Konfiguration und Management

StorageGRID

NetApp
November 05, 2025

This PDF was generated from https://docs.netapp.com/de-de/storagegrid-117/admin/index.html on November 05, 2025. Always check docs.netapp.com for the latest.

Inhalt

Konfiguration und Management . . . 1
StorageGRID verwalten . . . 1
Administration StorageGRID: Überblick . . . 1
Erste Schritte mit Grid Manager . . . 1
Kontrolle des Zugriffs auf StorageGRID . . . 31
Grid-Verbund verwenden . . . 79
Sicherheitsmanagement . . . 117
Verwalten von Mandanten . . . 194
Client-Verbindungen konfigurieren . . . 213
Netzwerke und Verbindungen verwalten . . . 256
Verwenden Sie AutoSupport . . . 273
Managen Sie Storage-Nodes . . . 288
Managen Sie Admin-Nodes . . . 312
Archiv-Nodes Managen . . . 323
Datenmigration zu StorageGRID . . . 346
Objektmanagement mit ILM . . . 348
Objekte mit ILM managen: Übersicht . . . 348
ILM und Objekt-Lebenszyklus . . . 349
Speicherklassen erstellen und zuweisen . . . 371
Nutzung von Speicherpools . . . 373
Verwendung Von Cloud Storage Pools . . . 382
Profile für das Erasure Coding managen . . . 403
Regionen konfigurieren (nur optional und S3) . . . 407
ILM-Regel erstellen . . . 409
ILM-Richtlinie erstellen . . . 426
Arbeiten mit ILM-Richtlinien und ILM-Regeln . . . 443
Verwenden Sie die S3-Objektsperre . . . 447
Beispiele für ILM-Regeln und -Richtlinien . . . 456
Systemhärtung . . . 475
Systemhärtung: Übersicht . . . 476
Hardening-Richtlinien für Software Upgrades . . . 476
Hardening Guidelines for StorageGRID Networks . . . 477
Hardening-Richtlinien für StorageGRID-Knoten . . . 478
Härtungsrichtlinien für TLS und SSH . . . 481
Andere Hinweise zur Verhärtung . . . 482
Konfigurieren Sie StorageGRID für FabricPool . . . 483
Configure StorageGRID for FabricPool: Übersicht . . . 484
Erforderliche Informationen zum Hinzufügen von StorageGRID als Cloud-Tier . . . 485
Verwenden Sie den FabricPool-Einrichtungsassistenten . . . 487
Konfigurieren Sie StorageGRID manuell . . . 502
Konfigurieren Sie ONTAP System Manager . . . 513
Konfigurieren Sie den DNS-Server . . . 515
StorageGRID Best Practices für FabricPool . . . 515

FabricPool-Daten aus StorageGRID entfernen 520

Konfiguration und Management

StorageGRID verwalten

Administration StorageGRID: Überblick

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

Informationen zu diesen Anweisungen

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

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

Bevor Sie beginnen

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

Erste Schritte mit Grid Manager

Anforderungen an einen Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	Unterstützte Mindestversion
Google Chrome	107
Microsoft Edge	107
Mozilla Firefox	106

Sie sollten das Browserfenster auf eine empfohlene Breite einstellen.

Browserbreite	Pixel
Minimum	1024
Optimal	1280

Melden Sie sich beim Grid Manager an

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

Überblick

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

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

Stellen Sie eine Verbindung mit der HA-Gruppe her

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

Verwenden Sie SSO

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

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

Bevor Sie beginnen

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

  `https://FQDN_or_Admin_Node_IP/`

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

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

  `https://FQDN_or_Admin_Node_IP:port/`

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

Schritte

1. Starten Sie einen unterstützten Webbrowser.
2. Geben Sie in der Adressleiste des Browsers die URL für den Grid Manager ein.
3. Wenn Sie aufgefordert werden, eine Sicherheitswarnung zu erhalten, installieren Sie das Zertifikat mithilfe des Browser-Installationsassistenten. Siehe "Verwalten von Sicherheitszertifikaten".
4. Melden Sie sich beim Grid Manager an.

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

SSO wird nicht verwendet

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

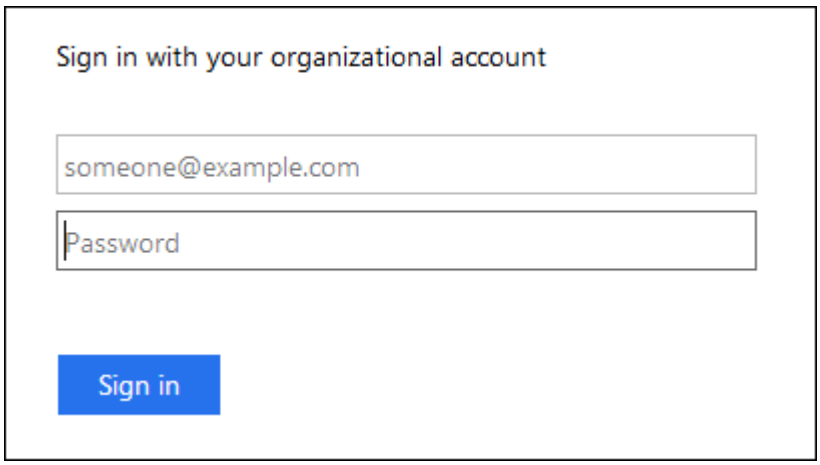
b. Wählen Sie **Anmelden**.

SSO wird verwendet

- Wenn StorageGRID SSO verwendet und Sie zum ersten Mal auf die URL in diesem Browser zugreifen:

  i. Wählen Sie **Anmelden**. Sie können die 0 im Feld „Konto“ belassen.

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



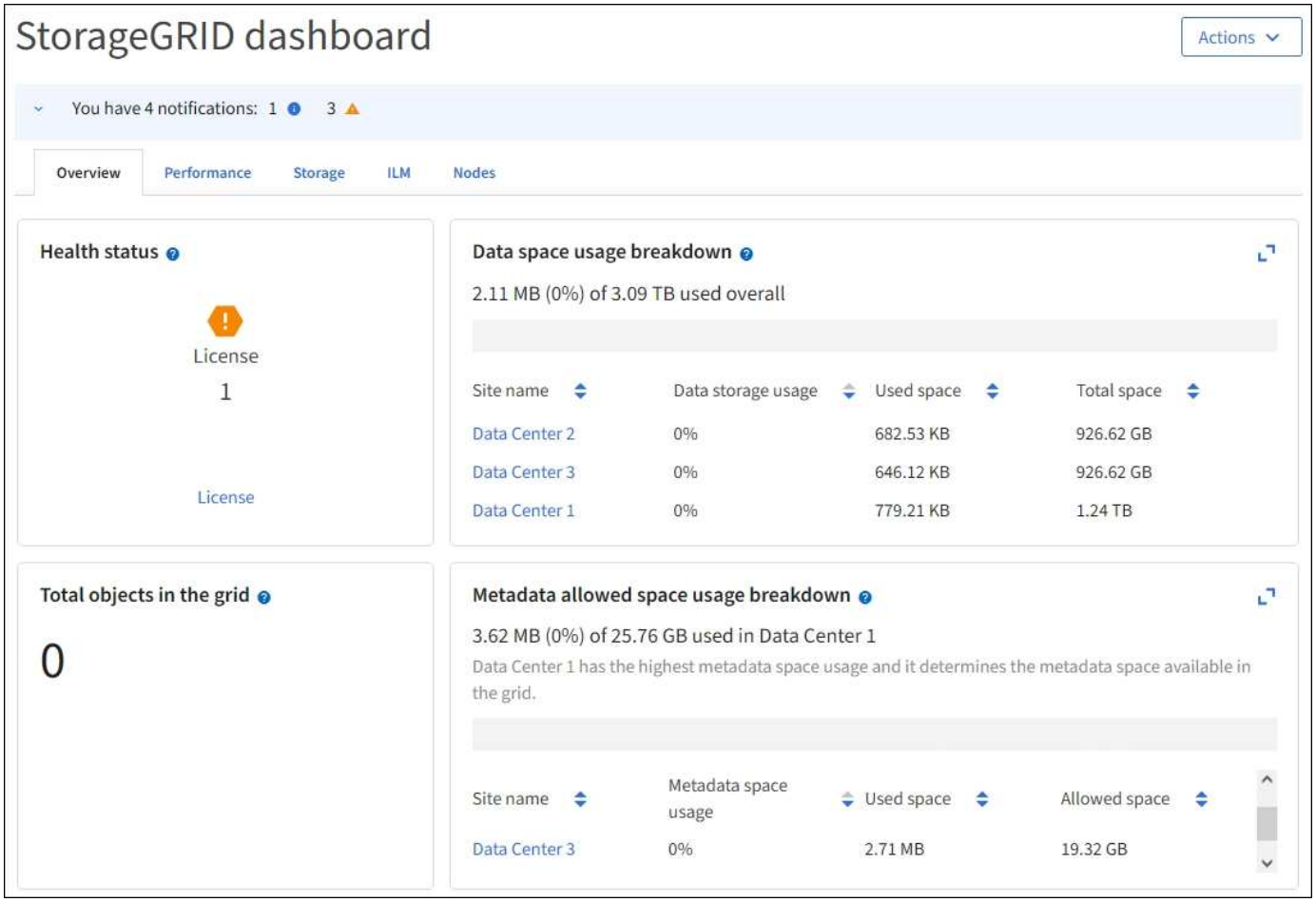
- Wenn StorageGRID SSO verwendet und Sie zuvor auf den Grid-Manager oder ein Mandantenkonto zugegriffen haben:

i. Geben Sie **0** (die Konto-ID für den Grid-Manager) ein oder wählen Sie **Grid-Manager** aus, wenn er in der Liste der letzten Konten angezeigt wird.

ii. Wählen Sie **Anmelden**.

iii. Melden Sie sich mit Ihren Standard-SSO-Anmeldedaten auf der SSO-Anmeldeseite Ihres Unternehmens an.

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



Melden Sie sich bei einem anderen Admin-Node an

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

SSO wird nicht verwendet

Schritte

1. Geben Sie in der Adressleiste des Browsers den vollständig qualifizierten Domänennamen oder die IP-Adresse des anderen Admin-Knotens ein. Geben Sie die Portnummer nach Bedarf an.
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort für den Grid Manager ein.
3. Wählen Sie **Anmelden**.

SSO wird verwendet

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

Schritte

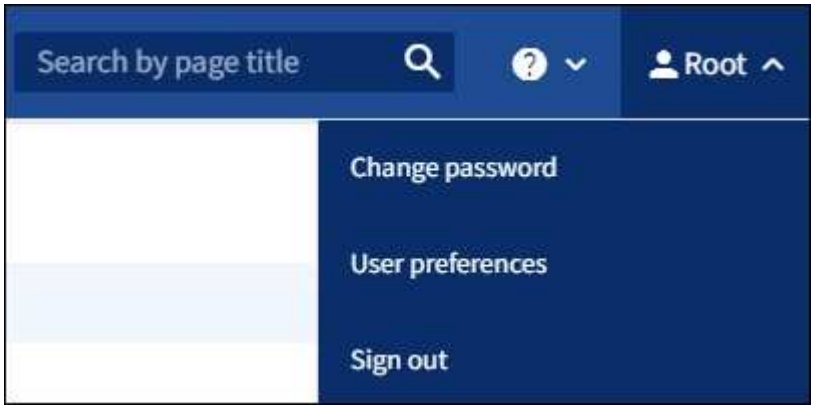
1. Geben Sie den vollständig qualifizierten Domänennamen oder die IP-Adresse des anderen Admin-Knotens in die Adressleiste des Browsers ein.
2. Wenn Ihre SSO-Sitzung abgelaufen ist, geben Sie Ihre Anmeldedaten erneut ein.

Melden Sie sich vom Grid Manager ab

Wenn Sie die Arbeit mit dem Grid-Manager abgeschlossen haben, müssen Sie sich abmelden, um sicherzustellen, dass nicht autorisierte Benutzer keinen Zugriff auf das StorageGRID-System haben. Wenn Sie Ihren Browser schließen, werden Sie möglicherweise aufgrund der Cookie-Einstellungen des Browsers nicht aus dem System abgesendet.

Schritte

1. Wählen Sie oben rechts Ihren Benutzernamen aus.



2. Wählen Sie **Abmelden**.

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

Passwort ändern

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

Schritte

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

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

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

Zeigen Sie StorageGRID Lizenzinformationen an

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

Schritte

1. Rufen Sie die Lizenzseite auf, indem Sie einen der folgenden Schritte ausführen:
   - Wählen Sie auf der Statuskarte für den Systemzustand im Dashboard das Symbol Lizenzstatus oder den Link **Lizenz** aus. Dieser Link wird nur angezeigt, wenn ein Problem mit der Lizenz vorliegt.
   - Wählen Sie **WARTUNG** > **System** > **Lizenz**.
2. Anzeigen der schreibgeschützten Details für die aktuelle Lizenz:
   - StorageGRID System-ID. Hierbei handelt es sich um die eindeutige Identifikationsnummer für diese StorageGRID Installation
   - Seriennummer der Lizenz
   - Lizenztyp, entweder **Perpetual** oder **Subscription**
   - Lizenzierte Storage-Kapazität des Grid
   - Unterstützte Storage-Kapazität
   - Enddatum der Lizenz. **N/A** erscheint für eine unbefristete Lizenz.
   - Enddatum des Support-Servicevertrags

     Dieses Datum wird aus der aktuellen Lizenzdatei gelesen und ist möglicherweise veraltet, wenn Sie den Supportvertrag nach Erhalt der Lizenzdatei verlängert oder verlängert haben. Informationen zum Aktualisieren dieses Werts finden Sie unter "Aktualisieren Sie die StorageGRID-Lizenzinformationen". Sie können auch das tatsächliche Vertragsenddatum mit dem digitalen Berater von Active IQ (auch als digitaler Berater bezeichnet) anzeigen.

   - Inhalt der Lizenztext-Datei

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

Aktualisieren Sie die StorageGRID-Lizenzinformationen

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

Bevor Sie beginnen

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

Schritte

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

   Die neue Lizenzdatei wird validiert und angezeigt.

4. Wählen Sie **Speichern**.

Verwenden Sie die API

Verwenden Sie die Grid-Management-API

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

Allgemeine Ressourcen

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

- `/grid`: Der Zugriff ist auf Grid Manager-Benutzer beschränkt und basiert auf den konfigurierten Gruppenberechtigungen.
- `/org`: Der Zugriff ist auf Benutzer beschränkt, die zu einer lokalen oder föderierten LDAP-Gruppe für ein Mandantenkonto gehören. Weitere Informationen finden Sie unter "Verwenden Sie ein Mandantenkonto".
- `/private`: Der Zugriff ist auf Grid Manager-Benutzer beschränkt und basiert auf den konfigurierten Gruppenberechtigungen. Die privaten APIs können ohne Vorankündigung geändert werden. Private StorageGRID-Endpunkte ignorieren auch die API-Version der Anforderung.

API-Anforderungen ausgeben

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

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

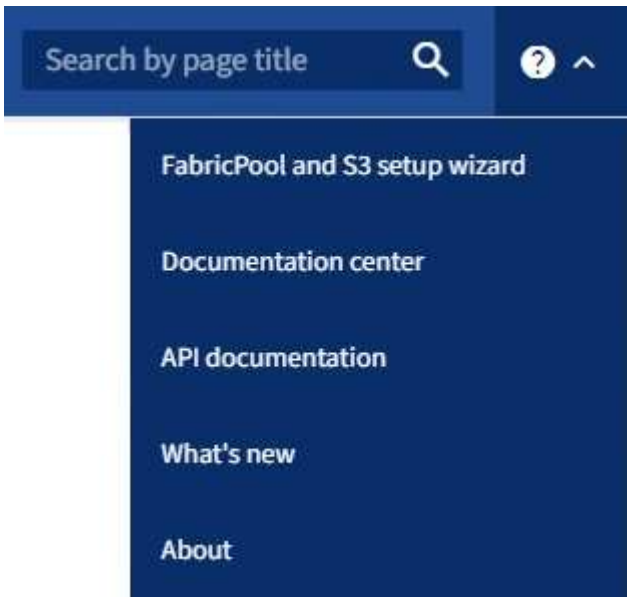
Bevor Sie beginnen

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

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

Schritte

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



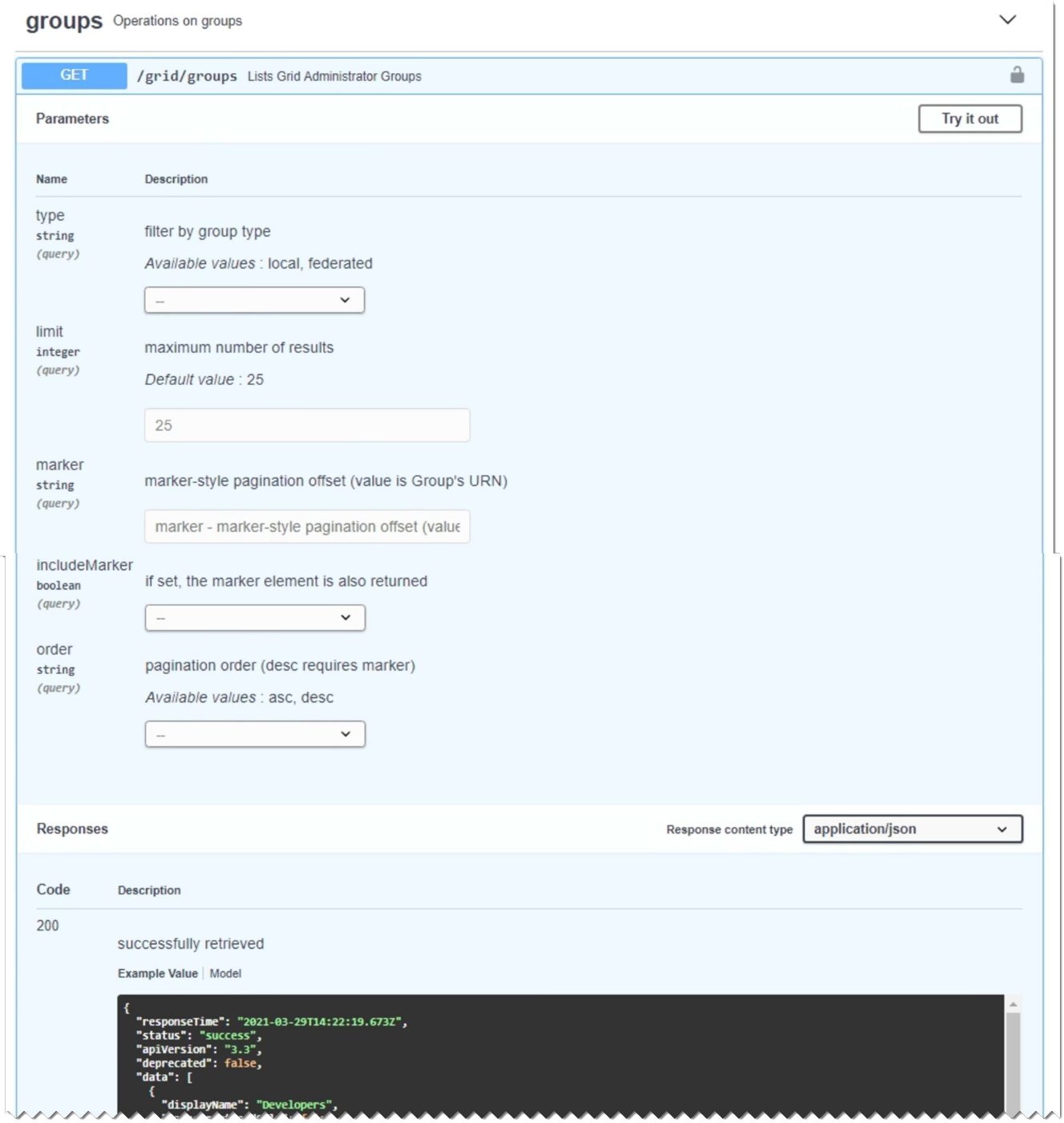
2. Um eine Operation mit der privaten API durchzuführen, wählen Sie auf der StorageGRID Management API-Seite **Gehe zur privaten API-Dokumentation** aus.

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

3. Wählen Sie den gewünschten Vorgang aus.

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

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



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

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

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

- **Accounts**: Operationen zur Verwaltung von Storage-Mandanten-Konten, einschließlich der Erstellung neuer Konten und dem Abruf der Speichernutzung für ein bestimmtes Konto.
- **Alarme**: Operationen zur Auflistung der aktuellen Alarme (Altsystem) und zur Rückgabe von Informationen über den Zustand des Rasters, einschließlich der aktuellen Warnungen und einer Zusammenfassung der Knotenverbindungszustände.
- **Alert-history**: Operationen bei aufgelösten Warnmeldungen.
- **Alert-Receivers**: Operationen auf Alert-Notification-Receivern (E-Mail).
- **Alert-rules**: Operationen auf Warnungsregeln.
- **Alert-Silences**: Operationen bei Alarmstummzuständen.
- **Alerts**: Operationen bei Alerts.
- **Audit**: Operationen zum Auflisten und Aktualisieren der Überwachungskonfiguration.
- **Auth**: Operationen zur Authentifizierung der Benutzersitzung.

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

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

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

- **Client-Certificates**: Operationen zur Konfiguration von Client-Zertifikaten, damit StorageGRID sicher über externe Überwachungstools aufgerufen werden kann.
- **Config**: Operationen im Zusammenhang mit der Produktfreigabe und den Versionen der Grid Management API. Sie können die Produktversion und die Hauptversionen der von dieser Version unterstützten Grid Management API auflisten und veraltete Versionen der API deaktivieren.
- **Deactivated-Features**: Operationen zum Anzeigen von Features, die möglicherweise deaktiviert wurden.
- **dns-Server**: Operationen zum Auflisten und Ändern von konfigurierten externen DNS-Servern.
- **Endpunktdomänennamen**: Operationen zum Auflisten und Ändern von S3-Endpunktdomänennamen.
- **Erasure-Coding**: Operationen auf Erasure Coding-Profilen.
- **Erweiterung**: Expansionsbetrieb (Verfahrensebene).
- **Expansion-Nodes**: Erweiterungsvorgänge (Node-Ebene).

- **Erweiterungsstandorte**: Expansionsbetrieb (Standort-Ebene).
- **Grid-Networks**: Operationen zum Auflisten und Ändern der Grid Network List.
- **Grid-passwords**: Operationen zur Grid-Passwortverwaltung.
- **Groups**: Operationen zur Verwaltung lokaler Grid-Administratorgruppen und zum Abrufen föderierter Grid-Administratorgruppen von einem externen LDAP-Server.
- **Identity-source**: Operationen zum Konfigurieren einer externen Identitätsquelle und zum manuellen Synchronisieren von föderierten Gruppen- und Benutzerinformationen.
- **ilm**: Operationen zum Information Lifecycle Management (ILM).
- **Lizenz**: Operationen zum Abrufen und Aktualisieren der StorageGRID-Lizenz.
- **Logs**: Operationen zum Sammeln und Herunterladen von Protokolldateien.
- **Metrics**: Operationen auf StorageGRID-Metriken einschließlich sofortiger metrischer Abfragen an einem einzelnen Zeitpunkt und Range metrischer Abfragen über einen bestimmten Zeitraum. Die Grid Management API verwendet das Prometheus Systems Monitoring Tool als Backend-Datenquelle. Informationen zum Erstellen von Prometheus-Abfragen finden Sie auf der Prometheus-Website.

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

- **Node-Details**: Operationen für Node-Details.
- **Node-Health**: Operationen auf dem Node-Status.
- **Node-Storage-State**: Vorgänge im Speicherstatus der Knoten.
- **ntp-Server**: Operationen zum Auflisten oder Aktualisieren externer NTP-Server (Network Time Protocol).
- **Objekte**: Operationen an Objekten und Objektmetadaten.
- **Erholung**: Operationen für die Wiederherstellung.
- **Recovery-Paket**: Operationen zum Herunterladen des Wiederherstellungspakets.
- **Regionen**: Operationen zum Anzeigen und Erstellen von Regionen.
- **s3-Object-Lock**: Operationen auf globalen S3 Object Lock Einstellungen.
- **Server-Zertifikat**: Operationen zum Anzeigen und Aktualisieren von Grid Manager-Serverzertifikaten.
- **snmp**: Operationen auf der aktuellen SNMP-Konfiguration.
- **Traffic-Klassen**: Operationen für Verkehrsklassifizierungsrichtlinien.
- **Nicht vertrauenswürdig-Client-Network**: Operationen auf der nicht vertrauenswürdigen Client-Netzwerk-Konfiguration.
- **Benutzer**: Operationen zum Anzeigen und Verwalten von Grid Manager-Benutzern.

Die Grid Management API-Versionierung

Die Grid Management API verwendet Versionierung zur Unterstützung unterbrechungsfreier Upgrades.

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

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

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

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

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

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

Veraltete Anfragen werden wie folgt als veraltet markiert:

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

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

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

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

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

Geben Sie eine API-Version für eine Anforderung an

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

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

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

Schutz vor standortübergreifenden Anfrageschmieden (CSRF)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

- Der `storagegrid-ssoauth.py` Python-Skript, das sich im Verzeichnis der Installationsdateien von StorageGRID befindet (`./rpms` Für Red hat Enterprise Linux oder CentOS, `./debs` Für Ubuntu oder Debian, und `./vsphere` Für VMware).
- Ein Beispielworkflow von Curl-Anforderungen.

  Der Curl-Workflow kann sich aushalten, wenn Sie ihn zu langsam ausführen. Möglicherweise wird der Fehler angezeigt: `A valid SubjectConfirmation was not found on this Response`.

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

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

Schritte

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

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

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

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

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

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

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

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

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

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

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

Dieses Beispiel zeigt eine POST-Anforderung für eine signierte Authentifizierungs-URL für `TENANTACCOUNTID`. Die Ergebnisse werden an weitergeleitet `python -m json.tool` Um die JSON-Kodierung zu entfernen.

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

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

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

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

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

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

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

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

Die Antwort umfasst die Client-Anforderungs-ID:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   Die Antwort umfasst das Authentifizierungs-Token.

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

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

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

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

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

Wenn Single Sign-On (SSO) aktiviert ist, müssen Sie eine Reihe von API-Anforderungen zum Abzeichnen der Grid Management API oder der Mandantenmanagement-API ausstellen. Diese Anweisungen gelten, wenn Sie Active Directory als SSO-Identitäts-Provider verwenden

Über diese Aufgabe

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

Schritte

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

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

Es wird eine Abmeldung-URL zurückgegeben:

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

2. Speichern Sie die Abmeldung-URL.

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

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

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

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

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

4. Löschen Sie das StorageGRID-Überträger-Token.

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

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

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

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

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

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

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

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

Bevor Sie beginnen

- Sie kennen die SSO E-Mail-Adresse und das Passwort für einen föderierten Benutzer, der zu einer StorageGRID Benutzergruppe gehört.
- Wenn Sie auf die Mandanten-Management-API zugreifen möchten, kennen Sie die Mandanten-Account-ID.

Über diese Aufgabe

Um ein Authentifizierungs-Token zu erhalten, können Sie die folgenden Beispielskripte verwenden:

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

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

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

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

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

Schritte

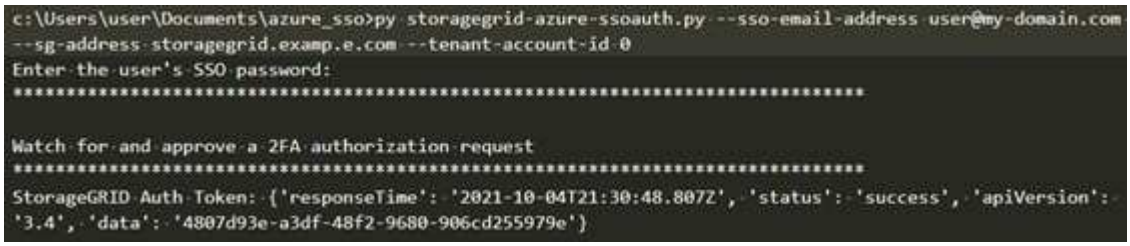
1. Installieren Sie die erforderlichen Abhängigkeiten:
   a. Installieren Sie Node.js (siehe) "https://nodejs.org/en/download/").
   b. Installieren Sie die erforderlichen Node.js-Module (Puppenspieler und jsdom):

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

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

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

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



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

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

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

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

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

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

Bevor Sie beginnen

- Sie kennen den SSO-Benutzernamen und das Passwort für einen föderierten Benutzer, der einer StorageGRID-Benutzergruppe angehört.

- Wenn Sie auf die Mandanten-Management-API zugreifen möchten, kennen Sie die Mandanten-Account-ID.

Über diese Aufgabe

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

- Der `storagegrid-ssoauth.py` Python-Skript, das sich im Verzeichnis der Installationsdateien von StorageGRID befindet (`./rpms` Für Red hat Enterprise Linux oder CentOS, `./debs` Für Ubuntu oder Debian, und `./vsphere` Für VMware).
- Ein Beispielworkflow von Curl-Anforderungen.

  Der Curl-Workflow kann sich aushalten, wenn Sie ihn zu langsam ausführen. Möglicherweise wird der Fehler angezeigt: `A valid SubjectConfirmation was not found on this Response`.

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

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

Schritte

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

g. Den Wert „Aktion“ exportieren:

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

h. Senden von Cookies zusammen mit den Zugangsdaten:

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

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

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

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

   Für `RelayState`, Verwenden Sie die Mandanten-Konto-ID oder verwenden Sie 0, wenn Sie sich bei

der Grid Management-API anmelden möchten.

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

Die Antwort umfasst das Authentifizierungs-Token.

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

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

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

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

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

Wenn Single Sign-On (SSO) aktiviert ist, müssen Sie eine Reihe von API-Anforderungen zum Abzeichnen der Grid Management API oder der Mandantenmanagement-API ausstellen. Diese Anweisungen gelten, wenn Sie PingFederate als SSO-Identitäts-Provider verwenden

Über diese Aufgabe

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

Schritte

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

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

Es wird eine Abmeldung-URL zurückgegeben:

```
{
    "apiVersion": "3.0",
    "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2021-10-12T22:20:30.839Z",
    "status": "success"
}
```

2. Speichern Sie die Abmeldung-URL.

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

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

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

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

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. Löschen Sie das StorageGRID-Überträger-Token.

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

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

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

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

Deaktivieren Sie Funktionen mit der API

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

Über diese Aufgabe

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

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

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

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

Schritte

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

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

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

Deaktivieren Funktionen erneut aktivieren

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

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

Schritte

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

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

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

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

Kontrolle des Zugriffs auf StorageGRID

Control StorageGRID Access: Übersicht

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

Den Zugriff auf den Grid Manager steuern

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

Wird Verwendet "Identitätsföderation" Einrichtung "Gruppen" Und "Benutzer" Schneller, und Benutzer können sich mit vertrauten Anmeldeinformationen bei StorageGRID anmelden. Sie können die Identitätsföderation konfigurieren, wenn Sie Active Directory, OpenLDAP oder Oracle Directory Server verwenden.

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

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

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

Aktivieren Sie Single Sign On

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

Provisionierungs-Passphrase ändern

Die Provisionierungs-Passphrase ist für viele Installations- und Wartungsverfahren und für das Herunterladen des StorageGRID Recovery Package erforderlich. Die Passphrase ist auch erforderlich, um Backups der Grid-Topologieinformationen und Verschlüsselungen für das StorageGRID System herunterzuladen. Das können Sie "Ändern Sie die Passphrase" Nach Bedarf.

Ändern der Passwörter für die Node-Konsole

Jeder Node in Ihrem Grid verfügt über ein eindeutiges Node-Konsolenpasswort, das Sie als „admin“ über SSH beim Node oder beim Root-Benutzer über eine VM-/physische Konsolenverbindung einloggen müssen. Nach Bedarf können Sie "Ändern Sie das Passwort für die Node-Konsole" Für jeden Node.

Ändern Sie die Provisionierungs-Passphrase

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

Schritte

1. Wählen Sie **KONFIGURATION** > **Zugangskontrolle**> **Grid-Passwörter**.
2. Wählen Sie unter **Change Provisioning Passphrase** die Option **make a change** aus
3. Geben Sie Ihre aktuelle Provisionierungs-Passphrase ein.
4. Geben Sie die neue Passphrase ein. Die Passphrase muss mindestens 8 und maximal 32 Zeichen enthalten. Passphrases sind Groß-/Kleinschreibung.
5. Speichern Sie die neue Provisionierungs-Passphrase an einem sicheren Ort. Sie ist für Installations-, Erweiterungs- und Wartungsverfahren erforderlich.
6. Geben Sie die neue Passphrase erneut ein, und wählen Sie **Speichern**.

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

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

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

Ändern der Passwörter für die Node-Konsole

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

Bevor Sie beginnen

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

Über diese Aufgabe

Melden Sie sich mit dem Passwort der Node-Konsole bei einem Node als „admin“ über SSH oder beim Root-Benutzer über eine VM/physische Konsolenverbindung an. Mit dem Passwort für die Änderungsknotenkonsole werden für jeden Knoten in der Tabelle neue Passwörter erstellt und die Passwörter in einem aktualisierten System gespeichert `Passwords.txt` Datei im Wiederherstellungspaket. Die Passwörter sind in der Spalte Passwort in der Datei Passwords.txt aufgelistet.

