer-Endpunkte legen die Ports und Netzwerkprotokolle fest, die S3-Clients für die Verbindung zum StorageGRID Load Balancer auf Gateway- und Admin-Knoten verwenden können. Endpunkte können auch für den Zugriff auf den Grid Manager, den Tenant Manager oder beide verwendet werden.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Root-Zugriffsberechtigung".
- Sie haben die "Überlegungen zum Lastausgleich" überprüft.
- Wenn Sie zuvor einen Port, den Sie für den Load-Balancer-Endpunkt verwenden möchten, neu zugeordnet haben, haben Sie "Port-Neuzuordnung entfernt".
- Sie haben alle Hochverfügbarkeitsgruppen (HA-Gruppen) erstellt, die Sie verwenden möchten. HA-Gruppen werden empfohlen, sind aber nicht erforderlich. Siehe "Hochverfügbarkeitsgruppen verwalten".
- Wenn der Load-Balancer-Endpunkt von "S3 Mandanten für S3 Select" verwendet wird, dürfen weder die IP-Adressen noch die FQDNs von Bare-Metal-Knoten genutzt werden. Für die Load-Balancer-Endpunkte, die für S3 Select verwendet werden, sind ausschließlich Service-Appliances und VMware-basierte Softwareknoten zulässig.
- Sie haben alle VLAN-Schnittstellen konfiguriert, die Sie verwenden möchten. Siehe "${post_edited_translations.segment}".
- Wenn Sie einen HTTPS-Endpunkt erstellen (empfohlen), liegen Ihnen die Informationen für das Serverzertifikat vor.

  Änderungen an einem Endpunktzertifikat können bis zu 15 Minuten benötigen, um auf alle Knoten angewendet zu werden.

  - Zum Hochladen eines Zertifikats benötigen Sie das Serverzertifikat, den privaten Schlüssel des Zertifikats und optional ein CA-Bundle.
  - Um ein Zertifikat zu generieren, benötigen Sie alle Domänennamen und IP-Adressen, die S3-Clients für den Zugriff auf den Endpunkt verwenden. Sie müssen außerdem den Betreff (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, von einer externen Zertifizierungsstelle signiertes Zertifikat ersetzt. Siehe "S3 API-Zertifikate konfigurieren".

${post_edited_translations.segment}

Jeder S3 Client Load Balancer Endpunkt spezifiziert einen Port, einen Clienttyp (S3) und ein Netzwerkprotokoll (HTTP oder HTTPS). Managementoberfläche Load Balancer Endpunkte spezifizieren einen Port, einen Schnittstellentyp und ein nicht vertrauenswürdiges Clientnetzwerk.

Assistenten aufrufen

Schritte

1. **Konfiguration** > **Netzwerk** > **Load balancer endpoints** auswählen.
2. Zum Erstellen eines Endpunkts für einen S3 Client die Registerkarte **S3 Client** auswählen.
3. Um einen Endpunkt für den Zugriff auf den Grid Manager, den Tenant Manager oder beide zu erstellen, ist die Registerkarte **Managementoberfläche** auszuwählen.
4. Wählen Sie **Create**.

Endpunktdetails eingeben

Schritte

1. Wählen Sie die passenden Anweisungen aus, um Details für den Typ des Endpunkts einzugeben, den Sie erstellen möchten.

S3 Client

Feld	Beschreibung
Name	Ein beschreibender Name für den Endpunkt, der in der Tabelle auf der Seite „Load balancer endpoints“ angezeigt wird.
Port	Der StorageGRID Port, den Sie für den Lastausgleich verwenden möchten. Dieses Feld ist standardmäßig für den ersten erstellten Endpunkt auf 10433 eingestellt, aber es kann jeder ungenutzte externe Port von 1 bis 65535 eingegeben werden. Wenn Sie **80** oder **8443** eingeben, wird der Endpunkt nur auf Gateway Nodes konfiguriert, es sei denn, Sie haben Port 8443 freigegeben. Dann kann Port 8443 als S3-Endpunkt verwendet werden, und der Port wird sowohl auf Gateway Nodes als auch auf Admin Nodes konfiguriert.
Clienttyp	Muss **S3** sein.
Netzwerkprotokoll	Das Netzwerkprotokoll, das Clients beim Verbinden mit diesem Endpunkt verwenden. • Wählen Sie **HTTPS** für eine sichere, TLS-verschlüsselte Kommunikation (empfohlen). Ein Sicherheitszertifikat muss angehängt werden, bevor der Endpunkt gespeichert werden kann. • **HTTP** für weniger sichere, unverschlüsselte Kommunikation auswählen. HTTP nur für ein Nicht-Produktions-Grid verwenden.
Caching aktivieren	Aktivieren oder deaktivieren Sie "Zwischenspeicherung auf den Gateway Nodes" für diesen Load-Balancer-Endpunkt. Wenn Probleme mit dem Caching auftreten, siehe "Fehlerbehebung beim Load Balancer Caching".

Managementoberfläche

Feld	Beschreibung
Name	Ein beschreibender Name für den Endpunkt, der in der Tabelle auf der Seite „Load balancer endpoints“ angezeigt wird.
Port	Der StorageGRID Port, der für den Zugriff auf den Grid Manager, den Tenant Manager oder beide verwendet werden soll. • Grid Manager: **8443** • Tenant Manager: **9443** • Sowohl Grid Manager als auch Tenant Manager: **443** **Hinweis**: Sie können diese voreingestellten Ports oder andere verfügbare Ports verwenden.

Feld	Beschreibung
Schnittstellentyp	Wählen Sie das Optionsfeld für die StorageGRID Schnittstelle aus, auf die über diesen Endpunkt zugegriffen wird.
Nicht vertrauenswürdiges Client-Netzwerk	**Ja** auswählen, wenn dieser Endpunkt für nicht vertrauenswürdige Clientnetzwerke zugänglich sein soll. Andernfalls **Nein** auswählen. Wenn **Ja** ausgewählt wird, ist der Port auf allen nicht vertrauenswürdigen Client-Netzwerken geöffnet. **Hinweis**: Sie können nur festlegen, ob ein Port für nicht vertrauenswürdige Clientnetzwerke geöffnet oder geschlossen ist, wenn Sie den Load Balancer-Endpunkt erstellen.

1. Wählen Sie **Weiter**.

Einen Bindungsmodus auswählen

Schritte

1. Wählen Sie einen Bindungsmodus für den Endpunkt, um zu steuern, wie auf den Endpunkt entweder über eine beliebige IP-Adresse oder über bestimmte IP-Adressen und Netzwerkschnittstellen zugegriffen wird.

   Einige Bindungsmodi sind entweder für Client-Endpunkte oder Managementoberfläche-Endpunkte verfügbar. Alle Modi für beide Endpunkttypen sind hier aufgelistet.

Modus	Beschreibung
Global (Standardeinstellung für Client-Endpunkte)	Clients können mit der IP-Adresse eines beliebigen Gateway-Knotens oder Admin-Knotens, der virtuellen IP-Adresse (VIP) einer beliebigen HA-Gruppe in einem beliebigen Netzwerk oder einem entsprechenden FQDN auf den Endpunkt zugreifen. Die Einstellung **Global** sollte verwendet werden, es sei denn, die Zugänglichkeit dieses Endpunkts muss eingeschränkt werden.
Virtuelle IPs von HA-Gruppen	Clients müssen eine virtuelle IP-Adresse (oder den entsprechenden FQDN) einer HA-Gruppe verwenden, um auf diesen Endpunkt zuzugreifen. Endpunkte mit diesem Bindungsmodus können alle die gleiche Portnummer verwenden, solange sich die für die Endpunkte ausgewählten HA-Gruppen nicht überschneiden.
Knotenschnittstellen	Clients müssen die IP-Adressen (oder die entsprechenden FQDNs) der ausgewählten Knotenschnittstellen verwenden, um auf diesen Endpunkt zuzugreifen.
Knotentyp (nur Client-Endpunkte)	${post_edited_translations.segment}

Modus	Beschreibung
Alle Admin-Knoten (Standard für Managementoberfläche-Endpunkte)	Clients müssen die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Admin Node verwenden, um auf diesen Endpunkt zuzugreifen.

Wenn mehrere Endpunkte denselben Port verwenden, verwendet StorageGRID diese Prioritätsreihenfolge, um zu entscheiden, welcher Endpunkt genutzt wird: **Virtuelle IPs von HA-Gruppen** > **Knotenschnittstellen** > **Knotentyp** > **Global**.

Wenn Managementoberfläche Endpunkte erstellt werden, sind nur Admin-Nodes zulässig.

2. Wenn **Virtuelle IPs von HA-Gruppen** ausgewählt wurden, eine oder mehrere HA-Gruppen auswählen.

   Wenn Managementoberfläche-Endpunkte erstellt werden, sollten nur VIPs ausgewählt werden, die mit Admin Nodes verknüpft sind.

3. Wenn Sie **Knotenschnittstellen** ausgewählt haben, wählen Sie eine oder mehrere Knotenschnittstellen für jeden Admin Node oder Gateway Node aus, die Sie mit diesem Endpunkt verknüpfen möchten.
4. Wenn Sie **Knotentyp** ausgewählt haben, wählen Sie entweder Admin Nodes, zu denen sowohl der primäre Admin Node als auch alle nicht-primären Admin Nodes gehören, oder Gateway Nodes.

Mandantenzugriff kontrollieren

Ein Managementoberfläche Endpunkt kann den Mandantenzugriff nur steuern, wenn der Endpunkt über die Schnittstellentyp des Tenant Manager verfügt.

Schritte

1. Für den Schritt **Mandantenzugriff** eine der folgenden Optionen auswählen:

Feld	Beschreibung
Alle Mandanten zulassen (Standard)	Alle Mandantenkonten können diesen Endpunkt verwenden, um auf ihre Buckets zuzugreifen. Diese Option ist auszuwählen, wenn noch keine Mandantenkonten erstellt wurden. Nachdem Mandantenkonten hinzugefügt wurden, lässt sich der Load Balancer-Endpunkt bearbeiten, um bestimmte Konten zuzulassen oder zu blockieren.
Ausgewählte Mandanten zulassen	Nur die ausgewählten Mandantenkonten können diesen Endpunkt verwenden, um auf ihre Buckets zuzugreifen.
Ausgewählte Mandanten blockieren	Die ausgewählten Mandantenkonten können diesen Endpunkt nicht für den Zugriff auf ihre Buckets verwenden. Alle anderen Mandanten können diesen Endpunkt verwenden.

2. Wenn Sie einen **HTTP**-Endpunkt erstellen, müssen Sie kein Zertifikat anhängen. **Erstellen** auswählen, um den neuen Load Balancer Endpunkt hinzuzufügen. Anschließend zu Nachdem Sie fertig sind gehen. Andernfalls **Weiter** auswählen, um das Zertifikat anzuhängen.

Zertifikat beifügen

Schritte

1. Wenn Sie einen **HTTPS**-Endpunkt erstellen, wählen Sie den Typ des Sicherheitszertifikats aus, das Sie dem Endpunkt zuordnen möchten.

   Das Zertifikat sichert die Verbindungen zwischen S3-Clients und dem Load Balancer Service auf dem Admin Node oder den Gateway Nodes.

   - **Zertifikat hochladen**. Diese Option ist auszuwählen, wenn benutzerdefinierte Zertifikate hochgeladen werden sollen.
   - **Zertifikat generieren**. Diese Option ist auszuwählen, wenn die erforderlichen Werte zum Generieren eines benutzerdefinierten Zertifikats vorliegen.
   - **StorageGRID S3-Zertifikat verwenden**. Diese Option ist auszuwählen, wenn das globale S3-API-Zertifikat genutzt werden soll, das auch für Verbindungen direkt zu Storage Nodes verwendet werden kann.

     Diese Option kann nicht ausgewählt werden, es sei denn, das standardmäßige S3-API-Zertifikat, das von der Grid-CA signiert ist, wurde durch ein benutzerdefiniertes Zertifikat ersetzt, das von einer externen Zertifizierungsstelle signiert ist. Siehe "S3 API-Zertifikate konfigurieren".

   - **Managementoberfläche-Zertifikat verwenden**. Diese Option ist auszuwählen, wenn das globale Managementoberfläche-Zertifikat verwendet werden soll, das auch für direkte Verbindungen zu Admin Nodes genutzt werden kann.
2. Falls das StorageGRID S3-Zertifikat nicht verwendet wird, das Zertifikat hochladen oder generieren.

Zertifikat hochladen

a. **Zertifikat hochladen** auswählen.

b. ${post_edited_translations.segment}

- **Serverzertifikat**: Die benutzerdefinierte Serverzertifikatdatei in PEM-Kodierung.
- **Privater Zertifikatsschlüssel**: Die benutzerdefinierte private Schlüsseldatei des Serverzertifikats (`.key`).

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

- **CA bundle**: Eine einzelne optionale Datei, die die Zertifikate aller zwischengeschalteten Zertifizierungsstellen (CAs) enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatsdateien, in der Reihenfolge der Zertifikatskette zusammengefügt, enthalten.

c. **Zertifikatsdetails** kann erweitert werden, um die Metadaten jedes hochgeladenen Zertifikats anzuzeigen. Wenn ein optionales CA-Bundle hochgeladen wurde, wird jedes Zertifikat auf einem eigenen Tab angezeigt.

- ${post_edited_translations.segment}

  Geben Sie den Namen der Zertifikatsdatei und den Speicherort für den Download an. Die Datei wird mit der Erweiterung `.pem` gespeichert.

  Zum Beispiel: `storagegrid_certificate.pem`

- ${post_edited_translations.segment}

d. **Erstellen** auswählen. + Der Load Balancer Endpunkt wird erstellt. Das benutzerdefinierte Zertifikat wird für alle nachfolgenden neuen Verbindungen zwischen S3 Clients oder der Managementoberfläche und dem Endpunkt verwendet.

Zertifikat generieren

a. **Zertifikat generieren** auswählen.

b. ${post_edited_translations.segment}

Feld	Beschreibung
Domainname	Ein oder mehrere vollqualifizierte Domain-Namen, die in das Zertifikat aufgenommen werden sollen. Ein * kann als Platzhalter verwendet werden, um mehrere Domain-Namen darzustellen.
${post_edited_translations.segment}	${post_edited_translations.segment}
Thema (optional)	${post_edited_translations.segment} Wird in diesem Feld kein Wert eingegeben, verwendet das generierte Zertifikat den ersten Domänennamen oder die erste IP-Adresse als allgemeinen Subjektnamen (CN).

Feld	Beschreibung
Gültigkeitstage	Anzahl der Tage nach der Erstellung, nach denen das Zertifikat abläuft.
Schlüsselverwendungserweiterungen hinzufügen	Wenn diese Option ausgewählt ist (Standard und empfohlen), werden die Schlüsselverwendungs- und erweiterten Schlüsselverwendungs-Erweiterungen dem generierten Zertifikat hinzugefügt. Diese Erweiterungen definieren den Zweck des im Zertifikat enthaltenen Schlüssels. **Hinweis**: Dieses Kontrollkästchen sollte aktiviert bleiben, es sei denn, bei älteren Clients treten Verbindungsprobleme auf, wenn die Zertifikate diese Erweiterungen enthalten.

c. Wählen Sie **Generieren**.

d. **Zertifikatdetails** zeigt die Metadaten des generierten Zertifikats an.

   - **Zertifikat herunterladen** auswählen, um die Zertifikatsdatei zu speichern.

     Geben Sie den Namen der Zertifikatsdatei und den Speicherort für den Download an. Die Datei wird mit der Erweiterung `.pem` gespeichert.

     Zum Beispiel: `storagegrid_certificate.pem`

   - **Zertifikat PEM kopieren** auswählen, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.

e. Wählen Sie **Create**.

   Der Load-Balancer-Endpunkt wurde 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, muss sichergestellt sein, dass der DNS einen Eintrag enthält, der den StorageGRID vollqualifizierte Domainnamen (FQDN) mit jeder IP-Adresse verknüpft, die Clients für Verbindungen verwenden.

   Die im DNS-Eintrag angegebene IP-Adresse hängt davon ab, ob Sie eine HA-Gruppe von Load-Balancing-Knoten verwenden:

   - Wenn Sie eine HA-Gruppe konfiguriert haben, verbinden sich die Clients mit den virtuellen IP-Adressen dieser HA-Gruppe.
   - Wenn keine HA-Gruppe verwendet wird, stellen Clients über die IP-Adresse eines Gateway-Knotens oder Admin-Knotens eine Verbindung zum StorageGRID Load Balancer Service her.

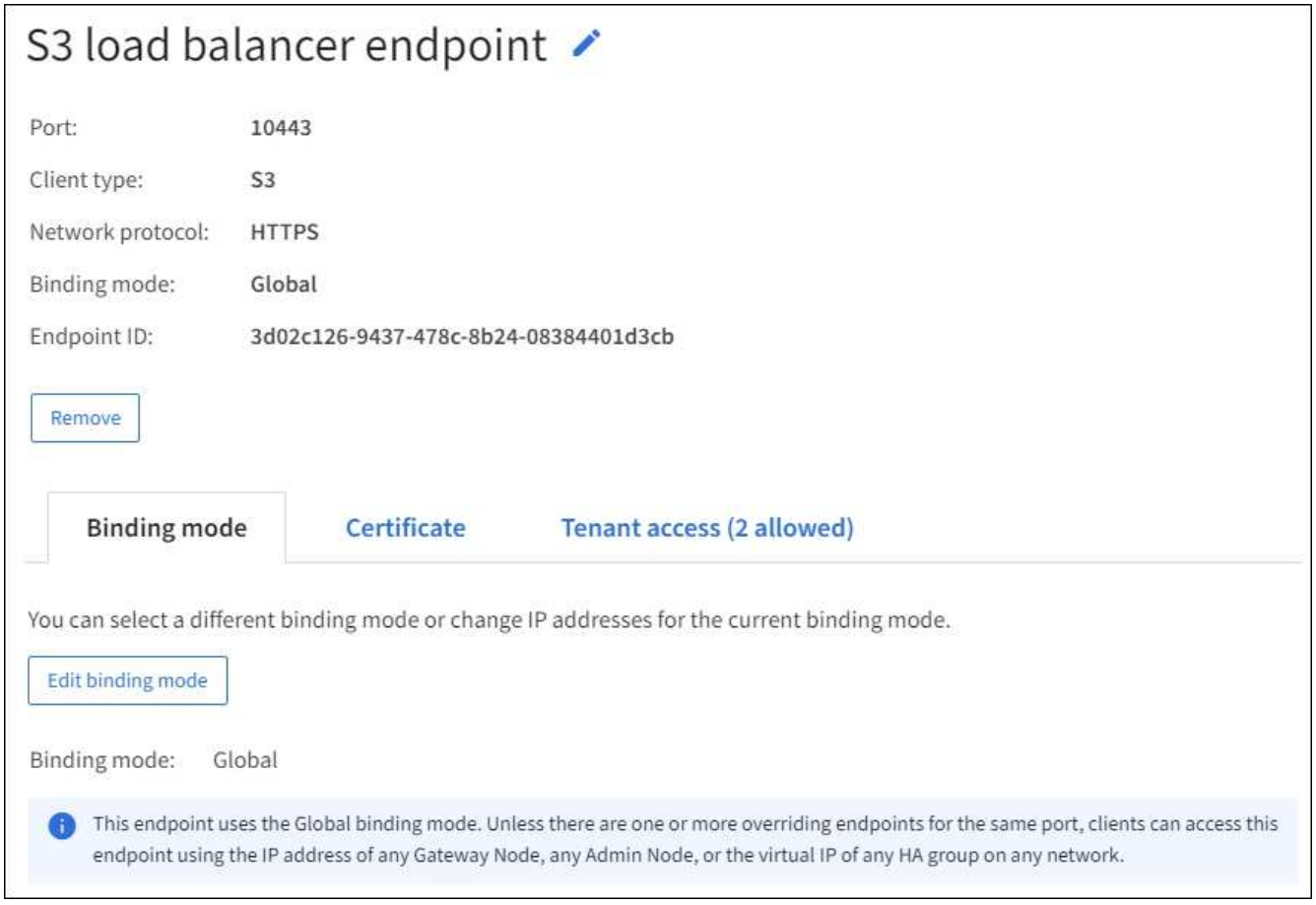
   Es ist außerdem sicherzustellen, dass der DNS-Eintrag alle erforderlichen Endpunktdomänennamen, einschließlich aller Wildcard-Namen, referenziert.

2. S3-Clients werden die Informationen bereitgestellt, die für die Verbindung zum Endpunkt erforderlich sind:
    - Portnummer
    - Vollqualifizierte Domain oder IP-Adresse
    - Angaben zu erforderlichen Zertifikaten

Load Balancer Endpunkte anzeigen und bearbeiten

Sie können Details zu bestehenden Load Balancer Endpunkten anzeigen, einschließlich der Zertifikatsmetadaten für einen gesicherten Endpunkt. Bestimmte Einstellungen für einen Endpunkt lassen sich ändern.

- Grundlegende Informationen zu allen Load Balancer Endpunkten finden sich in den Tabellen auf der Seite Load Balancer Endpunkte.
- Alle Details zu einem bestimmten Endpunkt, einschließlich der Zertifikatsmetadaten, werden angezeigt, wenn der Name des Endpunkts in der Tabelle ausgewählt wird. Die angezeigten Informationen variieren je nach Endpunkttyp und dessen Konfiguration.



- Um einen Endpunkt zu bearbeiten, verwenden Sie das Menü **Aktionen** auf der Seite Load balancer endpoints.

> Wenn während der Bearbeitung des Ports eines Managementoberfläche Endpunkts der Zugriff auf Grid Manager verloren geht, sollten URL und Port aktualisiert werden, um den Zugriff wiederzuerlangen.

Nach der Bearbeitung eines Endpunkts kann es bis zu 15 Minuten dauern, bis Ihre Änderungen auf alle Knoten angewendet werden.

Aufgabe	Aktionsmenü	Detailseite
Endpunktname bearbeiten	a. Das Kontrollkästchen für den Endpunkt auswählen. b. Wählen Sie **Aktionen** > **Endpunktname bearbeiten**. c. Geben Sie den neuen Namen ein. d. **Speichern** auswählen.	a. Den Endpunktnamen auswählen, um die Details anzuzeigen. b. Das Bearbeitungssymbol auswählen. c. Geben Sie den neuen Namen ein. d. **Speichern** auswählen.
Endpunktport bearbeiten	a. Das Kontrollkästchen für den Endpunkt auswählen. b. **Aktionen** > **Endpunktport bearbeiten** auswählen c. Geben Sie eine gültige Portnummer ein. d. **Speichern** auswählen.	*n. v.*
Endpunktbindungsmodus bearbeiten	a. Das Kontrollkästchen für den Endpunkt auswählen. b. **Aktionen** > **Endpunktbindungsmodus bearbeiten** auswählen. c. Der Bindungsmodus wird bei Bedarf aktualisiert. d. Wählen Sie **Save changes**.	a. Den Endpunktnamen auswählen, um die Details anzuzeigen. b. **Bindungsmodus bearbeiten** auswählen. c. Der Bindungsmodus wird bei Bedarf aktualisiert. d. Wählen Sie **Save changes**.
Endpunktzertifikat bearbeiten	a. Das Kontrollkästchen für den Endpunkt auswählen. b. Wählen Sie **Aktionen** > **Endpunktzertifikat bearbeiten**. c. Ein neues benutzerdefiniertes Zertifikat kann hochgeladen oder generiert werden, oder das globale S3-Zertifikat kann verwendet werden, je nach Bedarf. d. Wählen Sie **Save changes**.	a. Den Endpunktnamen auswählen, um die Details anzuzeigen. b. Die Registerkarte **Zertifikat** auswählen. c. **Zertifikat bearbeiten** auswählen. d. Ein neues benutzerdefiniertes Zertifikat kann hochgeladen oder generiert werden, oder das globale S3-Zertifikat kann verwendet werden, je nach Bedarf. e. Wählen Sie **Save changes**.