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

Greifen Sie auf den Assistenten zu

Schritte

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

Geben Sie die Provisionierungs-Passphrase ein

Schritte

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

Laden Sie das aktuelle Wiederherstellungspaket herunter

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

Schritte

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

   Die Wiederherstellungspaket-Datei muss gesichert werden, da sie Verschlüsselungsschlüssel und Passwörter enthält, die verwendet werden können, um Daten vom StorageGRID-System zu erhalten.

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

   Sie können diesen Vorgang nach dem Start nicht abbrechen.

Ändern der Passwörter für die Node-Konsole

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

Schritte

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

   a. Öffnen Sie das `.zip` Datei:

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

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

      Überschreiben Sie das alte Wiederherstellungspaket nicht.

   Die Wiederherstellungspaket-Datei muss gesichert werden, da sie Verschlüsselungsschlüssel und Passwörter enthält, die verwendet werden können, um Daten vom StorageGRID-System zu erhalten.

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

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

   Wenn während des Aktualisierungsvorgangs ein Fehler auftritt, zeigt eine Bannermeldung die Anzahl der Knoten an, bei denen die Passwörter nicht geändert wurden. Das System wiederholt den Prozess

automatisch auf jedem Knoten, bei dem das Kennwort nicht geändert wurde. Wenn der Prozess endet, wenn einige Knoten noch kein geändertes Kennwort haben, wird die Schaltfläche **Wiederholen** angezeigt.

Wenn die Kennwortaktualisierung für einen oder mehrere Knoten fehlgeschlagen ist:

a. Überprüfen Sie die in der Tabelle aufgeführten Fehlermeldungen.
b. Beheben Sie die Probleme.
c. Wählen Sie **Wiederholen**.

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

6. Nachdem die Passwörter für die Node-Konsole für alle Nodes geändert wurden, löschen Sie die Erstes heruntergeladenes Wiederherstellungspaket.
7. Verwenden Sie optional den Link **Recovery Package**, um eine zusätzliche Kopie des neuen Wiederherstellungspakets herunterzuladen.

Verwenden Sie den Identitätsverbund

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

Konfigurieren Sie die Identitätsföderation für Grid Manager

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

Bevor Sie beginnen

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

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

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

Über diese Aufgabe

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

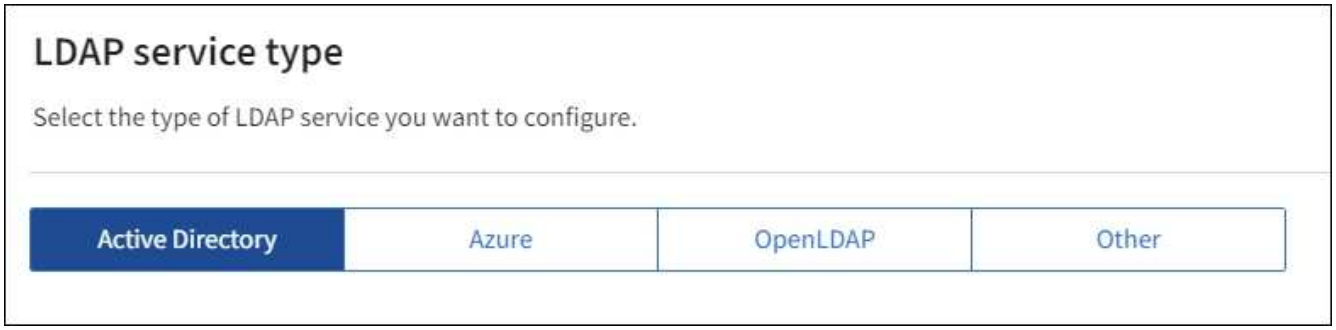
können die folgenden Gruppen importieren:

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

Geben Sie die Konfiguration ein

Schritte

1. Wählen Sie **KONFIGURATION** > **Zugriffskontrolle** > **Identitätsverbund** aus.
2. Wählen Sie **Identitätsföderation aktivieren**.
3. Wählen Sie im Abschnitt LDAP-Servicetyp den Typ des LDAP-Dienstes aus, den Sie konfigurieren möchten.



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

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

- **Hostname**: Der vollständig qualifizierte Domainname (FQDN) oder die IP-Adresse des LDAP-Servers.
- **Port**: Der Port, über den eine Verbindung zum LDAP-Server hergestellt wird.

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

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

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

  Der angegebene Benutzer muss über die Berechtigung zum Auflisten von Gruppen und Benutzern sowie zum Zugriff auf die folgenden Attribute verfügen:

  - `sAMAccountName` Oder `uid`
  - `objectGUID`, `entryUUID`, Oder `nsuniqueid`
  - `cn`
  - `memberOf` Oder `isMemberOf`
  - **Active Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, und `userPrincipalName`
  - **Azure**: `accountEnabled` Und `userPrincipalName`
- **Passwort**: Das mit dem Benutzernamen verknüpfte Passwort.
- **Group Base DN**: Der vollständige Pfad des Distinguished Name (DN) für einen LDAP-Unterbaum, nach dem Sie nach Gruppen suchen möchten. Im Active Directory-Beispiel (unten) können alle Gruppen, deren Distinguished Name relativ zum Basis-DN (DC=storagegrid,DC=example,DC=com) ist, als föderierte Gruppen verwendet werden.

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

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

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

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

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

  Geben Sie eines der folgenden Muster ein:

  - **UserPrincipalName pattern (Active Directory und Azure)**: `[USERNAME]@example.com`
  - **Namensmuster für Anmeldung auf der Ebene nach unten (Active Directory und Azure)**:

example\[USERNAME]

- * Distinguished Name pattern*: `CN=[USERNAME],CN=Users,DC=example,DC=com`

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

6. Wählen Sie im Abschnitt Transport Layer Security (TLS) eine Sicherheitseinstellung aus.
   - **Verwenden Sie STARTTLS**: Verwenden Sie STARTTLS, um die Kommunikation mit dem LDAP-Server zu sichern. Dies ist die empfohlene Option für Active Directory, OpenLDAP oder andere, diese Option wird jedoch für Azure nicht unterstützt.
   - **LDAPS verwenden**: Die Option LDAPS (LDAP über SSL) verwendet TLS, um eine Verbindung zum LDAP-Server herzustellen. Sie müssen diese Option für Azure auswählen.
   - **Verwenden Sie keine TLS**: Der Netzwerkverkehr zwischen dem StorageGRID-System und dem LDAP-Server wird nicht gesichert. Diese Option wird für Azure nicht unterstützt.

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

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

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

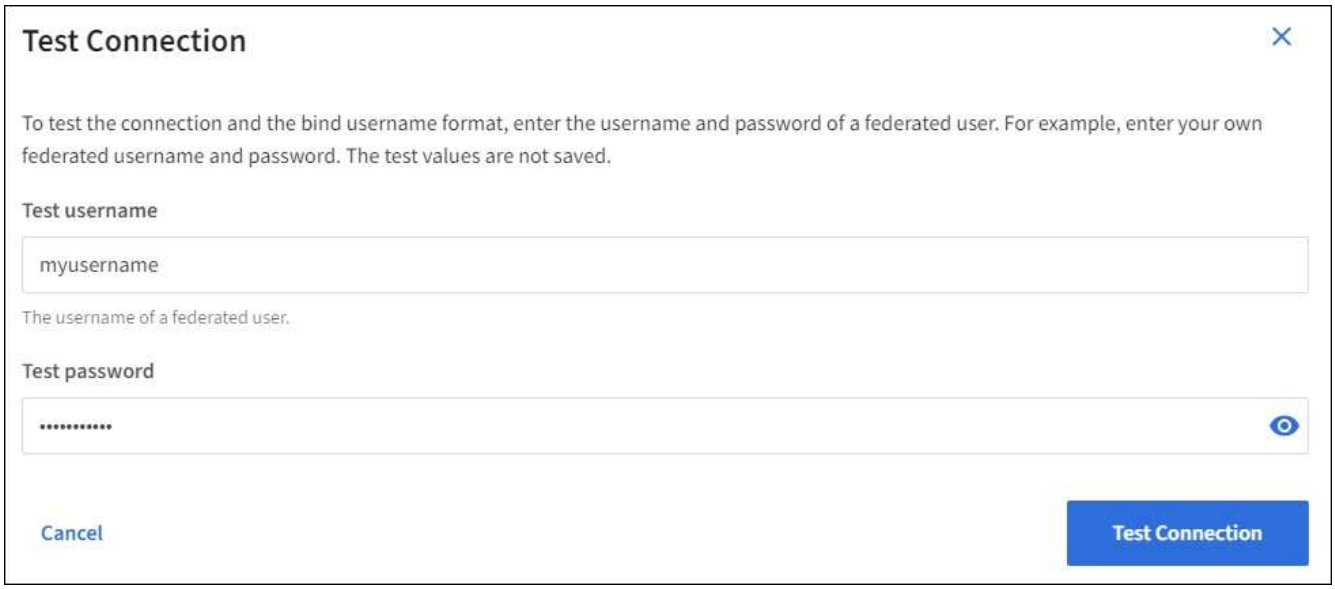
Testen Sie die Verbindung und speichern Sie die Konfiguration

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

Schritte

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

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



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

Synchronisierung mit der Identitätsquelle erzwingen

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

Schritte

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

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

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

Deaktivieren Sie den Identitätsverbund

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

Über diese Aufgabe

Bevor Sie die Identitätsföderation deaktivieren, sollten Sie Folgendes beachten:

- Verbundene Benutzer können sich nicht anmelden.
- Föderierte Benutzer, die sich derzeit anmelden, erhalten bis zu ihrem Ablauf Zugriff auf das StorageGRID-

System, können sich jedoch nach Ablauf der Sitzung nicht anmelden.

- Die Synchronisierung zwischen dem StorageGRID-System und der Identitätsquelle erfolgt nicht, und Warnmeldungen oder Alarme werden nicht für Konten ausgelöst, die nicht synchronisiert wurden.
- Das Kontrollkästchen **Enable Identity Federation** ist deaktiviert, wenn Single Sign-On (SSO) auf **enabled** oder **Sandbox Mode** eingestellt ist. Der SSO-Status auf der Seite Single Sign-On muss **deaktiviert** sein, bevor Sie die Identitätsföderation deaktivieren können. Siehe "Deaktivieren Sie Single Sign-On".

Schritte

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

Richtlinien für die Konfiguration eines OpenLDAP-Servers

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

> Bei Identitätsquellen, die nicht ActiveDirectory oder Azure sind, blockiert StorageGRID den S3-Zugriff nicht automatisch für Benutzer, die extern deaktiviert sind. Löschen Sie zum Blockieren des S3-Zugriffs alle S3-Schlüssel für den Benutzer oder entfernen Sie den Benutzer aus allen Gruppen.

Überlagerungen in Memberof und Refint

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

Indizierung

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

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

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

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

Managen von Admin-Gruppen

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

Bevor Sie beginnen

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

Erstellen einer Admin-Gruppe

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

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **KONFIGURATION** > **Zugriffskontrolle** > **Admin-Gruppen**.
2. Wählen Sie **Gruppe erstellen**.

Wählen Sie einen Gruppentyp aus

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

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

Lokale Gruppe

Schritte

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

Föderierte Gruppe

Schritte

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

Gruppenberechtigungen verwalten

Schritte

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

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

2. Wählen Sie eine oder mehrere Antworten aus "Berechtigungen für Administratorgruppen".

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

3. Wenn Sie eine lokale Gruppe erstellen, wählen Sie **Weiter**. Wenn Sie eine Verbundgruppe erstellen, wählen Sie **Gruppe erstellen** und **Fertig stellen** aus.

Benutzer hinzufügen (nur lokale Gruppen)

Schritte

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

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

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

Anzeigen und Bearbeiten von Admin-Gruppen

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

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

Aufgabe	Menü „Aktionen“	Detailseite
Zeigen Sie Gruppendetails an	a. Aktivieren Sie das Kontrollkästchen für die Gruppe. b. Wählen Sie **Aktionen** > **Gruppendetails anzeigen**.	Wählen Sie den Gruppennamen in der Tabelle aus.

Aufgabe	Menü „Aktionen“	Detailseite
Anzeigename bearbeiten (nur lokale Gruppen)	a. Aktivieren Sie das Kontrollkästchen für die Gruppe. b. Wählen Sie **Aktionen** > **Gruppenname bearbeiten**. c. Geben Sie den neuen Namen ein. d. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Gruppennamen aus, um die Details anzuzeigen. b. Wählen Sie das Bearbeitungssymbol . c. Geben Sie den neuen Namen ein. d. Wählen Sie **Änderungen speichern**.
Zugriffsmodus oder Berechtigungen bearbeiten	a. Aktivieren Sie das Kontrollkästchen für die Gruppe. b. Wählen Sie **Aktionen** > **Gruppendetails anzeigen**. c. Ändern Sie optional den Zugriffsmodus der Gruppe. d. Wählen Sie optional aus oder löschen Sie die Option "Berechtigungen für Administratorgruppen". e. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Gruppennamen aus, um die Details anzuzeigen. b. Ändern Sie optional den Zugriffsmodus der Gruppe. c. Wählen Sie optional aus oder löschen Sie die Option "Berechtigungen für Administratorgruppen". d. Wählen Sie **Änderungen speichern**.

Duplizieren einer Gruppe

Schritte

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

Gruppe löschen

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

Schritte

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

Berechtigungen für Admin-Gruppen

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

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

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

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

Interaktion zwischen Berechtigungen und Zugriffsmodus

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

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

Root-Zugriff

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

Alarme quittieren (alt)

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

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

Root-Passwort des Mandanten ändern

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

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

Konfiguration der Seite der Grid-Topologie

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

ILM

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

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

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

Wartung

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

- **KONFIGURATION** > **Zugangskontrolle**:
  - Grid-Passwörter
- **KONFIGURATION** > **Netzwerk**:
  - Domänennamen des S3-Endpunkts
- **WARTUNG** > **Aufgaben**:
  - Ausmustern
  - Erweiterung
  - Überprüfung der Objektexistenz
  - Recovery
- **WARTUNG** > **System**:
  - Recovery-Paket
  - Software-Update
- **SUPPORT** > **Tools**:
  - Protokolle

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

- **WARTUNG** > **Netzwerk**:
  - DNS-Server
  - Grid-Netzwerk
  - NTP-Server
- **WARTUNG** > **System**:

    - Lizenz
- **KONFIGURATION** > **Netzwerk**:
    - Domänennamen des S3-Endpunkts
- **KONFIGURATION** > **Sicherheit**:
    - Zertifikate
- **KONFIGURATION** > **Überwachung**:
    - Audit- und Syslog-Server

Verwalten von Meldungen

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

Abfrage von Kennzahlen

Diese Berechtigung bietet Zugriff auf:

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

Suche nach Objektmetadaten

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

Andere Grid-Konfiguration

Diese Berechtigung ermöglicht den Zugriff auf zusätzliche Grid-Konfigurationsoptionen.

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

- **ILM**:
    - Lagergüten
- **KONFIGURATION** > **System**:
    - Storage-Optionen
- **SUPPORT** > **Alarme (alt)**:
    - Benutzerdefinierte Events
    - Globale Alarme
    - Einrichtung alter E-Mail-Adressen
- **SUPPORT** > **andere**:
    - Verbindungskosten

Storage Appliance-Administrator

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

Mandantenkonten

Mit dieser Berechtigung können Sie:

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

Benutzer managen

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

Bevor Sie beginnen

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

Erstellen Sie einen lokalen Benutzer

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

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

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

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

Greifen Sie auf den Assistenten zu

Schritte

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

Geben Sie die Anmeldedaten des Benutzers ein

Schritte

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

Zu Gruppen zuweisen

Schritte

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

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

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

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

Lokale Benutzer anzeigen und bearbeiten

Details zu vorhandenen lokalen und föderierten Benutzern können angezeigt werden. Sie können einen lokalen Benutzer ändern, um den vollständigen Namen, das Kennwort oder die Gruppenmitgliedschaft des Benutzers zu ändern. Sie können auch vorübergehend verhindern, dass ein Benutzer auf den Grid Manager und die Grid Management API zugreift.

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

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

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

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

Aufgabe	Menü „Aktionen“	Detailseite
Zeigen Sie Benutzerdetails an	a. Aktivieren Sie das Kontrollkästchen für den Benutzer. b. Wählen Sie **Aktionen** > **Benutzerdetails anzeigen**.	Wählen Sie den Benutzernamen in der Tabelle aus.
Vollständigen Namen bearbeiten (nur lokale Benutzer)	a. Aktivieren Sie das Kontrollkästchen für den Benutzer. b. Wählen Sie **Aktionen** > **vollständigen Namen bearbeiten**. c. Geben Sie den neuen Namen ein. d. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Benutzernamen aus, um die Details anzuzeigen. b. Wählen Sie das Bearbeitungssymbol . c. Geben Sie den neuen Namen ein. d. Wählen Sie **Änderungen speichern**.

Aufgabe	Menü „Aktionen“	Detailseite
StorageGRID-Zugriff verweigern oder zulassen	a. Aktivieren Sie das Kontrollkästchen für den Benutzer. b. Wählen Sie **Aktionen** > **Benutzerdetails anzeigen**. c. Wählen Sie die Registerkarte Zugriff aus. d. Wählen Sie **Ja** aus, um zu verhindern, dass sich der Benutzer beim Grid Manager oder der Grid Management API anmeldet, oder wählen Sie **Nein** aus, damit der Benutzer sich anmelden kann. e. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Benutzernamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte Zugriff aus. c. Wählen Sie **Ja** aus, um zu verhindern, dass sich der Benutzer beim Grid Manager oder der Grid Management API anmeldet, oder wählen Sie **Nein** aus, damit der Benutzer sich anmelden kann. d. Wählen Sie **Änderungen speichern**.
Passwort ändern (nur lokale Benutzer)	a. Aktivieren Sie das Kontrollkästchen für den Benutzer. b. Wählen Sie **Aktionen** > **Benutzerdetails anzeigen**. c. Wählen Sie die Registerkarte Kennwort aus. d. Geben Sie ein neues Passwort ein. e. Wählen Sie **Passwort ändern**.	a. Wählen Sie den Benutzernamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte Kennwort aus. c. Geben Sie ein neues Passwort ein. d. Wählen Sie **Passwort ändern**.
Gruppen ändern (nur lokale Benutzer)	a. Aktivieren Sie das Kontrollkästchen für den Benutzer. b. Wählen Sie **Aktionen** > **Benutzerdetails anzeigen**. c. Wählen Sie die Registerkarte Gruppen aus. d. Wählen Sie optional den Link nach einem Gruppennamen aus, um die Details der Gruppe in einer neuen Browserregisterkarte anzuzeigen. e. Wählen Sie **Gruppen bearbeiten**, um verschiedene Gruppen auszuwählen. f. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Benutzernamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte Gruppen aus. c. Wählen Sie optional den Link nach einem Gruppennamen aus, um die Details der Gruppe in einer neuen Browserregisterkarte anzuzeigen. d. Wählen Sie **Gruppen bearbeiten**, um verschiedene Gruppen auszuwählen. e. Wählen Sie **Änderungen speichern**.

Duplizieren eines Benutzers

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

Schritte

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

Löschen Sie einen Benutzer

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

Sie können den Root-Benutzer nicht löschen.

Schritte

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

Single Sign On (SSO) verwenden

Konfigurieren Sie Single Sign-On

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

Funktionsweise von Single Sign-On

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

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

Melden Sie sich an, wenn SSO aktiviert ist

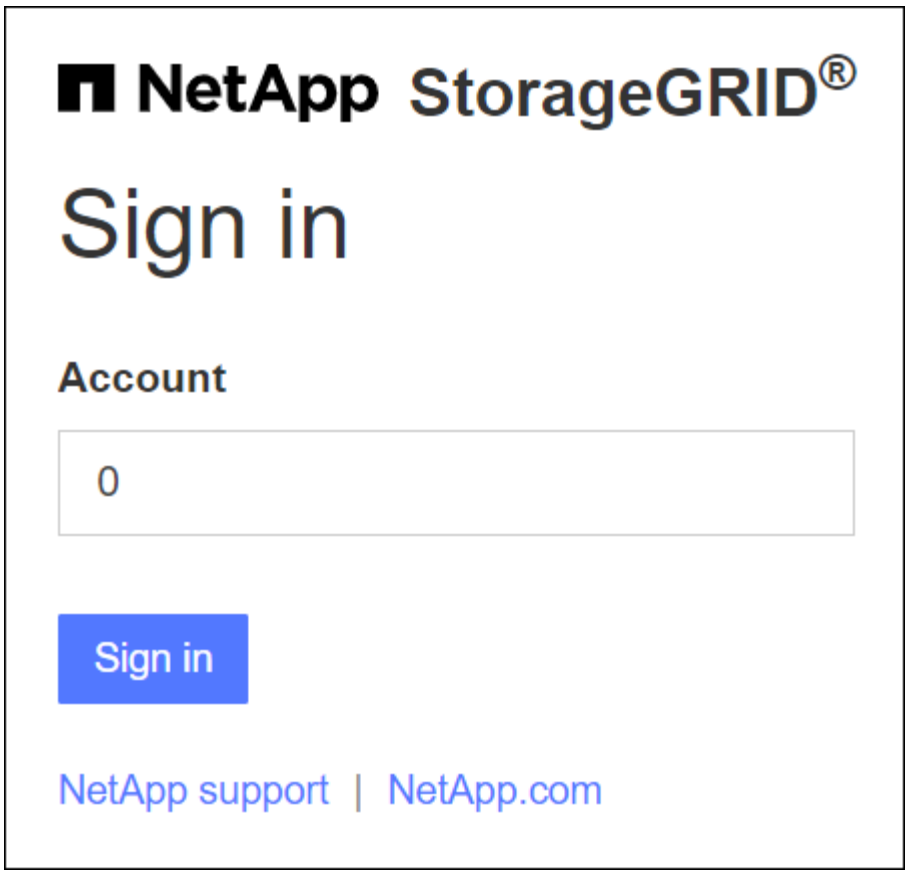
Wenn SSO aktiviert ist und Sie sich bei StorageGRID anmelden, werden Sie zur SSO-Seite Ihres Unternehmens weitergeleitet, um Ihre Anmeldedaten zu validieren.

Schritte

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

   Die Seite StorageGRID-Anmeldung wird angezeigt.

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

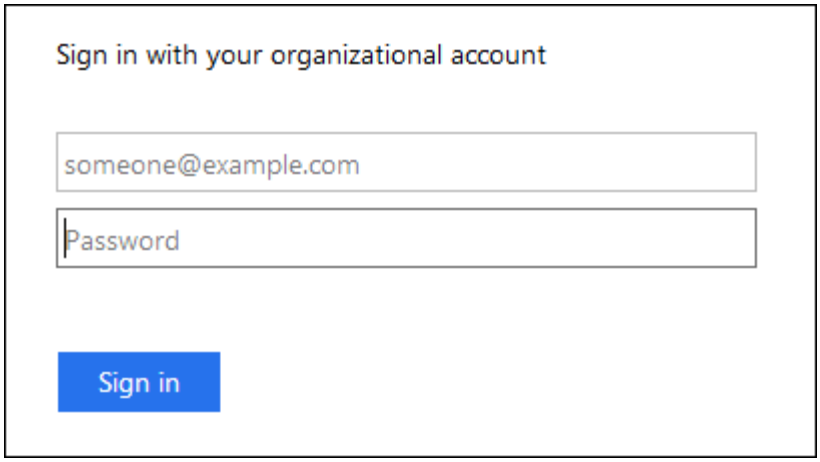


- Wenn Sie zuvor entweder auf den Grid Manager oder den Tenant Manager zugegriffen haben, werden Sie aufgefordert, ein aktuelles Konto auszuwählen oder eine Konto-ID einzugeben:

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

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

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



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

   Falls Ihre SSO-Anmeldedaten korrekt sind:

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

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

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

   Sie müssen Ihre SSO-Anmeldedaten nicht erneut eingeben.

Abmelden, wenn SSO aktiviert ist

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

Schritte

1. Suchen Sie den Link **Abmelden** in der oberen rechten Ecke der Benutzeroberfläche.
2. Wählen Sie **Abmelden**.

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

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

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

Voraussetzungen und Überlegungen für Single Sign-On

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

Anforderungen an Identitätsanbieter

StorageGRID unterstützt die folgenden SSO-Identitätsanbieter (IdP):

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

Sie müssen die Identitätsföderation für Ihr StorageGRID-System konfigurieren, bevor Sie einen SSO-Identitätsanbieter konfigurieren können. Der Typ des LDAP-Service, den Sie für die Identitätsföderation verwenden, steuert, welcher SSO-Typ Sie implementieren können.

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

AD-FS-Anforderungen

Sie können eine der folgenden Versionen von AD FS verwenden:

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

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

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

Zusätzlichen Anforderungen

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

Überlegungen zu Azure

Wenn Sie Azure als SSO-Typ verwenden und Benutzer über Hauptbenutzernamen verfügen, die den sAMAccountName nicht als Präfix verwenden, können Anmeldeprobleme auftreten, wenn StorageGRID seine Verbindung mit dem LDAP-Server verliert. Damit Benutzer sich anmelden können, müssen Sie die Verbindung zum LDAP-Server wiederherstellen.

Serverzertifikate-Anforderungen

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

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

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

Sie können auf das Serverzertifikat eines Admin-Knotens zugreifen, indem Sie sich bei der Befehlshülle des Knotens anmelden und auf die zugreifen `/var/local/mgmt-api` Verzeichnis. Ein benutzerdefiniertes Serverzertifikat ist benannt `custom-server.crt`. Das Standardserverzertifikat des Node wird mit benannt `server.crt`.

Port-Anforderungen

Single Sign-On (SSO) ist auf den Ports Restricted Grid Manager oder Tenant Manager nicht verfügbar. Sie

müssen den Standard-HTTPS-Port (443) verwenden, wenn Benutzer sich mit Single Sign-On authentifizieren möchten. Siehe "Kontrolle des Zugriffs über externe Firewall".

Bestätigen Sie, dass verbundene Benutzer sich anmelden können

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

Bevor Sie beginnen

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

Schritte

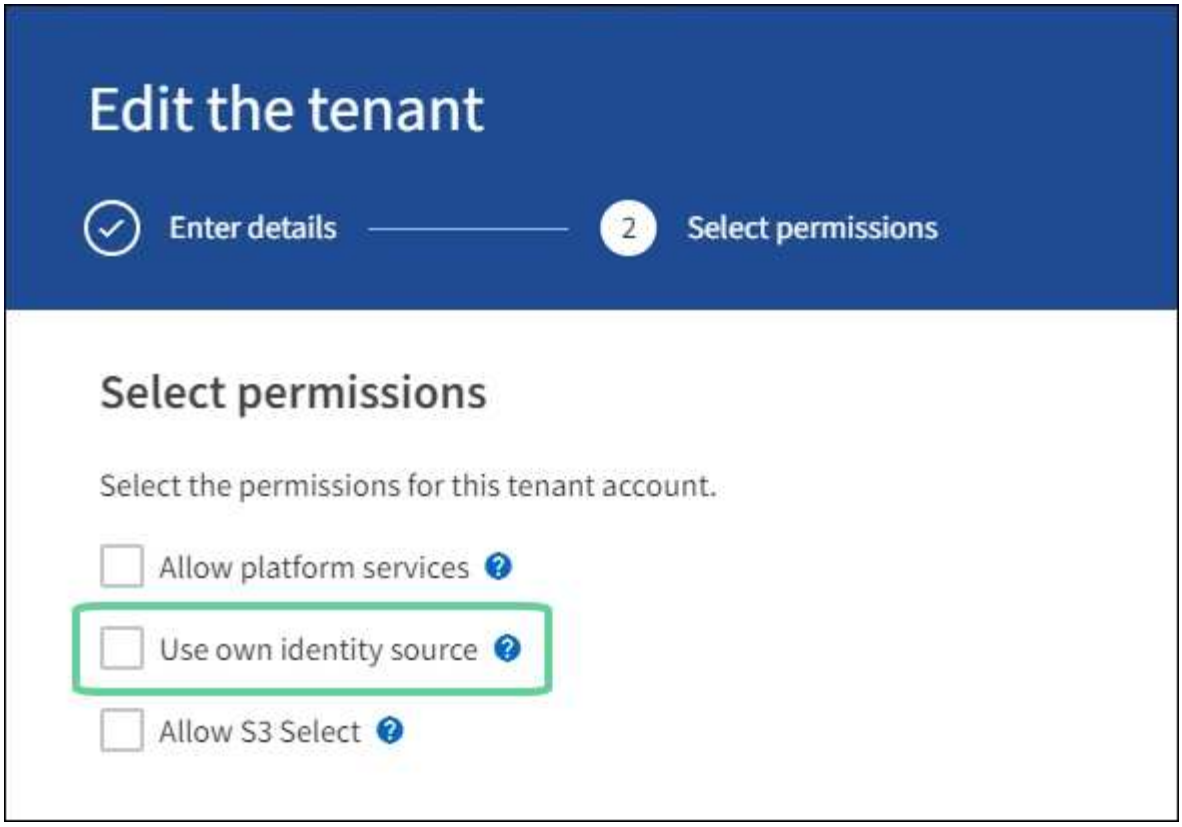
1. Falls bereits vorhandene Mandantenkonten vorhanden sind, bestätigen Sie, dass kein Mandant seine eigene Identitätsquelle verwendet.

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

   a. Melden Sie sich für jedes Mandantenkonto bei Tenant Manager an.
   b. Wählen Sie * ACCESS MANAGEMENT* > **Identity Federation**.
   c. Bestätigen Sie, dass das Kontrollkästchen **Enable Identity Federation** nicht aktiviert ist.
   d. Wenn dies der Fall ist, bestätigen Sie, dass keine föderierten Gruppen mehr für dieses Mandantenkonto benötigt werden, deaktivieren Sie das Kontrollkästchen und wählen Sie **Speichern**.

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

3. Wenn es bereits bestehende Mandantenkonten gibt, bestätigen Sie, dass sich ein föderaler Benutzer mit Root-Zugriffsberechtigung anmelden kann:
   a. Wählen Sie im Grid Manager die Option **MITERS** aus.
   b. Wählen Sie das Mandantenkonto aus und wählen Sie **Aktionen** > **Bearbeiten**.
   c. Wählen Sie auf der Registerkarte Details eingeben die Option **Weiter**.
   d. Wenn das Kontrollkästchen **eigene Identitätsquelle verwenden** aktiviert ist, deaktivieren Sie das Kontrollkästchen und wählen Sie **Speichern** aus.



Die Seite Mandant wird angezeigt.

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

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

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

d. Abmelden.

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

Verwandte Informationen

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

Verwenden Sie den Sandbox-Modus

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

Bevor Sie beginnen

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

- Sie haben die Root-Zugriffsberechtigung.
- Sie haben eine Identitätsföderation für Ihr StorageGRID System konfiguriert.
- Für die Identitätsföderation **LDAP-Diensttyp** haben Sie entweder Active Directory oder Azure ausgewählt, basierend auf dem SSO-Identitäts-Provider, den Sie verwenden möchten.

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

Über diese Aufgabe

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

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

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

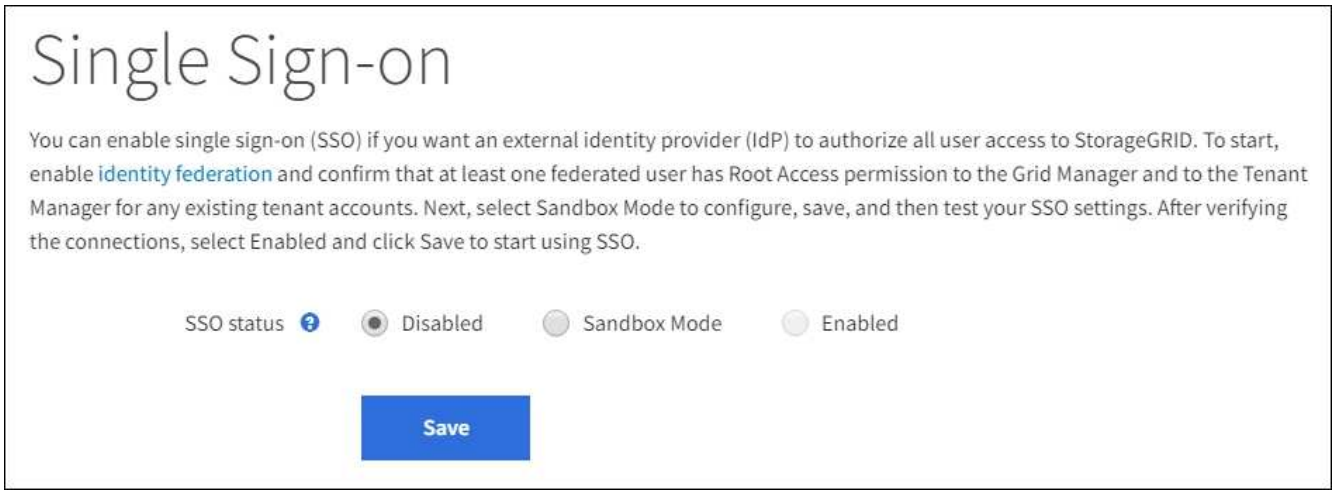
Im Sandbox-Modus ist es einfach, diese Rückkehrkonfiguration durchzuführen und alle Einstellungen zu testen, bevor Sie SSO aktivieren. Wenn Sie den Sandbox-Modus verwenden, können sich Benutzer nicht mit SSO anmelden.

Zugriff auf den Sandbox-Modus

Schritte

1. Wählen Sie **KONFIGURATION** > **Zugriffskontrolle** > **Single Sign-On**.

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



Wenn die SSO-Statusoptionen nicht angezeigt werden, vergewissern Sie sich, dass Sie den Identitätsanbieter als föderierte Identitätsquelle konfiguriert haben. Siehe "Voraussetzungen und Überlegungen für Single Sign-On".

2. Wählen Sie **Sandbox-Modus**.

   Der Abschnitt „Identitätsanbieter“ wird angezeigt.

Geben Sie die Daten des Identitätsanbieters ein

Schritte

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

Active Directory

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

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

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

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

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

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

4. Wählen Sie **Speichern**.

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

Azure

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

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

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

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

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

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

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

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

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

PingFederate

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

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

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

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

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

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

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

   Verwenden Sie das folgende Format:

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

4. Wählen Sie **Speichern**.

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

Konfigurieren Sie Vertrauensstellungen von Drittanbietern, Unternehmensanwendungen oder SP-Verbindungen

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

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

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

Active Directory

Schritte

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

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

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

Azure

Schritte

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

PingFederate

Schritte

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

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

Testen Sie SSO-Verbindungen

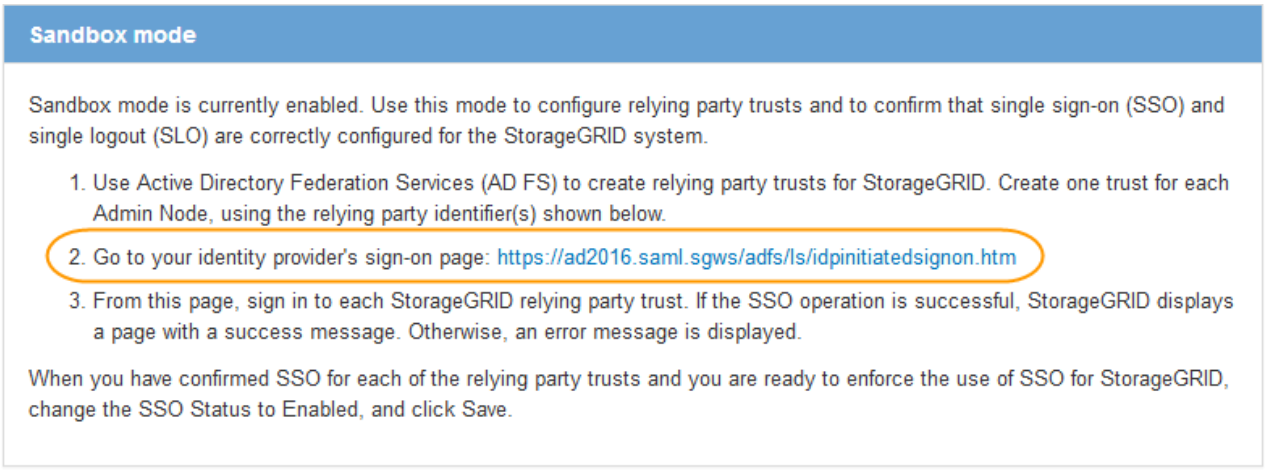
Bevor Sie die Verwendung von Single Sign-On für Ihr gesamtes StorageGRID-System erzwingen, sollten Sie bestätigen, dass Single Sign-On und Single Logout für jeden Admin-Knoten korrekt konfiguriert sind.

Active Directory

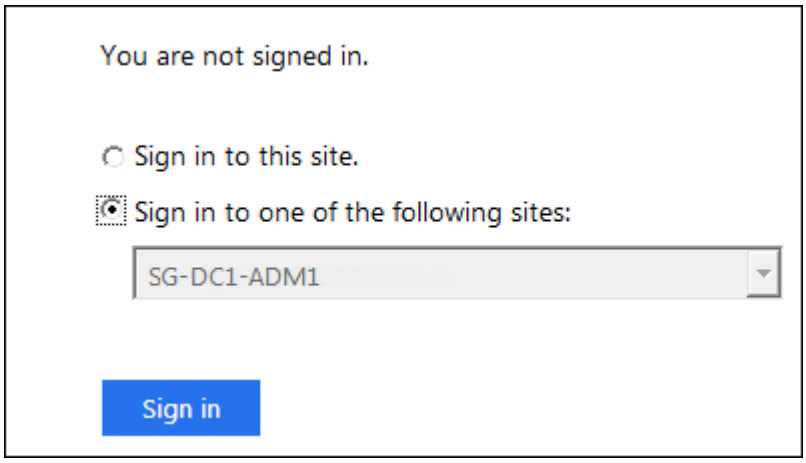
Schritte

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

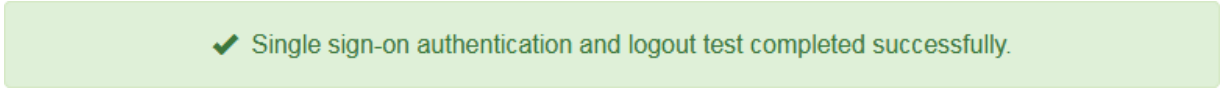
   Die URL wird aus dem Wert abgeleitet, den Sie im Feld **Federation Service Name** eingegeben haben.

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

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

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

überprüfen.

Azure

Schritte

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

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

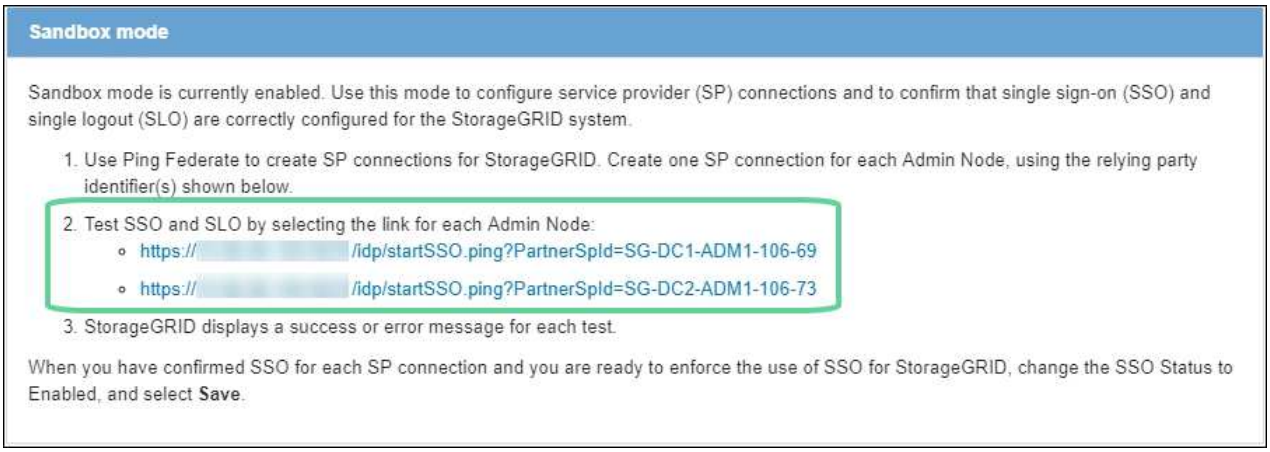
   - Wenn der SSO-Vorgang nicht erfolgreich ist, wird eine Fehlermeldung angezeigt. Beheben Sie das Problem, löschen Sie die Cookies des Browsers, und versuchen Sie es erneut.
4. Wiederholen Sie diese Schritte, um die SSO-Verbindung für jeden Admin-Node in Ihrem Raster zu überprüfen.

PingFederate

Schritte

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

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

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

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

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

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

Aktivieren Sie Single Sign On

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

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

Schritte

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

   Single Sign-On ist jetzt aktiviert.

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

Erstellen Sie Vertrauensstellungen von vertrauenswürdigen Parteien in AD FS

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

Bevor Sie beginnen

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

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

- Sie haben Erfahrung beim Erstellen von Vertrauensstellungen von Vertrauensstellen in AD FS, oder Sie haben Zugriff auf die Microsoft AD FS-Dokumentation.

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

Über diese Aufgabe

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

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

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

Schritte

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

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

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

   Das AD FS Management Tool wird angezeigt.
4. Wählen Sie **AD FS** > **vertraut auf Partei**.

   Die Liste der Vertrauensstellen wird angezeigt.
5. Fügen Sie eine Zugriffskontrollrichtlinie zum neu erstellten Vertrauen der Vertrauensstellenden Partei hinzu:
   a. Suchen Sie das Vertrauen der Vertrauensgesellschaft, das Sie gerade erstellt haben.
   b. Klicken Sie mit der rechten Maustaste auf das Vertrauen und wählen Sie **Zugriffskontrollrichtlinie bearbeiten**.
   c. Wählen Sie eine Zugriffskontrollrichtlinie aus.
   d. Wählen Sie **Anwenden**, und wählen Sie **OK**
6. Fügen Sie dem neu erstellten Treuhandgesellschaft eine Richtlinie zur Ausstellung von Forderungen hinzu:
   a. Suchen Sie das Vertrauen der Vertrauensgesellschaft, das Sie gerade erstellt haben.
   b. Klicken Sie mit der rechten Maustaste auf das Vertrauen und wählen Sie **Richtlinie zur Bearbeitung von Forderungen** aus.

c. Wählen Sie **Regel hinzufügen**.

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

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

   Beispiel: **ObjectGUID an Name ID**.

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

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

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

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

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

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

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

      Wenn die Metadaten fehlen, überprüfen Sie, ob die Metadatenadresse der Föderation korrekt ist, oder geben Sie die Werte manuell ein.

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

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

Erstellen Sie durch den Import von Federationmetadaten ein Vertrauen von Kunden

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

Schritte

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

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

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

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

vertrauenden Partei und schließen Sie den Assistenten.

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

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

      Beispiel: **ObjectGUID an Name ID**.

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

      Wenn die Metadaten fehlen, überprüfen Sie, ob die Metadatenadresse der Föderation korrekt ist, oder geben Sie die Werte manuell ein.
9. Wiederholen Sie diese Schritte, um ein Vertrauensverhältnis für alle Administratorknoten in Ihrem StorageGRID-System zu konfigurieren.
10. Wenn Sie fertig sind, kehren Sie zu StorageGRID zurück und testen Sie alle Treuhänder der Vertrauensstellen, um zu bestätigen, dass sie richtig konfiguriert sind. Siehe "Verwenden Sie den Sandbox-Modus" Weitere Anweisungen.

Erstellen Sie manuell ein Vertrauen der Vertrauensbasis

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

Schritte

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

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

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

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

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

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

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

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

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

   `Admin_Node_Identifier`

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

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

   Das Dialogfeld „Forderungsrichtlinie bearbeiten“ wird angezeigt.

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

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

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

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

      Beispiel: **ObjectGUID an Name ID**.

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

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

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

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

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

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

   a. Wählen Sie **SAML hinzufügen**.

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

c. Wählen Sie **Bindung** > **Umleiten**.

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

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

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

a. Wählen Sie **OK**.

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

   a. Fügen Sie das benutzerdefinierte Zertifikat hinzu:

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

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

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

      Die Eigenschaften der zu vertrauenden Partei werden gespeichert und geschlossen.

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

Erstellen von Enterprise-Applikationen in Azure AD

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

Bevor Sie beginnen

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

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

- Sie haben Erfahrung beim Erstellen von Enterprise-Applikationen in Azure Active Directory.
- Sie verfügen über ein Azure Konto mit einem aktiven Abonnement.
- Im Azure-Konto verfügen Sie über eine der folgenden Rollen: Global Administrator, Cloud Application Administrator, Application Administrator oder Eigentümer des Service-Principal.

Zugriff auf Azure AD

Schritte

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

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

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

Schritte

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

Laden Sie für jeden Admin-Node SAML-Metadaten herunter

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

Schritte

1. Wiederholen Sie diese Schritte für jeden Admin-Node.
   a. Melden Sie sich über den Admin-Node bei StorageGRID an.
   b. Wählen Sie **KONFIGURATION** > **Zugriffskontrolle** > **Single Sign-On**.
   c. Wählen Sie die Schaltfläche, um die SAML-Metadaten für diesen Admin-Node herunterzuladen.
   d. Speichern Sie die Datei, die Sie in Azure AD hochladen möchten.

Hochladen von SAML-Metadaten in jede Enterprise-Applikation

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

Schritte

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

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

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

Erstellen von SP-Verbindungen (Service Provider) in PingFederate

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

Bevor Sie beginnen

- Sie haben Single Sign-On für StorageGRID konfiguriert und als SSO-Typ * Ping föderate* ausgewählt.
- **Der Sandbox-Modus** ist auf der Single Sign-On-Seite im Grid Manager ausgewählt. Siehe "Verwenden Sie den Sandbox-Modus".
- Sie haben die **SP-Verbindungs-ID** für jeden Admin-Knoten in Ihrem System. Diese Werte finden Sie in der Detailtabelle Admin Nodes auf der StorageGRID Single Sign-On-Seite.
- Sie haben die **SAML-Metadaten** für jeden Admin-Knoten in Ihrem System heruntergeladen.
- Sie haben Erfahrung beim Erstellen von SP-Verbindungen in PingFederate Server.
- Sie haben diehttps://docs.pingidentity.com/bundle/pingfederate-

103/page/kfj1564002962494.html["Administrator's Reference Guide"^] Für PingFederate Server. Die PingFederate-Dokumentation bietet detaillierte Schritt-für-Schritt-Anleitungen und Erklärungen.

- Sie haben die Administratorberechtigung für PingFederate Server.

Über diese Aufgabe

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

Alle Voraussetzungen in PingFederate

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

Datenspeicher erstellen

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

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

Passwortvalididator[[Password-Validator] erstellen

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

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

IdP-Adapterinstanz erstellen

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

Schritte

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

7. Wählen Sie **Speichern**.

Signaturzertifikat erstellen oder importieren

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

Schritte

1. Gehen Sie zu **Sicherheit** > **Signieren & Entschlüsseln Schlüssel & Zertifikate**.
2. Erstellen oder importieren Sie das Signieren-Zertifikat.

Erstellen Sie eine SP-Verbindung in PingFederate

Wenn Sie eine SP-Verbindung in PingFederate erstellen, importieren Sie die SAML-Metadaten, die Sie für den Admin-Node von StorageGRID heruntergeladen haben. Die Metadatendatei enthält viele der spezifischen Werte, die Sie benötigen.

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

Wählen Sie den SP-Verbindungstyp

Schritte

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

Importieren der SP-Metadaten

Schritte

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

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

4. Wählen Sie **Weiter**.

Konfigurieren Sie SSO für den IdP-Browser

Schritte

1. Wählen Sie auf der Registerkarte Browser-SSO * die Option * Browser-SSO konfigurieren* aus.
2. Wählen Sie auf der Registerkarte SAML-Profile die Optionen **SP-initiated SSO**, **SP-initial SLO**, **IdP-initiated SSO** und **IdP-initiated SLO** aus.

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

Adapterinstanz zuordnen

Schritte

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

Konfigurieren von Protokolleinstellungen

Schritte

1. Wählen Sie auf der Registerkarte **SP-Verbindung** > **Browser SSO** > **Protokolleinstellungen** die Option **Protokolleinstellungen konfigurieren** aus.
2. Akzeptieren Sie auf der Registerkarte Assertion Consumer Service URL die Standardwerte, die aus den StorageGRID SAML Metadaten importiert wurden (**POST** für binding und `/api/saml-response` Für Endpunkt-URL).

3. Akzeptieren Sie auf der Registerkarte SLO-Dienst-URLs die Standardwerte, die aus den StorageGRID-SAML-Metadaten importiert wurden (**REDIRECT** für Binding und `/api/saml-logout` Für Endpunkt-URL.
4. Deaktivieren Sie auf der Registerkarte Allowable SAML Bindings **ARTIFACT** und **SOAP**. Es sind nur **POST** und **REDIRECT** erforderlich.
5. Lassen Sie auf der Registerkarte Signature Policy die Kontrollkästchen **require AUTHN Requests to be signed** und **always Sign Assertion** ausgewählt.
6. Wählen Sie auf der Registerkarte Verschlüsselungsrichtlinie die Option **Keine** aus.
7. Überprüfen Sie die Zusammenfassung und wählen Sie **Fertig**, um die Protokolleinstellungen zu speichern.
8. Überprüfen Sie die Zusammenfassung und wählen Sie **Fertig**, um die SSO-Einstellungen des Browsers zu speichern.

Anmeldedaten konfigurieren

Schritte

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

Erstellen Sie zusätzliche SP-Verbindungen

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

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

Schritte

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

b. Wählen Sie **Browser-SSO konfigurieren > Assertion-Erstellung konfigurieren > Attributvertrag** aus.

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

d. Wählen Sie **Speichern**.

Deaktivieren Sie Single Sign-On

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

Bevor Sie beginnen

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

Schritte

1. Wählen Sie **KONFIGURATION** > **Zugriffskontrolle** > **Single Sign-On**.

   Die Seite Single Sign-On wird angezeigt.

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

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

4. Wählen Sie **OK**.

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

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

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

Schritte

1. Melden Sie sich bei einem Admin-Knoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@Admin_Node_IP`
   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

      Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

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

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

3. Bestätigen Sie, dass Sie SSO deaktivieren möchten.

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

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

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

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

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

7. Wenn Sie SSO vorübergehend deaktiviert haben, weil Sie aus einem anderen Grund auf den Grid Manager zugreifen mussten:

   a. Führen Sie alle Aufgaben oder Aufgaben aus, die Sie ausführen müssen.
   b. Wählen Sie **Abmelden**, und schließen Sie den Grid Manager.
   c. SSO auf dem Admin-Node erneut aktivieren. Sie können einen der folgenden Schritte ausführen:

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

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

      Bestätigen Sie, dass Sie SSO aktivieren möchten.

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

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

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

Grid-Verbund verwenden

Was ist Grid Federation?

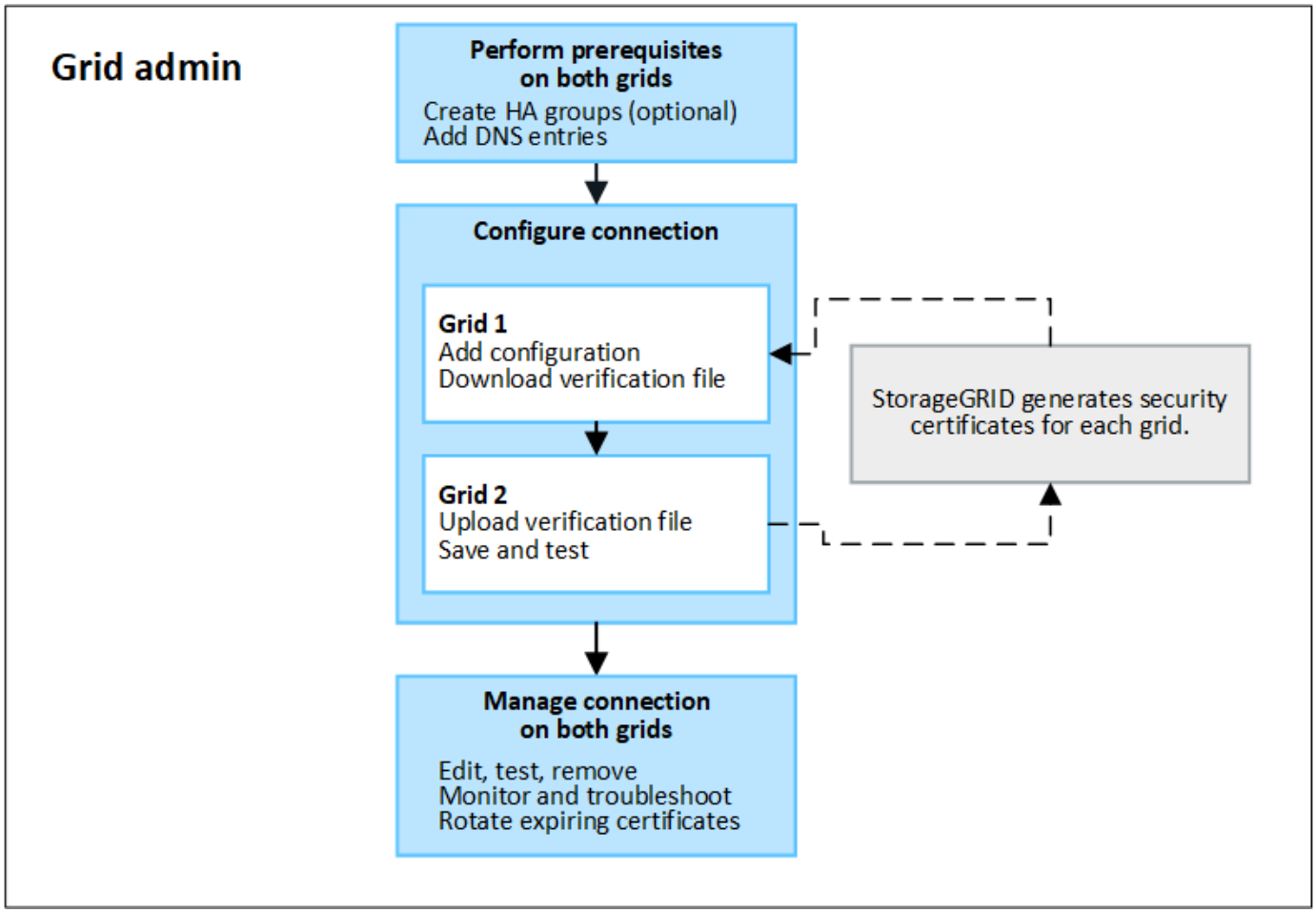
Mithilfe des Grid-Verbunds können Mandanten geklont und ihre Objekte zwischen zwei StorageGRID Systemen für das Disaster Recovery repliziert werden.

Was ist eine Netzverbundverbindung?

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

Workflow für Grid-Verbund

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



Überlegungen und Anforderungen für Netzverbundverbindungen

- Beide für den Grid-Verbund verwendeten Grids müssen StorageGRID 11.7 ausführen.
- Ein Grid kann eine oder mehrere Netzverbundverbindungen zu anderen Grids haben. Jede Netzverbundverbindung ist unabhängig von allen anderen Verbindungen. Wenn beispielsweise Grid 1 eine Verbindung mit Grid 2 und eine zweite Verbindung mit Grid 3 hat, besteht keine implizierte Verbindung zwischen Grid 2 und Grid 3.
- Netzverbundverbindungen sind bidirektional. Nachdem die Verbindung hergestellt wurde, können Sie die Verbindung von beiden Grids aus überwachen und verwalten.
- Es muss mindestens eine Netzverbundverbindung vorhanden sein, bevor Sie verwenden können "Konto-Klon" Oder "Grid-übergreifende Replizierung".

Netzwerkanforderungen und IP-Adresse

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

Verwenden Sie FQDNs, um die Verbindung auszugleichen

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

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

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

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

Port-Anforderungen

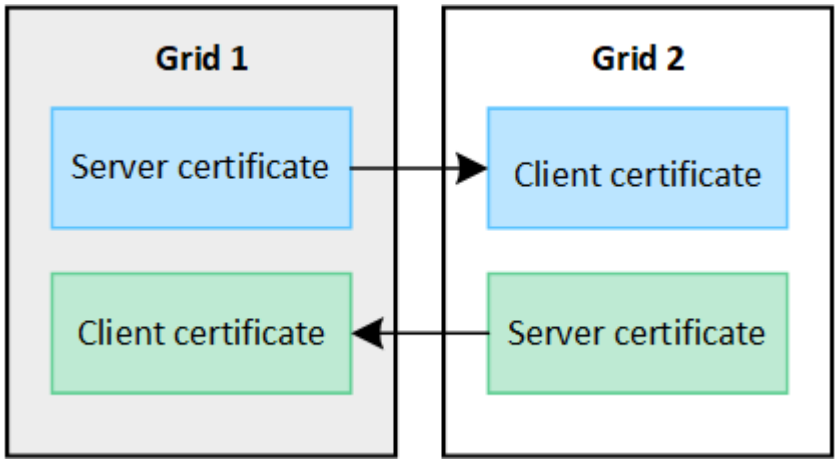
Beim Erstellen einer Grid-Federation-Verbindung können Sie alle nicht verwendeten Portnummern zwischen 23000 und 23999 angeben. Beide Grids in dieser Verbindung verwenden den gleichen Port.

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

Zertifikatanforderungen

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

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



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

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

Weitere Informationen .

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

Was ist Account-Klon?

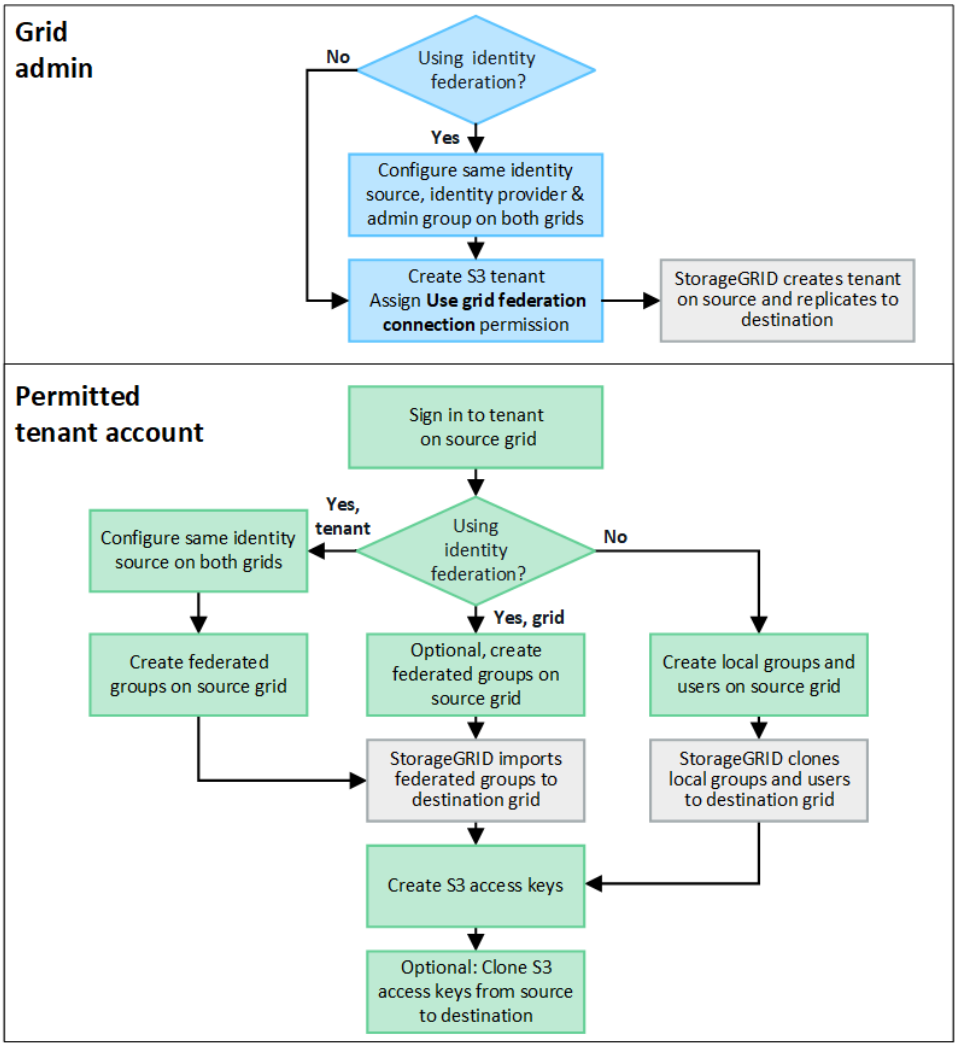
Der Account-Klon ist die automatische Replizierung eines Mandantenkontos, von Mandantengruppen und Mandantenbenutzern sowie optional: S3-Zugriffstasten zwischen den StorageGRID-Systemen in einem "Netzverbundverbindung".

Der Kontoklon ist für erforderlich "Grid-übergreifende Replizierung". Durch das Klonen von Kontoinformationen aus einem Quell-StorageGRID-System auf ein Ziel-StorageGRID-System wird sichergestellt, dass Mandantenbenutzer und -Gruppen auf die entsprechenden Buckets und Objekte in beiden Grids zugreifen

können.

Workflow für Konto-Klon

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



Grid-Administrator-Workflow

Die Schritte, die Grid-Administratoren durchführen, hängen davon ab, ob die StorageGRID Systeme im enthalten sind "Netzverbundverbindung" Verwenden Sie Single Sign-On (SSO) oder Identity Federation.

SSO für Kontoklone konfigurieren (optional)

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

Schritte

1. Konfigurieren Sie dieselbe Identitätsquelle für beide Raster. Siehe "Verwenden Sie den Identitätsverbund".
2. Konfigurieren Sie denselben SSO-Identitätsanbieter (IdP) für beide Grids. Siehe "Konfigurieren Sie Single Sign-On".

3. "Erstellen Sie dieselbe Administratorgruppe" Auf beiden Rastern durch Importieren derselben Verbundgruppe.

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

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

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

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

Schritte

1. Konfigurieren Sie dieselbe Identitätsquelle für beide Raster. Siehe "Verwenden Sie den Identitätsverbund".
2. Optional, wenn eine föderierte Gruppe erste Root-Zugriffsberechtigungen für die Quell- und Zielmandantenkonten hat, "Erstellen Sie dieselbe Administratorgruppe" Auf beiden Rastern durch Importieren derselben Verbundgruppe.

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

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

Zulässiges S3-Mandantenkonto erstellen

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

Schritte

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

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

2. Neues S3-Mandantenkonto in diesem Grid erstellen
3. Weisen Sie die Berechtigung **Grid Federation connection** zu.
4. Wenn das Mandantenkonto seine eigenen föderierten Benutzer verwalten wird, weisen Sie die Berechtigung **eigene Identitätsquelle verwenden** zu.

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

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

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

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

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

Zulässiger Mandantenkonto-Workflow

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

Schritte

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

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

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

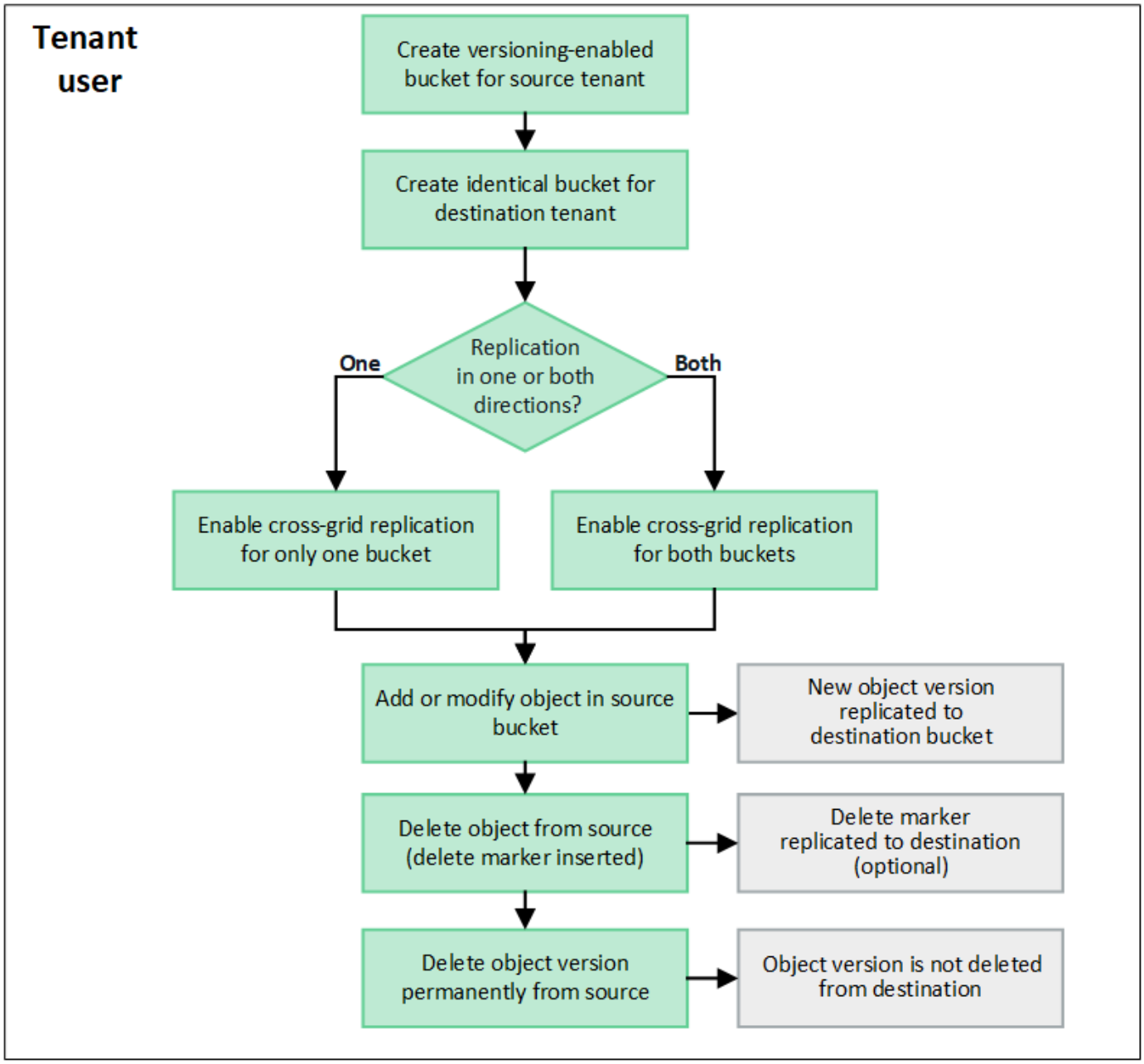
Informationen zum Workflow zulässiger Mandantenkonten und zum Klonen von Gruppen, Benutzern und S3-Zugriffsschlüsseln finden Sie unter "Klonen von Mandantengruppen und Benutzern" Und "Klonen von S3-Zugriffsschlüsseln mithilfe der API".