Aufgabe	Aktionsmenü	Detailseite
Mandantenzugriff bearbeiten	a. Das Kontrollkästchen für den Endpunkt auswählen. b. **Aktionen** > **Mandantenzugriff bearbeiten** auswählen. c. Eine andere Zugriffsoption kann gewählt, Mandanten aus der Liste ausgewählt oder entfernt werden, oder beides. d. Wählen Sie **Save changes**.	a. Den Endpunktnamen auswählen, um die Details anzuzeigen. b. Die Registerkarte **Mandantenzugriff** auswählen. c. **Mandantenzugriff bearbeiten** auswählen. d. Eine andere Zugriffsoption kann gewählt, Mandanten aus der Liste ausgewählt oder entfernt werden, oder beides. e. Wählen Sie **Save changes**.

Load Balancer Endpunkte entfernen

Sie können einen oder mehrere Endpunkte über das Menü **Aktionen** entfernen oder einen einzelnen Endpunkt auf der Detailseite entfernen.

> Um Client-Unterbrechungen zu vermeiden, sollten alle betroffenen S3-Client-Anwendungen aktualisiert werden, bevor ein Load Balancer Endpunkt entfernt wird. Jeder Client sollte so aktualisiert werden, dass er die Verbindung über einen Port herstellt, der einem anderen Load Balancer Endpunkt zugewiesen ist. Es ist darauf zu achten, dass auch alle erforderlichen Zertifikatsinformationen aktualisiert werden.

> Wenn beim Entfernen eines Managementoberfläche Endpunkts der Zugriff auf Grid Manager verloren geht, sollte die URL aktualisiert werden.

- Um einen oder mehrere Endpunkte zu entfernen:
  a. Auf der Load Balancer-Seite das Kontrollkästchen für jeden Endpunkt auswählen, der entfernt werden soll.
  b. **Aktionen** > **Entfernen** auswählen.
  c. Wählen Sie **OK**.
- Einen Endpunkt von der Detailseite entfernen:
  a. Auf der Load-Balancer-Seite den Endpunktnamen auswählen.
  b. Auf der Detailseite die Option **Entfernen** auswählen.
  c. Wählen Sie **OK**.

Konfigurieren Sie S3-Endpunkt-Domänennamen in StorageGRID

Um S3-Anfragen im virtuellen Hosting-Stil zu unterstützen, muss der Grid Manager verwendet werden, um die Liste der S3-Endpunktdomänennamen zu konfigurieren, mit denen sich S3-Clients verbinden.

Die Verwendung einer IP-Adresse als Endpunktdomänenname wird nicht unterstützt. Zukünftige Versionen werden diese Konfiguration verhindern.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Du hast "spezifische Zugriffsberechtigungen".
- Sie haben bestätigt, dass ein Grid-Upgrade nicht im Gange ist.

Während eines Grid-Upgrades sollten keine Änderungen an der Domänennamenkonfiguration vorgenommen werden.

Über diese Aufgabe

Damit Clients S3-Endpunktdomänennamen verwenden können, sind alle folgenden Schritte erforderlich:

- Mit dem Grid Manager werden die S3-Endpunktdomänennamen zum StorageGRID System hinzugefügt.
- Es ist sicherzustellen, dass die "Zertifikat, das der Client für HTTPS-Verbindungen zu StorageGRID verwendet" für alle vom Client benötigten Domainnamen signiert ist.

  Wenn der Endpunkt beispielsweise `s3.company.com` ist, muss sichergestellt werden, dass das für HTTPS-Verbindungen verwendete Zertifikat den `s3.company.com` Endpunkt und den Wildcard Subject Alternative Name (SAN) des Endpunkts enthält: `*.s3.company.com`.

- Der vom Client verwendete DNS-Server wird konfiguriert. DNS-Einträge für die IP-Adressen, die Clients für die Verbindungsherstellung verwenden, sind einzuschließen, wobei sichergestellt wird, dass die Einträge auf alle erforderlichen S3-Endpunkt-Domainnamen, einschließlich aller Wildcard-Namen, verweisen.

Clients können sich mit StorageGRID über die IP-Adresse eines Gateway Node, eines Admin Node oder eines Storage Node verbinden oder indem sie die virtuelle IP-Adresse einer Hochverfügbarkeitsgruppe verwenden. Es ist wichtig zu verstehen, wie Clientanwendungen eine Verbindung zum Grid herstellen, damit die korrekten IP-Adressen in die DNS-Einträge aufgenommen werden.

Clients, die HTTPS-Verbindungen (empfohlen) zum Grid nutzen, können eines dieser Zertifikate verwenden:

- Clients, die sich mit einem Load Balancer-Endpunkt verbinden, können ein benutzerdefiniertes Zertifikat für diesen Endpunkt verwenden. Jeder Load Balancer-Endpunkt kann so konfiguriert werden, dass er verschiedene 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 es alle erforderlichen S3-Endpunkt-Domainnamen enthält.

Wenn keine S3-Endpunktdomänennamen hinzugefügt werden und die Liste leer ist, ist die Unterstützung für S3-Anfragen im Virtual-Hosted-Style deaktiviert.

Einen S3-Endpunkt-Domänennamen hinzufügen

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerk** > **S3 endpoint domain names**.

2. Geben Sie den Domainnamen in das Feld **Domain name 1** ein. **Add another domain name** auswählen, um weitere Domainnamen hinzuzufügen.
3. **Speichern** auswählen.
4. Stellen Sie sicher, dass die von den Clients verwendeten Serverzertifikate mit den erforderlichen S3-Endpunkt-Domainnamen übereinstimmen.
   - Wenn Clients eine Verbindung zu einem Load-Balancer-Endpunkt herstellen, der ein eigenes Zertifikat verwendet, "Das dem Endpunkt zugeordnete Zertifikat aktualisieren".
   - Wenn Clients eine Verbindung zu einem Load-Balancer-Endpunkt herstellen, der das globale S3-API-Zertifikat verwendet, oder direkt zu Storage Nodes, "das globale S3 API-Zertifikat aktualisieren".
5. Fügen Sie die erforderlichen DNS-Einträge hinzu, damit Anfragen an Endpunktdomänennamen aufgelöst werden können.

Ergebnis

Wenn Clients nun den Endpunkt `bucket.s3.company.com` verwenden, löst der DNS-Server den korrekten Endpunkt auf und das Zertifikat authentifiziert den Endpunkt wie erwartet.

Einen S3-Endpunkt-Domänennamen umbenennen

Wenn ein von S3-Anwendungen verwendeter Name geändert wird, schlagen virtual-hosted-style Anfragen fehl.

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerk** > **S3 endpoint domain names**.
2. Wählen Sie das Feld mit dem Domänennamen aus, das bearbeitet werden soll, und nehmen Sie die erforderlichen Änderungen vor.
3. **Speichern** auswählen.
4. **Ja** auswählen, um die Änderung zu bestätigen.

Löschen eines S3-Endpunkt-Domänennamens

Wenn ein von S3-Anwendungen verwendeter Name entfernt wird, schlagen virtual-hosted-style Anfragen fehl.

Schritte

1. Wählen Sie **Konfiguration** > **Netzwerk** > **S3 endpoint domain names**.
2. Das Löschsymbol ✕ neben dem Domänennamen auswählen.
3. **Ja** auswählen, um die Löschung zu bestätigen.

Verwandte Informationen

- "S3 REST-API verwenden"
- "IP-Adressen anzeigen"
- "${post_edited_translations.segment}"

IP-Adressen und Ports für StorageGRID-Clientverbindungen

Zum Speichern oder Abrufen von Objekten stellen S3-Clientanwendungen eine Verbindung zum Load Balancer Service her, der auf allen Admin Nodes und Gateway Nodes enthalten ist, oder zum Local Distribution Router (LDR) Service, der auf allen Storage Nodes enthalten ist.

Clientanwendungen können sich mit StorageGRID über die IP-Adresse eines Grid-Knotens und die Portnummer des Dienstes auf diesem Knoten verbinden. Optional können hochverfügbare (HA-)Gruppen von Load-Balancing-Knoten erstellt werden, um hochverfügbare Verbindungen bereitzustellen, die virtuelle IP-Adressen (VIP) verwenden. Wenn eine Verbindung zu StorageGRID über eine vollqualifizierte Domain (FQDN) anstelle einer IP- oder VIP-Adresse hergestellt werden soll, können DNS-Einträge konfiguriert werden.

Diese Tabelle fasst die verschiedenen Verbindungsarten von Clients zu StorageGRID sowie die jeweils verwendeten IP-Adressen und Ports zusammen. Wenn bereits Load Balancer-Endpunkte und hochverfügbare (HA-)Gruppen erstellt wurden, siehe Wo IP-Adressen zu finden sind, um diese Werte im Grid Manager zu finden.

Wo die Verbindung hergestellt wird	Dienst, mit dem der Client eine Verbindung herstellt	IP-Adresse	Port
HA-Gruppe	Lastverteiler	${post_edited_translations.segment}	Dem Load Balancer-Endpunkt zugewiesener Port
Admin-Node	Lastverteiler	${post_edited_translations.segment}	Dem Load Balancer-Endpunkt zugewiesener Port
${post_edited_translations.segment}	Lastverteiler	IP-Adresse des Gateway-Knotens	Dem Load Balancer-Endpunkt zugewiesener Port
Speicherknoten	LDR	IP-Adresse des Storage Node	Standardmäßige S3 Ports: • HTTPS: 18082 • HTTP: 18084

${post_edited_translations.segment}

Um eine Clientanwendung mit dem Load Balancer-Endpunkt einer HA-Gruppe von Gateway-Knoten zu verbinden, wird eine URL mit folgender Struktur verwendet:

`https://VIP-of-HA-group:LB-endpoint-port`

Wenn beispielsweise die virtuelle IP-Adresse der HA-Gruppe 192.0.2.5 ist und die Portnummer des Load-Balancer-Endpunkts 10443 beträgt, kann eine Anwendung die folgende URL verwenden, um eine Verbindung zu StorageGRID herzustellen:

`https://192.0.2.5:10443`

Wo IP-Adressen zu finden sind

1. Melden Sie sich beim Grid Manager mit einem "unterstützte Webbrowser" an.
2. So lässt sich die IP-Adresse eines Grid-Knotens ermitteln:
   a. Wählen Sie **Knoten**.

b. ${post_edited_translations.segment}

c. Wählen Sie die Registerkarte **Overview** aus.

d. Im Abschnitt „Knoteninformationen“ sind die IP-Adressen des Knotens zu beachten.

e. ${post_edited_translations.segment}

Von Clientanwendungen aus lassen sich Verbindungen zu jeder der IP-Adressen in der Liste herstellen:

- ${post_edited_translations.segment}
- **eth1:** Admin-Netzwerk (optional)
- ${post_edited_translations.segment}

> Wenn ein Admin-Knoten oder ein Gateway-Knoten angezeigt wird und es sich um den aktiven Knoten in einer hochverfügbaren Gruppe handelt, wird die virtuelle IP-Adresse der HA-Gruppe auf eth2 angezeigt.

3. So wird die virtuelle IP-Adresse einer Hochverfügbarkeitsgruppe gefunden:
   a. **Konfiguration** > **Netzwerk** > **Hochverfügbarkeitsgruppen** auswählen.
   b. In der Tabelle ist die virtuelle IP-Adresse der HA-Gruppe zu beachten.
4. So wird die Portnummer eines Load Balancer Endpunkts ermittelt:
   a. **Konfiguration** > **Netzwerk** > **Load balancer endpoints** auswählen.
   b. Notieren Sie sich die Portnummer des Endpunkts, den Sie verwenden möchten.

> Wenn die Portnummer 80 oder 443 ist, wird der Endpoint nur auf Gateway Nodes konfiguriert, da diese Ports auf Admin Nodes reserviert sind. Alle anderen Ports werden sowohl auf Gateway Nodes als auch auf Admin Nodes konfiguriert.

   c. Den Namen des Endpunkts aus der Tabelle auswählen.
   d. ${post_edited_translations.segment}

Netzwerke und Verbindungen verwalten

StorageGRID-Netzwerkeinstellungen konfigurieren

Verschiedene Netzwerkeinstellungen lassen sich über den Grid Manager konfigurieren, um den Betrieb Ihres StorageGRID Systems zu optimieren.

${post_edited_translations.segment}

Sie können "Virtuelle LAN (VLAN)-Schnittstellen erstellen" verwenden, um den Datenverkehr zu isolieren und zu partitionieren und so Sicherheit, Flexibilität und Leistung zu gewährleisten. Jede VLAN-Schnittstelle ist einer oder mehreren übergeordneten Schnittstellen auf Admin-Nodes und Gateway-Nodes zugeordnet. VLAN-Schnittstellen können in HA-Gruppen und in Load-Balancer-Endpunkten eingesetzt werden, um Client- oder Admin-Datenverkehr nach Anwendung oder Mandant zu trennen.

Verkehrsklassifizierungsrichtlinien

Sie können "Verkehrsklassifizierungsrichtlinien" verwenden, um verschiedene Arten von Netzwerkverkehr zu identifizieren und zu steuern, einschließlich Verkehr, der mit bestimmten Buckets, Mandanten, Client-Subnetzen oder Load-Balancer-Endpunkten zusammenhängt. Diese Richtlinien können bei der Begrenzung und Überwachung des Datenverkehrs unterstützen.

Richtlinien für StorageGRID Netzwerke

Der Grid Manager ermöglicht die Konfiguration und Verwaltung von StorageGRID Netzwerken und Verbindungen.

Siehe "Konfiguration von S3 Clientverbindungen", um zu erfahren, wie S3-Clients verbunden werden.

Standard StorageGRID Netzwerke

Standardmäßig unterstützt StorageGRID drei Netzwerkschnittstellen pro Grid-Knoten, wodurch die Netzwerkkonfiguration für jeden einzelnen Grid-Knoten an die jeweiligen Sicherheits- und Zugriffsanforderungen angepasst werden kann.

Weitere Informationen zur Netzwerktopologie sind unter "Netzwerkrichtlinien" zu finden.

Grid-Netzwerk

Erforderlich. Das Grid Network wird für den gesamten internen StorageGRID Datenverkehr verwendet. Es stellt die Verbindung zwischen allen Knoten im Grid über alle Standorte und Subnetze hinweg her.

${post_edited_translations.segment}

Optional. Das Admin-Netzwerk wird in der Regel für die Systemadministration und -wartung verwendet. Es kann auch für den Client-Protokollzugriff verwendet werden. Das Admin-Netzwerk ist in der Regel ein privates Netzwerk und muss nicht zwischen Standorten routing-fähig sein.

Client-Netzwerk

Optional. Das Client Network ist ein offenes Netzwerk, das in der Regel für den Zugriff auf S3-Client-Anwendungen verwendet wird, sodass das Grid Network isoliert und gesichert werden kann. Das Client Network kann mit jedem Subnetz kommunizieren, das über das lokale Gateway erreichbar ist.

Richtlinien

- Jeder StorageGRID Knoten benötigt eine dedizierte Netzwerkschnittstelle, IP-Adresse, Subnetzmaske und Gateway für jedes Netzwerk, dem er zugewiesen ist.
- Ein Grid-Knoten kann nicht mehr als eine Schnittstelle in einem Netzwerk haben.
- Pro Netzwerk und pro Grid-Knoten wird ein einzelnes Gateway unterstützt, das sich im selben Subnetz wie der Knoten befinden muss. Komplexeres Routing kann bei Bedarf im Gateway implementiert werden.
- Auf jedem Knoten ist jedes Netzwerk einer bestimmten Netzwerkschnittstelle zugeordnet.

Netzwerk	Schnittstellenname
Grid	eth0

Netzwerk	Schnittstellenname
Administrator (optional)	eth1
Client (optional)	eth2

- Wenn der Knoten mit einem StorageGRID Appliance verbunden ist, werden für jedes Netzwerk spezifische Ports verwendet. Einzelheiten finden sich in den Installationsanweisungen für Ihre Appliance.
- Die Standardroute wird automatisch pro Knoten generiert. Wenn eth2 aktiviert ist, verwendet 0.0.0.0/0 das Client Network auf eth2. Wenn eth2 nicht aktiviert ist, verwendet 0.0.0.0/0 das Grid Network auf eth0.
- Das Client-Netzwerk wird erst betriebsbereit, wenn der Grid-Knoten dem Grid beigetreten ist
- Das Admin Network kann während der Bereitstellung der Grid-Knoten so konfiguriert werden, dass Zugriff auf die Installationsbenutzeroberfläche vor der vollständigen Installation des Grids möglich ist.

Optionale Schnittstellen

Optional können zusätzliche Schnittstellen zu einem Knoten hinzugefügt werden. Beispielsweise kann eine Trunk-Schnittstelle zu einem Admin Node oder Gateway Node hinzugefügt werden, sodass "VLAN Schnittstellen" zur Trennung des Datenverkehrs verschiedener Anwendungen oder Mandanten verwendet werden kann. Alternativ kann eine Zugriffsschnittstelle hinzugefügt werden, die in einem "Hochverfügbarkeitsgruppe (HA)" verwendet werden kann.

Zum Hinzufügen von Trunk- oder Zugriffsschnittstellen siehe Folgendes:

- **VMware (nach der Installation des Knotens)**: "VMware: Trunk- oder Access-Schnittstellen zu einem Node hinzufügen"
  - **Linux (vor der Installation des Node)**: "Knotenkonfigurationsdateien erstellen"
  - **Linux (nach der Installation des Nodes)**: "Trunk- oder Zugriffsschnittstellen zu einem Node hinzufügen"

> ⓘ „Linux“ bezieht sich auf eine RHEL-, Ubuntu- oder Debian-Installation. Eine Liste der unterstützten Versionen befindet sich unter "NetApp Interoperabilitätsmatrix Tool (IMT)".

IP-Adressen in StorageGRID anzeigen

Sie können die IP-Adresse jedes Grid-Knotens in Ihrem StorageGRID System anzeigen. Diese IP-Adresse kann dann verwendet werden, um sich an dem Grid-Knoten über die Befehlszeile anzumelden und verschiedene Wartungsverfahren durchzuführen.

Bevor Sie beginnen

Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.

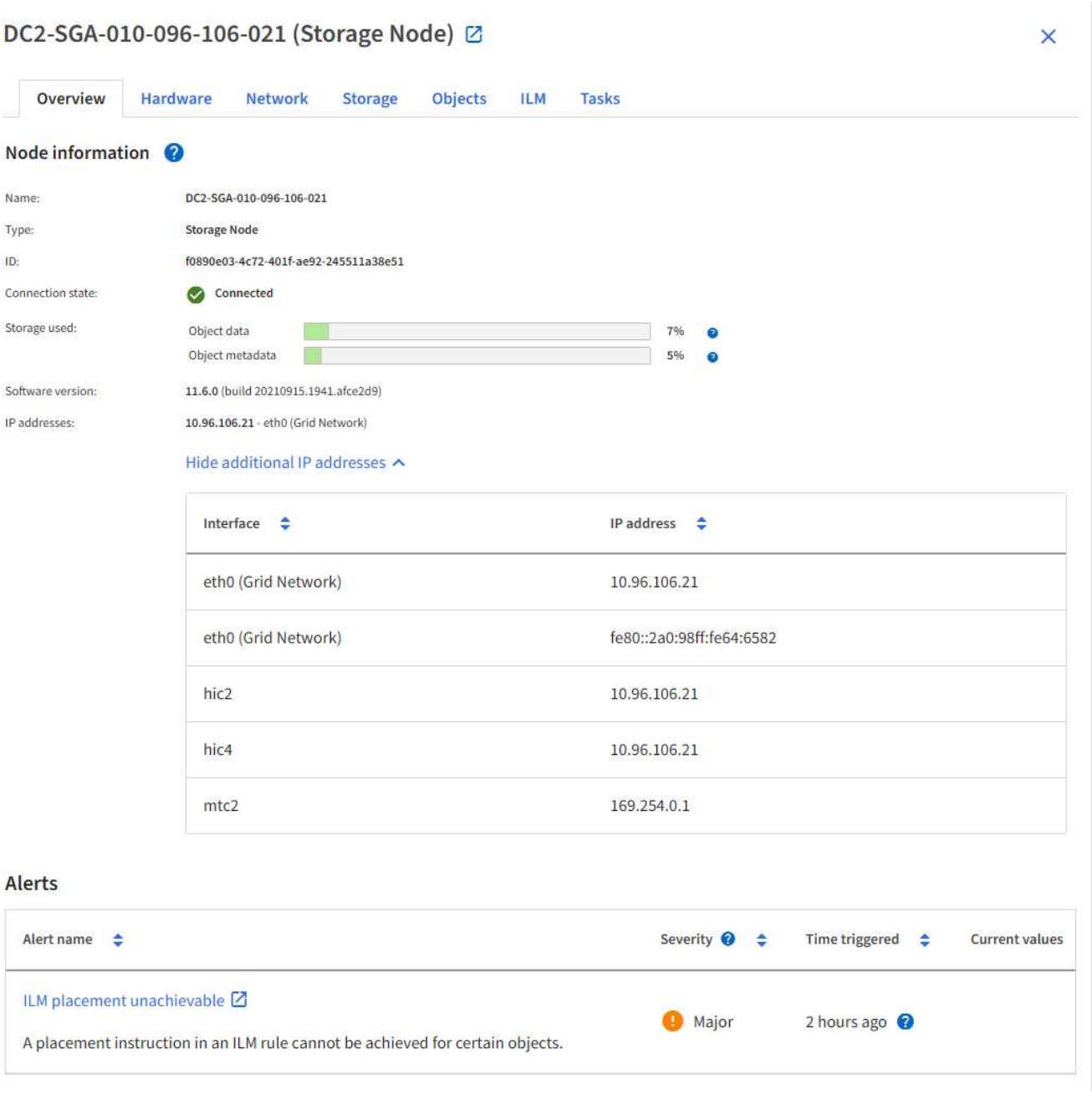
Über diese Aufgabe

Informationen zum Ändern von IP-Adressen sind unter "IP-Adressen konfigurieren" verfügbar.

Schritte

1. Wählen Sie **Nodes** > ***grid node*** > **Overview**.
2. Rechts neben dem Titel „IP Addresses“ die Option **Show more** auswählen.

Die IP-Adressen für diesen Grid-Knoten sind in einer Tabelle aufgeführt.



Konfigurieren Sie VLAN-Schnittstellen in StorageGRID

Virtuelle LAN-Schnittstellen (VLAN) auf Admin-Knoten und Gateway-Knoten erstellen und in HA-Gruppen sowie Load-Balancer-Endpunkten verwenden, um den Datenverkehr für Sicherheit, Flexibilität und Leistung zu isolieren und zu partitionieren. Die ausgewählten Knoten in der HA-Gruppe können die VLAN-Schnittstellen nutzen, um bis zu 10 virtuelle IP-Adressen gemeinsam zu verwenden, sodass bei Ausfall eines Knotens ein anderer Knoten den Datenverkehr zu und von den virtuellen IP-Adressen übernimmt.

Überlegungen zu VLAN-Schnittstellen

- ${post_edited_translations.segment}
- Eine übergeordnete Schnittstelle muss am Switch als Trunk Schnittstelle konfiguriert werden.
- Eine übergeordnete Schnittstelle kann das Grid Network (eth0), das Client Network (eth2) oder eine zusätzliche Trunk-Schnittstelle für die VM oder den Bare-Metal-Host (zum Beispiel ens256) sein.
- Für jede VLAN-Schnittstelle kann nur eine übergeordnete Schnittstelle für einen bestimmten Knoten ausgewählt werden. Beispielsweise können sowohl die Grid Network-Schnittstelle als auch die Client Network-Schnittstelle auf demselben Gateway Node nicht als übergeordnete Schnittstelle für dasselbe VLAN verwendet werden.
- Wenn die VLAN-Schnittstelle für den Datenverkehr des Admin-Knotens vorgesehen ist, der auch den Datenverkehr im Zusammenhang mit dem Grid Manager und dem Tenant Manager umfasst, sollten Schnittstellen nur auf den Admin-Knoten ausgewählt werden.
- ${post_edited_translations.segment}
- Falls Sie Trunk-Schnittstellen hinzufügen müssen, finden Sie weitere Informationen im Folgenden:
  - **VMware (nach der Installation des Knotens)**: "VMware: Trunk- oder Access-Schnittstellen zu einem Node hinzufügen"
  - **Linux (vor der Installation des Node)**: "Knotenkonfigurationsdateien erstellen"
  - **Linux (nach der Installation des Nodes)**: "Trunk- oder Zugriffsschnittstellen zu einem Node hinzufügen"

> ⓘ „Linux“ bezieht sich auf eine RHEL-, Ubuntu- oder Debian-Installation. Eine Liste der unterstützten Versionen befindet sich unter "NetApp Interoperabilitätsmatrix Tool (IMT)".

${post_edited_translations.segment}

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Root-Zugriffsberechtigung".
- Im Netzwerk wurde eine Trunk-Schnittstelle konfiguriert und an die VM oder den Linux-Knoten angebunden. Sie kennen den Namen der Trunk-Schnittstelle.
- Sie kennen die ID des VLAN, das Sie konfigurieren.

Über diese Aufgabe

Ihr Netzwerkadministrator hat möglicherweise eine oder mehrere Trunk-Schnittstellen und ein oder mehrere VLANs konfiguriert, um den Client- oder Administrator-Datenverkehr verschiedener Anwendungen 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.

Mit dem Grid Manager können Sie VLAN-Schnittstellen erstellen, die Clients den Zugriff auf StorageGRID über ein bestimmtes VLAN ermöglichen. Beim Erstellen von VLAN-Schnittstellen werden die VLAN-ID angegeben und übergeordnete (Trunk) Schnittstellen auf einem oder mehreren Knoten ausgewählt.

Assistenten aufrufen

Schritte

1. **Konfiguration** > **Netzwerk** > **VLAN Schnittstellen** auswählen.

2. Wählen Sie **Create**.

${post_edited_translations.segment}

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 kann die VLAN-ID 200 für administrativen Datenverkehr an einem Standort und dieselbe VLAN-ID für Client-Datenverkehr an einem anderen Standort verwendet werden. Separate VLAN-Schnittstellen mit unterschiedlichen Gruppen von übergeordneten Schnittstellen können an jedem Standort erstellt werden. Zwei VLAN-Schnittstellen mit derselben ID können jedoch nicht dieselbe Schnittstelle auf einem Node gemeinsam nutzen. Wird eine bereits verwendete ID angegeben, erscheint eine Meldung.

2. Optional kann eine kurze Beschreibung für die VLAN-Schnittstelle eingegeben werden.
3. Wählen Sie **Weiter**.

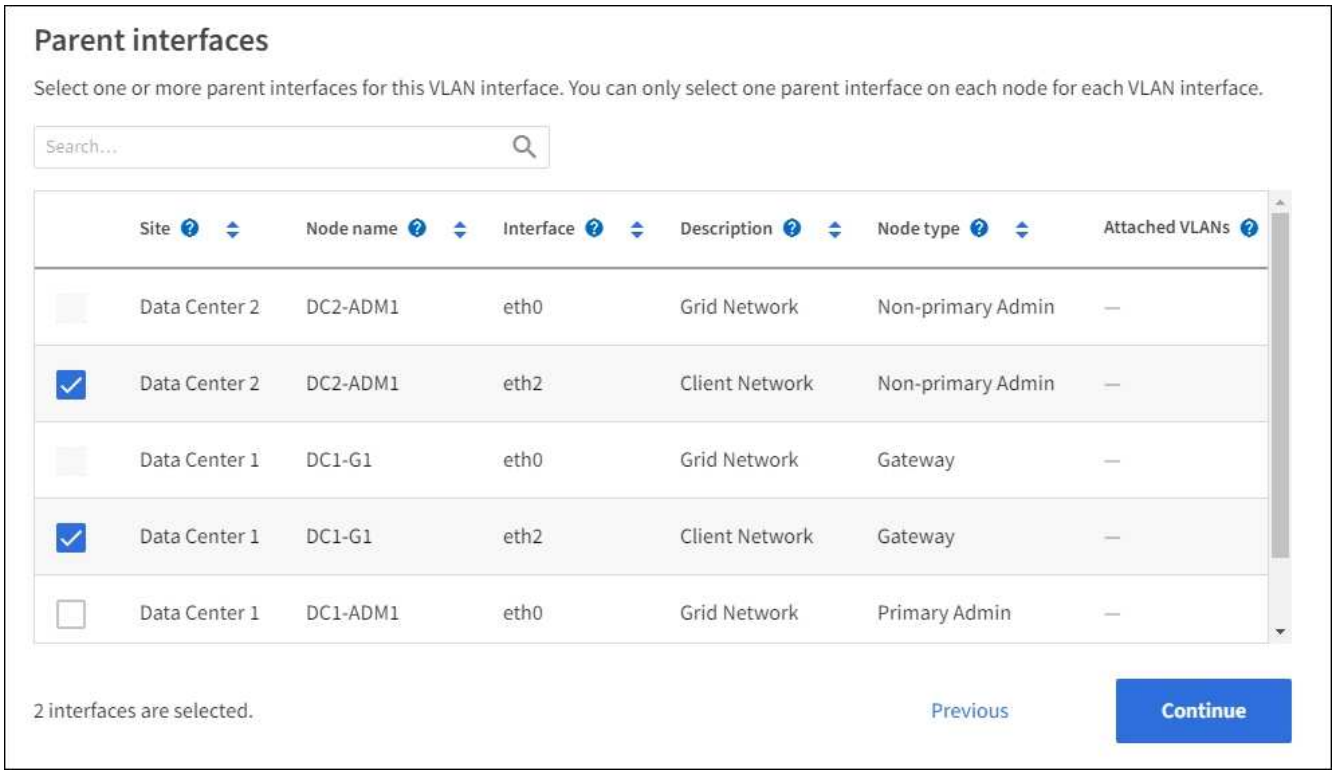
Übergeordnete Schnittstellen auswählen

Die Tabelle listet die verfügbaren Schnittstellen für alle Admin-Knoten und Gateway-Knoten an jedem Standort Ihres Grids auf. Admin Network (eth1)-Schnittstellen können nicht als übergeordnete Schnittstellen verwendet werden und werden nicht angezeigt.

Schritte

1. ${post_edited_translations.segment}

   Beispielsweise kann es erforderlich sein, ein VLAN an die Client Network (eth2) Schnittstelle eines Gateway Node und eines Admin Node anzubinden.



2. Wählen Sie **Weiter**.

Einstellungen bestätigen

Schritte

1. Die Konfiguration kann überprüft und bei Bedarf geändert werden.
   - Wenn eine Änderung der VLAN-ID oder der Beschreibung erforderlich ist, steht oben auf der Seite die Option **VLAN-Details eingeben** zur Verfügung.
   - Wenn eine übergeordnete Schnittstelle geändert werden muss, steht oben auf der Seite **Übergeordnete Schnittstellen auswählen** oder **Zurück** zur Auswahl.
   - Wenn Sie eine übergeordnete Schnittstelle entfernen müssen, wählen Sie den Papierkorb aus.
2. **Speichern** auswählen.
3. Bis zu 5 Minuten kann es dauern, bis die neue Schnittstelle auf der Seite „High availability groups“ als Auswahl erscheint und in der Tabelle „Network interfaces“ für den Node aufgeführt wird (**Nodes** > ***parent interface node*** > **Network**).

Bearbeiten einer VLAN-Schnittstelle

Beim Bearbeiten einer VLAN-Schnittstelle sind die folgenden Arten von Änderungen möglich:

- ${post_edited_translations.segment}
- Übergeordnete Schnittstellen hinzufügen oder entfernen.

Beispielsweise kann es sinnvoll sein, eine übergeordnete Schnittstelle von einer VLAN-Schnittstelle zu entfernen, wenn geplant ist, den zugehörigen Knoten außer Betrieb zu nehmen.

Dabei ist Folgendes zu beachten:

- Die VLAN-ID kann nicht geändert werden, wenn die VLAN-Schnittstelle in einer HA-Gruppe verwendet wird.
- ${post_edited_translations.segment}

  Angenommen, VLAN 200 ist an übergeordnete Schnittstellen auf den Nodes A und B angebunden. Wenn eine HA-Gruppe die VLAN 200 Schnittstelle für Node A und die eth2 Schnittstelle für Node B verwendet, kann die nicht verwendete übergeordnete Schnittstelle für Node B entfernt werden, jedoch nicht die verwendete übergeordnete Schnittstelle für Node A.

Schritte

1. **Konfiguration** > **Netzwerk** > **VLAN Schnittstellen** auswählen.
2. Das Kontrollkästchen für die VLAN-Schnittstelle, die bearbeitet werden soll, auswählen. Anschließend **Aktionen** > **Bearbeiten** auswählen.
3. Optional kann die VLAN-ID oder die Beschreibung aktualisiert werden. Anschließend **Weiter** auswählen.

   Eine VLAN-ID kann nicht aktualisiert werden, wenn das VLAN in einer HA-Gruppe verwendet wird.

4. Optional können die Kontrollkästchen aktiviert oder deaktiviert werden, um übergeordnete Schnittstellen hinzuzufügen oder nicht verwendete Schnittstellen zu entfernen. Anschließend **Weiter** auswählen.
5. Die Konfiguration kann überprüft und bei Bedarf geändert werden.
6. **Speichern** auswählen.

Entfernen einer VLAN-Schnittstelle

Sie können eine oder mehrere VLAN-Schnittstellen entfernen.

Eine VLAN-Schnittstelle kann nicht entfernt werden, wenn sie aktuell in einer HA-Gruppe verwendet wird. Die VLAN-Schnittstelle muss aus der HA-Gruppe entfernt werden, bevor sie entfernt werden kann.

Um Störungen im Client-Datenverkehr zu vermeiden, kann eine der folgenden Maßnahmen in Betracht gezogen werden:

- ${post_edited_translations.segment}
- Eine neue HA-Gruppe erstellen, die diese VLAN-Schnittstelle nicht verwendet.
- Wenn die VLAN-Schnittstelle, die entfernt werden soll, derzeit die aktive Schnittstelle ist, sollte die HA-Gruppe bearbeitet werden. Die VLAN-Schnittstelle, die entfernt werden soll, ist an das Ende der Prioritätsliste zu verschieben. Es ist abzuwarten, bis die Kommunikation über die neue primäre Schnittstelle hergestellt wurde, danach kann die alte Schnittstelle aus der HA-Gruppe entfernt werden. Abschließend ist die VLAN-Schnittstelle auf diesem Node zu löschen.

Schritte

1. **Konfiguration** > **Netzwerk** > **VLAN Schnittstellen** auswählen.
2. Aktivieren Sie das Kontrollkästchen für jede VLAN-Schnittstelle, die entfernt werden soll. Dann **Aktionen** > **Löschen** auswählen.
3. **Ja** auswählen, um die Auswahl zu bestätigen.

   Alle ausgewählten VLAN-Schnittstellen werden entfernt. Auf der Seite mit den VLAN-Schnittstellen erscheint ein grünes Erfolgsbanner.

StorageGRID CORS für eine Managementoberfläche aktivieren

Als Grid-Administrator besteht die Möglichkeit, Cross-Origin Resource Sharing (CORS) für Management-API-Anfragen an StorageGRID zu aktivieren, wenn Daten in StorageGRID über Management-APIs von einer anderen Domäne aus zugänglich sein sollen.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Das "Root-Zugriffsberechtigung" bietet Zugriff auf alle CORS-Konfigurationsanfragen.

Über diese Aufgabe

CORS ist ein Sicherheitsmechanismus, der es Client-Webanwendungen in einer Domäne ermöglicht, auf Ressourcen in einer anderen Domäne zuzugreifen. Beispielsweise kann ein Monitoring-Dashboard für StorageGRID in der Domäne `http://www.example.com` erstellt werden. Wenn CORS in StorageGRID für `http://www.example.com` und „Grid Manager“ aktiviert ist, beantwortet die StorageGRID-Domäne 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. Im Grid Manager zu **KONFIGURATION** > **Netzwerk** > **CORS-Einstellungen der Managementoberfläche**

wechseln.

2. **Grid Manager**, **Tenant Manager** oder beide Optionen auswählen.
   - **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 der anderen Domain im Feld **Domains** ein.

   Weitere Domäne hinzufügen auswählen, wenn CORS in StorageGRID für mehr als eine Domäne aktiviert werden soll.

4. **Speichern** auswählen.

Verwandte Informationen

"StorageGRID CORS für Buckets und Objekte konfigurieren"

Verkehrsklassifizierungsrichtlinien verwalten

Richtlinien zur Verkehrsklassifizierung in StorageGRID

Richtlinien zur Traffic-Klassifizierung ermöglichen es Ihnen, verschiedene Arten von Netzwerk-Traffic zu identifizieren und zu überwachen. Diese Richtlinien können bei der Traffic-Begrenzung und -Überwachung unterstützen, um Ihre Quality-of-Service-Angebote (QoS) zu verbessern.

Richtlinien zur Traffic-Klassifizierung werden auf Endpunkte des StorageGRID Load Balancer Dienstes für Gateway-Nodes und Admin-Nodes angewendet. Um Richtlinien zur Traffic-Klassifizierung zu erstellen, müssen Sie bereits Load-Balancer-Endpunkte erstellt haben.

Übereinstimmungsregeln

Jede Richtlinie zur Verkehrsklassifizierung enthält eine oder mehrere Abgleichsregeln, um den Netzwerkverkehr zu identifizieren, der mit einer oder mehreren der folgenden Entitäten in Verbindung steht:

- Buckets
- Subnetz
- Mandant
- Load Balancer Endpunkte

StorageGRID überwacht den Datenverkehr, der einer Regel innerhalb der Richtlinie entspricht, gemäß den Zielen dieser Regel. Jeglicher Datenverkehr, der einer Regel einer Richtlinie entspricht, wird von dieser Richtlinie verarbeitet. Umgekehrt können Regeln so festgelegt werden, dass sie den gesamten Datenverkehr mit Ausnahme einer bestimmten Entität erfassen.

${post_edited_translations.segment}

Optional lassen sich einer Richtlinie die folgenden Limittypen hinzufügen:

- Aggregatbandbreite
- Bandbreite pro Anforderung
- Gleichzeitige Anfragen

- Anfragerate

Die Grenzwerte werden pro Load Balancer durchgesetzt. Wenn der Datenverkehr gleichzeitig auf mehrere Load Balancer verteilt wird, entsprechen die maximalen Gesamtraten einem Vielfachen der von Ihnen festgelegten Grenzwerte.

> Es können Richtlinien erstellt werden, um die Aggregatbandbreite oder die Bandbreite pro Anfrage zu begrenzen. Allerdings kann StorageGRID nicht beide Arten von Bandbreite gleichzeitig begrenzen. Begrenzungen der Aggregatbandbreite können die Leistung des nicht begrenzten Datenverkehrs geringfügig beeinträchtigen.

Bei Aggregat- oder Anforderungs-Bandbreitenbegrenzungen werden die Anfragen mit der von Ihnen festgelegten Geschwindigkeit ein- oder ausgehend verarbeitet. StorageGRID kann nur eine Geschwindigkeit erzwingen, daher wird die spezifischste Richtlinienübereinstimmung nach Matcher-Typ angewendet. Die von der Anfrage verbrauchte Bandbreite wird nicht auf andere, weniger spezifische übereinstimmende Richtlinien mit Aggregatbandbreitenbegrenzungen angerechnet. Bei allen anderen Begrenzungstypen werden Clientanfragen um 250 Millisekunden verzögert und erhalten eine 503 Slow Down-Antwort, wenn sie eine der übereinstimmenden Richtlinienbegrenzungen überschreiten.

Im Grid Manager können Sie Verkehrsdiagramme einsehen und überprüfen, ob die Richtlinien die von Ihnen erwarteten Verkehrsbeschränkungen durchsetzen.

${post_edited_translations.segment}

Sie können Verkehrsklassifizierungsrichtlinien in Verbindung mit Kapazitätsgrenzen und Datenschutz verwenden, um Service-Level-Agreements (SLAs) durchzusetzen, die spezifische Vorgaben für Kapazität, Datenschutz und Leistung enthalten.

Das folgende Beispiel zeigt drei Stufen einer Service-Level-Vereinbarung (SLA). Es besteht die Möglichkeit, Richtlinien zur Datenverkehrsklassifizierung zu erstellen, um die Leistungsziele jeder SLA-Stufe zu erfüllen.

Service-Level-Tier	Kapazität	Datensicherung	Maximal zulässige Leistung	Kosten
Gold	${post_edited_translations.segment}	3-Kopien-ILM-Regel	${post_edited_translations.segment} 5 GB/s (40 Gbit/s) Bandbreite	$$$ pro Monat
${post_edited_translations.segment}	250 TB Speicherplatz zulässig	${post_edited_translations.segment}	10.000 Anfragen/s 1,25 GB/s (10 Gbit/s) Bandbreite	$$ pro Monat
Bronze	100 TB Speicherplatz zulässig	${post_edited_translations.segment}	5 K Anfragen/s ${post_edited_translations.segment}	${post_edited_translations.segment}

Erstellen Sie StorageGRID-Traffic-Klassifizierungsrichtlinien

Sie können Richtlinien zur Verkehrsklassifizierung erstellen, wenn Sie den Netzwerkverkehr nach Bucket, Bucket-Regex, CIDR, Load-Balancer-Endpunkt oder Mandant überwachen und optional einschränken möchten. Optional lassen sich für eine Richtlinie Grenzwerte auf Basis von Bandbreite, Anzahl gleichzeitiger Anfragen oder Anfragerate festlegen.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Root-Zugriffsberechtigung".
- Sie haben alle Load Balancer Endpunkte erstellt, die Sie abgleichen möchten.
- Sie haben alle gewünschten Mandanten erstellt.

Schritte

1. **Konfiguration** > **Netzwerk** > **Verkehrsklassifizierung** auswählen.
2. Wählen Sie **Create**.
3. Geben Sie einen Namen und eine optionale Beschreibung für die Richtlinie ein und wählen Sie **Weiter**.

   Beispielsweise kann beschrieben werden, worauf diese Verkehrsklassifizierungsrichtlinie angewendet wird und was sie einschränkt.

4. Wählen Sie **Regel hinzufügen** und geben Sie die folgenden Details an, um eine oder mehrere passende Regeln für die Richtlinie zu erstellen. Jede von Ihnen erstellte Richtlinie sollte mindestens eine passende Regel enthalten. **Weiter** auswählen.

Feld	Beschreibung
Typ	Wählen Sie die Datenverkehrstypen aus, auf die die Übereinstimmungsregel angewendet wird. Zu den Datenverkehrstypen gehören Bucket, Bucket Regex, CIDR, Load Balancer Endpoint und Mandant.

Feld	Beschreibung
Übereinstimmungswert	Geben Sie den Wert ein, der dem ausgewählten Typ entspricht. • Bucket: Ein oder mehrere Bucket-Namen eingeben. • Bucket Regex: Ein oder mehrere reguläre Ausdrücke, die zum Abgleich einer Menge von Bucket-Namen verwendet werden. Der reguläre Ausdruck ist nicht verankert. Der Anker ^ kann verwendet werden, um am Anfang des Bucket-Namens zu suchen, und der Anker $ kann verwendet werden, um am Ende des Namens zu suchen. Die Übereinstimmung mit regulären Ausdrücken unterstützt eine Teilmenge der PCRE-Syntax (Perl compatible regular expression). • CIDR: Ein oder mehrere IPv4-Subnetze in CIDR-Notation eingeben, die dem gewünschten Subnetz entsprechen. • Load Balancer-Endpunkt: Ein Endpunktname wird ausgewählt. Dies sind die Load Balancer-Endpunkte, die auf dem "Load Balancer-Endpunkte konfigurieren" definiert wurden. • Mandant: Die Mandantenzuordnung erfolgt anhand der Zugriffsschlüssel-ID. Wenn die Anfrage keine Zugriffsschlüssel-ID enthält (zum Beispiel anonymer Zugriff), wird der Mandant anhand der Eigentümerschaft des aufgerufenen Buckets bestimmt.
Inverse Übereinstimmung	Wenn aller Netzwerkverkehr mit Ausnahme des Verkehrs, der dem soeben definierten Typ und Übereinstimmungswert entspricht, abgeglichen werden soll, ist das Kontrollkästchen **Umgekehrte Übereinstimmung** auszuwählen. Andernfalls bleibt das Kontrollkästchen deaktiviert. Wenn Sie beispielsweise möchten, dass diese Richtlinie für alle Load Balancer Endpunkte außer einem gilt, geben Sie den auszuschließenden Load Balancer Endpunkt an und wählen Sie **Umgekehrte Übereinstimmung**. Bei einer Richtlinie mit mehreren Matchern, von denen mindestens einer ein inverser Matcher ist, ist darauf zu achten, dass keine Richtlinie erstellt wird, die auf alle Anfragen zutrifft.

5. ${post_edited_translations.segment}

> StorageGRID erfasst Metriken auch dann, wenn Sie keine Limits hinzufügen, sodass Sie die Verkehrstrends nachvollziehen können.

Feld	Beschreibung
Typ	Die Art der Beschränkung, die auf den von der Regel erfassten Netzwerkverkehr angewendet werden soll. Beispielsweise kann die Bandbreite oder die Anforderungsrate begrenzt werden. **Hinweis**: Es können Richtlinien erstellt werden, um die Aggregatbandbreite oder die Bandbreite pro Anfrage zu begrenzen. Allerdings kann StorageGRID nicht beide Arten von Bandbreite gleichzeitig begrenzen. Wenn die Aggregatbandbreite verwendet wird, steht die Bandbreite pro Anfrage nicht zur Verfügung. Umgekehrt steht die Aggregatbandbreite nicht zur Verfügung, wenn die Bandbreite pro Anfrage verwendet wird. Begrenzungen der Aggregatbandbreite können die Leistung des nicht begrenzten Datenverkehrs geringfügig beeinträchtigen. Für Bandbreitenbeschränkungen wendet StorageGRID die Richtlinie an, die am besten zum festgelegten Beschränkungstyp passt. Wenn beispielsweise eine Richtlinie vorhanden ist, die den Datenverkehr nur in eine Richtung beschränkt, bleibt der Datenverkehr in die entgegengesetzte Richtung unbegrenzt, selbst wenn es Datenverkehr gibt, der zusätzlichen Richtlinien mit Bandbreitenbeschränkungen entspricht. StorageGRID implementiert „beste“ Übereinstimmungen für Bandbreitenbeschränkungen in der folgenden Reihenfolge: • Exakte IP-Adresse (/32-Maske) • Exakter Bucket Name • Bucket Regex • Mandant • Endpunkt • Nicht exakte CIDR-Übereinstimmungen (nicht /32) • Inverse Übereinstimmungen
Gilt für	Ob diese Beschränkung für Client-Leseanfragen (GET oder HEAD) oder Schreibanfragen (PUT, POST oder DELETE) gilt.
Wert	Der Wert, auf den der Netzwerkverkehr begrenzt wird, basiert auf der von Ihnen gewählten Einheit. Beispielsweise 10 eingeben und MiB/s auswählen verhindert, dass der von dieser Regel erfasste Netzwerkverkehr 10 MiB/s überschreitet. **Hinweis**: Je nach Einheiteneinstellung stehen entweder binäre Einheiten (zum Beispiel GiB) oder dezimale Einheiten (zum Beispiel GB) zur Verfügung. Die Einheiteneinstellung lässt sich über das Benutzer-Drop-down-Menü oben rechts im Grid Manager unter **Benutzereinstellungen** anpassen.
Einheit	Die Einheit, die den von Ihnen eingegebenen Wert beschreibt.