Was ist Grid-übergreifende Replizierung?

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

Workflow für Grid-übergreifende Replizierung

Das Workflow-Diagramm fasst die Schritte zur Konfiguration der Grid-übergreifenden Replikation zwischen Buckets auf zwei Grids zusammen.



Anforderungen für die Grid-übergreifende Replizierung

Wenn ein Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat, um eine oder mehrere zu verwenden "Netzverbundverbindungen", Ein Mandantenbenutzer mit Root-Zugriffsberechtigung kann identische Buckets in den entsprechenden Mandantenkonten in jedem Grid erstellen. Diese Buckets:

- Muss denselben Namen und dieselbe Region haben
- Versionierung muss aktiviert sein
- S3-Objektsperre muss deaktiviert sein
- Muss leer sein

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

Weitere Informationen .

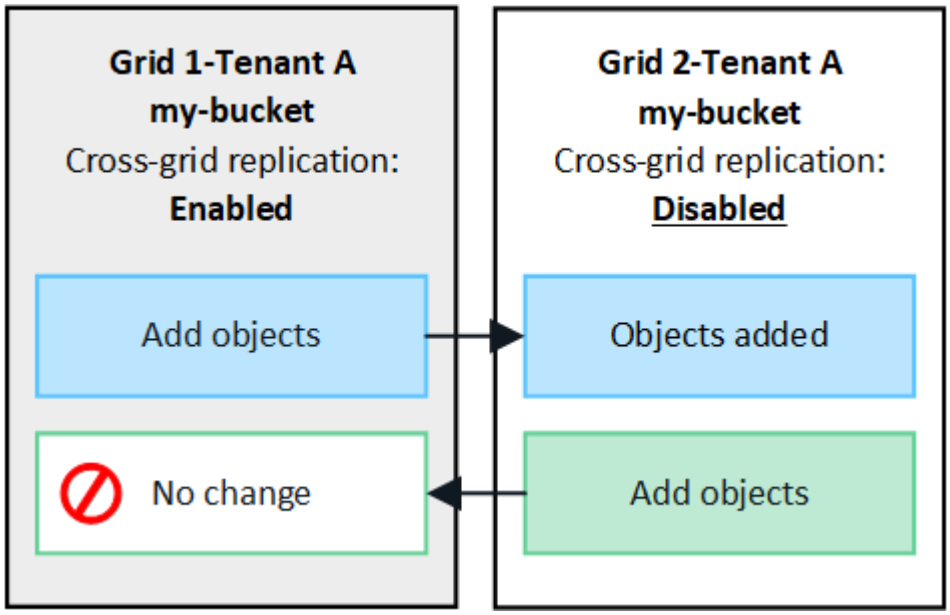
"Grid-übergreifende Replizierung managen"

Funktionsweise der Grid-übergreifenden Replizierung

Die Grid-übergreifende Replizierung kann so konfiguriert werden, dass sie in eine Richtung oder in beide Richtungen erfolgt.

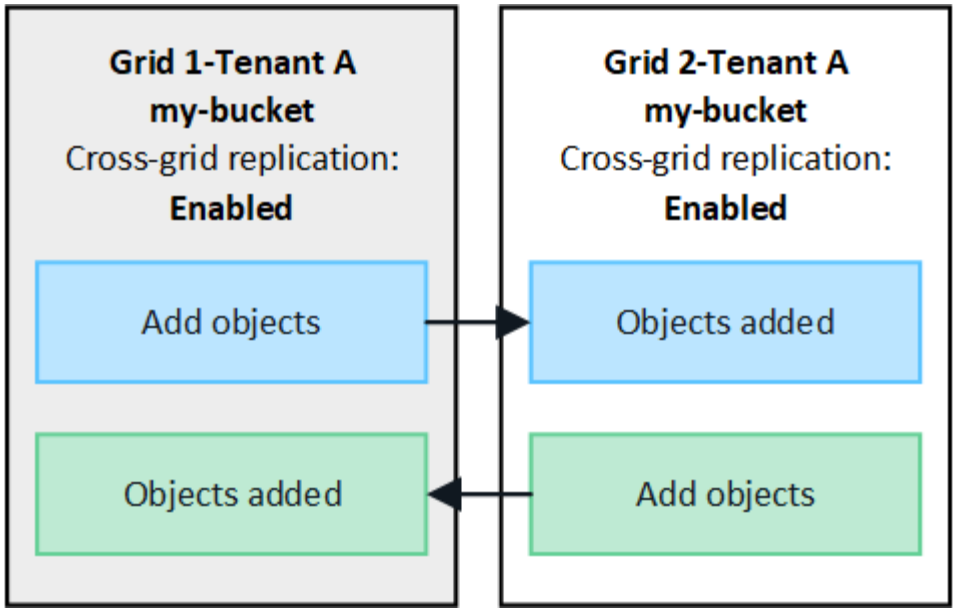
Replikation in eine Richtung

Wenn Sie die Grid-übergreifende Replizierung für einen Bucket nur in einem Grid aktivieren, werden die diesem Bucket (Quell-Bucket) hinzugefügten Objekte in den entsprechenden Bucket auf dem anderen Grid (dem Ziel-Bucket) repliziert. Zum Ziel-Bucket hinzugefügte Objekte werden jedoch nicht zurück in die Quelle repliziert. In der Abbildung ist die Grid-übergreifende Replizierung für aktiviert `my-bucket` Von Raster 1 bis Raster 2, aber nicht in die andere Richtung aktiviert.



Replikation in beide Richtungen

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



Was passiert, wenn Objekte aufgenommen werden?

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

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

   Der S3-Client kann den Replikationsstatus eines Objekts durch Ausgabe einer GET Object- oder HEAD Object-Anforderung überprüfen. Die Antwort bezieht sich auf ein StorageGRID-spezifisches `x-ntap-sg-cgr-replication-status` Antwortheader, der einen der folgenden Werte hat: Der S3-Client kann den Replikationsstatus eines Objekts überprüfen, indem er eine GET Object- oder HEAD Object-Anforderung ausgibt. Die Antwort bezieht sich auf ein StorageGRID-spezifisches `x-ntap-sg-cgr-replication-status` Antwortheader, der einen der folgenden Werte enthält:

Raster	Replikationsstatus
Quelle	• **SUCCESS**: Die Replikation war für alle Grid-Verbindungen erfolgreich. • **AUSSTEHEND**: Das Objekt wurde nicht auf mindestens eine Grid-Verbindung repliziert. • **FAILURE**: Die Replikation steht nicht für eine Netzverbindung aus und mindestens eine ist mit einem dauerhaften Fehler ausgefallen. Ein Benutzer muss den Fehler beheben.
Ziel	**REPLIKAT**: Das Objekt wurde aus dem Quellraster repliziert.

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

2. StorageGRID verwendet die aktiven ILM-Richtlinien der einzelnen Grids für das Management der Objekte wie bei jedem anderen Objekt. Objekt A in Tabelle 1 kann beispielsweise als zwei replizierte Kopien gespeichert und für immer aufbewahrt werden, während die Kopie von Objekt A, das in Tabelle 2 repliziert

wurde, unter Verwendung von 2+1 Erasure Coding gespeichert und nach drei Jahren gelöscht werden kann.

Was passiert, wenn Objekte gelöscht werden?

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

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

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

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

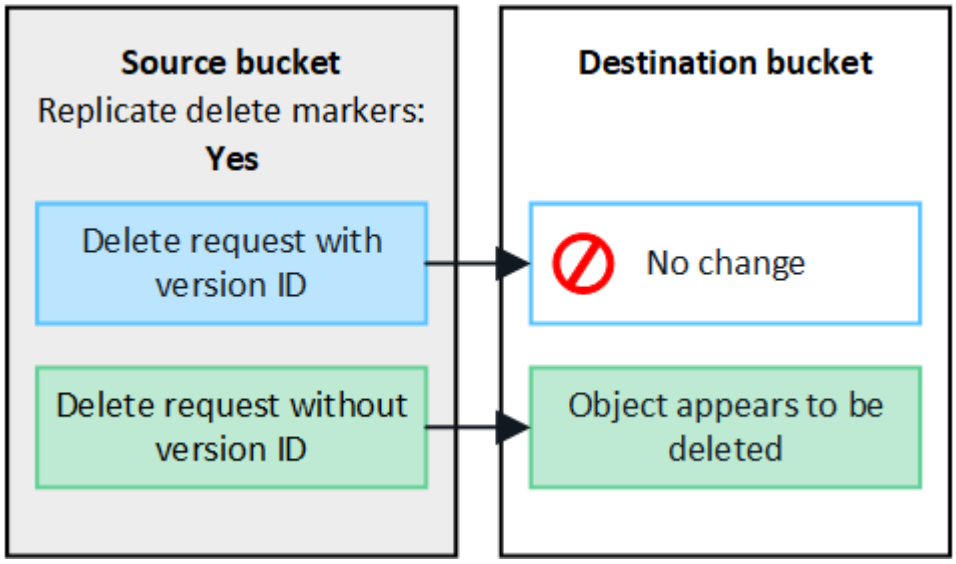
- Wenn ein S3-Client eine Löschanfrage mit einer Versions-ID ausstellt, wird diese Version des Objekts dauerhaft entfernt. Dem Bucket wurde keine Löschmarkierung hinzugefügt.
- Wenn ein S3-Client eine Löschanfrage ausstellt, die keine Versions-ID enthält, löscht StorageGRID keine Objektversionen. Stattdessen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

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

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

In der Abbildung wurde **replicate delete Markers** auf **Yes** gesetzt, wenn "Die Grid-übergreifende Replizierung wurde aktiviert". Löschanforderungen für den Quell-Bucket, der eine Versions-ID enthält, löschen keine

Objekte aus dem Ziel-Bucket. Löschanforderungen für den Quell-Bucket, die keine Versions-ID enthalten, werden angezeigt, um Objekte im Ziel-Bucket zu löschen.



Wenn Sie Objektlöschungen zwischen den Rastern synchron halten möchten, erstellen Sie entsprechende "S3 Lifecycle-Konfigurationen" Für die Eimer auf beiden Rastern.

Wie verschlüsselte Objekte repliziert werden

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

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

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

Um die Standardverschlüsselung für einen Bucket zu verwenden, verwenden Sie eine PUT-Bucket-Verschlüsselungsanforderung und legen Sie die fest `SSEAlgorithm` Parameter an `AES256`. Die Verschlüsselung auf Bucket-Ebene gilt für alle Objekte, die ohne den aufgenommen wurden `x-amz-server-side-encryption` Kopfzeile der Anfrage. Siehe "Operationen auf Buckets".

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

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

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

1. Verwenden Sie die `x-amz-server-side-encryption` Aufnahme-Header, falls vorhanden.
2. Wenn kein Ingest Header vorhanden ist, verwenden Sie gegebenenfalls die Standardeinstellung für die Bucket-Verschlüsselung.
3. Wenn keine Bucket-Einstellung konfiguriert ist, verwenden Sie, sofern konfiguriert, die Verschlüsselungseinstellung für das gesamte Grid.
4. Wenn keine rasterweite Einstellung vorhanden ist, verschlüsseln Sie das Quellobjekt nicht.

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

1. Verwenden Sie dieselbe Verschlüsselung wie das Quellobjekt, es sei denn, dieses Objekt verwendet AES-128-Verschlüsselung.
2. Wenn das Quellobjekt nicht verschlüsselt ist oder AES-128 verwendet wird, verwenden Sie, sofern konfiguriert, die Standardeinstellung für die Verschlüsselung des Ziel-Buckets.
3. Wenn der Ziel-Bucket keine Verschlüsselungseinstellung hat, verwenden Sie die gitterweite Verschlüsselungseinstellung des Ziels, sofern konfiguriert.
4. Wenn keine rasterweite Einstellung vorhanden ist, verschlüsseln Sie das Zielobjekt nicht.

PUT Objekt-Tagging und DELETE Objekt-Tagging werden nicht unterstützt

PUT-Anforderungen für Objekt-Tagging und DELETE Objekt-Tagging werden nicht für Objekte in Buckets unterstützt, für die die Grid-übergreifende Replizierung aktiviert ist.

Wenn ein S3-Client eine PUT-Objekt-Tagging- oder DELETE Objekt-Tagging-Anfrage ausstellt, `501 Not Implemented` Wird zurückgegeben. Die Meldung lautet `Put(Delete) ObjectTagging is not available for buckets that have cross-grid replication configured`.

Wie segmentierte Objekte repliziert werden

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

Vergleichen Sie Grid-Replizierung und CloudMirror Replizierung

Überprüfen Sie während der Nutzung von Grid Federation die Ähnlichkeiten und Unterschiede zwischen "Grid-übergreifende Replizierung" Und das "StorageGRID CloudMirror Replikationsservice".

	Grid-übergreifende Replizierung	CloudMirror Replikationsservice
Was ist der primäre Zweck?	Ein StorageGRID System fungiert als Disaster Recovery-System. Objekte in einem Bucket können zwischen den Grids in eine oder beide Richtungen repliziert werden.	Ermöglicht einem Mandanten, automatisch Objekte aus einem Bucket in StorageGRID (Quelle) in einen externen S3-Bucket (Ziel) zu replizieren Bei der CloudMirror-Replizierung wird eine unabhängige Kopie eines Objekts in einer unabhängigen S3-Infrastruktur erstellt. Diese unabhängige Kopie wird nicht als Backup verwendet, sondern häufig weiter in der Cloud verarbeitet.
Wie ist es eingerichtet?	1. Konfigurieren Sie eine Grid Federation-Verbindung zwischen zwei Grids. 2. Fügen Sie neue Mandantenkonten hinzu, die automatisch in der anderen Tabelle geklont werden. 3. Fügen Sie neue Mandantengruppen und -Benutzer hinzu, die ebenfalls geklont werden. 4. Erstellen Sie entsprechende Buckets in jedem Grid und ermöglichen Sie die Grid-übergreifende Replizierung in eine oder beide Richtungen.	1. Ein Mandantenbenutzer konfiguriert die CloudMirror-Replizierung mithilfe des Tenant Manager oder der S3-API durch Definition eines CloudMirror-Endpunkts (IP-Adresse, Anmeldeinformationen usw.). 2. Jeder Bucket dieses Mandantenkontos kann so konfiguriert werden, dass er auf den CloudMirror-Endpunkt verweisen kann.
Wer ist für die Einrichtung zuständig?	• Ein Grid-Administrator konfiguriert die Verbindung und die Mandanten. • Mandantenbenutzer konfigurieren die Gruppen, Benutzer, Schlüssel und Buckets.	Normalerweise wird ein Mandantenbenutzer verwendet.
Was ist das Ziel?	Ein entsprechender und identischer S3-Bucket auf dem anderen StorageGRID-System in der Grid-Federation-Verbindung.	• Kompatible S3-Infrastruktur (einschließlich Amazon S3) • Google Cloud Platform (GCP)
Ist eine Objektversionierung erforderlich?	Ja, sowohl in den Quell- als auch in den Ziel-Buckets muss die Objektversionierung aktiviert sein.	Nein, die CloudMirror Replizierung unterstützt beliebige Kombinationen aus unversionierten und versionierten Buckets sowohl am Quell- als auch am Zielsystem.

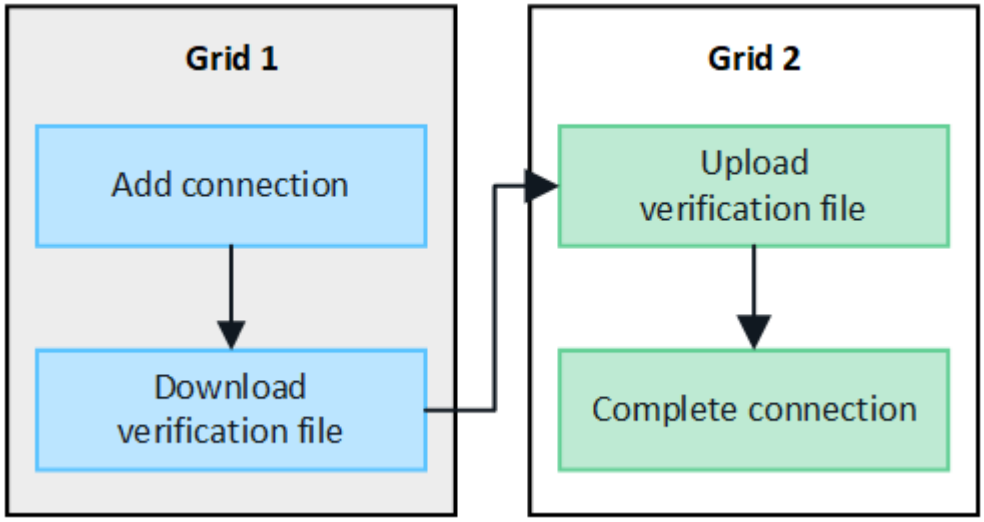
	Grid-übergreifende Replizierung	CloudMirror Replikationsservice
Was bewirkt, dass Objekte zum Ziel verschoben werden?	Objekte werden automatisch repliziert, wenn sie zu einem Bucket hinzugefügt werden, für den die Grid-übergreifende Replizierung aktiviert ist.	Objekte werden automatisch repliziert, wenn sie zu einem Bucket hinzugefügt werden, der mit einem CloudMirror-Endpunkt konfiguriert wurde. Objekte, die sich im Quell-Bucket befanden, bevor der Bucket mit dem CloudMirror-Endpunkt konfiguriert wurde, werden nur repliziert, wenn sie geändert wurden.
Wie werden Objekte repliziert?	Grid-übergreifende Replizierung erstellt versionierte Objekte und repliziert die Versions-ID vom Quell-Bucket auf den Ziel-Bucket. Dadurch kann die Versionsreihenfolge über beide Raster hinweg beibehalten werden.	Bei der CloudMirror Replizierung sind keine Buckets mit Versionierung erforderlich – CloudMirror kann also nur die Bestellung für einen Schlüssel innerhalb eines Standorts aufrechterhalten. Es gibt keine Garantie, dass die Bestellung für Anfragen an ein Objekt an einem anderen Standort aufrechterhalten wird.
Was ist, wenn ein Objekt nicht repliziert werden kann?	Das Objekt befindet sich in der Warteschlange zur Replizierung, vorbehaltlich der Speichergrenzen für Metadaten.	Das Objekt wird zur Replikation in die Warteschlange eingereiht, vorbehaltlich der Beschränkungen für Plattformdienste (siehe "Empfehlungen für die Nutzung von Plattform-Services").
Werden die System-Metadaten des Objekts repliziert?	Ja, wenn ein Objekt in das andere Grid repliziert wird, werden auch die Systemmetadaten repliziert. Die Metadaten sind auf beiden Grids identisch.	Nein, wenn ein Objekt in den externen Bucket repliziert wird, werden die Systemmetadaten aktualisiert. Die Metadaten unterscheiden sich je nach Zeitpunkt der Aufnahme und dem Verhalten der unabhängigen S3-Infrastruktur zwischen den Standorten.
Wie werden Objekte abgerufen?	Applikationen können Objekte abrufen oder lesen, indem sie an den Bucket auf beiden Grid eine Anfrage stellen.	Applikationen können Objekte abrufen oder lesen, indem sie eine Anfrage entweder an StorageGRID oder am S3-Ziel stellen. Angenommen, Sie verwenden CloudMirror Replizierung, um Objekte auf eine Partnerorganisation zu spiegeln. Der Partner kann mithilfe eigener Applikationen Objekte direkt vom S3-Ziel lesen oder aktualisieren. Die Verwendung von StorageGRID ist nicht erforderlich.

	Grid-übergreifende Replizierung	CloudMirror Replikationsservice
Was passiert, wenn ein Objekt gelöscht wird?	• Löschanforderungen, die eine Versions-ID enthalten, werden nie in das Zielraster repliziert. • Löschanforderungen, die keine Versions-ID enthalten, fügen dem Quell-Bucket eine Löschmarkierung hinzu, die optional in das Zielraster repliziert werden kann. • Wenn die Grid-übergreifende Replizierung nur für eine Richtung konfiguriert ist, können Objekte im Ziel-Bucket gelöscht werden, ohne die Quelle zu beeinträchtigen.	Die Ergebnisse variieren je nach Versionsstatus der Quell- und Ziel-Buckets (die nicht identisch sein müssen): • Wenn beide Buckets versioniert sind, wird bei einer Löschanforderung an beiden Standorten eine Löschmarkierung hinzugefügt. • Wenn nur der Quell-Bucket versioniert ist, fügt eine Löschanforderung der Quelle eine Löschmarkierung hinzu, nicht jedoch dem Ziel. • Wenn kein Bucket versioniert ist, wird das Objekt durch eine Löschanforderung aus der Quelle, aber nicht aus dem Ziel gelöscht. Ebenso können Objekte im Ziel-Bucket gelöscht werden, ohne dass die Quelle beeinträchtigt wird.

Erstellen von Grid Federation-Verbindungen

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

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



Bevor Sie beginnen

- Sie haben die geprüft "Überlegungen und Anforderungen" Zur Konfiguration von Grid Federation-Verbindungen.

- Wenn Sie für jedes Raster statt für IP- oder VIP-Adressen vollständig qualifizierte Domänennamen (FQDNs) verwenden möchten, wissen Sie, welche Namen verwendet werden sollen, und Sie haben bestätigt, dass der DNS-Server für jedes Raster die entsprechenden Einträge enthält.
- Sie verwenden ein "Unterstützter Webbrowser".
- Sie müssen über die Root-Zugriffsberechtigung und die Provisionierungs-Passphrase für beide Grids verfügen.

Verbindung hinzufügen

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

Schritte

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

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

Feld	Beschreibung
FQDN oder IP für das andere Raster	Eine der folgenden Optionen: • Der FQDN des Rasters, mit dem Sie eine Verbindung herstellen möchten • Eine VIP-Adresse einer HA-Gruppe im anderen Raster • Eine IP-Adresse eines Admin-Knotens oder Gateway-Knotens im anderen Grid. Die IP kann sich auf jedem Netzwerk befinden, das das Quellraster erreichen kann.

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

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

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

   Diese Datei enthält Geheimnisse (maskiert als *****) Und andere sensible Daten und müssen sicher gespeichert und übermittelt werden.

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

Vollständige Verbindung

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

Schritte

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

   Die Details für die Verbindung werden angezeigt.

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

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

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

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

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

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

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

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

Nachdem Sie fertig sind

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

Grid-Verbindungen verwalten

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

Bevor Sie beginnen

- Sie sind auf beiden Rastergitten mit einem beim Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie verfügen über die Root-Zugriffsberechtigung für das Raster, bei dem Sie angemeldet sind.

Bearbeiten einer Verbindung zum Grid Federation

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

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

Beginnen Sie mit der Bearbeitung der Verbindung

Schritte

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

   Beim Bearbeiten einer Grid-Federation-Verbindung versucht StorageGRID, eine Datei „`Candidate Configuration`“ auf allen Admin-Knoten im ersten Raster zu speichern. Wenn diese Datei nicht in allen Admin-Knoten gespeichert werden kann, wird eine Warnmeldung angezeigt, wenn Sie **Speichern und Testen** auswählen.

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

   Menü „Aktionen“

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

   Detailseite

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

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

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

7. Wählen Sie **Überprüfungsdatei herunterladen**.

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

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

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

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

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

11. Versorgen *connection-name*`.grid-federation` Datei an den Grid-Administrator für das andere Grid.

Schließen Sie die Bearbeitung der Verbindung ab

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

Schritte

1. Melden Sie sich über den primären Admin-Knoten beim Grid-Manager an.
2. Wählen Sie **CONFIGURATION** > **System** > **Grid Federation**.
3. Wählen Sie **Upload Verification file**, um auf die Upload-Seite zuzugreifen.
4. Wählen Sie **Überprüfungsdatei hochladen**. Navigieren Sie dann zu der Datei, die aus dem ersten Raster heruntergeladen wurde, und wählen Sie sie aus.
5. Geben Sie die Provisionierungs-Passphrase für das Raster ein, bei dem Sie derzeit angemeldet sind.
6. Wählen Sie **Speichern und testen**.

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

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

Testen einer Netzverbundverbindung

Schritte

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

Menü „Aktionen“

a. Wählen Sie das Optionsfeld für die Verbindung aus.

b. Wählen Sie **Actions** > **Test**.

Detailseite

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

b. Wählen Sie **Verbindung testen**.

4. Überprüfen Sie den Verbindungsstatus:

Verbindungsstatus	Beschreibung
Verbunden	Beide Netze sind angeschlossen und kommunizieren normal.
Fehler	Die Verbindung befindet sich in einem Fehlerzustand. Beispielsweise ist ein Zertifikat abgelaufen oder ein Konfigurationswert ist nicht mehr gültig.
Bearbeitung ausstehend	Sie haben die Verbindung in diesem Raster bearbeitet, aber die Verbindung verwendet weiterhin die vorhandene Konfiguration. Um die Bearbeitung abzuschließen, laden Sie die neue Überprüfungsdatei in das andere Raster hoch.
Warten auf Verbindung	Sie haben die Verbindung in diesem Raster konfiguriert, aber die Verbindung wurde auf dem anderen Raster nicht abgeschlossen. Laden Sie die Überprüfungsdatei von diesem Raster herunter, und laden Sie sie in das andere Raster hoch.
Unbekannt	Die Verbindung befindet sich in einem unbekannten Zustand, möglicherweise aufgrund eines Netzwerkproblems oder eines Offline-Knotens.

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

Verbindungszertifikate drehen

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

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

Schritte

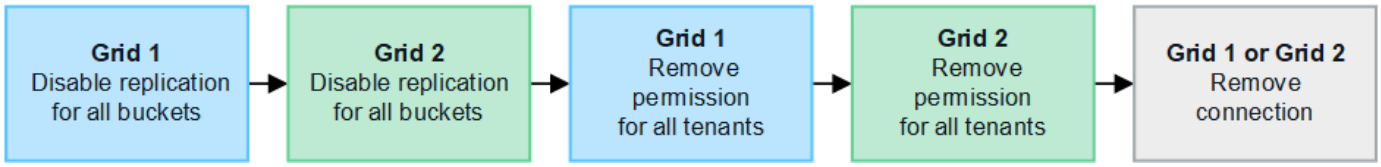
1. Melden Sie sich über den primären Admin-Node auf beiden Grids beim Grid-Manager an.
2. Wählen Sie **CONFIGURATION** > **System** > **Grid Federation**.

3. Wählen Sie auf einer der Registerkarten auf der Seite Grid Federation den Verbindungsnamen aus, um die zugehörigen Details anzuzeigen.
4. Wählen Sie die Registerkarte **Zertifikate** aus.
5. Wählen Sie **Zertifikate drehen**.
6. Geben Sie an, wie viele Tage die neuen Zertifikate gültig sein sollen.
7. Geben Sie die Provisionierungs-Passphrase für das Raster ein, bei dem Sie angemeldet sind.
8. Wählen Sie **Zertifikate drehen**.
9. Wiederholen Sie diese Schritte bei Bedarf auf dem anderen Raster der Verbindung.

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

Entfernen Sie eine Netzverbundverbindung

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



Beachten Sie vor dem Entfernen einer Verbindung Folgendes:

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

Deaktivieren Sie die Replizierung für alle Mandanten-Buckets

Schritte

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

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

Berechtigung für jeden Mandanten entfernen

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

Schritte

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

Verbindung entfernen

Schritte

1. Wenn keine Mieter in einem der beiden Raster die Verbindung verwenden, wählen Sie **Entfernen**.
2. Überprüfen Sie die Bestätigungsmeldung, und wählen Sie **Entfernen**.
   - Wenn die Verbindung entfernt werden kann, wird eine Erfolgsmeldung angezeigt. Die Netzverbundverbindung wird nun aus beiden Grids entfernt.
   - Wenn die Verbindung nicht entfernt werden kann (z. B. wird sie noch verwendet oder es liegt ein Verbindungsfehler vor), wird eine Fehlermeldung angezeigt. Sie können eine der folgenden Aktionen ausführen:
     - Beheben Sie den Fehler (empfohlen). Siehe "Fehler beim Grid-Verbund beheben".
     - Entfernen Sie die Verbindung mit Gewalt. Siehe nächster Abschnitt.

Entfernen Sie eine Verbindung zum Grid-Verbund mit Gewalt

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

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

Schritte

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

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

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

Verwalten Sie die zulässigen Mandanten für den Grid-Verbund

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

Bevor Sie beginnen

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

Erstellen Sie eine zulässige Serviceeinheit

Wenn Sie einem Mandantenkonto die Verwendung einer Grid-Federation-Verbindung für den Account-Klon und die Grid-übergreifende Replizierung erlauben möchten, befolgen Sie die allgemeinen Anweisungen auf "Erstellen Sie einen neuen S3-Mandanten" Und beachten Sie Folgendes:

- Sie können die Serviceeinheit aus jedem Raster der Verbindung erstellen. Das Raster, in dem ein Mandant erstellt wird, ist das Quellraster des *Mandanten*.
- Der Status der Verbindung muss **connected** sein.
- Sie können nur die Berechtigung **Grid Federation connection** verwenden auswählen, wenn Sie einen neuen S3-Mandanten erstellen; Sie können diese Berechtigung nicht aktivieren, wenn Sie einen vorhandenen Mandanten bearbeiten.
- Wenn der neue Mandant im ersten Grid gespeichert wird, wird ein identischer Mandant automatisch in das andere Grid repliziert. Das Grid, in dem der Mandant repliziert wird, ist das Zielraster des *Mandanten*.
- Die Mandanten in beiden Grids haben die gleiche 20-stellige Konto-ID, den gleichen Namen, die gleiche Beschreibung, das gleiche Kontingent und die gleichen Berechtigungen. Optional können Sie das Feld **Beschreibung** verwenden, um zu ermitteln, welcher Quellmandant und welcher Zielmandant ist. Beispielsweise wird diese Beschreibung für einen Mandanten, der in Grid 1 erstellt wurde, auch für den Mandanten angezeigt, der in Grid 2 repliziert wurde: „`dieser Mandant wurde in Grid 1 erstellt.`“
- Aus Sicherheitsgründen wird das Kennwort für einen lokalen Root-Benutzer nicht in das Zielraster kopiert.

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

- Nachdem der neue Mandant auf beiden Grids verfügbar ist, können Mandantenbenutzer die folgenden Aufgaben durchführen:
  - Erstellen Sie im Quellraster des Mandanten Gruppen und lokale Benutzer, die automatisch im Zielraster des Mandanten geklont werden. Siehe "Klonen von Mandantengruppen und Benutzern".
  - Erstellen neuer S3-Zugriffsschlüssel, die optional im Zielraster des Mandanten geklont werden können Siehe "Klonen von S3-Zugriffsschlüsseln mithilfe der API".

- Erstellen Sie auf beiden Grids in der Verbindung identische Buckets und ermöglichen Sie die Grid-übergreifende Replizierung in eine oder beide Richtungen. Siehe "Grid-übergreifende Replizierung managen".