Wenn beispielsweise ein Bandbreitenlimit von 4 GB/s für eine SLA-Stufe erstellt werden soll, sind zwei Aggregate Bandbreitenlimits zu erstellen: GET/HEAD mit 4 GB/s und PUT/POST/DELETE mit 4 GB/s.

6. Wählen Sie **Weiter**.
7. Die Richtlinie zur Verkehrsklassifizierung wird gelesen und geprüft. Mit der Schaltfläche **Zurück** besteht die Möglichkeit, bei Bedarf Änderungen vorzunehmen. Ist die Richtlinie zufriedenstellend, kann **Speichern und fortfahren** ausgewählt werden.

   Der S3-Client-Datenverkehr wird jetzt gemäß der Richtlinie zur Datenverkehrsklassifizierung behandelt.

Nachdem Sie fertig sind

"Netzwerkverkehrsmetriken"um zu überprüfen, ob die Richtlinien die erwarteten Verkehrsbeschränkungen durchsetzen.

Bearbeiten einer StorageGRID-Verkehrsklassifizierungsrichtlinie

Sie können eine Verkehrsklassifizierungsrichtlinie bearbeiten, um ihren Namen oder ihre Beschreibung zu ändern oder um Regeln oder Beschränkungen für die Richtlinie zu erstellen, zu bearbeiten oder zu löschen.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Root-Zugriffsberechtigung".

Schritte

1. **Konfiguration** > **Netzwerk** > **Verkehrsklassifizierung** auswählen.

   Die Seite mit den Richtlinien zur Verkehrsklassifizierung wird angezeigt und die bestehenden Richtlinien sind in einer Tabelle aufgeführt.

2. Die Richtlinie kann über das Menü „Aktionen“ oder die Detailseite bearbeitet werden. Siehe "Verkehrsklassifizierungsrichtlinien erstellen" für die erforderlichen Eingaben.

   Aktionsmenü

   a. Das Kontrollkästchen für die Richtlinie auswählen.

   b. **Aktionen** > **Bearbeiten** auswählen.

   Detailseite

   a. Wählen Sie den Richtliniennamen aus.

   b. Wählen Sie die Schaltfläche **Bearbeiten** neben dem Richtliniennamen aus.

3. Im Schritt „Richtliniennamen eingeben“ besteht die Möglichkeit, den Richtliniennamen oder die Beschreibung optional zu bearbeiten und **Weiter** auszuwählen.
4. Für den Schritt „Übereinstimmende Regeln hinzufügen“ kann optional eine Regel hinzugefügt oder der **Typ** und der **Übereinstimmungswert** der vorhandenen Regel bearbeitet werden, und es wird **Weiter** ausgewählt.
5. Im Schritt „Grenzwerte festlegen“ kann optional ein Grenzwert hinzugefügt, bearbeitet oder gelöscht werden, und **Weiter** wird ausgewählt.
6. Die aktualisierte Richtlinie wird überprüft, anschließend **Speichern und fortfahren** auswählen.

Die von Ihnen vorgenommenen Änderungen an der Richtlinie wurden gespeichert, und der Netzwerkverkehr wird nun gemäß den Richtlinien zur Verkehrsklassifizierung verarbeitet. Sie können Verkehrsdiagramme einsehen und überprüfen, ob die Richtlinien die erwarteten Verkehrsgrenzen durchsetzen.

Löschen einer StorageGRID traffic classification policy

Sie können eine Richtlinie zur Verkehrsklassifizierung löschen, wenn Sie sie nicht mehr benötigen. Achten Sie darauf, die richtige Richtlinie zu löschen, da eine gelöschte Richtlinie nicht wiederhergestellt werden kann.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Root-Zugriffsberechtigung".

Schritte

1. **Konfiguration** > **Netzwerk** > **Verkehrsklassifizierung** auswählen.

   Die Seite „Richtlinien zur Verkehrsklassifizierung“ wird angezeigt, die bestehenden Richtlinien sind in einer Tabelle aufgeführt.

2. Die Richtlinie kann über das Menü „Aktionen“ oder die Detailseite gelöscht werden.

   Aktionsmenü

   a. Das Kontrollkästchen für die Richtlinie auswählen.

   b. **Aktionen** > **Entfernen** auswählen.

   Seite mit Richtliniendetails

   a. Wählen Sie den Richtliniennamen aus.

   b. Die Schaltfläche **Entfernen** neben dem Richtliniennamen auswählen.

3. **Ja** auswählen, um zu bestätigen, dass die Richtlinie gelöscht werden soll.

   Die Richtlinie wurde gelöscht.

Netzwerkverkehrsmetriken in StorageGRID anzeigen

Der Netzwerkverkehr lässt sich überwachen, indem die auf der Seite „Richtlinien zur Verkehrsklassifizierung“ verfügbaren Diagramme angezeigt werden.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Root-Zugriff oder Berechtigung für Mandantenkonten".

Über diese Aufgabe

Für jede bestehende Traffic-Klassifizierungsrichtlinie können Sie Metriken für den Load Balancer Dienst anzeigen, um festzustellen, ob die Richtlinie den Traffic im Netzwerk erfolgreich begrenzt. Die Daten in den Diagrammen können Ihnen bei der Entscheidung helfen, ob Sie die Richtlinie anpassen müssen.

Auch wenn für eine Verkehrsklassifizierungsrichtlinie keine Grenzwerte festgelegt werden, werden Kennzahlen erfasst und die Diagramme liefern nützliche Informationen zum Verständnis von Verkehrstrends.

Schritte

1. **Konfiguration** > **Netzwerk** > **Verkehrsklassifizierung** auswählen.

   Die Seite mit den Richtlinien zur Verkehrsklassifizierung wird angezeigt, und die bestehenden Richtlinien sind in der Tabelle aufgeführt.

2. Den Namen der Datenverkehrsklassifizierungsrichtlinie auswählen, für die Metriken angezeigt werden sollen.
3. Die Registerkarte **Metriken** auswählen.

   Die Diagramme für die Richtlinie zur Datenverkehrsklassifizierung werden angezeigt. Die Diagramme zeigen Metriken nur für den Datenverkehr an, der mit der ausgewählten Richtlinie übereinstimmt.

   ${post_edited_translations.segment}

   - Anfragerate: Dieses Diagramm zeigt die Bandbreite, die gemäß dieser Richtlinie von allen Load Balancern verarbeitet wird. Die empfangenen Daten umfassen die Anfrageheader aller Anfragen sowie die Größe der Antwortdaten für Antworten, die Antwortdaten enthalten. Die gesendeten Daten umfassen die Antwortheader aller Anfragen sowie die Größe der Antwortdaten für Anfragen, bei denen die Antwort Antwortdaten enthält.

     > Wenn Anforderungen abgeschlossen sind, zeigt dieses Diagramm nur die Bandbreitennutzung an. Bei langsamen Anforderungen oder Anforderungen großer Objekte kann die tatsächliche momentane Bandbreite von den in diesem Diagramm gemeldeten Werten abweichen.

   - ${post_edited_translations.segment}
   - Durchschnittliche Anfragedauer (ohne Fehler): Dieses Diagramm zeigt die durchschnittliche Dauer erfolgreicher Anfragen, die dieser Richtlinie entsprechen.
   - Bandbreitennutzung gemäß Richtlinie: Dieses Diagramm zeigt die Menge der Bandbreite, die gemäß dieser Richtlinie von allen Load Balancern verarbeitet wird. Die empfangenen Daten umfassen die Anfrage-Header aller Anfragen sowie die Größe der Antwortdaten für Antworten, die Antwortdaten enthalten. Die gesendeten Daten umfassen die Antwort-Header aller Anfragen sowie die Größe der Antwortdaten für Anfragen, bei denen die Antwort Antwortdaten enthält.
4. Wenn der Cursor über ein Liniendiagramm bewegt wird, erscheint ein Popup mit Werten für einen bestimmten Teil des Diagramms.
5. Direkt unter dem Titel **Metrics** kann das **Grafana dashboard** ausgewählt werden, um alle Diagramme für eine Richtlinie anzuzeigen. Zusätzlich zu den vier Diagrammen aus dem Tab **Metrics** sind zwei weitere Diagramme sichtbar:
   - 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. Die in der Hover-Ansicht angezeigten Raten werden auf ganzzahlige Werte gekürzt und können 0 anzeigen, auch wenn sich nicht-null Anfragen im Bucket befinden.
   - Leseanforderungsrate nach Objektgröße: Die Rate für GET/HEAD-Anforderungen, die dieser Richtlinie entsprechen. Das Positionieren des Mauszeigers auf einer einzelnen Zelle zeigt die Raten pro Sekunde an. In der Hover-Ansicht angezeigte Raten werden auf ganzzahlige Werte abgeschnitten und weisen unter Umständen 0 aus, wenn im Bucket Anforderungen ungleich Null vorhanden sind.

6. Alternativ sind die Grafiken über das Menü **Support** zugänglich.
   a. **Support** > **Tools** > **Metrics** auswählen.
   b. Im Abschnitt **Grafana** ist **Traffic Classification Policy** auszuwählen.
   c. Die Richtlinie kann im Menü oben links auf der Seite ausgewählt werden.
   d. Wenn der Cursor über ein Diagramm positioniert wird, erscheint ein Popup, das das Datum und die Uhrzeit der Stichprobe, die in die Zählung aggregierten Objektgrößen sowie die Anzahl der Anfragen pro Sekunde während dieses Zeitraums anzeigt.

      Traffic-Klassifizierungsrichtlinien werden anhand ihrer ID identifiziert. Richtlinien-IDs sind auf der Seite für Traffic-Klassifizierungsrichtlinien aufgeführt.
7. Die Diagramme geben Aufschluss darüber, wie häufig die Richtlinie den Datenverkehr einschränkt und ob eine Anpassung der Richtlinie erforderlich ist.

Unterstützte Verschlüsselungsverfahren für ausgehende TLS-Verbindungen in StorageGRID

Das StorageGRID System unterstützt eine begrenzte Anzahl von Verschlüsselungssuiten für Transport Layer Security (TLS)-Verbindungen zu den externen Systemen, die für die Identitätsföderation und Cloud Storage Pools verwendet werden.

Unterstützte TLS-Versionen

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-Verschlüsselungsverfahren wurden so ausgewählt, dass die Kompatibilität mit einer Vielzahl externer Systeme gewährleistet ist. Die Liste ist umfangreicher als die Liste der für S3-Clientanwendungen unterstützten Verschlüsselungsverfahren. Die Konfiguration der Verschlüsselungsverfahren erfolgt unter **Konfiguration** > **Sicherheit** > **Sicherheitseinstellungen** durch Auswahl von **TLS- und SSH-Richtlinien**.

> TLS-Konfigurationsoptionen wie Protokollversionen, Verschlüsselungsverfahren, Schlüsselaustauschalgorithmen und MAC-Algorithmen sind in StorageGRID nicht konfigurierbar. Bei speziellen Anforderungen an diese Einstellungen kann Ihr NetApp Account Representative kontaktiert werden.

Vorteile von aktiven, inaktiven und gleichzeitigen HTTP-Verbindungen in StorageGRID

Wie Sie HTTP-Verbindungen konfigurieren, kann sich auf die Performance des StorageGRID Systems auswirken. Die Konfigurationen unterscheiden sich je nachdem, ob die HTTP-Verbindung aktiv oder im Leerlauf ist oder ob mehrere gleichzeitige Verbindungen bestehen.

Die Leistungsvorteile für die folgenden Arten von HTTP-Verbindungen können identifiziert werden:

- Leerlauf-HTTP-Verbindungen
- Aktive HTTP Verbindungen

- Gleichzeitige HTTP-Verbindungen

Vorteile des Offenhaltens inaktiver HTTP-Verbindungen

HTTP-Verbindungen geöffnet lassen, wenn Client-Anwendungen inaktiv sind, um spätere Transaktionen zu ermöglichen. Eine inaktive HTTP-Verbindung maximal 10 Minuten lang geöffnet lassen. StorageGRID schließt unter Umständen automatisch eine HTTP-Verbindung, die länger als 10 Minuten geöffnet und inaktiv ist.

Offene und inaktive HTTP-Verbindungen bieten folgende Vorteile:

- ${post_edited_translations.segment}

  Die geringere Latenz ist der Hauptvorteil, insbesondere im Hinblick auf die Zeit, die für den Aufbau von TCP/IP und TLS-Verbindungen erforderlich ist.

- ${post_edited_translations.segment}
- Sofortige Benachrichtigung über verschiedene Fehlerklassen, die die Verbindung zwischen der Clientanwendung und dem StorageGRID System unterbrechen

${post_edited_translations.segment}

Vorteile aktiver HTTP-Verbindungen

Bei direkten Verbindungen zu Storage Nodes sollte die Dauer einer aktiven HTTP-Verbindung auf maximal 10 Minuten begrenzt werden, auch wenn die HTTP-Verbindung kontinuierlich Transaktionen durchführt.

Die Bestimmung der maximalen Dauer, für die eine Verbindung offengehalten werden soll, ist ein Kompromiss zwischen den Vorteilen der Verbindungspersistenz und der idealen Zuweisung der Verbindung zu internen Systemressourcen.

${post_edited_translations.segment}

- ${post_edited_translations.segment}

  Im Laufe der Zeit kann eine HTTP-Verbindung aufgrund sich ändernder Anforderungen an die Lastverteilung unter Umständen nicht mehr optimal sein. Das System erzielt die beste Lastverteilung, wenn Client-Anwendungen für jede Transaktion eine separate HTTP-Verbindung herstellen, aber diese Methode hebt die wertvollen Vorteile persistenter Verbindungen auf.

- Ermöglicht Clientanwendungen, HTTP-Transaktionen an LDR-Dienste mit verfügbarem Speicherplatz zu richten.
- Ermöglicht den Start von Wartungsarbeiten.

  Manche Wartungsvorgänge beginnen erst, nachdem alle laufenden HTTP-Verbindungen abgeschlossen sind.

Bei Clientverbindungen zum Load Balancer Service kann die Begrenzung der Dauer offener Verbindungen hilfreich sein, damit einige Wartungsverfahren umgehend gestartet werden können. Wenn die Dauer der Clientverbindungen nicht begrenzt wird, kann es mehrere Minuten dauern, bis aktive Verbindungen automatisch beendet werden.

Vorteile gleichzeitiger HTTP-Verbindungen

Es empfiehlt sich, mehrere TCP/IP-Verbindungen zum StorageGRID System offen zu halten, um Parallelität zu ermöglichen, was die Leistung erhöht. Die optimale Anzahl paralleler Verbindungen hängt von verschiedenen Faktoren ab.

Gleichzeitige HTTP-Verbindungen bieten folgende Vorteile:

- Reduzierte Latenz

  Transaktionen können sofort gestartet werden, anstatt auf den Abschluss anderer Transaktionen zu warten.

- Erhöhter Durchsatz

  Das StorageGRID System kann parallele Transaktionen durchführen und den gesamten Transaktionsdurchsatz erhöhen.

Clientanwendungen sollten mehrere HTTP-Verbindungen aufbauen. Wenn eine Clientanwendung eine Transaktion durchführen muss, kann sie jede bestehende Verbindung auswählen und sofort nutzen, die aktuell keine Transaktion verarbeitet.

Die Topologie jedes StorageGRID Systems weist einen unterschiedlichen Spitzendurchsatz für gleichzeitige Transaktionen und Verbindungen auf. Der Spitzendurchsatz hängt von den Rechen-, Netzwerk- und Speicherressourcen, den WAN-Verbindungen sowie der Anzahl der vom StorageGRID System unterstützten Server, Dienste und Anwendungen ab.

StorageGRID-Systeme unterstützen häufig mehrere Clientanwendungen. Dies ist bei der Festlegung der maximalen Anzahl gleichzeitiger Verbindungen zu berücksichtigen. Besteht die Clientanwendung aus mehreren Softwarekomponenten, die jeweils Verbindungen zum StorageGRID-System herstellen, sind alle Verbindungen der einzelnen Komponenten zusammenzuzählen. In folgenden Situationen kann eine Anpassung der maximalen Anzahl gleichzeitiger Verbindungen erforderlich sein:

- Die Topologie des StorageGRID Systems beeinflusst die maximale Anzahl gleichzeitiger Transaktionen und Verbindungen, die das System unterstützen kann.
- Clientanwendungen, die mit dem StorageGRID System über ein Netzwerk mit begrenzter Bandbreite interagieren, müssen möglicherweise den Grad der Parallelität reduzieren, um sicherzustellen, dass einzelne Transaktionen in angemessener Zeit abgeschlossen werden.
- Wenn viele Clientanwendungen das StorageGRID System gemeinsam nutzen, kann es erforderlich sein, den Grad der Parallelität zu reduzieren, um die Systemgrenzen nicht zu überschreiten.

Trennung von HTTP-Verbindungspools für Lese- und Schreibvorgänge

Sie können separate Pools von HTTP-Verbindungen für Lese- und Schreibvorgänge verwenden und steuern, wie viel von einem Pool jeweils genutzt wird. Separate Pools von HTTP-Verbindungen ermöglichen eine bessere Kontrolle über Transaktionen und eine ausgewogene Lastverteilung.

Clientanwendungen können Datenlasten erzeugen, die entweder lese- oder schreiblastig sind. Mit separaten Pools von HTTP-Verbindungen für Lese- und Schreibvorgänge kann festgelegt werden, wie viel von jedem Pool für Lese- bzw. Schreibvorgänge bereitgestellt wird.

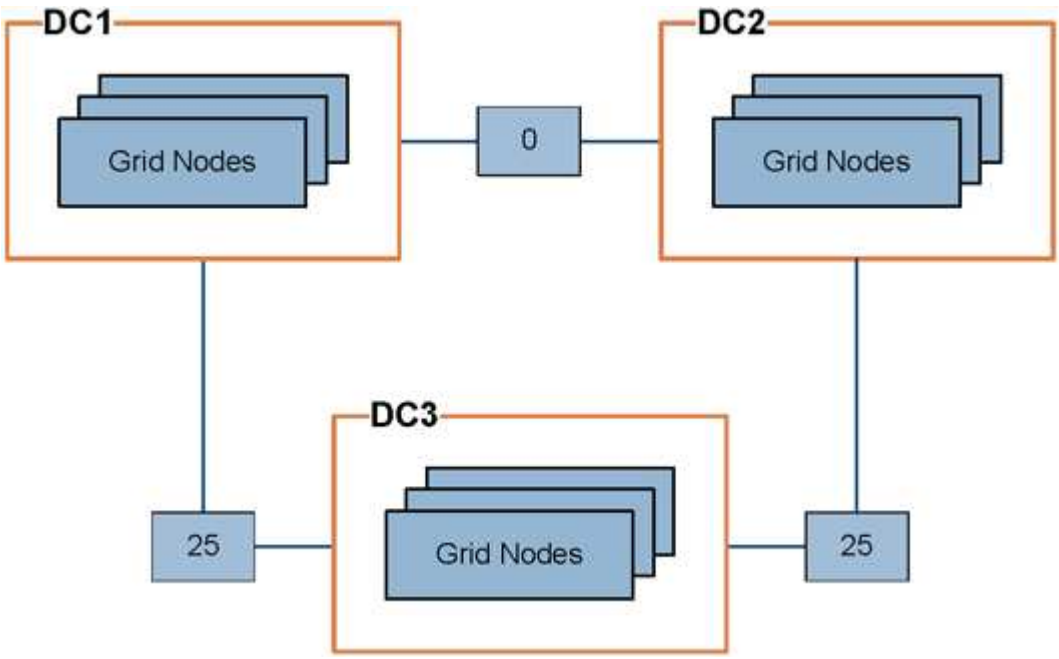
Linkkosten in StorageGRID verwalten

Mit Verbindungskosten lässt sich priorisieren, welcher Rechenzentrumsstandort einen angeforderten Dienst bereitstellt, wenn zwei oder mehr Rechenzentrumsstandorte vorhanden sind. Die Verbindungskosten können angepasst werden, um die Latenz zwischen den Standorten widerzuspiegeln.

Was sind Verbindungskosten?

- ${post_edited_translations.segment}
- Die Verbindungskosten werden von der Grid Management API und der Tenant Management API verwendet, um zu bestimmen, welche internen StorageGRID-Services genutzt werden.
- Die Verbindungskosten werden vom Load Balancer Service auf Admin Nodes und Gateway Nodes zur Steuerung von Clientverbindungen verwendet. Siehe "Überlegungen zum Lastausgleich".

${post_edited_translations.segment}



- Der Load Balancer Service auf Admin-Knoten und Gateway-Knoten verteilt Client-Verbindungen gleichmäßig auf alle Storage Nodes am selben Rechenzentrumsstandort und auf beliebige Rechenzentrumsstandorte mit Verbindungskosten von 0.

  In diesem Beispiel verteilt ein Gateway Node am Rechenzentrumsstandort 1 (DC1) Clientverbindungen gleichmäßig auf die Storage Nodes in DC1 und auf die Storage Nodes in DC2. Ein Gateway Node in DC3 sendet Clientverbindungen nur an die Storage Nodes in DC3.

- Beim Abrufen eines Objekts, das in mehreren replizierten Kopien existiert, ruft StorageGRID die Kopie im Rechenzentrum mit den niedrigsten Verbindungskosten ab.

  Wenn in diesem Beispiel eine Clientanwendung in DC2 ein Objekt abruft, das sowohl in DC1 als auch in DC3 gespeichert ist, wird das Objekt von DC1 abgerufen, da die Verbindungskosten von DC1 nach DC2 0 betragen, was niedriger ist als die Verbindungskosten von DC3 nach DC2 (25).

Linkkosten sind willkürliche relative Zahlen ohne spezifische Maßeinheit. Beispielsweise wird ein Linkkostenwert von 50 weniger bevorzugt verwendet als ein Wert von 25. Die Tabelle zeigt gängige Linkkosten.

Link	Verbindungskosten	Hinweise
Zwischen physischen Rechenzentrumsstandorten	25 (Standardwert)	Rechenzentren, die über eine WAN-Verbindung verbunden sind.
Zwischen logischen Daten Rechenzentrumsstandorten am selben physischen Standort	0	Logische Rechenzentren im selben physischen Gebäude oder Campus, verbunden durch ein LAN.

${post_edited_translations.segment}

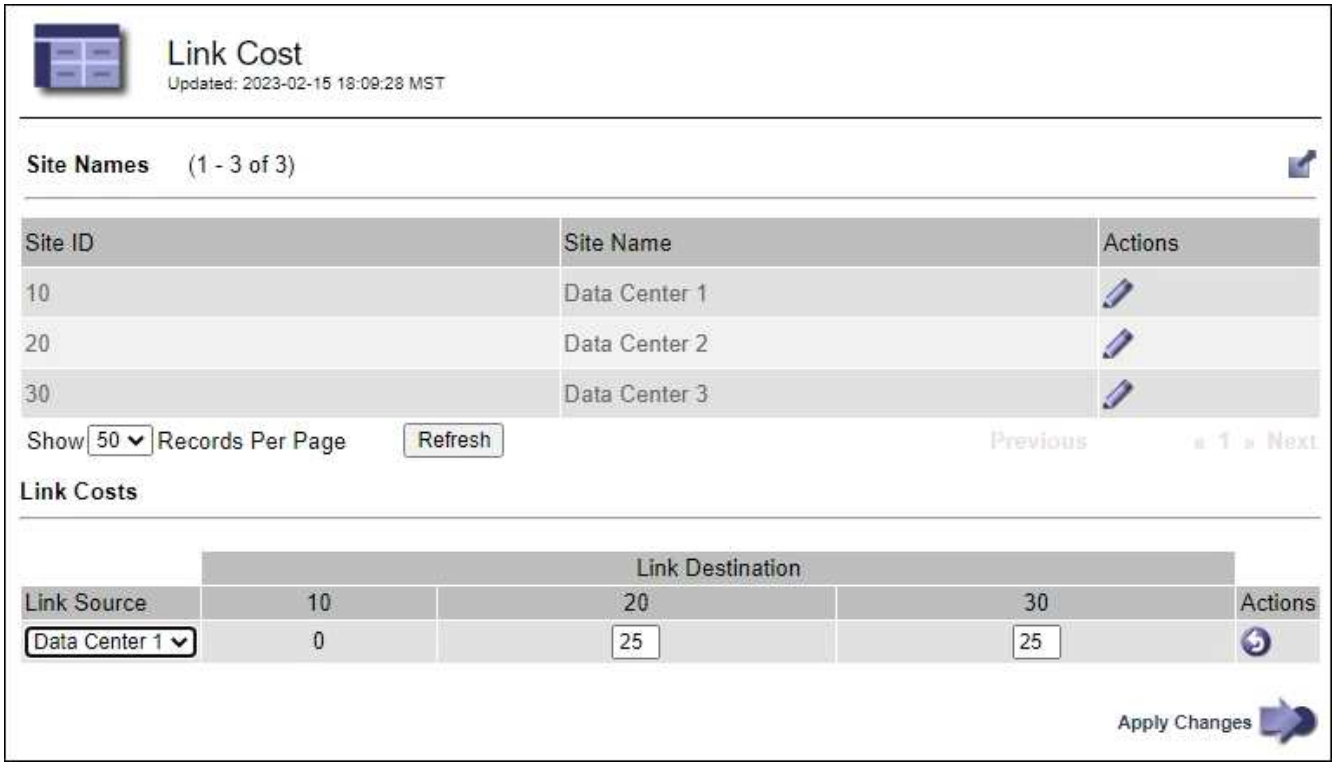
Sie können die Verbindungskosten zwischen den Rechenzentrumsstandorten aktualisieren, um die Latenz zwischen den Standorten widerzuspiegeln.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Weitere Berechtigungen für die Grid-Konfiguration".

Schritte

1. **Support** > **Sonstige** > **Linkkosten** auswählen.



2. Wählen Sie unter **Link Source** eine Site aus und geben Sie unter **Link Destination** einen Kostenwert zwischen 0 und 100 ein.

Die Linkkosten können nicht geändert werden, wenn Quelle und Ziel identisch sind.

Um Änderungen zu verwerfen, **Revert** auswählen.

3. **Änderungen anwenden** auswählen.

Verwendung von AutoSupport

Erfahren Sie mehr über AutoSupport in StorageGRID

Die AutoSupport Funktion ermöglicht es StorageGRID, Integritäts- und Statuspakete an den technischen Support von NetApp zu senden.

Die Nutzung von AutoSupport hilft, Probleme schneller zu lösen. Der technische Support kann den Speicherbedarf Ihres Systems überwachen und dabei unterstützen festzustellen, ob neue Knoten oder Standorte hinzugefügt werden müssen. Optional kann AutoSupport Pakete an ein zusätzliches Ziel senden.

StorageGRID kennt zwei Arten von AutoSupport:

- **StorageGRID AutoSupport** meldet Probleme mit der StorageGRID Software. Standardmäßig bei der ersten Installation von StorageGRID aktiviert. Eine Deaktivierung ist "die Standardkonfiguration von AutoSupport ändern" bei Bedarf möglich.

> Wenn StorageGRID AutoSupport nicht aktiviert ist, erscheint eine Meldung auf dem Grid Manager Dashboard. Die Meldung enthält einen Link zur AutoSupport Konfigurationsseite. Wenn die Meldung geschlossen wird, erscheint sie erst wieder, nachdem der Browser-Cache geleert wurde, selbst wenn AutoSupport weiterhin deaktiviert ist.

- **Gerätehardware AutoSupport** meldet StorageGRID Appliance-Probleme. Sie müssen "Hardware AutoSupport auf jedem Gerät konfigurieren".

Was ist Active IQ?

Active IQ ist ein Cloud-basierter digitaler Berater, der prädiktive Analysen und die Community-Erfahrung aus NetApps installierter Basis nutzt. Kontinuierliche Risikobewertungen, vorausschauende Warnmeldungen, präskriptive Empfehlungen und automatisierte Aktionen tragen dazu bei, Probleme zu verhindern, bevor sie auftreten, was zu einer verbesserten Systemgesundheit und einer höheren Systemverfügbarkeit führt.

Um die Active IQ Dashboards und Funktionen auf der NetApp Support Site zu nutzen, muss AutoSupport aktiviert sein.

"Active IQ Digital Advisor Dokumentation"

Im AutoSupport-Paket enthaltene Informationen

Ein AutoSupport Paket enthält die folgenden Dateien und Details.

Dateiname	Felder	Beschreibung
${post_edited_translations.segment}	AutoSupport Sequenznummer + Ziel für dieses AutoSupport + Zustellungsstatus + Zustellungsversuche + AutoSupport Betreff + Zustellungs-URI + Letzter Fehler + AutoSupport PUT-Dateiname + Erstellungszeit + Komprimierte AutoSupport Größe + Dekomprimierte AutoSupport Größe + Gesamte Erfassungszeit (ms)	AutoSupport-Verlaufsdatei.
AUTOSUPPORT.XML	Knoten + Protokoll zur Kontaktaufnahme mit dem Support + Support-URL für HTTP/HTTPS + Supportadresse + AutoSupport OnDemand State + AutoSupport OnDemand Server URL + AutoSupport OnDemand Polling Interval	AutoSupport Statusdatei. Bietet Details zum verwendeten Protokoll, zur technischen Support-URL und -Adresse, zum Abfrageintervall sowie zu OnDemand AutoSupport, falls aktiviert oder deaktiviert.
BUCKETS.XML	Bucket ID + Account ID + Build Version + Standortbeschränkungskonfiguration + Compliance aktiviert + Compliance-Konfiguration + S3 Object Lock aktiviert + S3 Object Lock-Konfiguration + Konsistenzkonfiguration + CORS aktiviert + CORS-Konfiguration + Letzte Zugriffszeit aktiviert + Richtlinie aktiviert + Richtlinienkonfiguration + Benachrichtigungen aktiviert + Benachrichtigungskonfiguration + Cloud Mirror aktiviert + Cloud Mirror-Konfiguration + Suche aktiviert + Suchkonfiguration + Bucket Tagging aktiviert + Bucket Tagging-Konfiguration + Versioning-Konfiguration	Bietet Konfigurationsdetails und Statistiken auf Bucket-Ebene. Beispiele für Bucket-Konfigurationen sind Plattformdienste, Compliance und Bucket-Konsistenz.

Dateiname	Felder	Beschreibung
${post_edited_translations.segment}	Attribut-ID + Attributname + Wert + Index + Tabellen-ID + Tabellenname	Gridweite Konfigurationsinformationsdatei. Enthält Informationen über Grid-Zertifikate, reservierten Speicherplatz, gridweite Konfigurationseinstellungen (Compliance, S3 Object Lock, Objektkomprimierung, Warnungen, Syslog und ILM-Konfiguration), Details zum Erasure-Coding-Profil, DNS-Name und "NMS-Name".
${post_edited_translations.segment}	Grid-Spezifikationen, Raw-XML	Wird zur Konfiguration und Bereitstellung von StorageGRID verwendet. Enthält Grid-Spezifikationen, NTP-Server-IP, DNS-Server-IP, Netzwerktopologie und Hardwareprofile der Knoten.
GRID-TASKS.XML	Knoten + Service Path + Attribut-ID + Attributname + Wert + Index + Tabellen-ID + Tabellenname	Statusdatei für Grid-Aufgaben (Wartungsvorgänge). Enthält Details zu den aktiven, beendeten, abgeschlossenen, fehlgeschlagenen und ausstehenden Aufgaben des Grids.
GRID.JSON	${post_edited_translations.segment}	Grid-Informationen.
ILM-CONFIGURATION.XML	Attribut-ID + Attributname + Wert + Index + Tabellen-ID + Tabellenname	${post_edited_translations.segment}
ILM-STATUS.XML	Knoten + Servicepfad + Attribut-ID + Attributname + Wert + Index + Tabellen-ID + Tabellenname	ILM-Metrikinformationsdatei. Enthält ILM-Bewertungsraten für jeden Knoten und gridweite Metriken.
${post_edited_translations.segment}	${post_edited_translations.segment}	Aktive ILM Richtliniendatei. Enthält Details zu den aktiven ILM Richtlinien, wie Speicherpool-ID, Aufnahmeverhalten, Filter, Regeln und Beschreibung.
LOG.TGZ	*n. v.*	Herunterladbare Protokolldatei. Enthält `bycast-err.log` und `servermanager.log` von jedem Knoten.

Dateiname	Felder	Beschreibung
${post_edited_translations.segment}	Erfassungsreihenfolge + AutoSupport Inhaltsdateiname für diese Daten + Beschreibung dieses Datenelements + Anzahl der erfassten Bytes + Für die Erfassung aufgewendete Zeit + Status dieses Datenelements + Beschreibung des Fehlers + AutoSupport Inhaltstyp für diese Daten	Enthält AutoSupport-Metadaten und Kurzbeschreibungen aller AutoSupport-Dateien.
${post_edited_translations.segment}	${post_edited_translations.segment}	Gruppen- und Service-Entitäten in der "${post_edited_translations.segment}". Stellt Details zur Grid-Topologie bereit. Der Node kann basierend auf den auf dem Node ausgeführten Services bestimmt werden.
${post_edited_translations.segment}	Knoten + Servicepfad + Attribut-ID + Attributname + Wert + Index + Tabellen-ID + Tabellenname	Objektstatus, einschließlich Hintergrundscan-Status, aktive Übertragung, Transferrate, Gesamtübertragungen, Löschrate, beschädigte Fragmente, verlorene Objekte, fehlende Objekte, Reparaturversuch, Scanrate, geschätzte Scanperiode und Reparaturabschlussstatus.
${post_edited_translations.segment}	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 ausgefallener Laufwerke des Storage-Controllers, Temperatur des Compute-Controller-Chassis, Compute-Hardware, Seriennummer des Compute-Controllers, Netzteil, Laufwerksgröße und Laufwerkstyp.
SERVICE-STATUS.XML	Knoten + Servicepfad + Attribut-ID + Attributname + Wert + Index + Tabellen-ID + Tabellenname	Service-Node-Informationsdatei. Enthält Details wie zugewiesenen Tabellenbereich, freien Tabellenbereich, Reaper-Metriken der Datenbank, Segmentreparaturdauer, Reparaturjobdauer, automatische Job-Neustarts und automatische Job-Beendigungen.
STORAGE-GRADES.XML	${post_edited_translations.segment}	Datei mit Storage-Grade-Definitionen für jeden Storage Node.

Dateiname	Felder	Beschreibung
SUMMARY-ATTRIBUTES.XML	${post_edited_translations.segment}	Systemstatusdaten auf hoher Ebene, die StorageGRID Nutzungsinformationen zusammenfassen. Bietet Details wie den Namen des Grids, Namen der Standorte, Anzahl der Storage Nodes pro Grid und pro Standort, Lizenztyp, Lizenzkapazität und -nutzung, Software-Supportbedingungen sowie Details zu S3-Vorgängen.
${post_edited_translations.segment}	${post_edited_translations.segment}	${post_edited_translations.segment}
${post_edited_translations.segment}	${post_edited_translations.segment}	Statistiken basierend auf den Anwendungsbenutzeragenten. Zum Beispiel die Anzahl der PUT/GET/DELETE/HEAD-Operationen pro Benutzeragent und die Gesamtgröße jeder Operation in Bytes.
X-HEADER-DATA	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 Kopfzeilendaten.

Konfigurieren Sie AutoSupport in StorageGRID

Standardmäßig ist die StorageGRID AutoSupport Funktion bei der ersten Installation von StorageGRID aktiviert. Die Hardware AutoSupport muss jedoch auf jedem Gerät konfiguriert werden. Bei Bedarf kann die AutoSupport Konfiguration geändert werden.

Wenn Sie die Konfiguration von StorageGRID AutoSupport ändern möchten, sollten Änderungen nur auf dem primären Admin-Knoten vorgenommen werden. Es ist erforderlich, Hardware AutoSupport konfigurieren auf jeder Appliance.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Root-Zugriffsberechtigung".
- Wenn Sie HTTPS zum Senden von AutoSupport-Paketen verwenden, wurde dem primären Admin-Node ausgehender Internetzugriff gewährt, entweder direkt oder "Verwendung eines Proxyservers" (eingehende Verbindungen sind nicht erforderlich).
- Wenn auf der StorageGRID AutoSupport-Seite HTTP ausgewählt ist, müssen Sie "einen Proxyserver konfiguriert", um AutoSupport-Pakete als HTTPS weiterzuleiten. Die AutoSupport Server von NetApp weisen über HTTP gesendete Pakete ab.
- 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**: AutoSupport-Pakete werden automatisch einmal pro Woche versendet. Standardeinstellung: Aktiviert.
- **Ereignisgesteuert**: AutoSupport-Pakete werden automatisch stündlich oder bei wichtigen Systemereignissen versendet. Standardeinstellung: Aktiviert.
- **Auf Anfrage**: Ermöglicht dem technischen Support, dass Ihr StorageGRID-System AutoSupport-Pakete automatisch sendet, was hilfreich ist, wenn aktiv an einem Problem gearbeitet wird (erfordert das HTTPS-AutoSupport-Übertragungsprotokoll). Standardeinstellung: Deaktiviert.
- **Vom Benutzer ausgelöst**: AutoSupport-Pakete können jederzeit manuell versendet werden.
- **Protokollsammlung**: "Protokolldateien und Systemdaten manuell sammeln und ein AutoSupport-Paket senden".

Protokoll für AutoSupport-Pakete angeben

Sie können eines der folgenden Protokolle für das Senden von AutoSupport-Paketen verwenden:

- **HTTPS**: Dies ist die Standard- und empfohlene Einstellung für Neuinstallationen. Dieses Protokoll verwendet Port 443. Wenn die Funktion AutoSupport on Demand aktivieren gewünscht wird, muss HTTPS verwendet werden.
- **HTTP**: Wenn Sie HTTP auswählen, müssen Sie einen Proxyserver konfigurieren, um AutoSupport Pakete als HTTPS weiterzuleiten. Die NetApp AutoSupport Server weisen über HTTP gesendete Pakete ab. Dieses Protokoll verwendet Port 80.
- **SMTP**: Diese Option ist zu wählen, wenn AutoSupport-Pakete per E-Mail versendet werden sollen.

Das von Ihnen festgelegte Protokoll wird für den Versand aller Arten von AutoSupport-Paketen verwendet.

Schritte

1. **Support** > **Tools** > **AutoSupport** > **Einstellungen** auswählen.
2. Wählen Sie das Protokoll aus, das Sie zum Senden von AutoSupport-Paketen verwenden möchten.
3. Wenn Sie **HTTPS** ausgewählt haben, wählen Sie aus, ob ein NetApp Support-Zertifikat (TLS-Zertifikat) zur Sicherung der Verbindung zum technischen Support-Server verwendet werden soll.
   - **Zertifikat prüfen** (Standard): Stellt sicher, dass die Übertragung von AutoSupport-Paketen sicher ist. Das NetApp Support-Zertifikat ist bereits mit der StorageGRID Software installiert.
   - **Zertifikat nicht überprüfen**: Diese Option sollte nur gewählt werden, wenn ein triftiger Grund vorliegt, auf die Zertifikatsvalidierung zu verzichten, etwa bei einem vorübergehenden Problem mit einem Zertifikat.
4. **Speichern** auswählen. Alle wöchentlichen, benutzergesteuerten und ereignisgesteuerten Pakete werden mit dem ausgewählten Protokoll gesendet.

Wöchentliche AutoSupport-Benachrichtigungen deaktivieren

Standardmäßig ist das StorageGRID-System so konfiguriert, dass es einmal pro Woche ein AutoSupport-Paket an den technischen Support sendet.

Um festzustellen, wann das wöchentliche AutoSupport-Paket gesendet wird, zur Registerkarte **AutoSupport** > **Ergebnisse** wechseln. Im Abschnitt **Wöchentlich AutoSupport** den Wert für **Nächster geplanter Zeitpunkt**

ansehen.

Sie können den automatischen Versand der wöchentlichen AutoSupport-Pakete jederzeit deaktivieren.

Schritte

1. **Support** > **Tools** > **AutoSupport** > **Einstellungen** auswählen.
2. Deaktivieren Sie das Kontrollkästchen **Wöchentliche AutoSupport Aktivierung**.
3. **Speichern** auswählen.

Ereignisgesteuertes AutoSupport deaktivieren

Standardmäßig ist das StorageGRID-System so konfiguriert, dass es stündlich ein AutoSupport-Paket an den technischen Support sendet.

Sie können die ereignisgesteuerte AutoSupport jederzeit deaktivieren.

Schritte

1. **Support** > **Tools** > **AutoSupport** > **Einstellungen** auswählen.
2. Deaktivieren Sie das Kontrollkästchen **Ereignisgesteuertes AutoSupport aktivieren**.
3. **Speichern** auswählen.

Bei Bedarf AutoSupport aktivieren

AutoSupport on Demand kann bei der Lösung von Problemen unterstützen, an denen der technische Support aktiv arbeitet.

Standardmäßig ist AutoSupport on Demand deaktiviert. Wenn diese Funktion aktiviert ist, kann der technische Support anfordern, dass Ihr StorageGRID System AutoSupport Pakete automatisch sendet. Der technische Support kann außerdem das Abfrageintervall für AutoSupport on Demand Abfragen festlegen.

Der technische Support kann AutoSupport on Demand nicht aktivieren oder deaktivieren.

Schritte

1. **Support** > **Tools** > **AutoSupport** > **Einstellungen** auswählen.
2. Das Protokoll **HTTPS** ist auszuwählen.
3. Aktivieren Sie das Kontrollkästchen **Wöchentliche AutoSupport Aktivierung**.
4. Das Kontrollkästchen **Enable AutoSupport on Demand** auswählen.
5. **Speichern** auswählen.

   AutoSupport on Demand ist aktiviert, und der technische Support kann AutoSupport on Demand-Anfragen an StorageGRID senden.

Überprüfungen auf Softwareupdates deaktivieren

Standardmäßig kontaktiert StorageGRID NetApp, um festzustellen, ob Software-Updates für Ihr System verfügbar sind. Wenn ein StorageGRID Hotfix oder eine neue Version verfügbar ist, wird die neue Version auf der StorageGRID Upgrade-Seite angezeigt.

Bei Bedarf kann die Suche nach Softwareupdates optional deaktiviert werden. Wenn das System beispielsweise keinen WAN-Zugang hat, empfiehlt es sich, die Suche zu deaktivieren, um Downloadfehler zu

vermeiden.

Schritte

1. **Support** > **Tools** > **AutoSupport** > **Einstellungen** auswählen.
2. Das Kontrollkästchen **Nach Software-Updates suchen** deaktivieren.
3. **Speichern** auswählen.

Fügen Sie ein weiteres AutoSupport-Ziel hinzu

Wenn AutoSupport aktiviert ist, werden Gesundheits- und Statuspakete an den technischen Support gesendet. Ein zusätzliches Ziel für alle AutoSupport-Pakete kann angegeben werden.

Um das zum Senden von AutoSupport-Paketen verwendete Protokoll zu überprüfen oder zu ändern, siehe die Anweisungen zu das Protokoll für AutoSupport-Pakete angeben.

Mit dem SMTP-Protokoll können AutoSupport-Pakete nicht an ein zusätzliches Ziel gesendet werden.

Schritte

1. **Support** > **Tools** > **AutoSupport** > **Einstellungen** auswählen.
2. **Zusätzliche AutoSupport Ziele aktivieren** auswählen.
3. Folgendes ist anzugeben:

   Hostname
   Der Server-Hostname oder die IP-Adresse eines zusätzlichen AutoSupport-Zielservers.

   Es kann nur ein weiteres Ziel eingegeben werden.

   Port
   Der Port, der für die Verbindung zu einem zusätzlichen AutoSupport Zielserver verwendet wird. Standardmäßig ist Port 80 für HTTP oder Port 443 für HTTPS voreingestellt.

   Zertifikatsvalidierung
   Ob ein TLS-Zertifikat verwendet wird, um die Verbindung zum zusätzlichen Ziel zu sichern.

   - **Zertifikat überprüfen** auswählen, um die Zertifikatsvalidierung zu nutzen.
   - **Zertifikat nicht überprüfen** auswählen, um Ihre AutoSupport-Pakete ohne Zertifikatsvalidierung zu senden.

     Diese Option ist nur auszuwählen, wenn ein triftiger Grund vorliegt, die Zertifikatsvalidierung nicht zu verwenden, etwa bei einem vorübergehenden Problem mit einem Zertifikat.

4. Wenn **Zertifikat überprüfen** ausgewählt wurde, ist Folgendes zu tun:
   a. Navigieren Sie zum Speicherort des CA-Zertifikats.
   b. Die CA-Zertifikatsdatei hochladen.

      Die Metadaten des CA-Zertifikats werden angezeigt.

5. **Speichern** auswählen.

Alle zukünftigen wöchentlichen, ereignisgesteuerten und benutzergesteuerten AutoSupport-Pakete werden an das zusätzliche Ziel gesendet.

AutoSupport für Appliances konfigurieren

AutoSupport für Appliances meldet StorageGRID Hardwareprobleme, und StorageGRID AutoSupport meldet StorageGRID Softwareprobleme, mit einer Ausnahme: Beim SGF6112 meldet StorageGRID AutoSupport sowohl Hardware- als auch Softwareprobleme. AutoSupport muss auf jeder Appliance konfiguriert werden, außer beim SGF6112, der keine zusätzliche Konfiguration erfordert. AutoSupport wird für Service-Appliances und Storage-Appliances unterschiedlich implementiert.

Mit SANtricity lässt sich AutoSupport für jedes Storage Appliance aktivieren. Die Konfiguration von SANtricity AutoSupport ist während der Ersteinrichtung eines Storage Appliance oder nach dessen Installation möglich:

- Für SG6000 und SG5700 Appliances, "Konfiguration von AutoSupport im SANtricity System Manager"

AutoSupport-Pakete von E-Series Appliances können in StorageGRID AutoSupport einbezogen werden, wenn die AutoSupport-Zustellung per Proxy in "SANtricity System Manager" konfiguriert wird.

StorageGRID AutoSupport meldet keine Hardwareprobleme wie DIMM- oder Host-Schnittstellenkarten (HIC)-Fehler. Allerdings können bestimmte Komponentenausfälle "Hardware-Warnmeldungen" auslösen. Für StorageGRID Appliances mit einem Baseboard Management Controller (BMC) besteht die Möglichkeit, E-Mail- und SNMP-Traps zu konfigurieren, um Hardwarefehler zu melden.

- "E-Mail-Benachrichtigungen für BMC-Warnungen einrichten"
- "SNMP-Einstellungen für BMC konfigurieren"

Verwandte Informationen

"NetApp Support"

Manuelles Auslösen eines AutoSupport-Pakets in StorageGRID

Um den technischen Support bei der Fehlerbehebung Ihres StorageGRID Systems zu unterstützen, kann ein AutoSupport-Paket manuell zum Senden ausgelöst werden.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie verfügen über die Root-Zugriffsberechtigung oder die Berechtigung zur Konfiguration anderer Grids.

Schritte

1. **Support** > **Tools** > **AutoSupport** auswählen.
2. Auf der Registerkarte **Aktionen Benutzerausgelöste AutoSupport senden** auswählen.