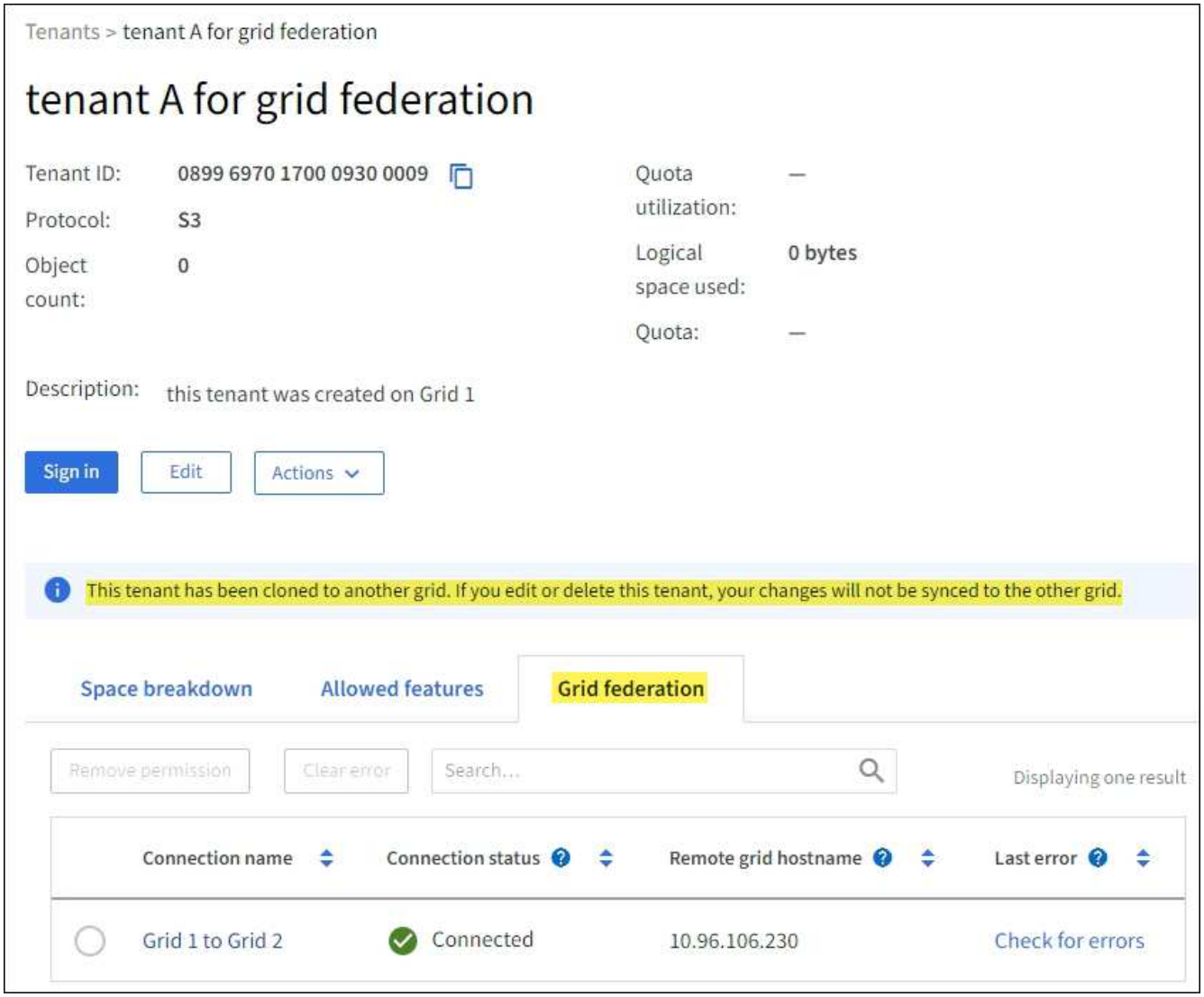
Zeigen Sie eine zulässige Serviceeinheit an

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

Schritte

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

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



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

Bearbeiten Sie eine zulässige Serviceeinheit

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

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

Löschen Sie eine zulässige Serviceeinheit

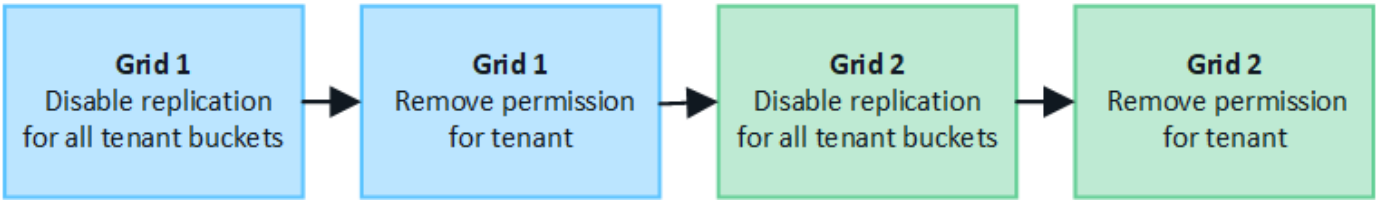
Wenn Sie einen Mieter entfernen müssen, der über die Berechtigung **Grid Federation connection** verfügt, befolgen Sie die allgemeinen Anweisungen für "Löschen eines Mandantenkontos" Und beachten Sie Folgendes:

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

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

Remove Use Grid Federation connection permission

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



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

- Das Entfernen der Berechtigung **use Grid Federation connection** von einem Mieter ist eine permanente Aktion. Sie können die Berechtigung für diesen Mandanten nicht erneut aktivieren.
- Sie können die Berechtigung **use Grid Federation connection** nicht entfernen, wenn eine der Buckets des Mandanten Grid-übergreifende Replikation aktiviert hat. Das Mandantenkonto muss zunächst die Grid-übergreifende Replizierung für alle Buckets deaktivieren.
- Wenn Sie die Berechtigung **Grid Federation connection** verwenden entfernen, werden keine Elemente gelöscht, die bereits zwischen den Rastern repliziert wurden. So werden beispielsweise alle Mandantenbenutzer, -Gruppen und -Objekte, die auf beiden Grids vorhanden sind, nicht aus beiden Grids gelöscht, wenn die Berechtigung des Mandanten entfernt wird. Wenn Sie diese Elemente löschen möchten, müssen Sie sie manuell aus beiden Rastern löschen.

Bevor Sie beginnen

- Sie verwenden ein "Unterstützter Webbrowser".
- Sie verfügen über die Root-Zugriffsberechtigung für beide Raster.

Deaktivieren Sie die Replizierung für Mandanten-Buckets

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

Schritte

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

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

Berechtigung für Serviceeinheit entfernen

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

Schritte

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

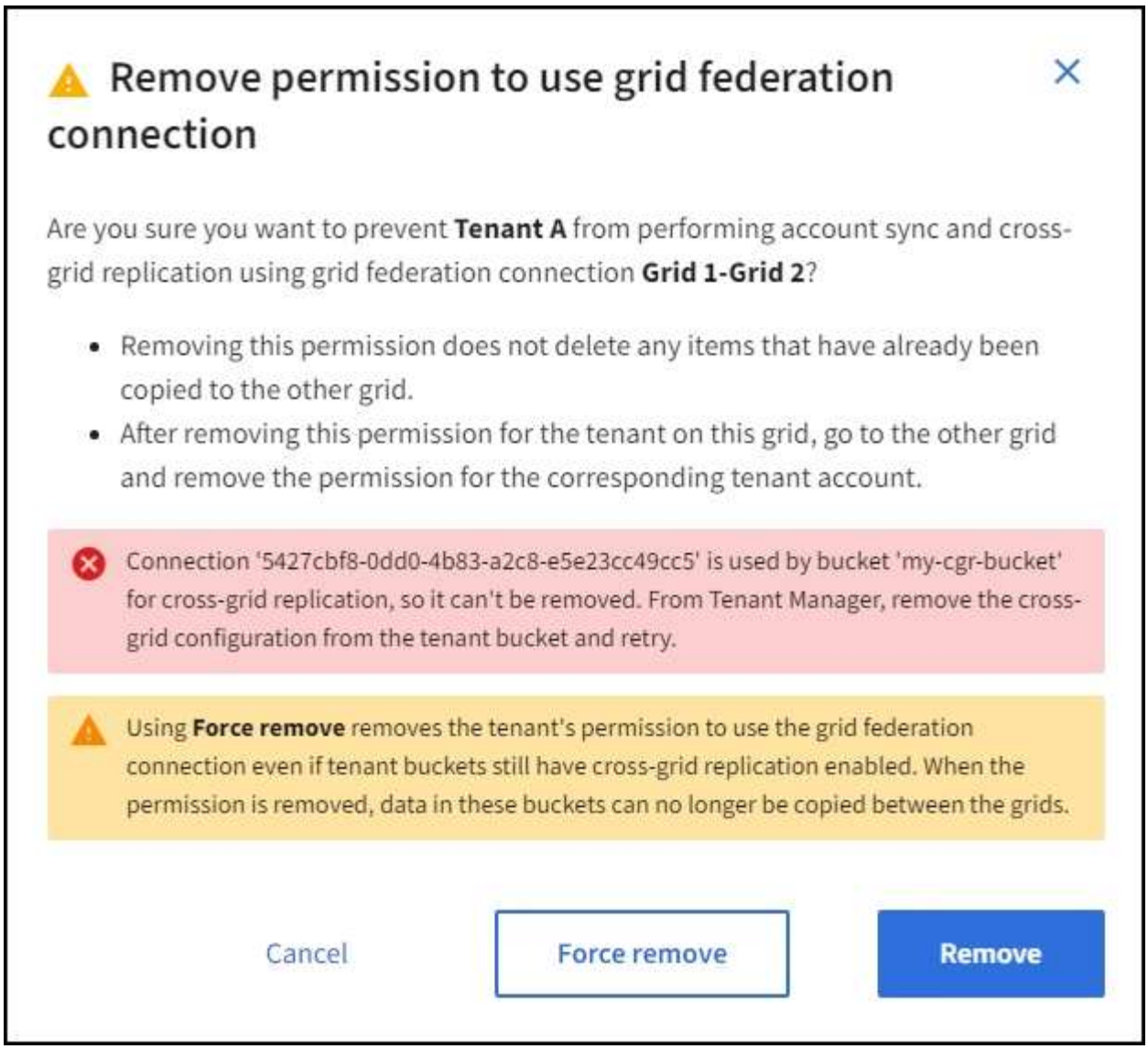
Seite „Grid Federation“

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

Mandanten werden gestartet

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

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



Sie können eine der folgenden Aktionen ausführen:

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

4. Gehen Sie zum anderen Raster, und wiederholen Sie diese Schritte, um die Berechtigung für denselben Mandanten auf dem anderen Raster zu entfernen.

Entfernen Sie die Berechtigung mit Gewalt

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

Bevor Sie die Erlaubnis eines Mandanten gewaltsam entfernen, beachten Sie die allgemeinen Überlegungen für Entfernen der Berechtigung Sowie folgende weitere Überlegungen anzustellen:

- Wenn Sie die Berechtigung **use Grid Federation connection** per Force entfernen, werden alle Objekte, die eine Replikation auf das andere Grid ausstehen (aufgenommen, aber noch nicht repliziert), weiterhin

repliziert. Um zu verhindern, dass diese in-Process-Objekte den Ziel-Bucket erreichen, müssen Sie auch die Berechtigung des Mandanten für das andere Raster entfernen.

- Alle Objekte, die in den Quell-Bucket aufgenommen wurden, nachdem Sie die Berechtigung **Grid Federation Connection** verwenden entfernt haben, werden niemals in den Ziel-Bucket repliziert.

Schritte

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

   Eine Erfolgsmeldung wird angezeigt. Dieser Mandant kann die Grid Federation-Verbindung nicht mehr verwenden.

7. Gehen Sie bei Bedarf zum anderen Raster, und wiederholen Sie diese Schritte, um die Berechtigung für das gleiche Mandantenkonto im anderen Raster zu erzwingen. Sie sollten diese Schritte beispielsweise auf dem anderen Raster wiederholen, um zu verhindern, dass in-Process-Objekte den Ziel-Bucket erreichen.

Fehler beim Grid-Verbund beheben

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

Warnungen und Fehler der Grid Federation-Verbindung

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

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

Warnmeldung bei Ausfall der Grid-Verbindung

Problem

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

Details

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

Empfohlene Maßnahmen

1. Überprüfen Sie die Einstellungen auf der Seite „Grid Federation“ für beide Raster. Vergewissern Sie sich, dass alle Werte korrekt sind. Siehe "Grid-Verbindungen verwalten".
2. Überprüfen Sie die für die Verbindung verwendeten Zertifikate. Stellen Sie sicher, dass keine Warnungen für abgelaufene Grid Federation-Zertifikate vorhanden sind und dass die Details für jedes Zertifikat gültig sind. Weitere Informationen finden Sie in den Anweisungen für rotierende Verbindungszertifikate unter "Grid-Verbindungen verwalten".
3. Vergewissern Sie sich, dass alle Admin- und Gateway-Nodes in beiden Grids online und verfügbar sind. Beheben Sie alle Warnmeldungen, die sich auf diese Knoten auswirken könnten, und versuchen Sie es

erneut.

4. Wenn Sie einen vollständig qualifizierten Domänennamen (FQDN) für das lokale oder Remote-Grid angegeben haben, vergewissern Sie sich, dass der DNS-Server online und verfügbar ist. Siehe "Was ist Grid Federation?" Für Netzwerk-, IP-Adresse- und DNS-Anforderungen.

Ablauf der Warnmeldung für das Grid-Verbundzertifikat

Problem

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

Details

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

Empfohlene Maßnahmen

Weitere Informationen finden Sie in den Anweisungen für rotierende Verbindungszertifikate unter "Grid-Verbindungen verwalten".

Fehler beim Bearbeiten einer Verbindung zum Grid Federation

Problem

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

Details

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

Empfohlene Maßnahmen

1. Wählen Sie aus dem Raster, mit dem Sie die Verbindung bearbeiten, **KNOTEN** aus.
2. Vergewissern Sie sich, dass alle Admin-Nodes für dieses Grid online sind.
3. Wenn Knoten offline sind, schalten Sie sie wieder online und versuchen Sie erneut, die Verbindung zu bearbeiten.

Fehler beim Klonen des Kontos

Keine Anmeldung bei einem geklonten Mandantenkonto möglich

Problem

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

Details

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

Empfohlene Maßnahmen

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

Bevor ein geklonter lokaler Benutzer sich im Zielraster des Mandanten anmelden kann, muss der Root-Benutzer für den geklonten Mandanten ein Passwort für den Benutzer im Zielraster hinzufügen. Anweisungen hierzu finden Sie unter "Managen Sie lokale Benutzer" In der Anleitung zur Verwendung des Tenant Managers.

Mandant wird ohne Klon erstellt

Problem

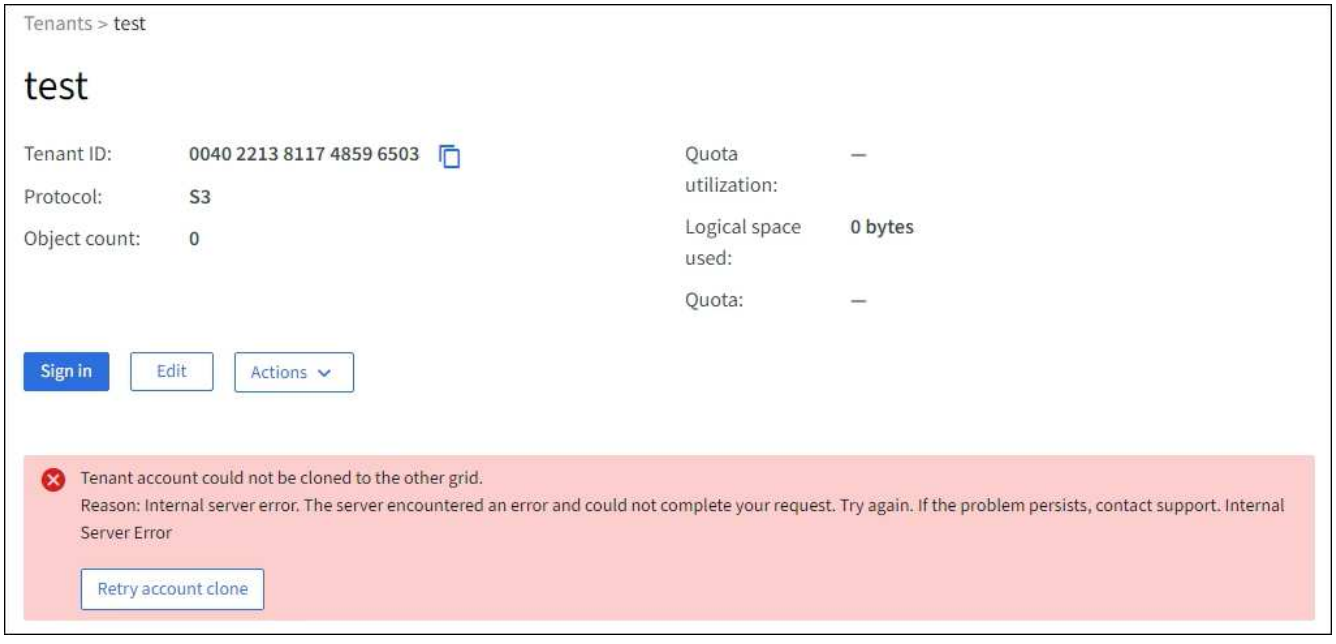
Sie sehen die Meldung “Tenant created without a Clone”, nachdem Sie einen neuen Tenant mit der Berechtigung **use Grid Federation connection** erstellt haben.

Details

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

Empfohlene Maßnahmen

1. Überprüfen Sie den in der Fehlermeldung aufgeführten Grund, und beheben Sie alle Netzwerk- oder anderen Probleme, die möglicherweise die Funktion der Verbindung verhindern. Siehe Warnmeldungen und Fehler bei der Grid-Verbundverbindung.
2. Befolgen Sie die Anweisungen, um eine Netzverbundverbindung in zu testen "Grid-Verbindungen verwalten" Um zu bestätigen, dass das Problem behoben wurde.
3. Wählen Sie im Quellraster des Mandanten **TENANTS** aus.
4. Suchen Sie das Mandantenkonto, das nicht geklont werden konnte.
5. Wählen Sie den Namen der Serviceeinheit aus, um die Detailseite anzuzeigen.
6. Wählen Sie **Kontoklone wiederholen**.

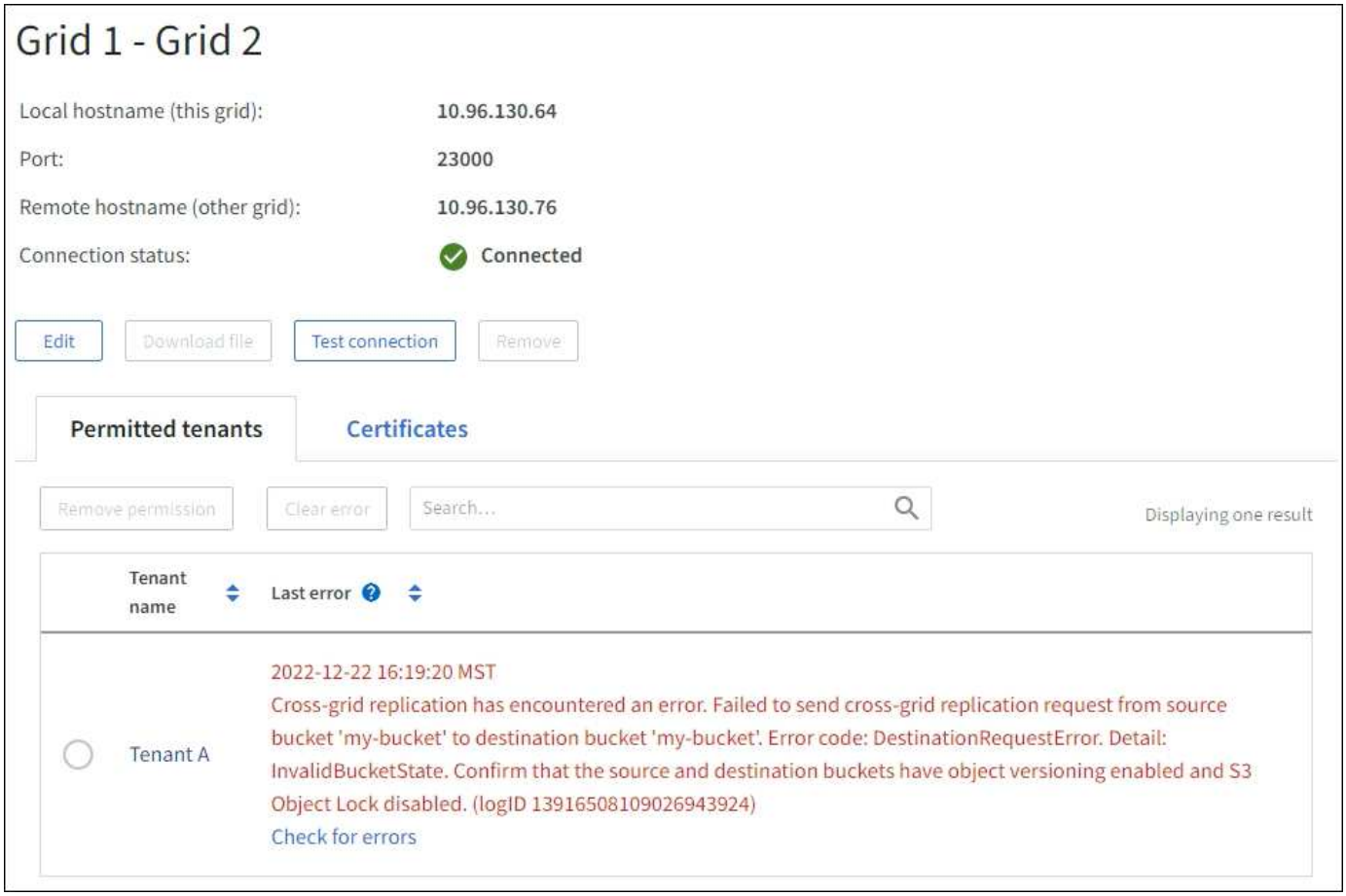


Wenn der Fehler behoben wurde, wird das Mandantenkonto jetzt in das andere Raster geklont.

Letzter Fehler für Verbindung oder Mandant

Problem

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



Details

Für jede Grid Federation-Verbindung zeigt die Spalte **Last error** den zuletzt auftretenden Fehler an, falls vorhanden, wenn die Daten eines Mandanten in das andere Grid repliziert wurden. In dieser Spalte wird nur der letzte gitterübergreifende Replikationsfehler angezeigt. Frühere Fehler, die möglicherweise aufgetreten sind, werden nicht angezeigt. Ein Fehler in dieser Spalte kann aus einem der folgenden Gründe auftreten:

- Die Version des Quellobjekts wurde nicht gefunden.
- Der Quell-Bucket wurde nicht gefunden.
- Der Ziel-Bucket wurde gelöscht.
- Der Ziel-Bucket wurde von einem anderen Konto neu erstellt.
- Im Ziel-Bucket ist die Versionierung angehalten.
- Der Ziel-Bucket wurde vom selben Konto neu erstellt, ist aber jetzt nicht mehr versioniert.

Empfohlene Maßnahmen

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

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

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

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

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

Grid-übergreifende Replizierung mit permanenter Fehlerwarnung

Problem

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

Details

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

Empfohlene Maßnahmen

1. Melden Sie sich am Raster an, in dem die Warnmeldung ausgelöst wurde.
2. Gehen Sie zu **CONFIGURATION** > **System** > **Grid Federation**, und suchen Sie den in der Warnung aufgeführten Verbindungsnamen.
3. Sehen Sie auf der Registerkarte zulässige Mieter in der Spalte **Letzter Fehler** nach, um zu bestimmen, welche Mandantenkonten Fehler aufweisen.
4. Weitere Informationen zum Fehler finden Sie in den Anweisungen unter "Überwachen von Netzverbundverbindungen" Um die Grid-übergreifenden Replizierungsmetriken zu überprüfen.
5. Für jedes betroffene Mandantenkonto:
   a. Siehe die Anweisungen unter "Überwachen Sie die Mandantenaktivität" Um zu bestätigen, dass der Mandant sein Kontingent im Zielraster für die Grid-übergreifende Replikation nicht überschritten hat.
   b. Erhöhen Sie bei Bedarf das Kontingent des Mandanten im Zielraster, damit neue Objekte gespeichert werden können.
6. Melden Sie sich für jeden betroffenen Mandanten in beiden Grids bei Tenant Manager an, damit Sie die Liste der Buckets vergleichen können.
7. Bestätigen Sie für jeden Bucket, für den die Grid-übergreifende Replizierung aktiviert ist:
   - Es gibt einen entsprechenden Bucket für denselben Mandanten auf dem anderen Grid (muss den

genauen Namen verwenden).

- Beide Buckets haben die Objektversionierung aktiviert (die Versionierung kann in keinem Grid ausgesetzt werden).
- Bei beiden Buckets ist die S3-Objektsperre deaktiviert.
- Keiner der Buckets befindet sich im Status **delete objects: Read-only**.

8. Um zu bestätigen, dass das Problem behoben wurde, lesen Sie die Anweisungen unter "Überwachen von Netzverbundverbindungen" So überprüfen Sie die Grid-übergreifenden Replikationsmetriken oder führen folgende Schritte aus:

   a. Kehren Sie zur Seite „Grid Federation“ zurück.

   b. Wählen Sie den betroffenen Mandanten aus, und wählen Sie in der Spalte **Letzter Fehler** die Option **Fehler löschen** aus.

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

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

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

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

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

Warnung: Grid-übergreifende Replikationsressource nicht verfügbar

Problem

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

Details

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

Empfohlene Maßnahmen

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

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

Identifizieren Sie fehlgeschlagene Replikationsvorgänge und versuchen Sie es erneut

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

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

Ermitteln Sie, ob Objekte nicht repliziert werden konnten

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

Sie können das verwenden "Audit-Explain-Tool" Die Ergebnisse in ein leserliches Format zu übersetzen.

Bevor Sie beginnen

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

Schritte

1. Melden Sie sich beim primären Admin-Node an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

   Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

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

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

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

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

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

Jeder Eintrag enthält folgende Informationen:

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

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

Wiederholen Sie fehlgeschlagene Replikationen

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

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

Schritte

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

> Die mit „`Privat`“ gekennzeichneten StorageGRID API-Endpunkte können ohne Vorankündigung geändert werden. Private StorageGRID-Endpunkte ignorieren auch die API-Version der Anforderung.

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

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

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

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

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

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

Überwachen Sie Wiederholungen der Replikation

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

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

Sie haben zwei Möglichkeiten, Wiederholungsoperationen zu überwachen:

- Verwenden Sie ein S3 "HEAD Objekt" Oder "GET Objekt" Anfrage. Die Antwort bezieht sich auf das StorageGRID-spezifische `x-ntap-sg-cgr-replication-status` Antwortheader, der einen der folgenden Werte enthält:

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

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

Schritte

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

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

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

Sicherheitsmanagement

Sicherheit managen: Übersicht

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

Verschlüsselung managen

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

Verwalten von Zertifikaten

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

Konfigurieren von Verschlüsselungsmanagement-Servern

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

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

Proxy-Einstellungen verwalten

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

Kontrollieren Sie Firewalls

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

Prüfen Sie die StorageGRID Verschlüsselungsmethoden

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

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

Verschlüsselungsoption	So funktioniert es	Gilt für
Verschlüsselungsmanagement-Server (KMS) in Grid Manager	Du "Konfigurieren eines Verschlüsselungsmanagement-Servers" Auf der StorageGRID-Website und "Aktivieren Sie die Node-Verschlüsselung für die Appliance". Anschließend stellt ein Appliance-Node eine Verbindung mit dem KMS her, um einen Schlüsselverschlüsselungsschlüssel (KEK) anzufordern. Dieser Schlüssel verschlüsselt und entschlüsselt den Datenverschlüsselungsschlüssel (DEK) auf jedem Volume.	Appliance-Knoten, deren **Node Encryption** während der Installation aktiviert ist. Alle Daten auf der Appliance sind gegen physischen Verlust oder aus dem Datacenter geschützt. Das Management von Verschlüsselungen mit einem KMS wird nur für Storage Nodes und Service-Appliances unterstützt.

Verschlüsselungsoption	So funktioniert es	Gilt für
Laufwerkssicherheit in SANtricity System Manager	Wenn die Laufwerkssicherheitsfunktion für eine SG5700- oder SG6000-Speicheranwendung aktiviert ist, können Sie diese verwenden "SANtricity System Manager" So erstellen und verwalten Sie den Sicherheitsschlüssel. Der Schlüssel ist erforderlich, um auf die Daten auf den gesicherten Laufwerken zuzugreifen.	Storage-Appliances mit Full Disk Encryption (FDE)-Laufwerken oder FIPS-Laufwerken. Alle Daten auf den gesicherten Laufwerken sind vor physischem Verlust oder Entfernung aus dem Datacenter geschützt. Kann nicht mit Storage Appliances oder Service-Appliances verwendet werden.
Verschlüsselung gespeicherter Objekte	Sie aktivieren die "Verschlüsselung gespeicherter Objekte" Im Grid-Manager. Wenn diese Option aktiviert ist, werden alle neuen Objekte, die nicht auf Bucket-Ebene oder Objektebene verschlüsselt sind, bei der Aufnahme verschlüsselt.	Neu aufgenommene S3- und Swift-Objektdaten Vorhandene gespeicherte Objekte werden nicht verschlüsselt. Objektmetadaten und andere sensible Daten werden nicht verschlüsselt.
S3-Bucket-Verschlüsselung	Sie stellen eine PUT-Bucket-Verschlüsselungsanforderung bereit, um die Verschlüsselung für den Bucket zu aktivieren. Alle neuen Objekte, die nicht auf Objektebene verschlüsselt werden, werden bei der Aufnahme verschlüsselt.	Nur neu aufgenommene S3-Objektdaten Für den Bucket muss eine Verschlüsselung angegeben werden. Vorhandene Bucket-Objekte werden nicht verschlüsselt. Objektmetadaten und andere sensible Daten werden nicht verschlüsselt. "Operationen auf Buckets"
S3-Objektserverseitige Verschlüsselung (SSE)	Sie geben eine S3-Anforderung zum Speichern eines Objekts aus und schließen das ein `x-amz-server-side-encryption` Kopfzeile der Anfrage.	Nur neu aufgenommene S3-Objektdaten Für das Objekt muss eine Verschlüsselung angegeben werden. Objektmetadaten und andere sensible Daten werden nicht verschlüsselt. StorageGRID verwaltet die Schlüssel. "Serverseitige Verschlüsselung"

Verschlüsselungsoption	So funktioniert es	Gilt für
S3 Objektserverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln (SSE-C)	Sie geben eine S3-Anforderung zum Speichern eines Objekts aus und enthalten drei Anfrageheader. • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	Nur neu aufgenommene S3-Objektdaten Für das Objekt muss eine Verschlüsselung angegeben werden. Objektmetadaten und andere sensible Daten werden nicht verschlüsselt. Schlüssel werden außerhalb von StorageGRID gemanagt. "Serverseitige Verschlüsselung"
Externe Volume- oder Datastore-Verschlüsselung	Sofern die Implementierungsplattform sie unterstützt, verwenden Sie eine Verschlüsselungsmethode außerhalb von StorageGRID, um ein gesamtes Volume oder Datastore zu verschlüsseln.	Alle Objektdaten, Metadaten und Systemkonfigurationsdaten, wobei jedes Volume oder jeder Datastore verschlüsselt ist Eine externe Verschlüsselungsmethode bietet eine engere Kontrolle über Verschlüsselungsalgorithmen und -Schlüssel. Kann mit den anderen aufgeführten Methoden kombiniert werden.
Objektverschlüsselung außerhalb von StorageGRID	Dabei kommt eine Verschlüsselungsmethode außerhalb von StorageGRID zum Einsatz, um Objektdaten und Metadaten zu verschlüsseln, bevor sie in StorageGRID aufgenommen werden.	Nur Objektdaten und Metadaten (Systemkonfigurationsdaten sind nicht verschlüsselt). Eine externe Verschlüsselungsmethode bietet eine engere Kontrolle über Verschlüsselungsalgorithmen und -Schlüssel. Kann mit den anderen aufgeführten Methoden kombiniert werden. "Amazon Simple Storage Service – Developer Guide: Schutz von Daten mit Client-seitiger Verschlüsselung"

Verwendung mehrerer Verschlüsselungsmethoden

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

- Mit einem KMS können Appliance-Nodes geschützt werden. Außerdem kann mithilfe der

Laufwerksicherheitsfunktion in SANtricity System Manager die Daten „`double verschlüsselte`“ auf den Self-Encrypting Drives in denselben Appliances verschlüsselt werden.

- Sie können ein KMS verwenden, um Daten auf Appliance-Nodes zu sichern, und die Option gespeicherte Objektverschlüsselung verwenden, um alle Objekte bei der Aufnahme zu verschlüsseln.

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

Verwalten von Zertifikaten

Sicherheitszertifikate verwalten: Übersicht

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

StorageGRID verwendet zwei Arten von Sicherheitszertifikaten:

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

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

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

Standard Grid CA-Zertifikat

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

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

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

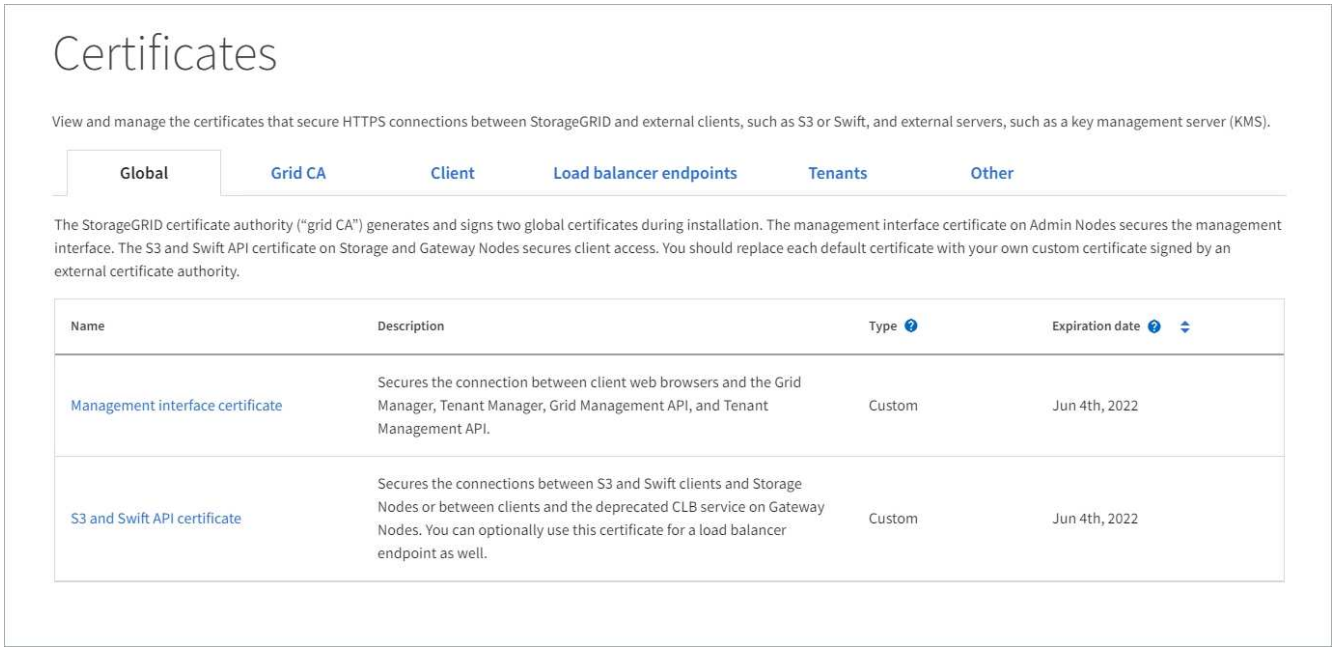
Varianten der Server- und Client-Zertifikatstypen werden auf verschiedene Weise implementiert. Vor der Konfiguration des Systems sollten Sie alle erforderlichen Zertifikate für Ihre spezifische StorageGRID-Konfiguration bereithaben.