   StorageGRID versucht, ein AutoSupport-Paket an die NetApp Support Site zu senden. Bei Erfolg werden die Werte für **Letztes Ergebnis** und **Letzter erfolgreicher Zeitpunkt** auf der Registerkarte **Ergebnisse** aktualisiert. Tritt ein Problem auf, wird der Wert für **Letztes Ergebnis** auf „Fehlgeschlagen“ gesetzt, und StorageGRID versucht nicht, das AutoSupport-Paket erneut zu senden.

3. Nach einer Minute die AutoSupport-Seite im Browser aktualisieren, um auf die neuesten Ergebnisse zuzugreifen.

Außerdem können Sie "umfangreichere Protokolldateien und Systemdaten erfassen" und sie an die NetApp Support Site senden.

Fehlerbehebung bei StorageGRID AutoSupport-Paketen

Schlägt der Versand eines AutoSupport-Pakets fehl, ergreift das StorageGRID-System je nach Typ des AutoSupport-Pakets unterschiedliche Maßnahmen. Der Status der AutoSupport-Pakete kann unter **Support** > **Tools** > **AutoSupport** > **Results** überprüft werden.

Wenn das AutoSupport-Paket nicht gesendet werden kann, erscheint "Fehlgeschlagen" auf der Registerkarte **Ergebnisse** der **AutoSupport**-Seite.

Wenn ein Proxyserver konfiguriert wurde, um AutoSupport-Pakete an NetApp weiterzuleiten, sollte "Es sollte überprüft werden, ob die Proxyserver Konfigurationseinstellungen korrekt sind.".

Wöchentlicher AutoSupport Paketausfall

Wenn der Versand eines wöchentlichen AutoSupport-Pakets fehlschlägt, führt das StorageGRID System die folgenden Aktionen aus:

1. Aktualisiert das Attribut „Letztes Ergebnis“ auf „Wiederholen“.
2. Es wird versucht, das AutoSupport-Paket eine Stunde lang alle vier Minuten insgesamt 15 Mal erneut zu senden.
3. Nach einer Stunde fehlgeschlagener Sendevorgänge wird das Attribut „Letztes Ergebnis“ auf „Fehlgeschlagen“ aktualisiert.
4. Es wird versucht, das AutoSupport-Paket zum nächsten geplanten Zeitpunkt erneut zu versenden.
5. Behält den regulären AutoSupport Zeitplan bei, wenn das Paket fehlschlägt, weil der NMS-Dienst nicht verfügbar ist, und wenn ein Paket vor Ablauf von sieben Tagen gesendet wird.
6. Wenn der NMS-Dienst wieder verfügbar ist, wird ein AutoSupport-Paket umgehend gesendet, falls seit sieben Tagen oder länger kein Paket gesendet wurde.

Benutzer- oder ereignisgesteuerter AutoSupport-Paketausfall

Wenn ein vom Benutzer oder durch ein Ereignis ausgelöstes AutoSupport-Paket nicht gesendet werden kann, ergreift das StorageGRID-System die folgenden Maßnahmen:

1. Zeigt eine Fehlermeldung an, wenn der Fehler bekannt ist. Wenn ein Benutzer beispielsweise das SMTP-Protokoll auswählt, ohne korrekte E-Mail-Konfigurationseinstellungen anzugeben, wird der folgende Fehler angezeigt: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. Es erfolgt kein erneuter Versand des Pakets.
3. Protokolliert den Fehler in `nms.log`.

Tritt ein Fehler auf und ist SMTP als Protokoll ausgewählt, ist zu überprüfen, ob der E-Mail-Server des StorageGRID-Systems korrekt konfiguriert ist und ob Ihr E-Mail-Server läuft (**Support** > **Alarms (legacy)** > **Legacy Email Setup**). Die folgende Fehlermeldung kann auf der AutoSupport-Seite erscheinen: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Informationen dazu, wie "E-Mail-Servereinstellungen konfigurieren".

Einen AutoSupport Paketfehler korrigieren

Tritt ein Fehler auf und ist SMTP als Protokoll ausgewählt, sollte überprüft werden, ob der E-Mail-Server des StorageGRID-Systems korrekt konfiguriert ist und ob Ihr E-Mail-Server läuft. Die folgende Fehlermeldung kann auf der AutoSupport-Seite erscheinen: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

E-Series AutoSupport-Pakete über StorageGRID senden

Sie können E-Series SANtricity System Manager AutoSupport Pakete über einen StorageGRID Admin Node statt über den Management-Port des Storage Appliance an den technischen Support senden.

Weitere Informationen zur Verwendung von AutoSupport mit E-Series Appliances sind unter "E-Series Hardware AutoSupport" verfügbar.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Administrator- oder Root-Zugriffsberechtigung für Storage Appliance".
- Sie haben SANtricity AutoSupport konfiguriert:
  - Für SG6000 und SG5700 Appliances, "Konfiguration von AutoSupport im SANtricity System Manager"

> Für den Zugriff auf SANtricity System Manager mit dem Grid Manager ist SANtricity Firmware 8.70 oder höher erforderlich.

Über diese Aufgabe

E-Series AutoSupport-Pakete enthalten Details zur Speicherhardware und sind spezifischer als andere AutoSupport-Pakete, die vom StorageGRID System gesendet werden.

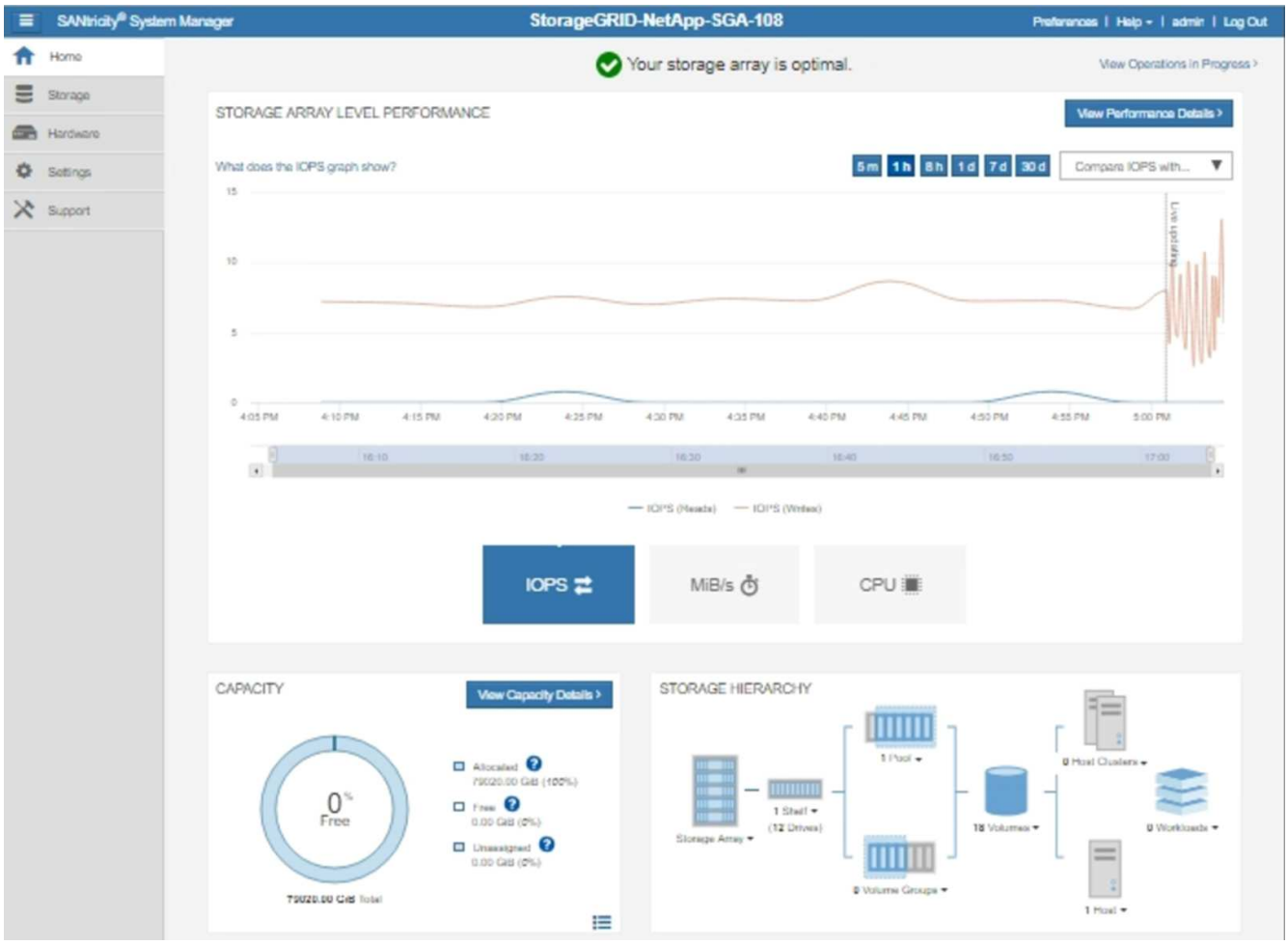
Im SANtricity System Manager kann eine spezielle Proxyserver-Adresse konfiguriert werden, um AutoSupport-Pakete über einen StorageGRID Admin-Node ohne Verwendung des Management-Ports des Geräts zu übertragen. AutoSupport-Pakete, die auf diese Weise übertragen werden, werden vom "bevorzugter Absender Admin Node" gesendet und verwenden alle "Administrator-Proxy-Einstellungen" , die im Grid Manager konfiguriert wurden.

> Dieses Verfahren ist ausschließlich für die Konfiguration eines StorageGRID Proxyserver für E-Series AutoSupport Pakete vorgesehen. Weitere Details zur E-Series AutoSupport Konfiguration finden sich unter "NetApp E-Series und SANtricity Dokumentation".

Schritte

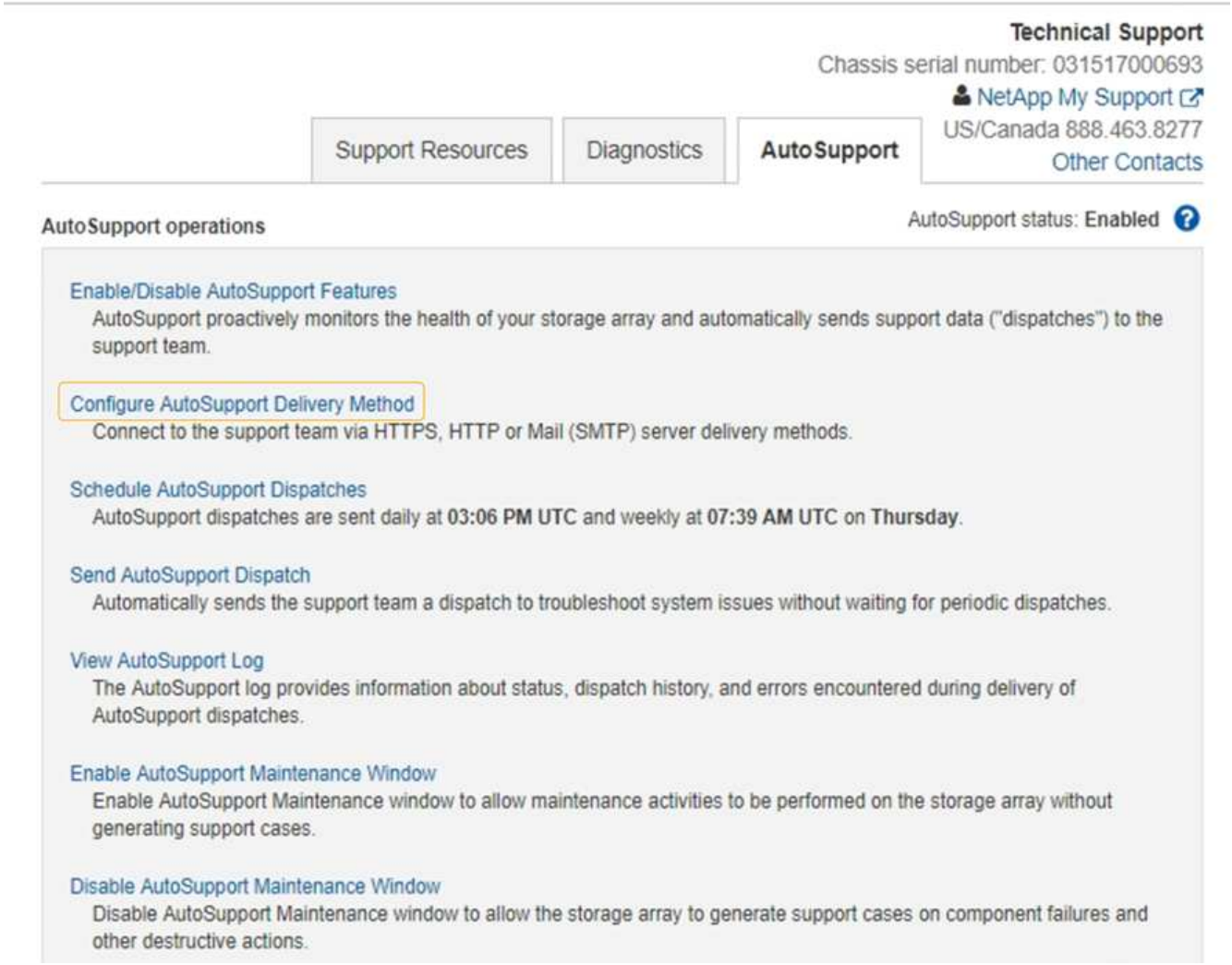
1. Im Grid Manager wählen Sie **Knoten** aus.
2. Wählen Sie in der Liste der Knoten auf der linken Seite den Speichergeräteknoten aus, den Sie konfigurieren möchten.
3. **SANtricity System Manager** auswählen.

   Die Startseite des SANtricity System Managers wird angezeigt.



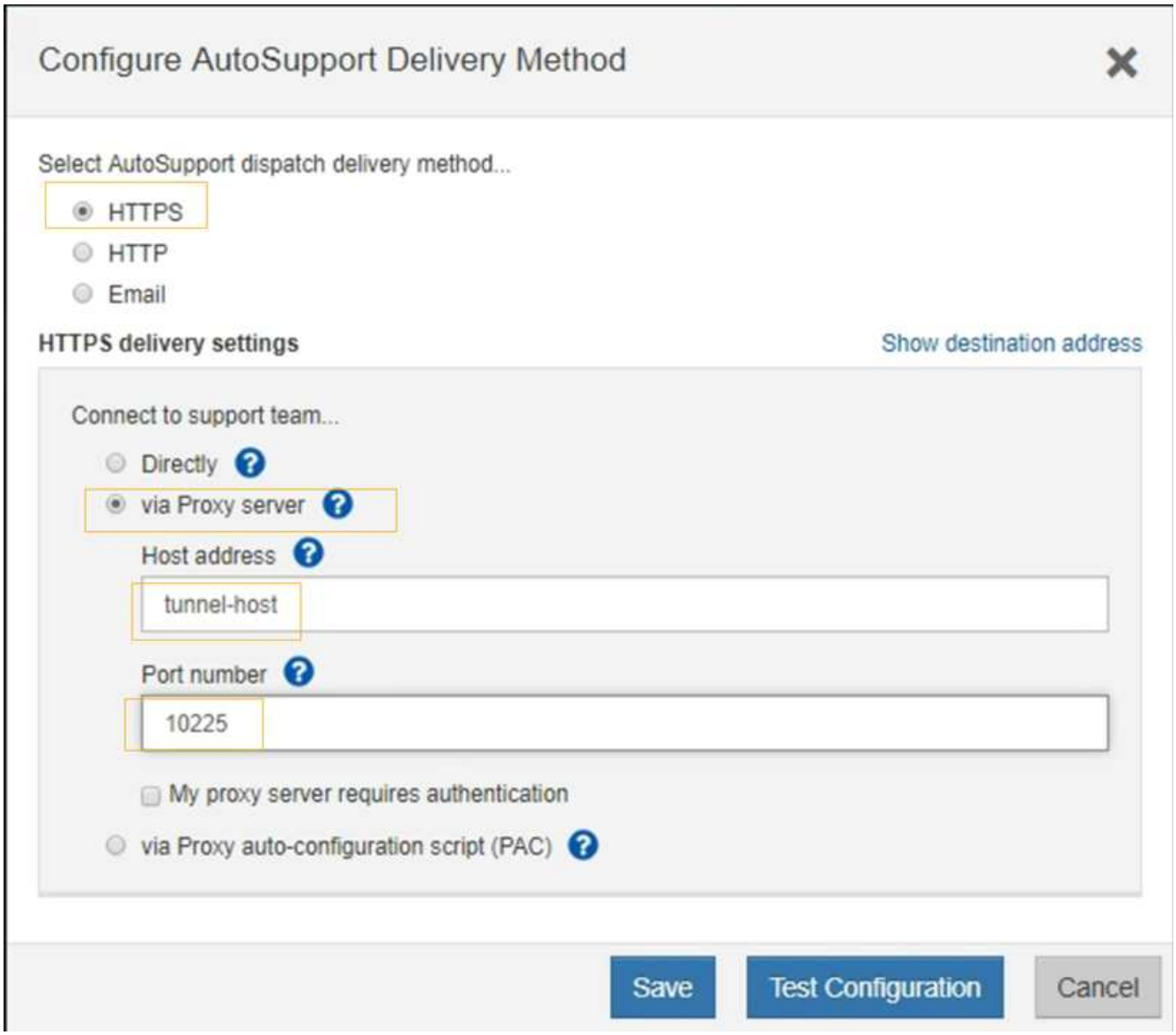
4. **Support** > **Support center** > **AutoSupport** auswählen.

   Die AutoSupport Operationsseite wird angezeigt.



5. Wählen Sie **Configure AutoSupport Delivery Method**.

   Die Seite „AutoSupport Zustellmethode konfigurieren“ wird angezeigt.



6. **HTTPS** als Zustellungsmethode auswählen.

   Das Zertifikat, das HTTPS ermöglicht, ist vorinstalliert.

7. **Über Proxyserver** auswählen.
8. Geben Sie `tunnel-host` für die **Hostadresse** ein.

   `tunnel-host` ist die spezielle Adresse, um einen Admin-Knoten zum Senden von E-Series AutoSupport Paketen zu verwenden.

9. Geben Sie `10225` für die **Portnummer** ein.

   `10225` ist die Portnummer auf dem StorageGRID Proxyserver, der AutoSupport-Pakete vom E-Series Controller im Gerät empfängt.

10. **Konfiguration testen** dient zum Testen des Routings und der Konfiguration Ihres AutoSupport Proxyserver.

Wenn alles korrekt ist, erscheint eine Meldung in einem grünen Banner: „Ihre AutoSupport Konfiguration wurde überprüft.“

Schlägt der Test fehl, erscheint eine Fehlermeldung in einem roten Banner. Die StorageGRID DNS-Einstellungen und die Netzwerkkonfiguration sollten überprüft werden, zudem ist sicherzustellen, dass der "bevorzugter Absender Admin Node" eine Verbindung zur NetApp Support Site herstellen kann; anschließend kann der Test erneut durchgeführt werden.

11. **Speichern** auswählen.

    Die Konfiguration wird gespeichert, und eine Bestätigungsmeldung erscheint: „AutoSupport delivery method has been configured.“

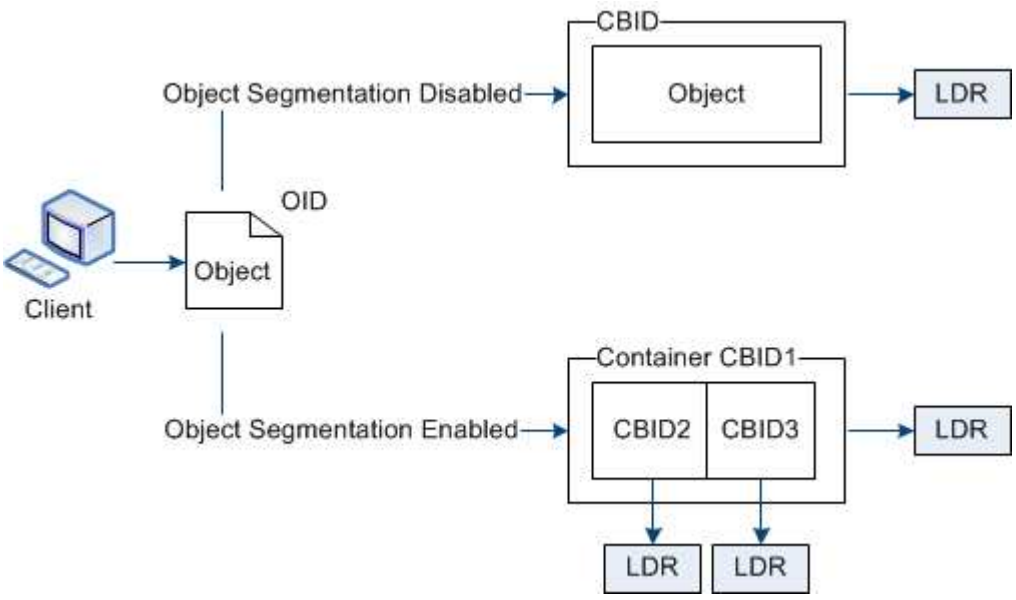
Speicherknoten verwalten

Speicheroptionen verwenden

Erfahren Sie mehr über die Objektsegmentierung in StorageGRID

Die Objektsegmentierung ist der Prozess des Aufteilens eines Objekts in eine Sammlung kleinerer Objekte fester Größe, um die Speicher- und Ressourcennutzung für große Objekte zu optimieren. Der S3 Multipart-Upload erstellt ebenfalls segmentierte Objekte, wobei ein Objekt jeden Teil darstellt.

${post_edited_translations.segment}



Beim Abruf eines Segmentcontainers setzt der LDR Service das ursprüngliche Objekt aus seinen Segmenten zusammen und gibt das Objekt an den Client zurück.

Der Container und die Segmente müssen nicht zwingend auf demselben Storage Node gespeichert werden. Container und Segmente können auf jedem Storage Node innerhalb des in der ILM-Regel angegebenen Speicherpools gespeichert werden.