Greifen Sie auf Sicherheitszertifikate zu

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

Schritte

1. Wählen Sie im Grid Manager **CONFIGURATION** > **Security** > **Certificates**.



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

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

   Jede Registerkarte wird unten mit Links zu weiteren Zertifikatdetails beschrieben.

Weltweit

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

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

Informationen zu den installierten globalen Zertifikaten umfassen:

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

Ihre Vorteile:

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

Grid CA

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

Zertifikatsinformationen umfassen das Ablaufdatum des Zertifikats und den Zertifikatinhalt.

Das können Sie "Kopieren oder laden Sie das Zertifikat der Grid-Zertifizierungsstelle herunter", Aber man kann es nicht ändern.

Client

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

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

verwendet werden kann.

Ihre Vorteile:

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

Load Balancer-Endpunkte

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

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

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

Ihre Vorteile:

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

Mandanten

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

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

Ihre Vorteile:

- "Wählen Sie einen Mandantennamen aus, um sich beim Mandanten-Manager anzumelden"
- "Wählen Sie einen Mandantennamen aus, um Details zur Identitätsföderation des Mandanten anzuzeigen"
- "Wählen Sie einen Mandantennamen aus, um Details zu den Services der Mandantenplattform anzuzeigen"

- "Festlegen eines Endpunktzertifikats für den Plattformservice während der Endpunkterstellung"

Andere

StorageGRID verwendet andere Sicherheitszertifikate zu bestimmten Zwecken. Diese Zertifikate werden nach ihrem Funktionsnamen aufgelistet. Weitere Sicherheitszertifikate:

- Cloud Storage Pool-Zertifikate
- Benachrichtigungszertifikate per E-Mail senden
- Externe Syslog-Server-Zertifikate
- Verbindungszertifikate für Grid Federation
- Zertifikate für Identitätsföderation
- KMS-Zertifikate (Key Management Server)
- Einzelanmelde-Zertifikate

Informationen geben den Zertifikattyp an, den eine Funktion verwendet, sowie die Gültigkeitsdaten des Server- und Clientzertifikats. Wenn Sie einen Funktionsnamen auswählen, wird eine Browserregisterkarte geöffnet, auf der Sie die Zertifikatdetails anzeigen und bearbeiten können.

> Sie können nur Informationen zu anderen Zertifikaten anzeigen und darauf zugreifen, wenn Sie über die entsprechende Berechtigung verfügen.

Ihre Vorteile:

- "Festlegen eines Cloud-Storage-Pool-Zertifikats für S3, C2S S3 oder Azure"
- "Legen Sie ein Zertifikat für Benachrichtigungen per E-Mail fest"
- "Geben Sie ein externes Syslog-Serverzertifikat an"
- "Verbindungszertifikate für Netzverbund drehen"
- "Anzeigen und Bearbeiten eines Zertifikats für die Identitätsföderation"
- "Laden Sie den KMS-Server (Key Management Server) und die Clientzertifikate hoch"
- "Geben Sie manuell ein SSO-Zertifikat für eine vertrauenswürdige Partei an"

Details zum Sicherheitszertifikat

Jede Art von Sicherheitszertifikat wird unten beschrieben, mit Links zu den Implementierungsanleitungen.

Zertifikat für die Managementoberfläche

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	Authentifiziert die Verbindung zwischen Client-Webbrowsern und der StorageGRID-Managementoberfläche, sodass Benutzer ohne Sicherheitswarnungen auf Grid-Manager und Mandantenmanager zugreifen können. Dieses Zertifikat authentifiziert auch Grid Management-API- und Mandantenmanagement-API-Verbindungen. Sie können das bei der Installation erstellte Standardzertifikat verwenden oder ein benutzerdefiniertes Zertifikat hochladen.	**KONFIGURATION** > **Sicherheit** > **Zertifikate**, wählen Sie die Registerkarte **Global** und wählen Sie dann **Management Interface Certificate** aus	"Konfigurieren Sie Zertifikate für die Managementoberfläche"

S3- und Swift-API-Zertifikat

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	Authentifizierung von sicheren S3- oder Swift-Client-Verbindungen zu einem Storage Node und Load Balancer-Endpunkten (optional)	**KONFIGURATION** > **Sicherheit** > **Zertifikate**, wählen Sie die Registerkarte **Global** und wählen Sie dann **S3 und Swift API Zertifikat** aus	"Konfigurieren von S3- und Swift-API-Zertifikaten"

Grid-CA-Zertifikat

Siehe Beschreibung des Standard Grid CA-Zertifikats.

Administrator-Client-Zertifikat

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Client	Wird auf jedem Client installiert, sodass StorageGRID den externen Client-Zugriff authentifizieren kann. • Ermöglicht autorisierten externen Clients den Zugriff auf die StorageGRID Prometheus-Datenbank. • Ermöglicht die sichere Überwachung von StorageGRID mit externen Tools.	**KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Client** wählen	"Konfigurieren Sie Client-Zertifikate"

Endpunkt-Zertifikat für Load Balancer

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	Authentifiziert die Verbindung zwischen S3- oder Swift-Clients und dem StorageGRID Load Balancer-Service auf Gateway-Nodes und Admin-Nodes. Sie können ein Load Balancer-Zertifikat hochladen oder generieren, wenn Sie einen Load Balancer-Endpunkt konfigurieren. Client-Applikationen verwenden das Load Balancer-Zertifikat, wenn Sie eine Verbindung zu StorageGRID herstellen, um Objektdaten zu speichern und abzurufen. Sie können auch eine benutzerdefinierte Version des globalen verwenden S3- und Swift-API-Zertifikat Zertifikat zur Authentifizierung von Verbindungen zum Lastverteilungsservice. Wenn das globale Zertifikat zur Authentifizierung von Load Balancer-Verbindungen verwendet wird, müssen Sie kein separates Zertifikat für jeden Load Balancer-Endpunkt hochladen oder generieren. **Hinweis:** das Zertifikat, das für die Load Balancer Authentifizierung verwendet wird, ist das am häufigsten verwendete Zertifikat während des normalen StorageGRID-Betriebs.	**KONFIGURATION** > **Netzwerk** > **Load Balancer-Endpunkte**	• "Konfigurieren von Load Balancer-Endpunkten" • "Erstellen eines Load Balancer-Endpunkts für FabricPool"

Endpunkt-Zertifikat für Cloud Storage Pool

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	Authentifiziert die Verbindung von einem StorageGRID Cloud Storage Pool auf einem externen Storage-Standort wie S3 Glacier oder Microsoft Azure Blob Storage. Für jeden Cloud-Provider-Typ ist ein anderes Zertifikat erforderlich.	**ILM** > **Speicherpools**	"Erstellen Sie einen Cloud-Storage-Pool"

Zertifikat für eine E-Mail-Benachrichtigung

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server und Client	Authentifiziert die Verbindung zwischen einem SMTP-E-Mail-Server und StorageGRID, die für Benachrichtigungen verwendet werden. • Wenn die Kommunikation mit dem SMTP-Server TLS (Transport Layer Security) erfordert, müssen Sie das CA-Zertifikat für den E-Mail-Server angeben. • Geben Sie ein Clientzertifikat nur an, wenn für den SMTP-E-Mail-Server Clientzertifikate zur Authentifizierung erforderlich sind.	**ALARME** > **E-Mail-Einrichtung**	"Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein"

Externes Syslog-Serverzertifikat

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	Authentifiziert die TLS- oder RELP/TLS-Verbindung zwischen einem externen Syslog-Server, der Ereignisse in StorageGRID protokolliert. **Hinweis:** für TCP-, RELP/TCP- und UDP-Verbindungen zu einem externen Syslog-Server ist kein externes Syslog-Serverzertifikat erforderlich.	**KONFIGURATION** > **Überwachung** > **Audit- und Syslog-Server** und dann **externen Syslog-Server konfigurieren** wählen	"Konfigurieren Sie einen externen Syslog-Server"

Verbindungszertifikat für Grid Federation

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server und Client	Authentifizieren und verschlüsseln Sie Informationen, die zwischen dem aktuellen StorageGRID-System und einem anderen Grid in einer Grid-Verbundverbindung gesendet werden.	**KONFIGURATION** > **System** > **Grid Federation**	• "Erstellen von Grid Federation-Verbindungen" • "Verbindungszertifikate drehen"

Zertifikat für Identitätsföderation

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	Authentifiziert die Verbindung zwischen StorageGRID und einem externen Identitäts-Provider, z. B. Active Directory, OpenLDAP oder Oracle Directory Server. Wird für Identitätsföderation verwendet, durch die Administratoren und Benutzer von einem externen System gemanagt werden können.	**KONFIGURATION** > **Zugangskontrolle** > **Identitätsverbund**	"Verwenden Sie den Identitätsverbund"

KMS-Zertifikat (Key Management Server)

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server und Client	Authentifiziert die Verbindung zwischen StorageGRID und einem externen Verschlüsselungsmanagement-Server (KMS), der Verschlüsselungsschlüssel für die StorageGRID Appliance-Nodes bereitstellt.	**KONFIGURATION** > **Sicherheit** > **Schlüsselverwaltungsserver**	"Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)"

Endpoint-Zertifikat für Plattform-Services

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	Authentifiziert die Verbindung vom StorageGRID Plattform-Service zu einer S3-Storage-Ressource.	**Tenant Manager** > **STORAGE (S3)** > **Plattform-Services-Endpunkte**	"Endpunkt für Plattformservices erstellen" "Endpunkt der Plattformdienste bearbeiten"

SSO-Zertifikat (Single Sign On)

Zertifikatstyp	Beschreibung	Speicherort für die Navigation	Details
Server	Authentifiziert die Verbindung zwischen Services der Identitätsföderation, z. B. Active Directory Federation Services (AD FS) und StorageGRID, die für SSO-Anforderungen (Single Sign On) verwendet werden.	**KONFIGURATION** > **Zugangskontrolle** > **Single Sign-On**	"Konfigurieren Sie Single Sign-On"

Beispiele für Zertifikate

Beispiel 1: Load Balancer Service

In diesem Beispiel fungiert StorageGRID als Server.

1. Sie konfigurieren einen Load Balancer-Endpunkt und laden ein Serverzertifikat in StorageGRID hoch oder erstellen.
2. Sie konfigurieren eine S3- oder Swift-Client-Verbindung zum Endpunkt des Load Balancer und laden dasselbe Zertifikat auf den Client hoch.
3. Wenn der Client Daten speichern oder abrufen möchte, stellt er über HTTPS eine Verbindung zum Load Balancer-Endpunkt her.
4. StorageGRID antwortet mit dem Serverzertifikat, das einen öffentlichen Schlüssel enthält, und mit einer Signatur auf Grundlage des privaten Schlüssels.
5. Der Client überprüft dieses Zertifikat, indem er die Serversignatur mit der Signatur seiner Kopie des Zertifikats vergleicht. Wenn die Signaturen übereinstimmen, startet der Client eine Sitzung mit demselben öffentlichen Schlüssel.
6. Der Client sendet Objektdaten an StorageGRID.

Beispiel 2: Externer KMS (Key Management Server)

In diesem Beispiel fungiert StorageGRID als Client.

1. Mithilfe der Software für den externen Verschlüsselungsmanagement-Server konfigurieren Sie StorageGRID als KMS-Client und erhalten ein von einer Zertifizierungsstelle signiertes Serverzertifikat, ein öffentliches Clientzertifikat und den privaten Schlüssel für das Clientzertifikat.
2. Mit dem Grid Manager konfigurieren Sie einen KMS-Server und laden die Server- und Client-Zertifikate sowie den privaten Client-Schlüssel hoch.
3. Wenn ein StorageGRID-Node einen Verschlüsselungsschlüssel benötigt, fordert er den KMS-Server an, der Daten des Zertifikats enthält und eine auf dem privaten Schlüssel basierende Signatur.
4. Der KMS-Server validiert die Zertifikatsignatur und entscheidet, dass er StorageGRID vertrauen kann.
5. Der KMS-Server antwortet über die validierte Verbindung.

Unterstützte Serverzertifikatstypen

Das StorageGRID-System unterstützt benutzerdefinierte Zertifikate, die mit RSA oder ECDSA (Algorithmus für digitale Signaturen der Elliptischen Kurve) verschlüsselt sind.

Der Verschlüsselungstyp für die Sicherheitsrichtlinie muss mit dem Serverzertifikattyp übereinstimmen. RSA-Chiffren erfordern beispielsweise RSA-Zertifikate, und ECDSA-Chiffren erfordern ECDSA-Zertifikate. Siehe "Verwalten von Sicherheitszertifikaten". Wenn Sie eine benutzerdefinierte Sicherheitsrichtlinie konfigurieren, die nicht mit dem Serverzertifikat kompatibel ist, können Sie dies tun "Vorübergehendes Zurücksetzen auf die Standard-Sicherheitsrichtlinie".

Weitere Informationen darüber, wie StorageGRID Client-Verbindungen für die REST-API sichert, finden Sie unter "Sicherheit für S3-REST-API konfigurieren" Oder "Konfigurieren Sie die Sicherheit für Swift REST API".

Konfigurieren Sie Zertifikate für die Managementoberfläche

Sie können das Standardzertifikat für die Verwaltungsschnittstelle durch ein einzelnes benutzerdefiniertes Zertifikat ersetzen, das Benutzern den Zugriff auf den Grid Manager und den Tenant Manager ermöglicht, ohne dass Sicherheitswarnungen auftreten. Sie können auch das Standard-Zertifikat für die Managementoberfläche zurücksetzen oder ein neues erstellen.

Über diese Aufgabe

Standardmäßig wird jeder Admin-Node ein von der Grid-CA signiertes Zertifikat ausgestellt. Diese CA-signierten Zertifikate können durch ein einziges allgemeines Zertifikat für benutzerdefinierte Verwaltungsschnittstellen und einen entsprechenden privaten Schlüssel ersetzt werden.

Da für alle Admin-Nodes ein einzelnes Zertifikat für eine benutzerdefinierte Managementoberfläche verwendet wird, müssen Sie das Zertifikat als Platzhalter- oder Multi-Domain-Zertifikat angeben, wenn Clients den Hostnamen bei der Verbindung mit Grid Manager und Tenant Manager überprüfen müssen. Definieren Sie das benutzerdefinierte Zertifikat so, dass es mit allen Admin-Nodes im Raster übereinstimmt.

Sie müssen die Konfiguration auf dem Server abschließen. Je nach der von Ihnen verwendeten Root Certificate Authority (CA) müssen Benutzer möglicherweise auch das Grid CA-Zertifikat in den Webbrowser installieren, mit dem sie auf den Grid Manager und den Tenant Manager zugreifen können.

Um sicherzustellen, dass der Betrieb nicht durch ein fehlerhaftes Serverzertifikat unterbrochen wird, wird die Warnmeldung **Ablauf des Serverzertifikats für die Managementoberfläche** ausgelöst, wenn dieses Serverzertifikat abläuft. Wenn erforderlich, können Sie anzeigen, wann das aktuelle Zertifikat abläuft, indem Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate** auswählen und das Ablaufdatum für das Zertifikat der Verwaltungsschnittstelle auf der Registerkarte Global anzeigen.

Wenn Sie mit einem Domänennamen anstelle einer IP-Adresse auf den Grid Manager oder den Tenant Manager zugreifen, zeigt der Browser einen Zertifikatfehler ohne eine Option zum Umgehen an, wenn eine der folgenden Fälle auftritt:

- Ihr Zertifikat für die benutzerdefinierte Managementoberfläche läuft ab.
- Du Zurücksetzen von einem Zertifikat der benutzerdefinierten Managementoberfläche auf das Standard-Serverzertifikat.

Fügen Sie ein Zertifikat für eine benutzerdefinierte Managementoberfläche hinzu

Zum Hinzufügen eines Zertifikats einer benutzerdefinierten Managementoberfläche können Sie Ihr eigenes Zertifikat bereitstellen oder mit dem Grid Manager ein Zertifikat erstellen.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global** die Option **Management Interface Certificate** aus.
3. Wählen Sie **Benutzerdefiniertes Zertifikat verwenden**.
4. Hochladen oder Generieren des Zertifikats

Zertifikat hochladen

Laden Sie die erforderlichen Serverzertifikatdateien hoch.

a. Wählen Sie **Zertifikat hochladen**.

b. Laden Sie die erforderlichen Serverzertifikatdateien hoch:

- **Server-Zertifikat**: Die benutzerdefinierte Server-Zertifikatdatei (PEM-codiert).
- **Zertifikat privater Schlüssel**: Die benutzerdefinierte Server Zertifikat private Schlüssel Datei (`.key`).

> Private EC-Schlüssel müssen 224 Bit oder größer sein. RSA Private Keys müssen mindestens 2048 Bit groß sein.

- **CA-Paket**: Eine einzelne optionale Datei, die die Zertifikate jeder Intermediate-Zertifizierungsstelle (CA) enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatdateien enthalten, die in der Reihenfolge der Zertifikatskette verkettet sind.

c. Erweitern Sie **Zertifikatdetails**, um die Metadaten für jedes hochgeladene Zertifikat anzuzeigen. Wenn Sie ein optionales CA-Paket hochgeladen haben, wird jedes Zertifikat auf seiner eigenen Registerkarte angezeigt.

- Wählen Sie **Zertifikat herunterladen**, um die Zertifikatdatei zu speichern, oder wählen Sie **CA-Paket herunterladen**, um das Zertifikatspaket zu speichern.

  Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung `.pem`.

  Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Zertifikat kopieren PEM** oder **CA-Paket kopieren PEM** aus, um den Zertifikatinhalt zum Einfügen an eine andere Stelle zu kopieren.

d. Wählen Sie **Speichern**. + das Zertifikat der benutzerdefinierten Managementoberfläche wird für alle nachfolgenden neuen Verbindungen mit Grid Manager, Tenant Manager, Grid Manager API oder Tenant Manager API verwendet.

Zertifikat wird generiert

Erstellen Sie die Serverzertifikatdateien.

> Die beste Vorgehensweise für eine Produktionsumgebung ist die Verwendung eines Zertifikats der benutzerdefinierten Management-Schnittstelle, das von einer externen Zertifizierungsstelle signiert wurde.

a. Wählen Sie **Zertifikat erstellen**.

b. Geben Sie die Zertifikatsinformationen an:

Feld	Beschreibung
Domain-Name	Mindestens ein vollständig qualifizierter Domänenname, der in das Zertifikat aufgenommen werden soll. Verwenden Sie ein * als Platzhalter, um mehrere Domain-Namen darzustellen.

Feld	Beschreibung
IP	Mindestens eine IP-Adresse, die in das Zertifikat aufgenommen werden soll.
Betreff (optional)	X.509 Subject oder Distinguished Name (DN) des Zertifikateigentümers. Wenn in diesem Feld kein Wert eingegeben wird, verwendet das generierte Zertifikat den ersten Domänennamen oder die IP-Adresse als allgemeinen Studienteilnehmer (CN).
Tage gültig	Anzahl der Tage nach Erstellung, nach denen das Zertifikat abläuft.
Fügen Sie wichtige Nutzungserweiterungen hinzu	Wenn diese Option ausgewählt ist (Standard und empfohlen), werden die Schlüsselnutzung und die erweiterten Schlüsselnutzungserweiterungen dem generierten Zertifikat hinzugefügt. Diese Erweiterungen definieren den Zweck des Schlüssels, der im Zertifikat enthalten ist. **Hinweis**: Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, Sie haben Verbindungsprobleme mit älteren Clients, wenn Zertifikate diese Erweiterungen enthalten.

c. Wählen Sie **Erzeugen**.

d. Wählen Sie **Zertifikatdetails** aus, um die Metadaten für das generierte Zertifikat anzuzeigen.

   - Wählen Sie **Zertifikat herunterladen**, um die Zertifikatdatei zu speichern.

     Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung `.pem`.

   Beispiel: `storagegrid_certificate.pem`

   - Wählen Sie **Zertifikat kopieren PEM** aus, um den Zertifikatinhalt zum Einfügen an eine andere Stelle zu kopieren.

e. Wählen Sie **Speichern**. + das Zertifikat der benutzerdefinierten Managementoberfläche wird für alle nachfolgenden neuen Verbindungen mit Grid Manager, Tenant Manager, Grid Manager API oder Tenant Manager API verwendet.

5. Aktualisieren Sie die Seite, um sicherzustellen, dass der Webbrowser aktualisiert wird.

> Nachdem Sie ein Zertifikat hochgeladen oder generiert haben, lassen Sie sich bis zu einen Tag lang alle damit verbundenen Warnmeldungen zum Ablauf des Zertifikats löschen.

6. Nachdem Sie ein Zertifikat für eine benutzerdefinierte Managementoberfläche hinzugefügt haben, werden auf der Seite Zertifikat der Verwaltungsschnittstelle detaillierte Zertifikatsinformationen für die verwendeten Zertifikate angezeigt. + Sie können das PEM-Zertifikat nach Bedarf herunterladen oder kopieren.

Stellen Sie das Standardzertifikat für die Managementoberfläche wieder her

Sie können das Standardzertifikat zur Managementoberfläche für Grid Manager- und Tenant-Manager-Verbindungen wiederherstellen.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global** die Option **Management Interface Certificate** aus.
3. Wählen Sie **Standard-Zertifikat verwenden**.

   Wenn Sie das Standardzertifikat der Verwaltungsschnittstelle wiederherstellen, werden die von Ihnen konfigurierten benutzerdefinierten Serverzertifikatdateien gelöscht und können nicht vom System wiederhergestellt werden. Das Standardzertifikat für die Verwaltungsschnittstelle wird für alle nachfolgenden neuen Clientverbindungen verwendet.

4. Aktualisieren Sie die Seite, um sicherzustellen, dass der Webbrowser aktualisiert wird.

Erstellen Sie mit einem Skript ein neues Zertifikat für die selbstsignierte Managementoberfläche

Wenn eine strikte Host-Validierung erforderlich ist, können Sie das Zertifikat der Managementoberfläche mithilfe eines Skripts generieren.

Bevor Sie beginnen

- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben die `Passwords.txt` Datei:

Über diese Aufgabe

Die beste Vorgehensweise für eine Produktionsumgebung ist die Verwendung eines Zertifikats, das von einer externen Zertifizierungsstelle signiert wurde.

Schritte

1. Ermitteln Sie den vollständig qualifizierten Domänennamen (FQDN) jedes Admin-Knotens.
2. Melden Sie sich beim primären Admin-Node an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

      Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

3. Konfigurieren Sie StorageGRID mit einem neuen selbstsignierten Zertifikat.

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - Für `--domains`, Verwenden Sie Platzhalter, um die vollständig qualifizierten Domänennamen aller Admin-Knoten darzustellen. Beispiel: `*.ui.storagegrid.example.com` Verwendet den Platzhalter * für die Darstellung `admin1.ui.storagegrid.example.com` Und `admin2.ui.storagegrid.example.com`.

- Einstellen `--type` Bis `management` Zum Konfigurieren des Zertifikats der Managementoberfläche, das von Grid Manager und Tenant Manager verwendet wird.
- Die erstellten Zertifikate sind standardmäßig für ein Jahr (365 Tage) gültig und müssen vor Ablauf neu erstellt werden. Sie können das verwenden `--days` Argument zum Überschreiben des standardmäßigen Gültigkeitszeitraums.

> ⓘ Die Gültigkeitsdauer eines Zertifikats beginnt, wenn `make-certificate` Wird ausgeführt. Sie müssen sicherstellen, dass der Management-Client mit der gleichen Datenquelle wie StorageGRID synchronisiert wird. Andernfalls kann der Client das Zertifikat ablehnen.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 720
```

Die resultierende Ausgabe enthält das öffentliche Zertifikat, das vom Management-API-Client benötigt wird.

4. Wählen Sie das Zertifikat aus, und kopieren Sie es.

   Geben Sie DIE START- und DAS ENDE-Tags in Ihre Auswahl ein.

5. Melden Sie sich von der Eingabeaufforderung-Shell ab. `$ exit`
6. Bestätigen Sie, dass das Zertifikat konfiguriert wurde:
   a. Greifen Sie auf den Grid Manager zu.
   b. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate**
   c. Wählen Sie auf der Registerkarte **Global** die Option **Management Interface Certificate** aus.
7. Konfigurieren Sie den Management-Client so, dass er das öffentliche Zertifikat verwendet, das Sie kopiert haben. Geben Sie DIE START- und END-Tags an.

Laden Sie das Zertifikat für die Managementoberfläche herunter oder kopieren Sie es

Sie können den Inhalt des Zertifikats der Managementoberfläche speichern oder kopieren, um ihn an einer anderen Stelle zu verwenden.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global** die Option **Management Interface Certificate** aus.
3. Wählen Sie die Registerkarte **Server** oder **CA Bundle** aus und laden Sie das Zertifikat herunter oder kopieren Sie es.

Laden Sie die Zertifikatdatei oder das CA-Paket herunter

Laden Sie das Zertifikat oder das CA-Paket herunter `.pem` Datei: Wenn Sie ein optionales CA-Bundle verwenden, wird jedes Zertifikat im Paket auf seiner eigenen Unterregisterkarte angezeigt.

a. Wählen Sie **Zertifikat herunterladen** oder **CA-Paket herunterladen**.

   Wenn Sie ein CA-Bundle herunterladen, werden alle Zertifikate in den sekundären Registerkarten des CA-Pakets als einzelne Datei heruntergeladen.

b. Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung `.pem`.

   Beispiel: `storagegrid_certificate.pem`

Zertifikat oder CA-Bundle-PEM kopieren

Kopieren Sie den Zertifikatstext, um ihn an eine andere Stelle einzufügen. Wenn Sie ein optionales CA-Bundle verwenden, wird jedes Zertifikat im Paket auf seiner eigenen Unterregisterkarte angezeigt.

a. Wählen Sie **Zertifikat kopieren PEM** oder **CA-Paket kopieren PEM**.

   Wenn Sie ein CA-Bundle kopieren, kopieren alle Zertifikate in den sekundären Registerkarten des CA-Bundles zusammen.

b. Fügen Sie das kopierte Zertifikat in einen Texteditor ein.

c. Speichern Sie die Textdatei mit der Erweiterung `.pem`.

   Beispiel: `storagegrid_certificate.pem`

Konfigurieren von S3- und Swift-API-Zertifikaten

Sie können das Serverzertifikat ersetzen oder wiederherstellen, das für S3- oder Swift-Clientverbindungen zu Storage Nodes oder zu Load Balancer-Endpunkten verwendet wird. Das benutzerdefinierte Ersatzserverzertifikat ist speziell für Ihr Unternehmen bestimmt.

Über diese Aufgabe

Standardmäßig wird jeder Speicherknoten ein X.509-Serverzertifikat ausgestellt, das von der Grid-CA signiert wurde. Diese CA-signierten Zertifikate können durch ein einziges allgemeines benutzerdefiniertes Serverzertifikat und den entsprechenden privaten Schlüssel ersetzt werden.

Für alle Speicherknoten wird ein einzelnes benutzerdefiniertes Serverzertifikat verwendet. Sie müssen daher das Zertifikat als Platzhalter- oder Multidomain-Zertifikat angeben, wenn Clients den Hostnamen bei der Verbindung mit dem Speicherendpunkt überprüfen müssen. Definieren Sie das benutzerdefinierte Zertifikat, sodass es mit allen Speicherknoten im Raster übereinstimmt.

Nach Abschluss der Konfiguration auf dem Server müssen Sie möglicherweise auch das Grid CA-Zertifikat im S3- oder Swift-API-Client installieren, über den Sie je nach der von Ihnen verwendeten Root-Zertifizierungsstelle (CA) auf das System zugreifen können.

Um sicherzustellen, dass der Betrieb nicht durch ein fehlerhaftes Serverzertifikat unterbrochen wird, wird die Warnung **Ablauf des globalen Serverzertifikats für S3 und Swift API** ausgelöst, wenn das Stammserverzertifikat abläuft. Wenn erforderlich, können Sie anzeigen, wann das aktuelle Zertifikat abläuft, indem Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate** und das Ablaufdatum für das S3- und Swift-API-Zertifikat auf der Registerkarte Global auswählen.

Sie können ein benutzerdefiniertes S3- und Swift-API-Zertifikat hochladen oder erstellen.

Fügen Sie ein benutzerdefiniertes S3- und Swift-API-Zertifikat hinzu

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global S3 und Swift API Zertifikat**.
3. Wählen Sie **Benutzerdefiniertes Zertifikat verwenden**.
4. Hochladen oder Generieren des Zertifikats

Zertifikat hochladen

Laden Sie die erforderlichen Serverzertifikatdateien hoch.

a. Wählen Sie **Zertifikat hochladen**.

b. Laden Sie die erforderlichen Serverzertifikatdateien hoch:

- **Server-Zertifikat**: Die benutzerdefinierte Server-Zertifikatdatei (PEM-codiert).
- **Zertifikat privater Schlüssel**: Die benutzerdefinierte Server Zertifikat private Schlüssel Datei (`.key`).

> Private EC-Schlüssel müssen 224 Bit oder größer sein. RSA Private Keys müssen mindestens 2048 Bit groß sein.

- **CA-Paket**: Eine einzelne optionale Datei, die die Zertifikate jeder Intermediate-Zertifizierungsstelle enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatdateien enthalten, die in der Reihenfolge der Zertifikatskette verkettet sind.

c. Wählen Sie die Zertifikatsdetails aus, um die Metadaten und PEM für jedes benutzerdefinierte S3- und Swift-API-Zertifikat anzuzeigen, das hochgeladen wurde. Wenn Sie ein optionales CA-Paket hochgeladen haben, wird jedes Zertifikat auf seiner eigenen Registerkarte angezeigt.

- Wählen Sie **Zertifikat herunterladen**, um die Zertifikatdatei zu speichern, oder wählen Sie **CA-Paket herunterladen**, um das Zertifikatspaket zu speichern.

  Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung `.pem`.

  Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Zertifikat kopieren PEM** oder **CA-Paket kopieren PEM** aus, um den Zertifikatinhalt zum Einfügen an eine andere Stelle zu kopieren.

d. Wählen Sie **Speichern**.

Das benutzerdefinierte Serverzertifikat wird für nachfolgende neue S3- und Swift-Client-Verbindungen verwendet.

Zertifikat wird generiert

Erstellen Sie die Serverzertifikatdateien.

a. Wählen Sie **Zertifikat erstellen**.

b. Geben Sie die Zertifikatsinformationen an:

Feld	Beschreibung
Domain-Name	Mindestens ein vollständig qualifizierter Domänenname, der in das Zertifikat aufgenommen werden soll. Verwenden Sie ein * als Platzhalter, um mehrere Domain-Namen darzustellen.
IP	Mindestens eine IP-Adresse, die in das Zertifikat aufgenommen werden soll.

Feld	Beschreibung
Betreff (optional)	X.509 Subject oder Distinguished Name (DN) des Zertifikateigentümers. Wenn in diesem Feld kein Wert eingegeben wird, verwendet das generierte Zertifikat den ersten Domänennamen oder die IP-Adresse als allgemeinen Studienteilnehmer (CN).
Tage gültig	Anzahl der Tage nach Erstellung, nach denen das Zertifikat abläuft.
Fügen Sie wichtige Nutzungserweiterungen hinzu	Wenn diese Option ausgewählt ist (Standard und empfohlen), werden die Schlüsselnutzung und die erweiterten Schlüsselnutzungserweiterungen dem generierten Zertifikat hinzugefügt. Diese Erweiterungen definieren den Zweck des Schlüssels, der im Zertifikat enthalten ist. **Hinweis**: Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, Sie haben Verbindungsprobleme mit älteren Clients, wenn Zertifikate diese Erweiterungen enthalten.

c. Wählen Sie **Erzeugen**.

d. Wählen Sie **Zertifikatdetails** aus, um die Metadaten und das PEM für das benutzerdefinierte S3- und Swift-API-Zertifikat anzuzeigen, das erstellt wurde.

   - Wählen Sie **Zertifikat herunterladen**, um die Zertifikatdatei zu speichern.

     Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung `.pem`.

   Beispiel: `storagegrid_certificate.pem`

   - Wählen Sie **Zertifikat kopieren PEM** aus, um den Zertifikatinhalt zum Einfügen an eine andere Stelle zu kopieren.

e. Wählen Sie **Speichern**.

   Das benutzerdefinierte Serverzertifikat wird für nachfolgende neue S3- und Swift-Client-Verbindungen verwendet.

5. Wählen Sie eine Registerkarte aus, um Metadaten für das Standard-StorageGRID-Serverzertifikat, ein Zertifikat mit einer Zertifizierungsstelle, das hochgeladen wurde, oder ein benutzerdefiniertes Zertifikat anzuzeigen, das erstellt wurde.

   Nachdem Sie ein Zertifikat hochgeladen oder generiert haben, lassen Sie sich bis zu einen Tag lang alle damit verbundenen Warnmeldungen zum Ablauf des Zertifikats löschen.

6. Aktualisieren Sie die Seite, um sicherzustellen, dass der Webbrowser aktualisiert wird.

7. Nachdem Sie ein benutzerdefiniertes S3- und Swift-API-Zertifikat hinzugefügt haben, zeigt die S3- und Swift-API-Zertifikatsseite detaillierte Zertifikatsinformationen für das verwendete S3- und Swift-API-

Zertifikat an. + Sie können das PEM-Zertifikat nach Bedarf herunterladen oder kopieren.

Stellen Sie das S3- und Swift-API-Standardzertifikat wieder her

Sie können die Wiederherstellung auf die Verwendung des standardmäßigen S3- und Swift-API-Zertifikats für S3- und Swift-Client-Verbindungen zu Storage Nodes durchführen. Sie können jedoch nicht das standardmäßige S3- und Swift-API-Zertifikat für einen Load Balancer-Endpunkt verwenden.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global S3 und Swift API Zertifikat**.
3. Wählen Sie **Standard-Zertifikat verwenden**.

   Wenn Sie die Standardversion des globalen S3- und Swift-API-Zertifikats wiederherstellen, werden die von Ihnen konfigurierten benutzerdefinierten Serverzertifikatdateien gelöscht und können nicht vom System wiederhergestellt werden. Das standardmäßige S3- und Swift-API-Zertifikat wird für nachfolgende neue S3- und Swift-Client-Verbindungen zu Storage-Nodes verwendet.

4. Wählen Sie **OK**, um die Warnung zu bestätigen und das Standard-S3- und Swift-API-Zertifikat wiederherzustellen.

   Wenn Sie über Root-Zugriffsberechtigungen verfügen und das benutzerdefinierte S3- und Swift-API-Zertifikat für Endpoint-Verbindungen für den Load Balancer verwendet wurde, wird eine Liste mit Endpunkten für Load Balancer angezeigt, auf die über das Standard-S3- und Swift-API-Zertifikat nicht mehr zugegriffen werden kann. Gehen Sie zu "Konfigurieren von Load Balancer-Endpunkten" Zum Bearbeiten oder Entfernen der betroffenen Endpunkte.

5. Aktualisieren Sie die Seite, um sicherzustellen, dass der Webbrowser aktualisiert wird.

Laden Sie das S3- und Swift-API-Zertifikat herunter oder kopieren Sie es

Sie können Inhalte des S3- und Swift-API-Zertifikats zur anderen Verwendung speichern oder kopieren.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global S3 und Swift API Zertifikat**.
3. Wählen Sie die Registerkarte **Server** oder **CA Bundle** aus und laden Sie das Zertifikat herunter oder kopieren Sie es.

Laden Sie die Zertifikatdatei oder das CA-Paket herunter

Laden Sie das Zertifikat oder das CA-Paket herunter `.pem` Datei: Wenn Sie ein optionales CA-Bundle verwenden, wird jedes Zertifikat im Paket auf seiner eigenen Unterregisterkarte angezeigt.

a. Wählen Sie **Zertifikat herunterladen** oder **CA-Paket herunterladen**.

   Wenn Sie ein CA-Bundle herunterladen, werden alle Zertifikate in den sekundären Registerkarten des CA-Pakets als einzelne Datei heruntergeladen.

b. Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung `.pem`.

   Beispiel: `storagegrid_certificate.pem`

Zertifikat oder CA-Bundle-PEM kopieren

Kopieren Sie den Zertifikatstext, um ihn an eine andere Stelle einzufügen. Wenn Sie ein optionales CA-Bundle verwenden, wird jedes Zertifikat im Paket auf seiner eigenen Unterregisterkarte angezeigt.

a. Wählen Sie **Zertifikat kopieren PEM** oder **CA-Paket kopieren PEM**.

   Wenn Sie ein CA-Bundle kopieren, kopieren alle Zertifikate in den sekundären Registerkarten des CA-Bundles zusammen.

b. Fügen Sie das kopierte Zertifikat in einen Texteditor ein.

c. Speichern Sie die Textdatei mit der Erweiterung `.pem`.

   Beispiel: `storagegrid_certificate.pem`

Verwandte Informationen

- "S3-REST-API VERWENDEN"
- "Nutzen Sie die Swift REST API"
- "Konfigurieren Sie die Domänennamen des S3-Endpunkts"

Kopieren Sie das Grid-CA-Zertifikat

StorageGRID verwendet eine interne Zertifizierungsstelle (Certificate Authority, CA) zum Schutz des internen Datenverkehrs. Dieses Zertifikat ändert sich nicht, wenn Sie Ihre eigenen Zertifikate hochladen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Wenn ein benutzerdefiniertes Serverzertifikat konfiguriert wurde, sollten Client-Anwendungen den Server anhand des benutzerdefinierten Serverzertifikats überprüfen. Sie sollten das CA-Zertifikat nicht aus dem StorageGRID-System kopieren.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Raster CA** aus.
2. Laden Sie das Zertifikat im Abschnitt **Zertifikat PEM** herunter oder kopieren Sie es.

Laden Sie die Zertifikatdatei herunter

Laden Sie das Zertifikat herunter `.pem` Datei:

a. Wählen Sie **Zertifikat herunterladen**.
b. Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung `.pem`.

   Beispiel: `storagegrid_certificate.pem`

Zertifikat PEM kopieren

Kopieren Sie den Zertifikatstext, um ihn an eine andere Stelle einzufügen.

a. Wählen Sie **Zertifikat kopieren PEM**.
b. Fügen Sie das kopierte Zertifikat in einen Texteditor ein.
c. Speichern Sie die Textdatei mit der Erweiterung `.pem`.

   Beispiel: `storagegrid_certificate.pem`

Konfigurieren Sie StorageGRID-Zertifikate für FabricPool

Für S3-Clients, die strenge Hostnamen-Validierungen durchführen und die eine strikte Hostname-Validierung nicht unterstützen, z. B. ONTAP-Clients mit FabricPool, können Sie beim Konfigurieren des Load Balancer-Endpunkts ein Serverzertifikat generieren oder hochladen.

Bevor Sie beginnen

- Sie haben spezifische Zugriffsberechtigungen.
- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".

Über diese Aufgabe

Wenn Sie einen Load Balancer-Endpunkt erstellen, können Sie ein selbstsigniertes Serverzertifikat generieren oder ein Zertifikat hochladen, das von einer bekannten Zertifizierungsstelle signiert ist. In Produktionsumgebungen sollten Sie ein Zertifikat verwenden, das von einer bekannten Zertifizierungsstelle signiert ist. Von einer Zertifizierungsstelle signierte Zertifikate können unterbrechungsfrei gedreht werden. Sie sind außerdem sicherer, weil sie einen besseren Schutz vor man-in-the-Middle-Angriffen bieten.

In den folgenden Schritten finden Sie allgemeine Richtlinien für S3-Clients, die FabricPool verwenden. Weitere Informationen und Verfahren finden Sie unter "Konfigurieren Sie StorageGRID für FabricPool".

Schritte

1. Konfigurieren Sie optional eine HA-Gruppe (High Availability, Hochverfügbarkeit) für die Verwendung von FabricPool.

2. Einen S3-Load-Balancer-Endpunkt für FabricPool erstellen.

   Wenn Sie einen HTTPS-Load-Balancer-Endpunkt erstellen, werden Sie aufgefordert, Ihr Serverzertifikat, den privaten Zertifikatschlüssel und das optionale CA-Bundle hochzuladen.

3. Fügen Sie StorageGRID als Cloud-Tier in ONTAP bei.

   Geben Sie den Endpunkt-Port des Load Balancer und den vollständig qualifizierten Domänennamen an, der im hochgeladenen CA-Zertifikat verwendet wird. Geben Sie dann das CA-Zertifikat ein.

> ⓘ Wenn eine Zwischenzertifizierungsstelle das StorageGRID-Zertifikat ausgestellt hat, müssen Sie das Zertifikat der Zwischenzertifizierungsstelle vorlegen. Wenn das StorageGRID-Zertifikat direkt von der Root-CA ausgestellt wurde, müssen Sie das Root-CA-Zertifikat bereitstellen.

Konfigurieren Sie Client-Zertifikate

Mit Clientzertifikaten können autorisierte externe Clients auf die StorageGRID Prometheus-Datenbank zugreifen und externe Tools zur Überwachung von StorageGRID sicher einsetzen.

Wenn Sie mit einem externen Monitoring-Tool auf StorageGRID zugreifen müssen, müssen Sie mithilfe des Grid Managers ein Clientzertifikat hochladen oder generieren und die Zertifikatsinformationen in das externe Tool kopieren.

Siehe "Verwalten von Sicherheitszertifikaten" Und "Konfigurieren Sie benutzerdefinierte Serverzertifikate".

> ⓘ Um sicherzustellen, dass der Betrieb nicht durch ein fehlerhaftes Serverzertifikat unterbrochen wird, wird die Warnung **Ablauf von Client-Zertifikaten, die auf der Seite Zertifikate konfiguriert ist** ausgelöst, wenn dieses Serverzertifikat abläuft. Wenn erforderlich, können Sie anzeigen, wann das aktuelle Zertifikat abläuft, indem Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate** und das Ablaufdatum des Clientzertifikats auf der Registerkarte Client auswählen.

> ⓘ Wenn Sie zum Schutz der Daten auf speziell konfigurierten Appliance-Nodes einen Verschlüsselungsmanagement-Server (KMS) verwenden, lesen Sie die spezifischen Informationen zu "Hochladen eines KMS-Clientzertifikats".

Bevor Sie beginnen

- Sie haben Root-Zugriffsberechtigung.
- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- So konfigurieren Sie ein Clientzertifikat:
  - Sie haben die IP-Adresse oder den Domänennamen des Admin-Knotens.
  - Wenn Sie das Zertifikat für die StorageGRID-Managementoberfläche konfiguriert haben, verfügen Sie über die CA, das Client-Zertifikat und den privaten Schlüssel, mit dem Sie das Zertifikat für die Managementoberfläche konfigurieren können.
  - Um Ihr eigenes Zertifikat hochzuladen, steht der private Schlüssel für das Zertifikat auf Ihrem lokalen Computer zur Verfügung.
  - Der private Schlüssel muss zum Zeitpunkt der Erstellung gespeichert oder aufgezeichnet worden sein. Wenn Sie nicht über den ursprünglichen privaten Schlüssel verfügen, müssen Sie einen neuen

erstellen.

- So bearbeiten Sie ein Clientzertifikat:
  - Sie haben die IP-Adresse oder den Domänennamen des Admin-Knotens.
  - Um Ihr eigenes Zertifikat oder ein neues Zertifikat hochzuladen, sind der private Schlüssel, das Clientzertifikat und die CA (sofern verwendet) auf Ihrem lokalen Computer verfügbar.

Fügen Sie Client-Zertifikate hinzu

Gehen Sie wie folgt vor, um das Clientzertifikat hinzuzufügen:

- Das Zertifikat der Managementoberfläche ist bereits konfiguriert
- KANN Client-Zertifikat AUSGESTELLT haben
- Zertifikat vom Grid Manager generiert

Das Zertifikat der Managementoberfläche ist bereits konfiguriert

Verwenden Sie diese Vorgehensweise, um ein Clientzertifikat hinzuzufügen, wenn bereits ein Zertifikat für eine Managementoberfläche mit einer vom Kunden bereitgestellten CA, einem Clientzertifikat und einem privaten Schlüssel konfiguriert wurde.

Schritte

1. Wählen Sie im Grid Manager die Option **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Client** aus.
2. Wählen Sie **Hinzufügen**.
3. Geben Sie einen Zertifikatnamen ein.
4. Um über Ihr externes Monitoring-Tool auf Prometheus-Kennzahlen zuzugreifen, wählen Sie **prometheus zulassen**.
5. Wählen Sie **Weiter**.
6. Laden Sie für den Schritt **Attach certificates** das Management Interface Zertifikat hoch.
   a. Wählen Sie **Zertifikat hochladen**.
   b. Wählen Sie **Browse** und wählen Sie die Zertifikatdatei der Verwaltungsschnittstelle aus (`.pem`).
      - Wählen Sie **Client Certificate Details** aus, um die Zertifikatmetadaten und das Zertifikat PEM anzuzeigen.
      - Wählen Sie **Zertifikat kopieren PEM** aus, um den Zertifikatinhalt zum Einfügen an eine andere Stelle zu kopieren.
   c. Wählen Sie **Erstellen**, um das Zertifikat im Grid Manager zu speichern.

      Das neue Zertifikat wird auf der Registerkarte Client angezeigt.
7. Konfiguration eines externen Überwachungstools, Wie Grafana.

KANN Client-Zertifikat AUSGESTELLT haben

Verwenden Sie dieses Verfahren, um ein Administrator-Client-Zertifikat hinzuzufügen, wenn ein Zertifikat der Verwaltungsschnittstelle nicht konfiguriert wurde und Sie planen, ein Client-Zertifikat für Prometheus hinzuzufügen, das ein vom Zertifizierungsstellen ausgestelltes Clientzertifikat und einen privaten Schlüssel verwendet.

Schritte

1. Führen Sie die Schritte zu aus "Konfigurieren Sie ein Zertifikat für die Managementoberfläche".
2. Wählen Sie im Grid Manager die Option **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Client** aus.
3. Wählen Sie **Hinzufügen**.
4. Geben Sie einen Zertifikatnamen ein.
5. Um über Ihr externes Monitoring-Tool auf Prometheus-Kennzahlen zuzugreifen, wählen Sie **prometheus zulassen**.
6. Wählen Sie **Weiter**.
7. Laden Sie für den Schritt **Attach certificates** das Clientzertifikat, den privaten Schlüssel und die CA-Bundle-Dateien hoch:
   a. Wählen Sie **Zertifikat hochladen**.
   b. Wählen Sie **Browse** aus, und wählen Sie das Clientzertifikat, den privaten Schlüssel und die CA-Paketdateien aus (`.pem`).
      - Wählen Sie **Client Certificate Details** aus, um die Zertifikatmetadaten und das Zertifikat PEM anzuzeigen.
      - Wählen Sie **Zertifikat kopieren PEM** aus, um den Zertifikatinhalt zum Einfügen an eine andere Stelle zu kopieren.
   c. Wählen Sie **Erstellen**, um das Zertifikat im Grid Manager zu speichern.

      Die neuen Zertifikate werden auf der Registerkarte Client angezeigt.
8. Konfiguration eines externen Überwachungstools, Wie Grafana.

Zertifikat vom Grid Manager generiert

Verwenden Sie dieses Verfahren, um ein Administrator-Client-Zertifikat hinzuzufügen, wenn ein Zertifikat der Verwaltungsschnittstelle nicht konfiguriert wurde und Sie planen, ein Clientzertifikat für Prometheus hinzuzufügen, das die Funktion Zertifikat generieren in Grid Manager verwendet.

Schritte

1. Wählen Sie im Grid Manager die Option **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Client** aus.
2. Wählen Sie **Hinzufügen**.
3. Geben Sie einen Zertifikatnamen ein.
4. Um über Ihr externes Monitoring-Tool auf Prometheus-Kennzahlen zuzugreifen, wählen Sie **prometheus zulassen**.
5. Wählen Sie **Weiter**.
6. Wählen Sie für den Schritt **Zertifikate anhängen Zertifikat generieren** aus.
7. Geben Sie die Zertifikatsinformationen an:
   - **Subject** (optional): X.509 Subject oder Distinguished Name (DN) des Zertifikateigentümers.
   - **Tage gültig**: Die Anzahl der Tage, an denen das generierte Zertifikat gültig ist, beginnend mit dem Zeitpunkt, an dem es generiert wird.
   - **Key-Usage-Erweiterungen hinzufügen**: Wenn ausgewählt (Standard und empfohlen), werden Key-

Usage und erweiterte Key-Usage-Erweiterungen zum generierten Zertifikat hinzugefügt.

Diese Erweiterungen definieren den Zweck des Schlüssels, der im Zertifikat enthalten ist.

Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, es treten Verbindungsprobleme mit älteren Clients auf, wenn diese Erweiterungen in Zertifikaten enthalten sind.

8. Wählen Sie **Erzeugen**.
9. Wählen Sie **Client-Zertifikatsdetails** aus, um die Zertifikatmetadaten und das PEM-Zertifikat anzuzeigen.

   Nach dem Schließen des Dialogfelds können Sie den privaten Zertifikatschlüssel nicht anzeigen. Kopieren Sie den Schlüssel an einem sicheren Ort.

   - Wählen Sie **Zertifikat kopieren PEM** aus, um den Zertifikatinhalt zum Einfügen an eine andere Stelle zu kopieren.
   - Wählen Sie **Zertifikat herunterladen**, um die Zertifikatdatei zu speichern.

     Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung `.pem`.

     Beispiel: `storagegrid_certificate.pem`

   - Wählen Sie **Privatschlüssel kopieren**, um den privaten Zertifikatschlüssel zum Einfügen an andere Orte zu kopieren.
   - Wählen Sie **privaten Schlüssel herunterladen**, um den privaten Schlüssel als Datei zu speichern.

     Geben Sie den Dateinamen des privaten Schlüssels und den Speicherort für den Download an.

10. Wählen Sie **Erstellen**, um das Zertifikat im Grid Manager zu speichern.

    Das neue Zertifikat wird auf der Registerkarte Client angezeigt.

11. Wählen Sie im Grid Manager die Option **KONFIGURATION** > **Sicherheit** > **Zertifikate** und wählen Sie dann die Registerkarte **Global** aus.
12. Wählen Sie **Management Interface Certificate** aus.
13. Wählen Sie **Benutzerdefiniertes Zertifikat verwenden**.
14. Laden Sie die Dateien Certificate.pem und private_key.pem aus dem hoch Details zum Clientzertifikat Schritt: Es ist nicht erforderlich, das CA-Paket hochzuladen.
    a. Wählen Sie **Zertifikat hochladen** und dann **Weiter**.
    b. Laden Sie jede Zertifikatdatei hoch (`.pem`).
    c. Wählen Sie **Erstellen**, um das Zertifikat im Grid Manager zu speichern.

       Das neue Zertifikat wird auf der Registerkarte Client angezeigt.

15. Konfiguration eines externen Überwachungstools, Wie Grafana.

Konfigurieren Sie ein externes Monitoring-Tool

Schritte

1. Konfigurieren Sie die folgenden Einstellungen für Ihr externes Monitoring-Tool, z. B. Grafana.
   a. **Name**: Geben Sie einen Namen für die Verbindung ein.

      StorageGRID benötigt diese Informationen nicht, Sie müssen jedoch einen Namen angeben, um die Verbindung zu testen.

   b. **URL**: Geben Sie den Domain-Namen oder die IP-Adresse für den Admin-Node ein. Geben Sie HTTPS und Port 9091 an.

      Beispiel: `https://admin-node.example.com:9091`

   c. Aktivieren Sie **TLS Client Auth** und **mit CA Cert**.
   d. Kopieren Sie unter TLS/SSL Auth Details und fügen Sie: + ein
      - Das Management-Interface-CA-Zertifikat nach **CA-Zertifikat**
      - Das Client-Zertifikat an **Client-Zertifikat**
      - Der private Schlüssel zu **Client Key**
   e. **ServerName**: Geben Sie den Domainnamen des Admin-Knotens ein.

      Servername muss mit dem Domänennamen übereinstimmen, wie er im Zertifikat der Verwaltungsschnittstelle angezeigt wird.

2. Speichern und testen Sie das Zertifikat und den privaten Schlüssel, das Sie aus StorageGRID oder einer lokalen Datei kopiert haben.

   Sie können jetzt mit Ihrem externen Monitoring Tool auf die Prometheus Kennzahlen von StorageGRID zugreifen.

   Weitere Informationen zu den Metriken finden Sie im "Anweisungen zur Überwachung von StorageGRID".

Client-Zertifikate bearbeiten

Sie können ein Administrator-Clientzertifikat bearbeiten, um seinen Namen zu ändern, Prometheus-Zugriff zu aktivieren oder zu deaktivieren oder ein neues Zertifikat hochzuladen, wenn das aktuelle Zertifikat abgelaufen ist.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Client** aus.

   In der Tabelle sind die Daten zum Ablauf des Zertifikats und die Zugriffsrechte für Prometheus aufgeführt. Wenn ein Zertifikat bald abläuft oder bereits abgelaufen ist, wird in der Tabelle eine Meldung angezeigt, und eine Warnmeldung wird ausgelöst.

2. Wählen Sie das Zertifikat aus, das Sie bearbeiten möchten.
3. Wählen Sie **Bearbeiten** und dann **Name und Berechtigung bearbeiten** aus
4. Geben Sie einen Zertifikatnamen ein.
5. Um über Ihr externes Monitoring-Tool auf Prometheus-Kennzahlen zuzugreifen, wählen Sie **prometheus zulassen**.

6. Wählen Sie **Weiter**, um das Zertifikat im Grid Manager zu speichern.

   Das aktualisierte Zertifikat wird auf der Registerkarte Client angezeigt.

Verbinden Sie das neue Clientzertifikat

Sie können ein neues Zertifikat hochladen, wenn das aktuelle Zertifikat abgelaufen ist.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Client** aus.

   In der Tabelle sind die Daten zum Ablauf des Zertifikats und die Zugriffsrechte für Prometheus aufgeführt. Wenn ein Zertifikat bald abläuft oder bereits abgelaufen ist, wird in der Tabelle eine Meldung angezeigt, und eine Warnmeldung wird ausgelöst.

2. Wählen Sie das Zertifikat aus, das Sie bearbeiten möchten.
3. Wählen Sie **Bearbeiten** und dann eine Bearbeitungsoption aus.

Zertifikat hochladen

Kopieren Sie den Zertifikatstext, um ihn an eine andere Stelle einzufügen.

a. Wählen Sie **Zertifikat hochladen** und dann **Weiter**.

b. Laden Sie den Namen des Clientzertifikats hoch (`.pem`).

   Wählen Sie **Client Certificate Details** aus, um die Zertifikatmetadaten und das Zertifikat PEM anzuzeigen.

   - Wählen Sie **Zertifikat herunterladen**, um die Zertifikatdatei zu speichern.

     Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung `.pem`.

   Beispiel: `storagegrid_certificate.pem`

   - Wählen Sie **Zertifikat kopieren PEM** aus, um den Zertifikatinhalt zum Einfügen an eine andere Stelle zu kopieren.