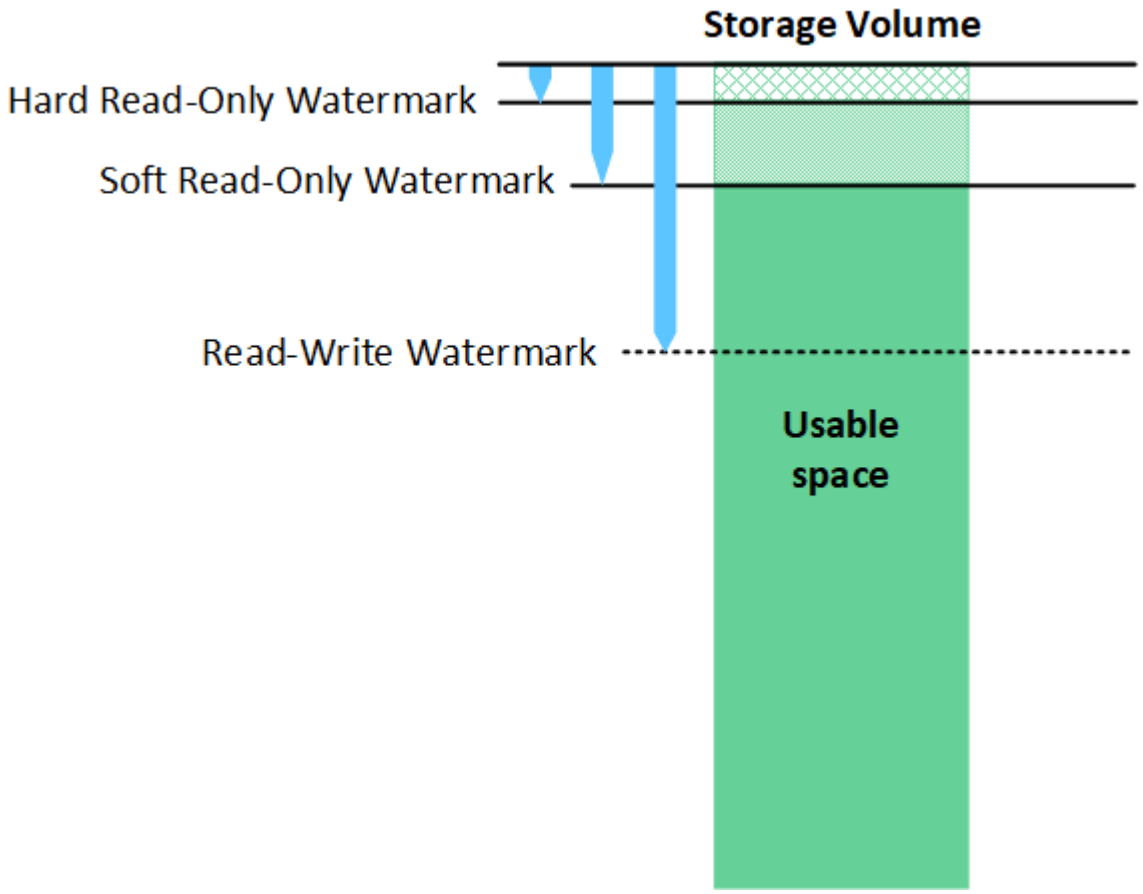
Jedes Segment wird vom StorageGRID System unabhängig behandelt und trägt zur Anzahl von Attributen wie

Managed Objects und Stored Objects bei. Wenn beispielsweise ein im StorageGRID System gespeichertes Objekt in zwei Segmente aufgeteilt wird, erhöht sich der Wert von Managed Objects nach Abschluss des Ingest-Vorgangs wie folgt um drei:

```
segment container + segment 1 + segment 2 = three stored objects
```

Erfahren Sie mehr über Speicher-Volume-Wasserzeichen in StorageGRID

${post_edited_translations.segment}



Speichervolumen-Wasserzeichen gelten nur für den Speicherplatz, der für replizierte und löschcodierte Objektdaten verwendet wird. Informationen zum für Objektmetadaten auf Volume 0 reservierten Speicherplatz sind unter "Objekt-Metadaten-Speicher verwalten" zu finden.

Was ist das Soft-Read-Only-Wasserzeichen?

Das **Speichervolumen Soft Read-Only-Wasserzeichen** ist das erste Wasserzeichen, das anzeigt, dass der nutzbare Speicherplatz eines Storage Node für Objektdaten fast voll ist.

Wenn auf jedem Volume eines Storage Node weniger freier Speicherplatz vorhanden ist als der Soft-Read-only-Grenzwert dieses Volumes, wechselt der Storage Node in den schreibgeschützten Modus. Schreibgeschützter Modus bedeutet, dass der Storage Node dem restlichen StorageGRID System schreibgeschützte Dienste anbietet, aber alle ausstehenden Schreibanforderungen erfüllt.

Angenommen, jedes Volume in einem Storage Node hat eine weiche schreibgeschützte Markierung von 10 GB. Sobald jedes Volume weniger als 10 GB freien Speicherplatz hat, wechselt der Storage Node in den

weichen schreibgeschützten Modus.

${post_edited_translations.segment}

Das **Speichervolumen Hard Read-Only Watermark** ist das nächste Watermark, das anzeigt, dass der nutzbare Speicherplatz eines Knotens für Objektdaten fast voll ist.

Wenn der freie Speicherplatz auf einem Volume geringer ist als der harte Read-Only-Grenzwert dieses Volumes, schlagen Schreibvorgänge auf dem Volume fehl. Schreibvorgänge auf anderen Volumes können jedoch fortgesetzt werden, bis der freie Speicherplatz auf diesen Volumes geringer ist als deren harte Read-Only-Grenzwerte.

Nehmen wir beispielsweise an, dass jedes Volume in einem Storage Node einen harten schreibgeschützten Grenzwert von 5 GB aufweist. Sobald jedes Volume weniger als 5 GB freien Speicherplatz aufweist, akzeptiert der Storage Node keine Schreibanforderungen mehr.

Das harte schreibgeschützte Wasserzeichen ist immer kleiner als das weiche schreibgeschützte Wasserzeichen.

${post_edited_translations.segment}

Die **Speichervolumen Lese-/Schreibgrenze** gilt nur für Storage Nodes, die in den Nur-Lese-Modus gewechselt haben. Sie legt fest, wann der Node wieder in den Lese-/Schreibmodus wechseln kann. Wenn der freie Speicherplatz auf einem Speichervolumen eines Storage Nodes größer als die Lese-/Schreibgrenze dieses Volumens ist, wechselt der Node automatisch zurück in den Lese-/Schreibmodus.

Angenommen, der Storage Node ist beispielsweise in den schreibgeschützten Modus gewechselt. Zudem wird angenommen, dass jedes Volume einen Lese-Schreib-Grenzwert von 30 GB hat. Sobald der freie Speicherplatz für ein beliebiges Volume auf 30 GB ansteigt, ist der Node wieder beschreib- und lesbar.

Das Lese-/Schreibwasserzeichen ist immer größer als sowohl das weiche Lesewasserzeichen als auch das harte Lesewasserzeichen.

${post_edited_translations.segment}

Sie können die aktuellen Watermark-Einstellungen und die systemoptimierten Werte anzeigen. Wenn keine optimierten Watermarks verwendet werden, können Sie feststellen, ob Sie die Einstellungen anpassen können oder sollten.

Bevor Sie beginnen

- ${post_edited_translations.segment}
- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Root-Zugriffsberechtigung".

Aktuelle Wasserzeicheneinstellungen anzeigen

Die aktuellen Einstellungen für das Speicherwasserzeichen sind im Grid Manager einsehbar.

Schritte

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}
    - ${post_edited_translations.segment}

Dies ist die standardmäßige und empfohlene Einstellung. Diese Werte sollten nicht aktualisiert werden. Optional können Sie Optimierte Speicherwasserzeichen anzeigen.

- Wenn das Kontrollkästchen „Optimierte Werte verwenden“ deaktiviert ist, werden benutzerdefinierte (nicht optimierte) Wasserzeichen verwendet. Die Verwendung benutzerdefinierter Wasserzeicheneinstellungen wird nicht empfohlen. Die Anweisungen für "Fehlerbehebung bei Warnmeldungen zur Überschreibung des Low read-only watermark" geben Aufschluss darüber, ob eine Anpassung der Einstellungen möglich oder sinnvoll ist.

  ${post_edited_translations.segment}

Optimierte Speicherwasserzeichen anzeigen

StorageGRID verwendet zwei Prometheus-Metriken, um die optimierten Werte anzuzeigen, die für das Soft-Read-Only-Watermark des Speichervolumens berechnet wurden. Die minimalen und maximalen optimierten Werte für jeden Storage Node im Grid sind einsehbar.

1. **Support** > **Tools** > **Metrics** auswählen.
2. Im Abschnitt Prometheus den Link auswählen, um auf die Prometheus Benutzeroberfläche zuzugreifen.
3. ${post_edited_translations.segment}

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   Die letzte Spalte zeigt den minimalen optimierten Wert des weichen Grenzwerts für Schreibschutz für alle Speichervolumina auf jedem Storage Node. Wenn dieser Wert größer ist als die benutzerdefinierte Einstellung für den weichen Grenzwert für Schreibschutz des Speichervolumens, wird die Warnmeldung **Low read-only watermark override** für den Storage Node ausgelöst.

4. Das empfohlene maximale Soft-Read-Only-Watermark wird angezeigt, wenn die folgende Prometheus-Metrik eingegeben und **Ausführen** ausgewählt wird:

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   Die letzte Spalte zeigt den maximal optimierten Wert des Soft-Read-Only-Wasserzeichens für alle Storage Volumes auf jedem Storage Node.

Verwalten Sie die Speicherung von Objektmetadaten in StorageGRID

Die Metadatenkapazität eines StorageGRID Systems bestimmt die maximale Anzahl an Objekten, die auf diesem System gespeichert werden können. Damit Ihr StorageGRID System über ausreichend Speicherplatz für neue Objekte verfügt, ist es erforderlich zu verstehen, wo und wie StorageGRID Objektmetadaten speichert.

Was sind Objektmetadaten?

Objektmetadaten sind alle Informationen, die ein Objekt beschreiben. StorageGRID verwendet Objektmetadaten, um die Standorte aller Objekte im Grid zu verfolgen und den Lebenszyklus jedes Objekts im Laufe der Zeit zu verwalten.

Für ein Objekt in StorageGRID umfassen die Objektmetadaten die folgenden Arten von Informationen:

- Systemmetadaten, einschließlich einer eindeutigen ID für jedes Objekt (UUID), des Objektnamens, des

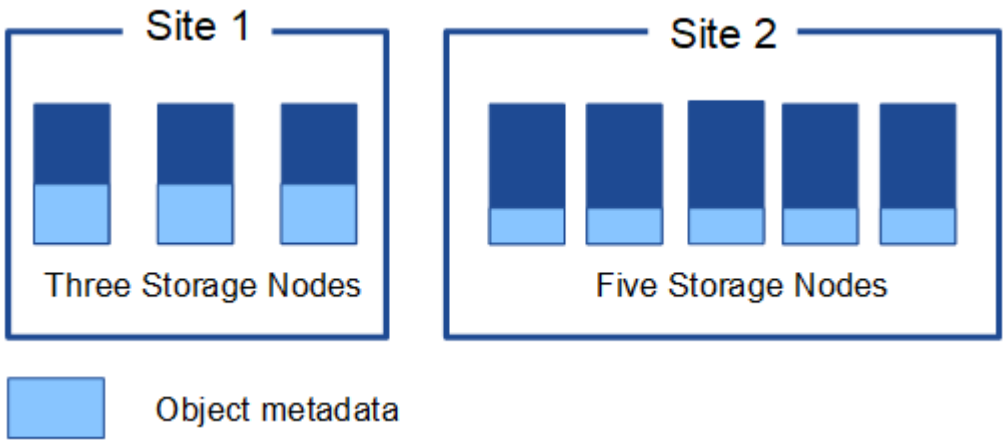
Namens des S3-Buckets, des Mandantenkontonamens oder der Mandanten-ID, der logischen Größe des Objekts, des Datums und der Uhrzeit der ersten Erstellung des Objekts sowie des Datums und der Uhrzeit der letzten Änderung des Objekts.

- Alle benutzerdefinierten Metadaten-Schlüssel-Wert-Paare, die dem Objekt zugeordnet sind.
- Bei S3-Objekten alle Objekt-Tag-Schlüssel-Wert-Paare, die dem Objekt zugeordnet sind.
- Für replizierte Objektkopien der aktuelle Speicherort jeder Kopie.
- Für mit Erasure-Codierung versehene Objektkopien ist der aktuelle Speicherort jedes Fragments.
- Bei Objektkopien in einem Cloud-Speicherpool ist der Speicherort des Objekts, einschließlich des Namens des externen Buckets und der eindeutigen Kennung des Objekts.
- Für segmentierte Objekte und mehrteilige Objekte, Segmentkennungen und Datengrößen.

Wie werden Objektmetadaten gespeichert?

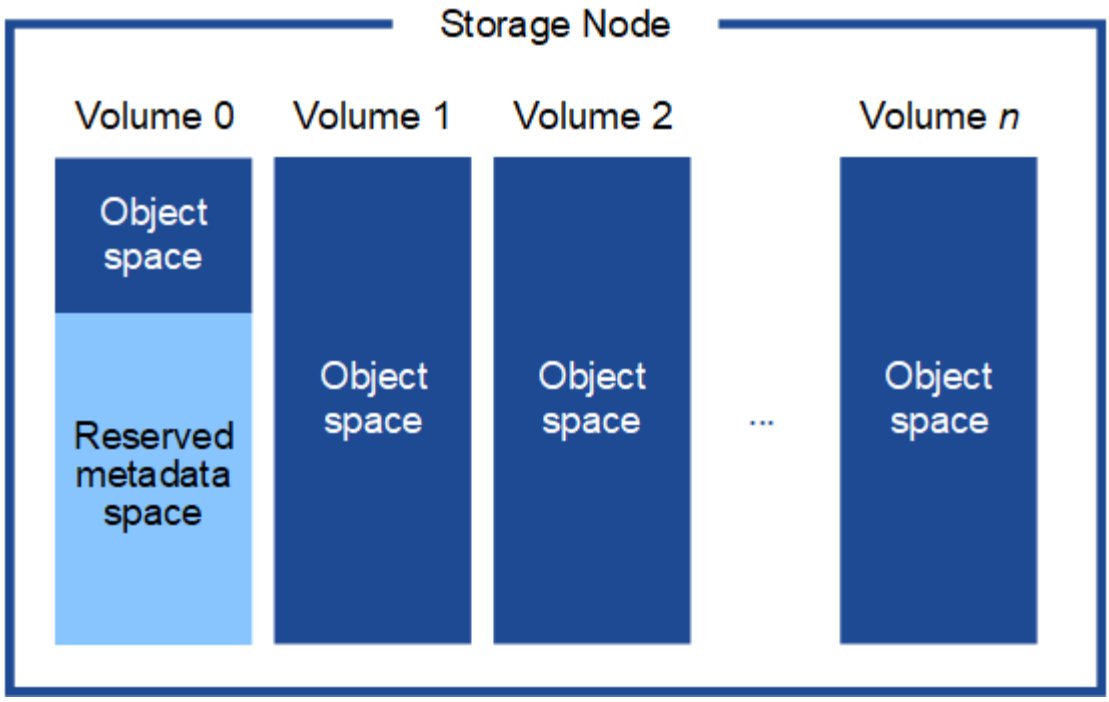
StorageGRID verwaltet Objektmetadaten in einer Cassandra Datenbank, die unabhängig von den Objektdaten gespeichert wird. Zur Gewährleistung von Redundanz und zum Schutz der Objektmetadaten vor Verlust speichert StorageGRID an jedem Standort drei Kopien der Metadaten für alle Objekte im System.

Diese Abbildung stellt die Storage Nodes an zwei Standorten dar. Jeder Standort verfügt über die gleiche Menge an Objektmetadaten, und die Metadaten jedes Standorts sind auf alle Storage Nodes an diesem Standort aufgeteilt.



Wo werden Objektmetadaten gespeichert?

Diese Abbildung stellt die Speichervolumina für einen einzelnen Storage Node dar.



Wie in der Abbildung dargestellt, reserviert StorageGRID Speicherplatz für Objektmetadaten auf Speichervolume 0 jedes Storage Node. Der reservierte Speicherplatz wird zum Speichern von Objektmetadaten und zur Durchführung wichtiger Datenbankoperationen verwendet. Der verbleibende Speicherplatz auf Speichervolume 0 und allen anderen Speichervolumes im Storage Node wird ausschließlich für Objektdaten (replizierte Kopien und Erasure-Coding-Fragmente) genutzt.

Der für Objektmetadaten auf einem bestimmten Storage Node reservierte Speicherplatz hängt von mehreren Faktoren ab, die im Folgenden beschrieben werden.

Metadaten reservierter Speicherplatz Einstellung

Der *reservierte Speicherplatz für Metadaten* ist eine systemweite Einstellung, die die Menge an Speicherplatz angibt, die auf Volume 0 jedes Storage Node für Metadaten reserviert wird. Wie in der Tabelle dargestellt, basiert der Standardwert dieser Einstellung auf:

- Die Softwareversion, die bei der Erstinstallation von StorageGRID verwendet wurde.
- Die Menge an RAM auf jedem Storage Node.

Version, die für die Erstinstallation von StorageGRID verwendet wurde	Menge an RAM auf Storage Nodes	Standardeinstellung für reservierten Metadatenbereich
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 einem beliebigen Storage Node im Grid	3 TB (3.000 GB)
11,1 bis 11,4	128 GB oder mehr auf jedem Storage Node an einem beliebigen Standort	4 TB (4.000 GB)

Version, die für die Erstinstallation von StorageGRID verwendet wurde	Menge an RAM auf Storage Nodes	Standardeinstellung für reservierten Metadatenbereich
	Weniger als 128 GB auf einem beliebigen Storage Node an jedem Standort	3 TB (3.000 GB)
11.0 oder früher	Beliebiger Betrag	2 TB (2.000 GB)

Einstellung für reservierten Speicherplatz für Metadaten anzeigen

Die folgenden Schritte zeigen die Einstellung für den reservierten Speicherplatz für Metadaten Ihres StorageGRID Systems an.

Schritte

1. ${post_edited_translations.segment}
2. Auf der Seite „Speichereinstellungen“ den Abschnitt **Reservierter Metadatenspeicherplatz** erweitern.

Für StorageGRID 11.8 oder höher muss der Wert für den reservierten Metadatenspeicher mindestens 100 GB und höchstens 1 PB betragen.

Die Standardeinstellung für eine neue StorageGRID 11.6 oder höhere Installation, bei der jeder Speicherknoten über 128 GB oder mehr RAM verfügt, beträgt 8.000 GB (8 TB).

Tatsächlich reservierter Speicherplatz für Metadaten

Im Gegensatz zur systemweiten Einstellung für reservierten Speicherplatz für Metadaten wird der tatsächlich reservierte Speicherplatz für Objektmetadaten für jeden Storage Node bestimmt. Für einen bestimmten Storage Node hängt der tatsächlich reservierte Speicherplatz für Metadaten von der Größe von Volume 0 des Knotens und der systemweiten Einstellung für reservierten Speicherplatz für Metadaten ab.

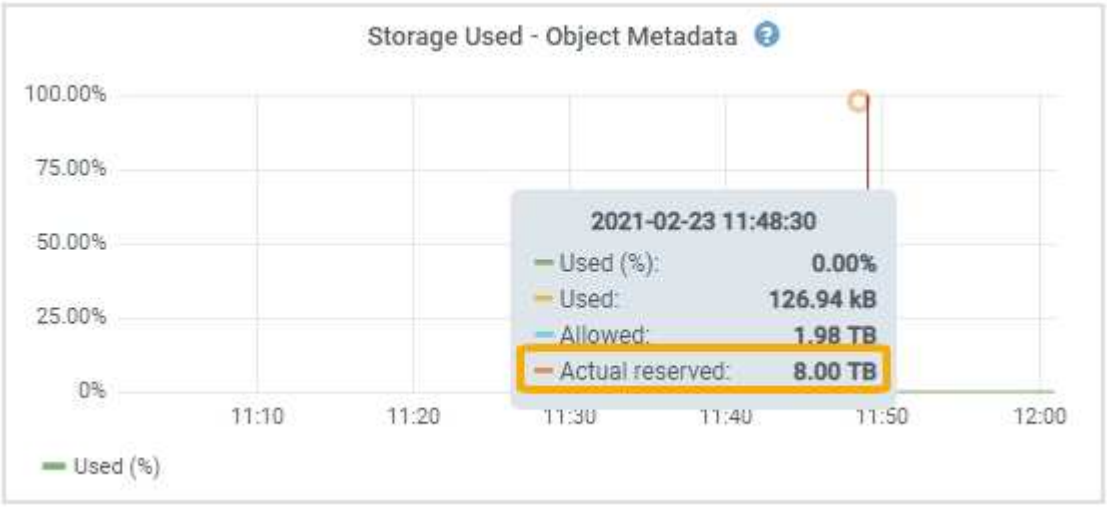
Größe des Volumens 0 für den Knoten	Tatsächlich reservierter Speicherplatz für Metadaten
Weniger als 500 GB (nicht für Produktionszwecke)	10 % des Volume 0
500 GB oder mehr + oder + nur Metadaten-Speicherknoten	Der kleinere dieser Werte: • Volume 0 • Metadaten reservierter Speicherplatz Einstellung **Hinweis**: Für reine Metadaten-Storage Nodes wird nur eine rangedb benötigt.

Tatsächlich reservierter Speicherplatz für Metadaten

Die folgenden Schritte zeigen den tatsächlich reservierten Speicherplatz für Metadaten auf einem bestimmten Storage Node.

Schritte

1. Im Grid Manager **Knoten** > ***Speicherknoten*** auswählen.
2. Die Registerkarte **Speicher** auswählen.
3. Fahren Sie mit dem Cursor über das Diagramm „Speicherplatznutzung Objektmetadaten“ und suchen Sie den Wert **Tatsächlich reserviert**.



Im Screenshot beträgt der Wert für den **tatsächlich reservierten Speicherplatz** 8 TB. Dieser Screenshot zeigt einen großen Storage Node in einer neuen StorageGRID 11.6 Installation. Da die systemweite Einstellung für den reservierten Metadatenspeicherplatz kleiner ist als Volume 0 für diesen Storage Node, entspricht der tatsächlich reservierte Speicherplatz für diesen Node der Einstellung für den reservierten Metadatenspeicherplatz.

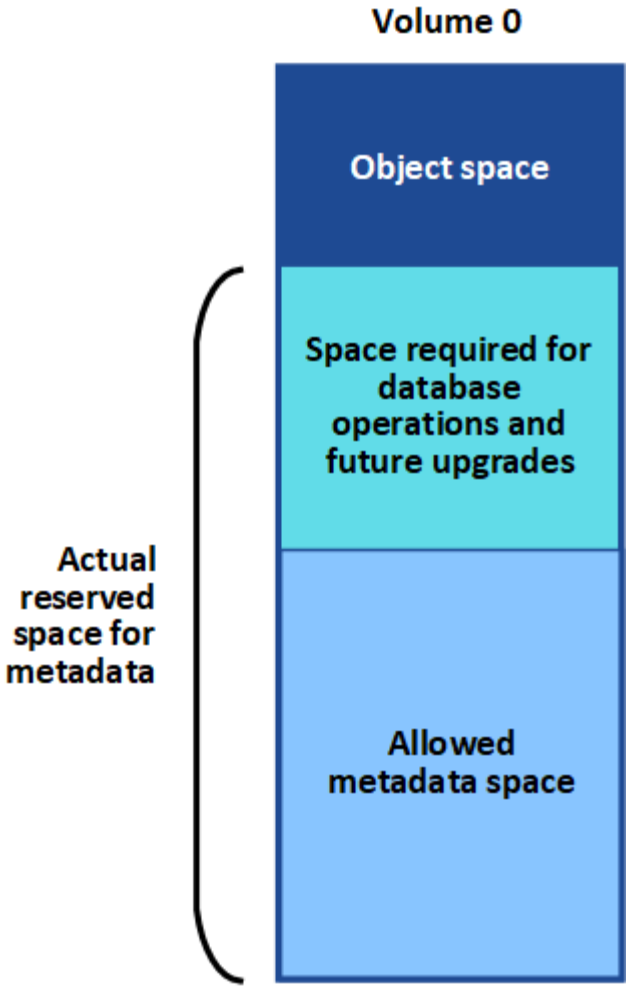
Beispiel für tatsächlich reservierten Metadaten-Speicherplatz

Angenommen, Sie installieren ein neues StorageGRID System mit Version 11.7 oder höher. Für dieses Beispiel wird angenommen, dass jeder Storage Node über mehr als 128 GB RAM verfügt und dass Volume 0 von Storage Node 1 (SN1) 6 TB groß ist. Basierend auf diesen Werten:

- Der systemweite **Metadata reservierter Speicherplatz** ist auf 8 TB festgelegt. (Dies ist der Standardwert für eine neue StorageGRID 11.6 oder höher Installation, wenn jeder Storage Node über mehr als 128 GB RAM verfügt.)
- Der tatsächlich reservierte Speicherplatz für Metadaten für SN1 beträgt 6 TB. (Das gesamte Volume ist reserviert, da Volume 0 kleiner ist als die Einstellung **Reservierter Speicherplatz für Metadaten**.)

Zulässiger Metadatenspeicherplatz

Der tatsächlich reservierte Speicherplatz für Metadaten jedes Storage Node ist unterteilt in den für Objektmetadaten verfügbaren Speicherplatz (den *zulässigen Metadatenspeicherplatz*) und den Speicherplatz, der für essentielle Datenbankoperationen (wie Komprimierung und Reparatur) sowie zukünftige Hardware- und Software-Upgrades benötigt wird. Der zulässige Metadatenspeicherplatz bestimmt die Gesamtkapazität der Objekte.



Die folgende Tabelle zeigt, wie StorageGRID den **zulässigen Metadatenspeicherplatz** für verschiedene Speicherknoten berechnet, basierend auf dem Arbeitsspeicher des Knotens und dem tatsächlich reservierten Speicherplatz für Metadaten.

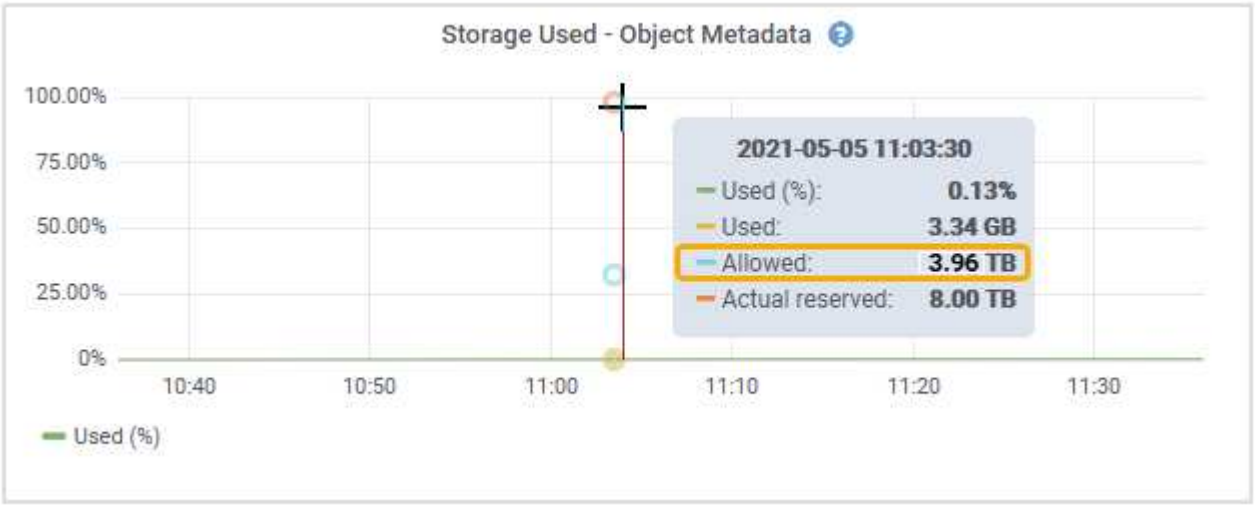
		Speichermenge auf dem Storage Node	
	< 128 GB	>= 128 GB	**Tatsächlich reservierter Speicherplatz für Metadaten**
⇐ 4 TB	60 % des tatsächlich reservierten Speicherplatzes für Metadaten, bis zu maximal 1,32 TB	60 % des tatsächlich reservierten Speicherplatzes für Metadaten, bis zu maximal 1,98 TB	4 TB

Zulässigen Metadatenbereich anzeigen

Führen Sie die folgenden Schritte aus, um den zulässigen Metadatenspeicherplatz für einen Storage Node anzuzeigen.

Schritte

1. Im Grid Manager wählen Sie **Knoten** aus.
2. ${post_edited_translations.segment}
3. Die Registerkarte **Speicher** auswählen.
4. Fahren Sie mit dem Cursor über das Diagramm „Storage used – Objektmetadaten“ und suchen Sie den Wert **Allowed**.



Im Screenshot beträgt der **Zulässige** Wert 3,96 TB, was der Maximalwert für einen Storage Node ist, dessen tatsächlich reservierter Speicherplatz für Metadaten mehr als 4 TB beträgt.

Der **Allowed**-Wert entspricht dieser Prometheus-Metrik:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Beispiel für zulässigen Metadatenbereich

Angenommen, Sie installieren ein StorageGRID System mit Version 11.6. Für dieses Beispiel wird angenommen, dass jeder Storage Node über mehr als 128 GB RAM verfügt und dass Volume 0 von Storage Node 1 (SN1) 6 TB groß ist. Basierend auf diesen Werten:

- Der systemweite **reservierte Speicherplatz** ist auf 8 TB festgelegt. (Dies ist der Standardwert für StorageGRID 11.6 oder höher, wenn jeder Storage Node über mehr als 128 GB RAM verfügt.)
- Der tatsächlich reservierte Speicherplatz für Metadaten für SN1 beträgt 6 TB. (Das gesamte Volume ist reserviert, da Volume 0 kleiner ist als die Einstellung **Reservierter Speicherplatz für Metadaten**.)
- Der zulässige Speicherplatz für Metadaten auf SN1 beträgt 3 TB, basierend auf der in der Tabelle für den zulässigen Speicherplatz für Metadaten dargestellten Berechnung: (Tatsächlich reservierter Speicherplatz für Metadaten − 1 TB) × 60 %, bis zu einem Maximum von 3,96 TB.

Wie sich Storage Nodes unterschiedlicher Größe auf die Objektkapazität auswirken

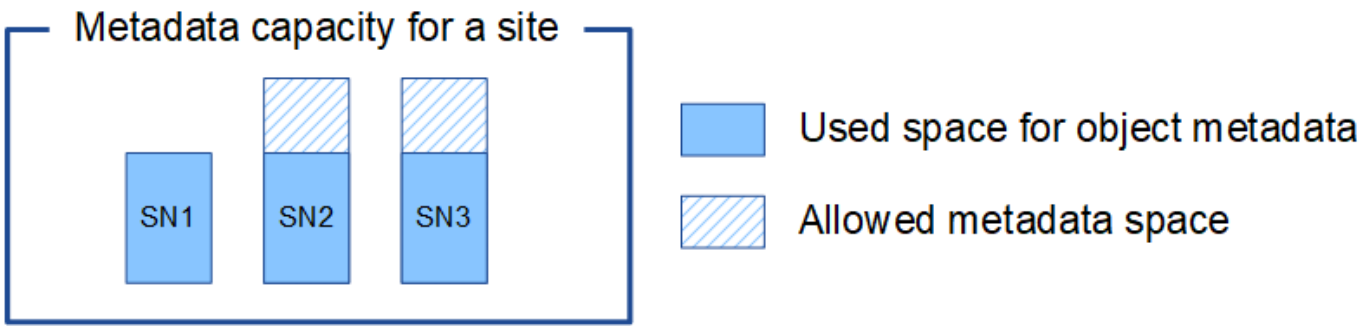
Wie oben beschrieben, verteilt StorageGRID die Objektmetadaten gleichmäßig auf die Speicherknoten an jedem Standort. Aus diesem Grund bestimmt bei einem Standort mit Speicherknoten unterschiedlicher Größe der kleinste Knoten die Metadatenkapazität des Standorts.

Das folgende Beispiel ist zu berücksichtigen:

- Sie verfügen über ein Single-Site-Grid mit drei Storage Nodes unterschiedlicher Größe.
- Die Einstellung **Metadata reserved space** beträgt 4 TB.
- ${post_edited_translations.segment}

Speicherknoten	Größe von Volume 0	Tatsächlich reservierter Metadaten-Speicherplatz	Zulässiger Metadatenspeicherplatz
SN1	2,2 TB	2,2 TB	1,32 TB
SN2	5 TB	4 TB	1,98 TB
SN3	6 TB	4 TB	1,98 TB

Da die Objektmetadaten gleichmäßig auf die Storage Nodes eines Standorts verteilt sind, kann jeder Node in diesem Beispiel nur 1,32 TB Metadaten speichern. Der zusätzliche, für SN2 und SN3 zulässige Metadatenspeicherplatz von 0,66 TB kann nicht genutzt werden.



Ebenso wird, da StorageGRID an jedem Standort alle Objektmetadaten für ein StorageGRID-System verwaltet, die Gesamtmetadatenkapazität eines StorageGRID-Systems durch die Objektmetadatenkapazität des kleinsten Standorts bestimmt.

Und da die Metadatenkapazität eines Objekts die maximale Objektanzahl steuert, ist das Grid effektiv voll, wenn einem Knoten die Metadatenkapazität ausgeht.

Verwandte Informationen

- Informationen zur Überwachung der Objektmetadatenkapazität für jeden Storage Node finden sich in der Anleitung für "Überwachung von StorageGRID".
- Um die Metadatenkapazität Ihres Systems zu erhöhen, "ein Grid erweitern" durch das Hinzufügen neuer Storage Nodes.

Erhöhen Sie die Einstellung „Metadata Reserved Space“ in StorageGRID

Möglicherweise kann die Systemeinstellung „Metadata Reserved Space“ erhöht werden, wenn die Storage Nodes bestimmte Anforderungen an RAM und verfügbaren Speicherplatz erfüllen.

Was Sie benötigen

- Sie sind beim Grid Manager mit einem "unterstützte Webbrowser" angemeldet.
- Sie haben die "Root-Zugriffsberechtigung oder die Berechtigung für andere Grid-Konfigurationen".

Über diese Aufgabe

${post_edited_translations.segment}

Sie können den Wert der systemweiten Einstellung „Reservierter Metadatenspeicher“ nur dann erhöhen, wenn beide folgenden Aussagen zutreffen:

- Die Storage Nodes an jedem Standort Ihres Systems verfügen jeweils über mindestens 128 GB RAM.
- Die Storage Nodes an jedem Standort in Ihrem System verfügen jeweils über ausreichend verfügbaren Speicherplatz auf Storage Volume 0.

Beachten Sie, dass eine Erhöhung dieser Einstellung gleichzeitig den für die Objektspeicherung auf Speichervolumen 0 aller Storage Nodes verfügbaren Speicherplatz verringert. Aus diesem Grund kann es sinnvoll sein, den Metadata Reserved Space basierend auf Ihren erwarteten Anforderungen an Objektmetadaten auf einen Wert unter 8 TB festzulegen.

> Im Allgemeinen ist es besser, einen höheren Wert anstelle eines niedrigeren Werts zu verwenden. Wenn die Einstellung „Metadata Reserved Space“ zu groß ist, können Sie diese später verringern. Wenn Sie den Wert hingegen später erhöhen, muss das System unter Umständen Objektdaten verschieben, um Speicherplatz freizugeben.

Eine detaillierte Erklärung dazu, wie sich die Einstellung „Reservierter Metadatenspeicherplatz“ auf den für die Speicherung von Objektmetadaten auf einem bestimmten Storage Node zulässigen Speicherplatz auswirkt, siehe "Objekt-Metadaten-Speicher verwalten".

Schritte

1. Die aktuelle Einstellung für den reservierten Metadatenbereich feststellen.
   a. ${post_edited_translations.segment}
   b. Der Wert von **Reservierter Metadatenbereich** ist zu beachten.
2. Stellen Sie sicher, dass auf Speichervolume 0 jedes Storage Node genügend verfügbarer Speicherplatz vorhanden ist, um diesen Wert zu erhöhen.
   a. Wählen Sie **Knoten**.
   b. Wählen Sie den ersten Storage Node im Grid aus.
   c. Die Registerkarte „Storage“ auswählen.
   d. Im Abschnitt Volumes befindet sich der Eintrag **/var/local/rangedb/0**.
   e. Bestätigen Sie, dass der verfügbare Wert gleich oder größer ist als die Differenz zwischen dem neuen Wert, den Sie verwenden möchten, und dem aktuellen Wert des reservierten Metadatenspeichers.

      ${post_edited_translations.segment}

   f. Wiederholen Sie diese Schritte für alle Storage Nodes.
      - Wenn auf einem oder mehreren Storage Nodes nicht genügend Speicherplatz verfügbar ist, kann der Wert für den Metadata Reserved Space nicht erhöht werden. Mit diesem Verfahren sollte nicht fortgefahren werden.
      - Wenn auf jedem Storage Node genügend Speicherplatz auf Volume 0 verfügbar ist, kann mit dem

nächsten Schritt fortgefahren werden.

3. Auf jedem Storage Node sollten mindestens 128 GB RAM vorhanden sein.
   a. Wählen Sie **Knoten**.
   b. Wählen Sie den ersten Storage Node im Grid aus.
   c. Die Registerkarte **Hardware** auswählen.
   d. Bewegen Sie den Mauszeiger über das Diagramm zur Speichernutzung. Sichergestellt ist, dass der **Gesamtspeicher** mindestens 128 GB beträgt.
   e. Wiederholen Sie diese Schritte für alle Storage Nodes.
      - Wenn auf einem oder mehreren Storage Nodes nicht genügend Gesamtspeicher verfügbar ist, kann der Wert für den reservierten Metadatenspeicherplatz nicht erhöht werden. Mit diesem Verfahren sollte nicht fortgefahren werden.
      - Wenn jeder Storage Node über mindestens 128 GB Gesamtspeicher verfügt, gehen Sie zum nächsten Schritt.
4. Die Einstellung „Reservierter Metadatenbereich“ wird aktualisiert.
   a. ${post_edited_translations.segment}
   b. **Reservierter Metadatenbereich** auswählen.
   c. Geben Sie den neuen Wert ein.

      Beispielsweise entspricht die Eingabe von 8 TB, dem maximal unterstützten Wert, der Eingabe von **8000000000000** (8, gefolgt von 12 Nullen)

   d. **Speichern** auswählen.

Komprimieren Sie gespeicherte Objekte in StorageGRID

Sie können die Objektkomprimierung aktivieren, um die Größe der in StorageGRID gespeicherten Objekte zu reduzieren, sodass die Objekte weniger Speicherplatz belegen.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Du hast "spezifische Zugriffsberechtigungen".

Über diese Aufgabe

Standardmäßig ist die Objektkomprimierung deaktiviert. Wenn Sie die Komprimierung aktivieren, versucht StorageGRID, jedes Objekt beim Speichern mithilfe einer verlustfreien Komprimierung zu komprimieren.

> Wenn diese Einstellung geändert wird, dauert es etwa eine Minute, bis die neue Einstellung wirksam wird. Der konfigurierte Wert wird aus Performance- und Skalierungsgründen zwischengespeichert.

${post_edited_translations.segment}

- Die Option **Gespeicherte Objekte komprimieren** sollte nur ausgewählt werden, wenn bekannt ist, dass die gespeicherten Daten komprimierbar sind.
- Anwendungen, die Objekte in StorageGRID speichern, komprimieren Objekte möglicherweise vor dem Speichern. Wenn eine Client-Anwendung ein Objekt bereits vor dem Speichern in StorageGRID komprimiert hat, wird die Auswahl dieser Option die Größe des Objekts nicht weiter reduzieren.

- Die Option **Gespeicherte Objekte komprimieren** sollte nicht ausgewählt werden, wenn Sie NetApp FabricPool mit StorageGRID verwenden.
- Wenn die Option „Gespeicherte Objekte komprimieren“ ausgewählt ist, sollten S3-Clientanwendungen GetObject-Operationen vermeiden, die einen Bytebereich zur Rückgabe angeben. Diese „Bereichsleseoperationen“ sind ineffizient, da StorageGRID die Objekte effektiv dekomprimieren muss, um auf die angeforderten Bytes zuzugreifen. GetObject-Operationen, die einen kleinen Bytebereich aus einem sehr großen Objekt anfordern, sind besonders ineffizient; beispielsweise ist es ineffizient, einen 10 MB großen Bereich aus einem 50 GB großen komprimierten Objekt zu lesen.

  Wenn Bereiche aus komprimierten Objekten gelesen werden, kann die Clientanfrage eine Zeitüberschreitung aufweisen.

> ⓘ Wenn Objekte komprimiert werden müssen und die Clientanwendung Bereichslesevorgänge verwenden muss, sollte das Zeitüberschreitung für die Anwendung erhöht werden.

Schritte

1. **Konfiguration** > **System** > **Speichereinstellungen** > **Objektkomprimierung** auswählen.
2. Das Kontrollkästchen **Gespeicherte Objekte komprimieren** auswählen.
3. **Speichern** auswählen.

Verwalten Sie vollständige Storage Nodes in StorageGRID

Sobald die Speicherkapazität der Storage Nodes erreicht ist, muss das StorageGRID System durch das Hinzufügen von neuem Speicher erweitert werden. Es stehen drei Optionen zur Verfügung: Hinzufügen von Speichervolumes, Hinzufügen von Speichererweiterungsregalen und Hinzufügen von Storage Nodes.

Speichervolumen hinzufügen

Jeder Storage Node unterstützt eine maximale Anzahl an Speichervolumes. Die definierte maximale Anzahl variiert je nach Plattform. Wenn ein Storage Node weniger als die maximale Anzahl an Speichervolumes enthält, können Volumes hinzugefügt werden, um die Kapazität zu erhöhen. Siehe die Anweisungen für "${post_edited_translations.segment}".

${post_edited_translations.segment}

Einige StorageGRID Appliance-Speicherknoten, wie der SG6060 oder SG6160, können zusätzliche Speicher-Shelves unterstützen. Wenn Sie über StorageGRID Appliances mit Erweiterungsfunktionen verfügen, die noch nicht auf die maximale Kapazität erweitert wurden, können Sie Speicher-Shelves hinzufügen, um die Kapazität zu erhöhen. Siehe die Anweisungen für "${post_edited_translations.segment}".

${post_edited_translations.segment}

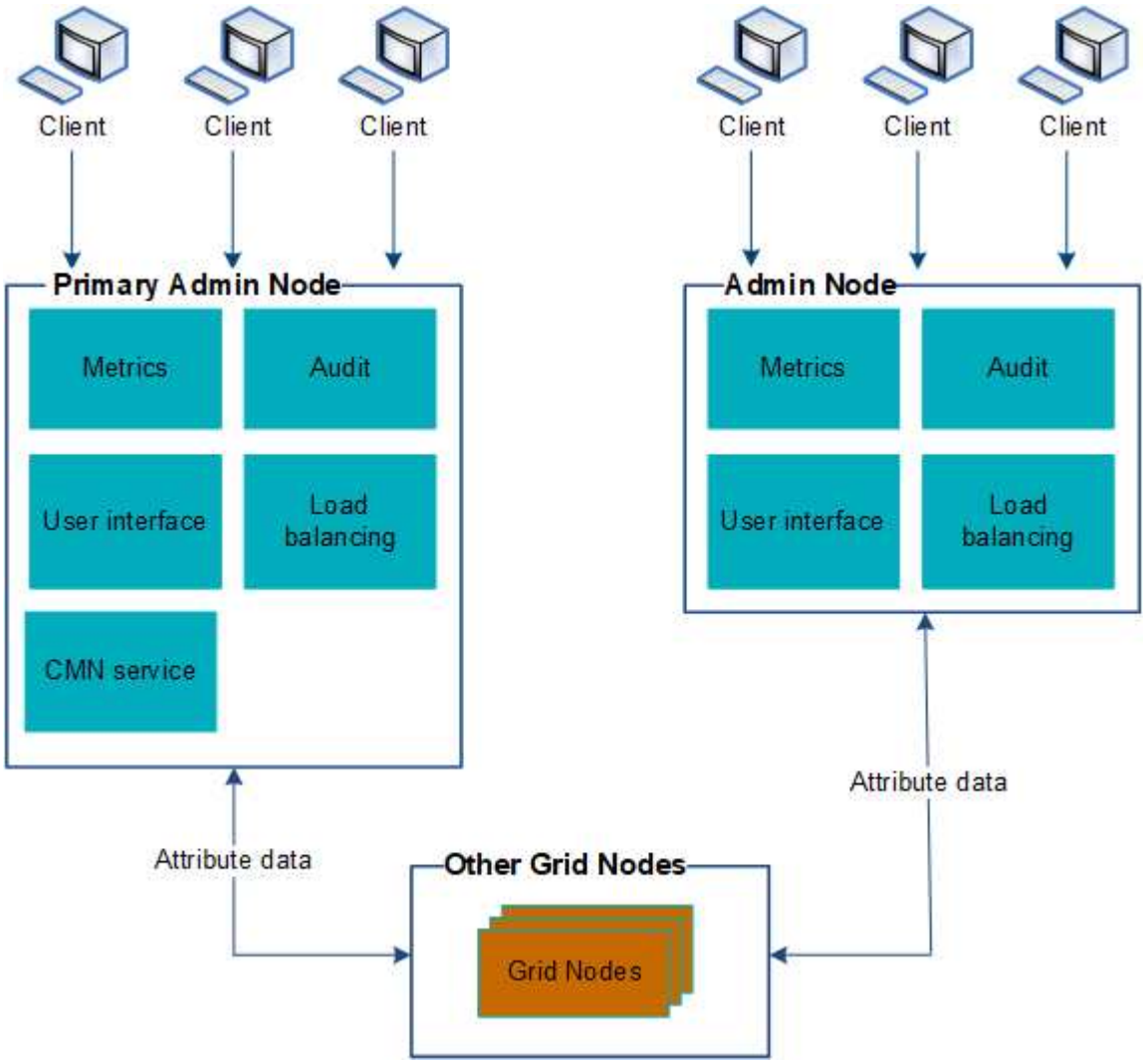
Sie können die Speicherkapazität durch Hinzufügen von Storage Nodes erhöhen. Beim Hinzufügen von Speicher sind die aktuell aktiven ILM-Regeln und Kapazitätsanforderungen sorgfältig zu berücksichtigen. Siehe die Anweisungen für "${post_edited_translations.segment}".

Administratorknoten verwalten

Verwenden Sie mehrere Admin-Knoten in StorageGRID

Ein StorageGRID System kann mehrere Admin-Knoten umfassen, sodass eine kontinuierliche Überwachung und Konfiguration des StorageGRID Systems auch dann möglich ist, wenn ein Admin-Knoten ausfällt.

Wenn ein Admin-Knoten ausfällt, wird die Attributverarbeitung fortgesetzt, Warnmeldungen werden weiterhin ausgelöst und E-Mail-Benachrichtigungen sowie AutoSupport-Pakete werden weiterhin versendet. Mehrere Admin-Knoten bieten jedoch keinen Ausfallschutz, außer für Benachrichtigungen und AutoSupport-Pakete.



Es gibt zwei Optionen, um das StorageGRID System weiterhin anzuzeigen und zu konfigurieren, falls ein Admin-Knoten ausfällt:

- Webclients können sich mit jedem anderen verfügbaren Admin Node wieder verbinden.
- Wenn ein Systemadministrator eine Hochverfügbarkeitsgruppe von Admin-Knoten konfiguriert hat, können Webclients weiterhin über die virtuelle IP-Adresse der HA-Gruppe auf den Grid Manager oder den Tenant Manager zugreifen. Siehe "Hochverfügbarkeitsgruppen verwalten".

Bei Verwendung einer HA-Gruppe wird der Zugriff unterbrochen, wenn der aktive Admin-Knoten ausfällt. Benutzer müssen sich erneut anmelden, nachdem die virtuelle IP-Adresse der HA-Gruppe auf einen anderen Admin-Knoten innerhalb der Gruppe umgeschaltet ist.

Einige Wartungsaufgaben können nur mit dem primären Admin Node durchgeführt werden. Fällt der primäre Admin Node aus, muss er wiederhergestellt werden, bevor das StorageGRID System wieder voll funktionsfähig ist.

Identifizieren Sie den primären Admin-Node in StorageGRID

Der primäre Admin-Node bietet mehr Funktionalität als nicht-primäre Admin-Nodes. Beispielsweise müssen einige Wartungsverfahren über den primären Admin-Node durchgeführt werden.

Weitere Informationen zu Admin Nodes finden sich unter "${post_edited_translations.segment}".

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Du hast "spezifische Zugriffsberechtigungen".

Schritte

1. Wählen Sie **Knoten**.
2. **primary** in das Suchfeld eingeben.

   In den Suchergebnissen den Knoten identifizieren, bei dem in der Spalte „Typ“ „Primary Admin Node“ angezeigt wird. Es sollte ein Primary Admin Node aufgeführt sein.