c. Wählen Sie **Erstellen**, um das Zertifikat im Grid Manager zu speichern.

   Das aktualisierte Zertifikat wird auf der Registerkarte Client angezeigt.

Zertifikat wird generiert

Generieren Sie den Zertifikattext, um ihn an anderer Stelle einzufügen.

a. Wählen Sie **Zertifikat erstellen**.

b. Geben Sie die Zertifikatsinformationen an:

   - **Subject** (optional): X.509 Subject oder Distinguished Name (DN) des Zertifikateigentümers.
   - **Tage gültig**: Die Anzahl der Tage, an denen das generierte Zertifikat gültig ist, beginnend mit dem Zeitpunkt, an dem es generiert wird.
   - **Key-Usage-Erweiterungen hinzufügen**: Wenn ausgewählt (Standard und empfohlen), werden Key-Usage und erweiterte Key-Usage-Erweiterungen zum generierten Zertifikat hinzugefügt.

     Diese Erweiterungen definieren den Zweck des Schlüssels, der im Zertifikat enthalten ist.

     Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, es treten Verbindungsprobleme mit älteren Clients auf, wenn diese Erweiterungen in Zertifikaten enthalten sind.

c. Wählen Sie **Erzeugen**.

d. Wählen Sie **Client Certificate Details** aus, um die Zertifikatmetadaten und das Zertifikat PEM anzuzeigen.

   Nach dem Schließen des Dialogfelds können Sie den privaten Zertifikatschlüssel nicht anzeigen. Kopieren Sie den Schlüssel an einem sicheren Ort.

   - Wählen Sie **Zertifikat kopieren PEM** aus, um den Zertifikatinhalt zum Einfügen an eine

andere Stelle zu kopieren.

- Wählen Sie **Zertifikat herunterladen**, um die Zertifikatdatei zu speichern.

  Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung `.pem`.

  Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Privatschlüssel kopieren**, um den privaten Zertifikatschlüssel zum Einfügen an andere Orte zu kopieren.
- Wählen Sie **privaten Schlüssel herunterladen**, um den privaten Schlüssel als Datei zu speichern.

  Geben Sie den Dateinamen des privaten Schlüssels und den Speicherort für den Download an.

e. Wählen Sie **Erstellen**, um das Zertifikat im Grid Manager zu speichern.

   Das neue Zertifikat wird auf der Registerkarte Client angezeigt.

Herunterladen oder Kopieren von Clientzertifikaten

Sie können ein Clientzertifikat zur Verwendung an anderer Stelle herunterladen oder kopieren.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Client** aus.
2. Wählen Sie das Zertifikat aus, das Sie kopieren oder herunterladen möchten.
3. Laden Sie das Zertifikat herunter oder kopieren Sie es.

Laden Sie die Zertifikatdatei herunter

Laden Sie das Zertifikat herunter `.pem` Datei:

a. Wählen Sie **Zertifikat herunterladen**.
b. Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung `.pem`.

   Beispiel: `storagegrid_certificate.pem`

Zertifikat kopieren

Kopieren Sie den Zertifikatstext, um ihn an eine andere Stelle einzufügen.

a. Wählen Sie **Zertifikat kopieren PEM**.
b. Fügen Sie das kopierte Zertifikat in einen Texteditor ein.
c. Speichern Sie die Textdatei mit der Erweiterung `.pem`.

   Beispiel: `storagegrid_certificate.pem`

Entfernen Sie Client-Zertifikate

Wenn Sie kein Administrator-Clientzertifikat mehr benötigen, können Sie es entfernen.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Client** aus.
2. Wählen Sie das Zertifikat aus, das Sie entfernen möchten.
3. Wählen Sie **Löschen** und bestätigen Sie dann.

> Um bis zu 10 Zertifikate zu entfernen, wählen Sie auf der Registerkarte Client jedes zu entfernende Zertifikat aus und wählen dann **Aktionen** > **Löschen** aus.

Nachdem ein Zertifikat entfernt wurde, müssen Clients, die das Zertifikat verwendet haben, ein neues Clientzertifikat angeben, um auf die StorageGRID Prometheus-Datenbank zuzugreifen.

Konfigurieren Sie die Sicherheitseinstellungen

Verwalten Sie die TLS- und SSH-Richtlinie

Die TLS- und SSH-Richtlinie legt fest, welche Protokolle und Chiffren verwendet werden, um sichere TLS-Verbindungen mit Clientanwendungen und sichere SSH-Verbindungen zu internen StorageGRID-Diensten herzustellen.

Die Sicherheitsrichtlinie steuert, wie TLS und SSH Daten in Bewegung verschlüsseln. Verwenden Sie im Allgemeinen die moderne Kompatibilitätsrichtlinie (Standard), es sei denn, Ihr System muss Common Criteria-konform sein oder Sie müssen andere Chiffren verwenden.

> Einige StorageGRID-Dienste wurden nicht aktualisiert, um die Chiffren in diesen Richtlinien zu verwenden.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Root-Zugriffsberechtigung".

Wählen Sie eine Sicherheitsrichtlinie aus

Schritte

1. Wählen Sie **CONFIGURATION** > **Security** > **Security settings**.

   Auf der Registerkarte **TLS und SSH Policies** werden die verfügbaren Richtlinien angezeigt. Die derzeit aktive Richtlinie wird durch ein grünes Häkchen auf der Kachel „Richtlinie“ gekennzeichnet.

2. Lesen Sie die Kacheln, um mehr über die verfügbaren Richtlinien zu erfahren.

Richtlinie	Beschreibung
Moderne Kompatibilität (Standard)	Verwenden Sie die Standardrichtlinie, wenn Sie eine starke Verschlüsselung benötigen und wenn Sie keine besonderen Anforderungen haben. Diese Richtlinie ist mit den meisten TLS- und SSH-Clients kompatibel.
Kompatibilität mit älteren Systemen	Verwenden Sie diese Richtlinie, wenn Sie zusätzliche Kompatibilitätsoptionen für ältere Clients benötigen. Die zusätzlichen Optionen in dieser Richtlinie machen sie möglicherweise weniger sicher als die moderne Kompatibilitätsrichtlinie.
Gemeinsame Kriterien	Verwenden Sie diese Richtlinie, wenn Sie eine Common Criteria-Zertifizierung benötigen.
FIPS-strikt	Verwenden Sie diese Richtlinie, wenn Sie eine Common Criteria-Zertifizierung benötigen und das NetApp Cryptographic Security Module 3.0.0 für externe Client-Verbindungen zu Load Balancer-Endpunkten, Tenant Manager und Grid Manager verwenden müssen. Die Verwendung dieser Richtlinie kann die Performance beeinträchtigen.
Individuell	Erstellen Sie eine benutzerdefinierte Richtlinie, wenn Sie Ihre eigenen Chiffren anwenden müssen.

3. Um Details zu den Chiffren, Protokollen und Algorithmen der einzelnen Richtlinien anzuzeigen, wählen Sie **Details anzeigen**.
4. Um die aktuelle Richtlinie zu ändern, wählen Sie **Richtlinie verwenden**.

   Ein grünes Häkchen erscheint neben **Aktuelle Richtlinie** auf der Policy-Kachel.

Erstellen Sie eine benutzerdefinierte Sicherheitsrichtlinie

Sie können eine benutzerdefinierte Richtlinie erstellen, wenn Sie Ihre eigenen Chiffren anwenden müssen.

Schritte

1. Wählen Sie auf der Kachel der Richtlinie, die der benutzerdefinierten Richtlinie, die Sie erstellen möchten, am ähnlichsten ist, **Details anzeigen** aus.
2. Wählen Sie **in Zwischenablage kopieren**, und wählen Sie dann **Abbrechen**.

3. Wählen Sie in der Kachel **Benutzerdefinierte Richtlinie** die Option **Konfigurieren und Verwenden** aus.
4. Fügen Sie die JSON ein, die Sie kopiert haben, und nehmen Sie alle erforderlichen Änderungen vor.
5. Wählen Sie **Richtlinie verwenden**.

   Auf der Kachel „Benutzerdefinierte Richtlinie“ wird ein grünes Häkchen neben **Aktuelle Richtlinie** angezeigt.

6. Wählen Sie optional **Konfiguration bearbeiten**, um weitere Änderungen an der neuen benutzerdefinierten Richtlinie vorzunehmen.

Vorübergehendes Zurücksetzen auf die Standard-Sicherheitsrichtlinie

Wenn Sie eine benutzerdefinierte Sicherheitsrichtlinie konfiguriert haben, können Sie sich möglicherweise nicht beim Grid Manager anmelden, wenn die konfigurierte TLS-Richtlinie nicht mit dem kompatibel ist "Serverzertifikat konfiguriert".

Sie können vorübergehend auf die Standard-Sicherheitsrichtlinie zurücksetzen.

Schritte

1. Melden Sie sich bei einem Admin-Knoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@Admin_Node_IP`
   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

      Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Führen Sie den folgenden Befehl aus:

   ```
   restore-default-cipher-configurations
   ```

3. Greifen Sie über einen Webbrowser auf den Grid Manager auf demselben Admin-Node zu.
4. Befolgen Sie die Schritte unter Wählen Sie eine Sicherheitsrichtlinie aus Um die Richtlinie erneut zu

konfigurieren.

Konfigurieren Sie die Netzwerk- und Objektsicherheit

Sie können die Netzwerk- und Objektsicherheit so konfigurieren, dass gespeicherte Objekte verschlüsselt, bestimmte S3- und Swift-Anforderungen verhindert oder Client-Verbindungen zu Storage-Nodes HTTP anstelle von HTTPS verwenden.

Verschlüsselung gespeicherter Objekte

Die gespeicherte Objektverschlüsselung ermöglicht die Verschlüsselung aller Objektdaten bei der Aufnahme über S3. Gespeicherte Objekte werden standardmäßig nicht verschlüsselt, aber Sie können Objekte mit dem AES-128- oder AES-256-Verschlüsselungsalgorithmus verschlüsseln. Wenn Sie die Einstellung aktivieren, werden alle neu aufgenommenen Objekte verschlüsselt, aber es werden keine Änderungen an vorhandenen gespeicherten Objekten vorgenommen. Wenn Sie die Verschlüsselung deaktivieren, bleiben derzeit verschlüsselte Objekte verschlüsselt, neu aufgenommene Objekte werden jedoch nicht verschlüsselt.

Die Einstellung für die Verschlüsselung gespeicherter Objekte ist nur für S3-Objekte anwendbar, die nicht durch Verschlüsselung auf Bucket-Ebene oder Objekt-Ebene verschlüsselt wurden.

Weitere Informationen zu Verschlüsselungsmethoden von StorageGRID finden Sie unter "Prüfen Sie die StorageGRID Verschlüsselungsmethoden".

Client-Änderung verhindern

Die Einstellung „Client-Änderung verhindern“ ist eine systemweite Einstellung. Wenn die Option **Client-Änderung verhindern** ausgewählt ist, werden die folgenden Anfragen abgelehnt.

S3-REST-API

- Bucket-Anforderungen löschen
- Alle Anforderungen, die das Ändern von Daten eines vorhandenen Objekts, benutzerdefinierter Metadaten oder S3-Objekt-Tagging zum Einsatz kommen

Swift REST API

- Container-Anforderungen löschen
- Anträge zum Ändern vorhandener Objekte. Beispielsweise werden folgende Vorgänge verweigert: Put Overwrite, Delete, Metadata Update usw.

Aktivieren Sie HTTP für Storage Node-Verbindungen

Standardmäßig verwenden Clientanwendungen das HTTPS-Netzwerkprotokoll für alle direkten Verbindungen zu Storage-Nodes. Optional können Sie HTTP für diese Verbindungen aktivieren, z. B. beim Testen eines nicht produktiven Grids.

Verwenden Sie HTTP für Storage-Node-Verbindungen nur, wenn S3- und Swift-Clients HTTP-Verbindungen direkt zu Storage-Nodes herstellen müssen. Sie müssen diese Option nicht für Clients verwenden, die nur HTTPS-Verbindungen verwenden, oder für Clients, die eine Verbindung zum Load Balancer-Dienst herstellen (weil Sie dies können "Konfigurieren Sie jeden Endpunkt der Lastverteilung" Zur Verwendung von HTTP oder HTTPS).

Siehe "Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen" Um zu erfahren, welche Ports S3

und Swift-Clients bei der Verbindung zu Storage-Nodes über HTTP oder HTTPS verwenden.

Wählen Sie Optionen aus

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben Root-Zugriffsberechtigung.

Schritte

1. Wählen Sie **CONFIGURATION** > **Security** > **Security settings**.
2. Wählen Sie die Registerkarte **Netzwerk und Objekte**.
3. Verwenden Sie für die Verschlüsselung gespeicherter Objekte die Einstellung **None** (Standard), wenn Sie keine Verschlüsselung gespeicherter Objekte wünschen, oder wählen Sie **AES-128** oder **AES-256**, um gespeicherte Objekte zu verschlüsseln.
4. Wählen Sie optional **Client-Änderung verhindern**, wenn Sie S3- und Swift-Clients daran hindern möchten, spezifische Anforderungen zu stellen.

   Wenn Sie diese Einstellung ändern, dauert es etwa eine Minute, bis die neue Einstellung angewendet wird. Der konfigurierte Wert wird für Performance und Skalierung zwischengespeichert.

5. Wählen Sie optional **HTTP für Storage Node-Verbindungen aktivieren**, wenn Clients direkt mit Storage Nodes verbunden sind und Sie HTTP-Verbindungen verwenden möchten.

   Gehen Sie vorsichtig vor, wenn Sie HTTP für ein Produktions-Grid aktivieren, da die Anforderungen unverschlüsselt gesendet werden.

6. Wählen Sie **Speichern**.

Zeitlimit für Inaktivität des Browsers ändern

Sie können steuern, ob Grid Manager und Tenant Manager-Benutzer abgemeldet werden, wenn sie länger als eine bestimmte Zeit inaktiv sind.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben Root-Zugriffsberechtigung.

Über diese Aufgabe

Das Zeitlimit für die Inaktivität des Browsers beträgt standardmäßig 15 Minuten. Wenn der Browser eines Benutzers für diese Zeit nicht aktiv ist, wird der Benutzer abgemeldet.

Bei Bedarf können Sie die Sperrzeit erhöhen oder verringern, indem Sie die Option * Inaktive Benutzer abmelden nach* einstellen.

Das Zeitlimit für die Inaktivität des Browsers wird auch durch Folgendes gesteuert:

- Ein separater, nicht konfigurierbarer StorageGRID-Timer, der für die Systemsicherheit enthalten ist. Standardmäßig läuft das Authentifizierungs-Token jedes Benutzers 16 Stunden nach der Anmeldung des Benutzers ab. Wenn die Authentifizierung eines Benutzers abläuft, wird dieser Benutzer automatisch

abgemeldet, auch wenn das Zeitlimit für die Inaktivität des Browsers deaktiviert ist oder der Wert für das Browsertimeout nicht erreicht wurde. Um das Token zu erneuern, muss sich der Benutzer erneut anmelden.

- Timeout-Einstellungen für den Identitäts-Provider, vorausgesetzt, Single Sign-On (SSO) ist für StorageGRID aktiviert.

  Wenn SSO aktiviert ist und der Browser eines Benutzers eine Zeitdauer ausläuft, muss der Benutzer seine SSO-Anmeldeinformationen erneut eingeben, um erneut auf StorageGRID zuzugreifen. Siehe "Konfigurieren Sie Single Sign-On".

Schritte

1. Wählen Sie **CONFIGURATION** > **Security** > **Security settings**.
2. Wählen Sie die Registerkarte **Browser Inaktivität Timeout**.
3. Geben Sie im Feld **Abmelden inaktiver Benutzer nach** einen Browser-Timeout-Zeitraum zwischen 60 Sekunden und 7 Tagen an.

   Sie können die Zeitüberschreitung des Browsers in Sekunden, Minuten, Stunden oder Tagen angeben.

4. Wählen Sie **Speichern**. Wenn ein Browser für die angegebene Zeit inaktiv ist, wird der Benutzer vom Grid Manager oder Tenant Manager abgemeldet.

   Die neue Einstellung hat keine Auswirkung auf die derzeit angemeldenen Benutzer. Benutzer müssen sich erneut anmelden oder ihre Browser aktualisieren, damit die neue Timeout-Einstellung wirksam wird.

Konfigurieren von Verschlüsselungsmanagement-Servern

Key Management-Server konfigurieren: Übersicht

Sie können einen oder mehrere externe Verschlüsselungsmanagement-Server (KMS) konfigurieren, um die Daten auf speziell konfigurierten Appliance-Nodes zu schützen.

Was ist ein KMS (Key Management Server)?

Ein Verschlüsselungsmanagement-Server (KMS) ist ein externes Drittanbietersystem, das mithilfe des Key Management Interoperability Protocol (KMIP) Verschlüsselungen für die StorageGRID Appliance-Nodes am zugehörigen StorageGRID Standort bereitstellt.

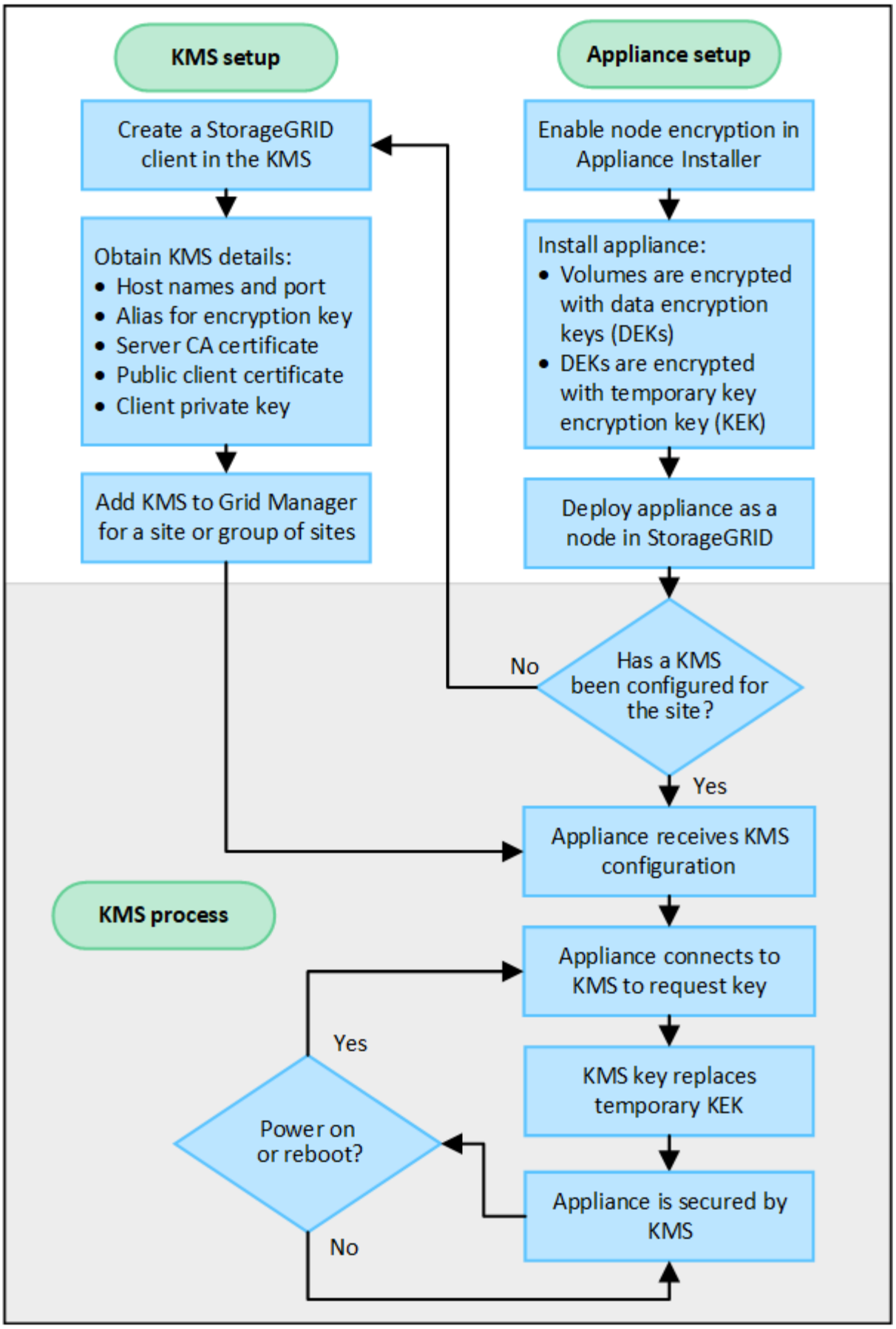
Sie können einen oder mehrere Schlüsselverwaltungsserver verwenden, um die Knotenverschlüsselungsschlüssel für alle StorageGRID Appliance-Knoten zu verwalten, deren **Node-Verschlüsselung**-Einstellung während der Installation aktiviert ist. Durch den Einsatz von Verschlüsselungsmanagement-Servern mit diesen Appliance-Nodes können Sie Ihre Daten selbst dann schützen, wenn eine Appliance aus dem Datacenter entfernt wird. Nachdem die Appliance-Volumes verschlüsselt wurden, können Sie nur auf Daten auf der Appliance zugreifen, wenn der Node mit dem KMS kommunizieren kann.

StorageGRID erstellt oder verwaltet keine externen Schlüssel, die zur Verschlüsselung und Entschlüsselung von Appliance-Nodes verwendet werden. Wenn Sie Vorhaben, einen externen Verschlüsselungsmanagementserver zum Schutz von StorageGRID-Daten zu verwenden, müssen Sie wissen, wie Sie diesen Server einrichten, und wissen, wie Sie die Verschlüsselungsschlüssel managen. Die Ausführung wichtiger Managementaufgaben geht über diesen Anweisungen hinaus. Wenn Sie Hilfe benötigen, lesen Sie die Dokumentation für Ihren zentralen Managementserver, oder wenden Sie sich an den technischen Support.

Überblick über die KMS- und Appliance-Konfiguration

Bevor der Verschlüsselungsmanagement-Server (KMS) die StorageGRID-Daten auf Appliance-Nodes sichern kann, müssen zwei Konfigurationsaufgaben durchgeführt werden: Ein oder mehrere KMS-Server einrichten und die Node-Verschlüsselung für die Appliance-Nodes aktivieren. Wenn diese beiden Konfigurationsaufgaben abgeschlossen sind, erfolgt automatisch der Verschlüsselungsmanagementprozess.

Das Flussdiagramm zeigt die grundlegenden Schritte bei der Verwendung eines KMS zur Sicherung von StorageGRID-Daten auf Appliance-Nodes.



Das Flussdiagramm zeigt die parallele Einrichtung von KMS und die Einrichtung der Appliance. Sie können

jedoch die Verschlüsselungsmanagement-Server je nach Ihren Anforderungen vor oder nach Aktivierung der Node-Verschlüsselung für neue Appliance-Nodes einrichten.

Einrichten des Verschlüsselungsmanagement-Servers (KMS)

Die Einrichtung eines Schlüsselverwaltungsservers umfasst die folgenden grundlegenden Schritte.

Schritt	Siehe
Greifen Sie auf die KMS-Software zu und fügen Sie jedem KMS- oder KMS-Cluster einen Client für StorageGRID hinzu.	"Konfigurieren Sie StorageGRID als Client im KMS"
Erhalten Sie die erforderlichen Informationen für den StorageGRID-Client auf dem KMS.	"Konfigurieren Sie StorageGRID als Client im KMS"
Fügen Sie den KMS dem Grid Manager hinzu, weisen Sie ihn einer einzelnen Site oder einer Standardgruppe von Standorten zu, laden Sie die erforderlichen Zertifikate hoch und speichern Sie die KMS-Konfiguration.	"Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)"

Richten Sie das Gerät ein

Die Einrichtung eines Appliance-Nodes für die KMS-Nutzung umfasst die folgenden grundlegenden Schritte.

1. Verwenden Sie während der Hardware-Konfigurationsphase der Appliance-Installation das Installationsprogramm von StorageGRID Appliance, um die Einstellung **Node-Verschlüsselung** für die Appliance zu aktivieren.

   > Sie können die Einstellung **Node Encryption** nicht aktivieren, nachdem eine Appliance zum Grid hinzugefügt wurde, und Sie können keine externe Schlüsselverwaltung für Geräte verwenden, für die keine Knotenverschlüsselung aktiviert ist.

2. Führen Sie das Installationsprogramm für die StorageGRID-Appliance aus. Während der Installation wird jedem Appliance-Volume ein zufälliger Datenverschlüsselungsschlüssel (random Data Encryption Key, DEK) zugewiesen:
   - Die DEKs werden verwendet, um die Daten auf jedem Volume zu verschlüsseln. Diese Schlüssel werden mit der Linux Unified Key Setup (LUKS)-Festplattenverschlüsselung im Betriebssystem der Appliance generiert und können nicht geändert werden.
   - Jede einzelne DEK wird durch einen Master Key Encryption Key (KEK) verschlüsselt. Bei der ersten KEK handelt es sich um einen temporären Schlüssel, der die DEKs verschlüsselt, bis das Gerät eine Verbindung mit dem KMS herstellen kann.
3. Fügen Sie den Appliance-Node StorageGRID hinzu.

Siehe "Aktivieren Sie die Node-Verschlüsselung" Entsprechende Details.

Verschlüsselungsmanagementprozess (wird automatisch durchgeführt)

Die Verschlüsselung des Verschlüsselungsmanagement umfasst die folgenden grundlegenden Schritte, die automatisch durchgeführt werden.

1. Wenn Sie eine Appliance installieren, bei der die Node-Verschlüsselung im Grid aktiviert ist, bestimmt StorageGRID, ob für den Standort, der den neuen Node enthält, eine KMS-Konfiguration vorhanden ist.
   - Wenn bereits ein KMS für den Standort konfiguriert wurde, erhält die Appliance die KMS-Konfiguration.
   - Wenn ein KMS für den Standort noch nicht konfiguriert wurde, werden die Daten auf der Appliance weiterhin durch die temporäre KEK verschlüsselt, bis Sie einen KMS für den Standort konfigurieren und die Appliance die KMS-Konfiguration erhält.
2. Die Appliance verwendet die KMS-Konfiguration, um eine Verbindung zum KMS herzustellen und einen Verschlüsselungsschlüssel anzufordern.
3. Der KMS sendet einen Verschlüsselungsschlüssel an die Appliance. Der neue Schlüssel des KMS ersetzt die temporäre KEK und wird nun zur Verschlüsselung und Entschlüsselung der DEKs für die Appliance-Volumes verwendet.

> Alle Daten, die vor der Verbindung des verschlüsselten Appliance-Nodes mit dem konfigurierten KMS vorhanden sind, werden mit einem temporären Schlüssel verschlüsselt. Die Appliance-Volumes sollten jedoch erst dann als vor Entfernung aus dem Datacenter geschützt betrachtet werden, wenn der temporäre Schlüssel durch den KMS-Schlüssel ersetzt wird.

4. Wenn die Appliance eingeschaltet oder neu gestartet wird, stellt sie eine Verbindung zum KMS her, um den Schlüssel anzufordern. Der Schlüssel, der im flüchtigen Speicher gespeichert ist, kann einen Stromausfall oder einen Neustart nicht überleben.

Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers

Bevor Sie einen externen KMS (Key Management Server) konfigurieren, müssen Sie die Überlegungen und Anforderungen verstehen.

Was sind die KMIP-Anforderungen?

StorageGRID unterstützt KMIP Version 1.4.

"Spezifikation Des Key Management Interoperability Protocol Version 1.4"

Für die Kommunikation zwischen den Appliance-Nodes und dem konfigurierten KMS werden sichere TLS-Verbindungen verwendet. StorageGRID unterstützt die folgenden TLS v1.2-Chiffren für KMIP:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Sie müssen sicherstellen, dass jeder Appliance-Node, der Node-Verschlüsselung verwendet, Netzwerkzugriff auf den für den Standort konfigurierten KMS- oder KMS-Cluster hat.

Die Netzwerk-Firewall-Einstellungen müssen es jedem Appliance-Node ermöglichen, über den Port zu kommunizieren, der für KMIP-Kommunikation (Key Management Interoperability Protocol) verwendet wird. Der KMIP-Standardport ist 5696.

Welche Appliances werden unterstützt?

Sie können einen Schlüsselverwaltungsserver (KMS) verwenden, um Verschlüsselungsschlüssel für jede StorageGRID-Appliance in Ihrem Grid zu verwalten, auf der die Einstellung **Node-Verschlüsselung** aktiviert ist. Diese Einstellung kann nur während der Hardware-Konfigurationsphase der Appliance-Installation mithilfe des StorageGRID Appliance Installer aktiviert werden.

Nach dem Hinzufügen einer Appliance zum Grid kann die Node-Verschlüsselung nicht aktiviert werden. Zudem kann kein externes Verschlüsselungsmanagement für Appliances verwendet werden, bei denen die Node-Verschlüsselung nicht aktiviert ist.

Sie können das konfigurierte KMS für StorageGRID-Appliances und Appliance-Nodes verwenden.

Sie können das konfigurierte KMS nicht für softwarebasierte (nicht-Appliance-)Knoten verwenden, einschließlich der folgenden:

- Als Virtual Machines (VMs) implementierte Nodes
- Nodes, die in Container-Engines auf Linux Hosts implementiert sind

Auf diesen anderen Plattformen implementierte Nodes können Verschlüsselung außerhalb von StorageGRID auf Datenspeicher- oder Festplattenebene verwenden.

Wann sollte ich wichtige Management-Server konfigurieren?

Bei einer neuen Installation sollten Sie in der Regel einen oder mehrere Schlüsselverwaltungsserver im Grid Manager einrichten, bevor Sie Mandanten erstellen. Diese Reihenfolge stellt sicher, dass die Nodes geschützt sind, bevor Objektdaten auf ihnen gespeichert werden.

Sie können die Schlüsselverwaltungsserver im Grid Manager vor oder nach der Installation der Appliance-Knoten konfigurieren.

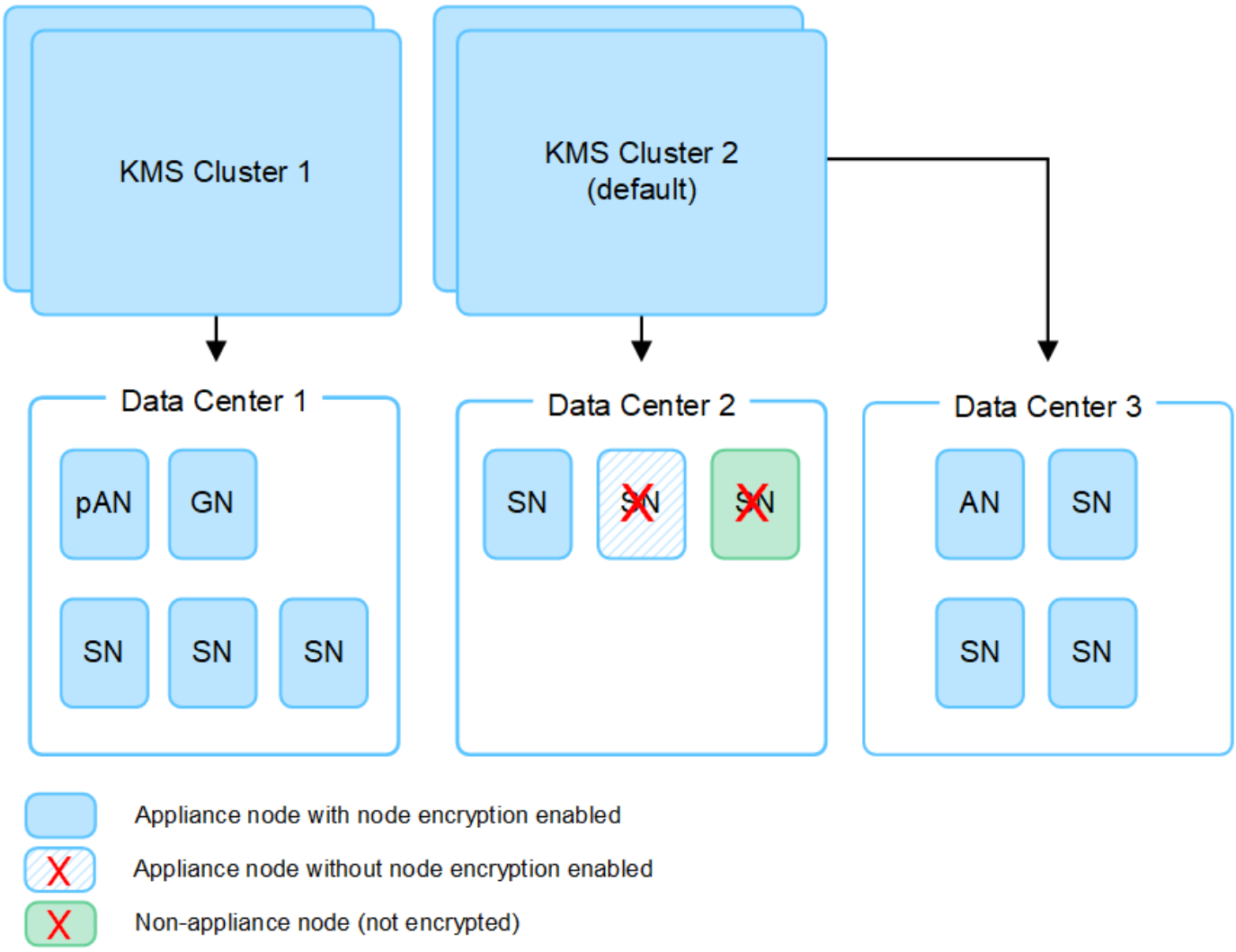
Wie viele wichtige Management Server brauche ich?

Sie können einen oder mehrere externe Verschlüsselungsmanagementserver konfigurieren, um die Appliance-Nodes in Ihrem StorageGRID-System Verschlüsselungen bereitzustellen. Jeder KMS stellt den StorageGRID Appliance-Nodes an einem einzelnen Standort oder einer Gruppe von Standorten einen einzelnen Verschlüsselungsschlüssel zur Verfügung.

StorageGRID unterstützt die Verwendung von KMS-Clustern. Jeder KMS-Cluster enthält mehrere replizierte Verschlüsselungsmanagement-Server, die Konfigurationseinstellungen und Verschlüsselungen teilen. Die Verwendung von KMS-Clustern für das Verschlüsselungsmanagement wird empfohlen, da dadurch die Failover-Funktionen einer Hochverfügbarkeitskonfiguration verbessert werden.

Nehmen Sie beispielsweise an, Ihr StorageGRID System verfügt über drei Datacenter-Standorte. Sie können ein KMS-Cluster konfigurieren, um allen Appliance-Nodes in Datacenter 1 und einem zweiten KMS-Cluster einen Schlüssel für alle Appliance-Nodes an allen anderen Standorten bereitzustellen. Wenn Sie den zweiten KMS-Cluster hinzufügen, können Sie einen Standard-KMS für Datacenter 2 und Datacenter 3 konfigurieren.

Beachten Sie, dass Sie kein KMS für nicht-Appliance-Knoten oder für alle Appliance-Knoten verwenden können, für die die Einstellung **Node Encryption** während der Installation nicht aktiviert war.



Was passiert, wenn eine Taste gedreht wird?

Als bewährte Sicherheitsmethode sollten Sie den Verschlüsselungsschlüssel, der von jedem konfigurierten KMS verwendet wird, regelmäßig drehen.

Wenn Sie den Verschlüsselungsschlüssel drehen, verwenden Sie die KMS-Software, um von der letzten verwendeten Version des Schlüssels auf eine neue Version desselben Schlüssels zu drehen. Drehen Sie nicht zu einer ganz anderen Taste.

> Versuchen Sie niemals, einen Schlüssel zu drehen, indem Sie den Schlüsselnamen (Alias) für den KMS im Grid Manager ändern. Drehen Sie stattdessen den Schlüssel, indem Sie die Schlüsselversion in der KMS-Software aktualisieren. Verwenden Sie denselben Schlüssel-Alias für neue Schlüssel, wie sie für vorherige Schlüssel verwendet wurden. Wenn Sie den Schlüssel-Alias für einen konfigurierten KMS ändern, kann StorageGRID Ihre Daten möglicherweise nicht entschlüsseln.

Wenn die neue Schlüsselversion verfügbar ist:

- Die Appliance wird automatisch auf die verschlüsselten Appliance-Nodes am Standort oder an den dem KMS zugeordneten Standorten verteilt. Die Verteilung sollte innerhalb einer Stunde erfolgen, wenn der Schlüssel gedreht wird.

- Wenn der Node der verschlüsselten Appliance offline ist, wenn die neue Schlüsselversion verteilt ist, erhält der Node den neuen Schlüssel, sobald er neu gebootet wird.
- Wenn die neue Schlüsselversion aus irgendeinem Grund nicht zur Verschlüsselung von Appliance-Volumes verwendet werden kann, wird der Alarm **KMS-Schlüsselrotation fehlgeschlagen** für den Appliance-Knoten ausgelöst. Möglicherweise müssen Sie sich an den technischen Support wenden, um Hilfe bei der Lösung dieses Alarms zu erhalten.

Kann ich einen Appliance-Knoten nach der Verschlüsselung wiederverwenden?

Wenn Sie eine verschlüsselte Appliance in einem anderen StorageGRID System installieren müssen, müssen Sie zuerst den Grid-Node außer Betrieb nehmen, um Objektdaten auf einen anderen Node zu verschieben. Anschließend können Sie das Installationsprogramm der StorageGRID-Appliance für verwenden "Löschen Sie die KMS-Konfiguration". Durch das Löschen der KMS-Konfiguration wird die **Node Encryption**-Einstellung deaktiviert und die Zuordnung zwischen dem Appliance-Knoten und der KMS-Konfiguration für den StorageGRID-Standort wird aufgehoben.

> Der Zugriff auf den KMS-Verschlüsselungsschlüssel ist ausgeschlossen, dass alle Daten, die auf der Appliance verbleiben, nicht mehr zugänglich sind und dauerhaft gesperrt werden.

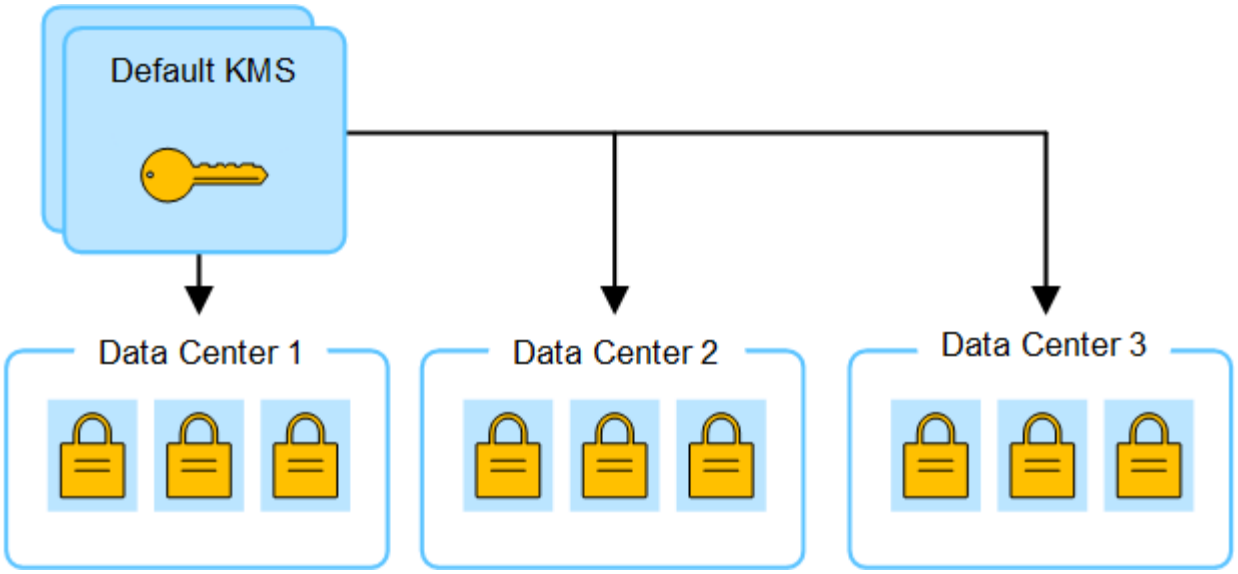
Überlegungen für das Ändern des KMS für einen Standort

Jeder Verschlüsselungsmanagement-Server (KMS) oder KMS-Cluster gewährt allen Appliance-Nodes an einem einzelnen Standort oder einer Gruppe von Standorten einen Verschlüsselungsschlüssel. Wenn Sie ändern müssen, welcher KMS für einen Standort verwendet wird, müssen Sie den Verschlüsselungsschlüssel möglicherweise von einem KMS auf einen anderen kopieren.

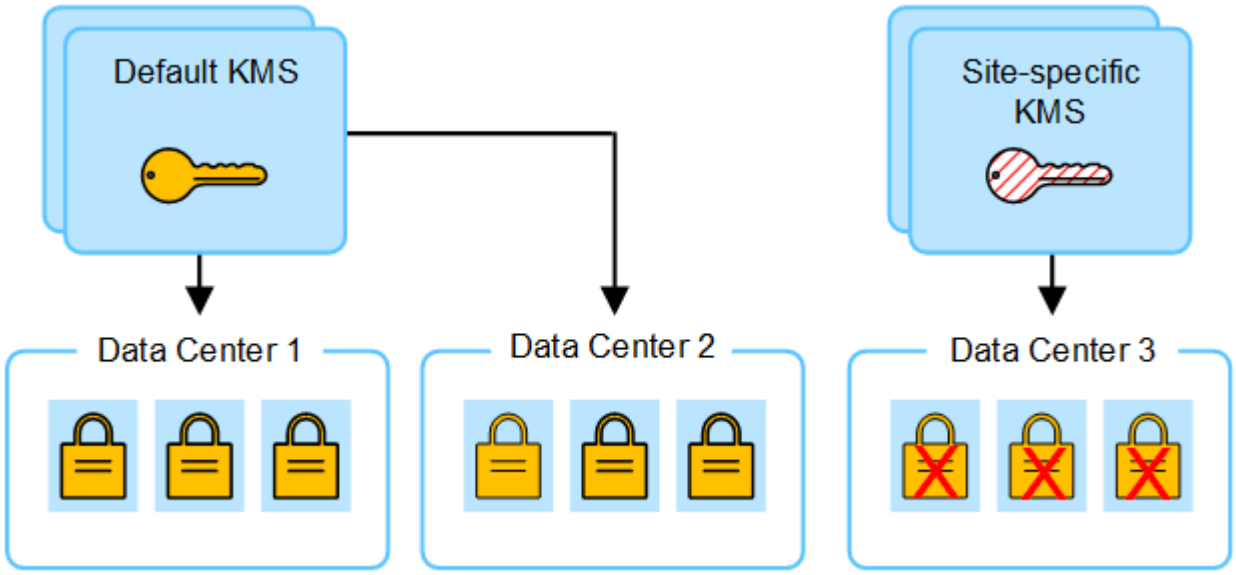
Wenn Sie den KMS ändern, der für einen Standort verwendet wird, müssen Sie sicherstellen, dass die zuvor verschlüsselten Appliance-Nodes an diesem Standort mit dem auf dem neuen KMS gespeicherten Schlüssel entschlüsselt werden können. In einigen Fällen müssen Sie möglicherweise die aktuelle Version des Verschlüsselungsschlüssels vom ursprünglichen KMS auf den neuen KMS kopieren. Sie müssen sicherstellen, dass der KMS über den richtigen Schlüssel verfügt, um die verschlüsselten Appliance-Nodes am Standort zu entschlüsseln.

Beispiel:

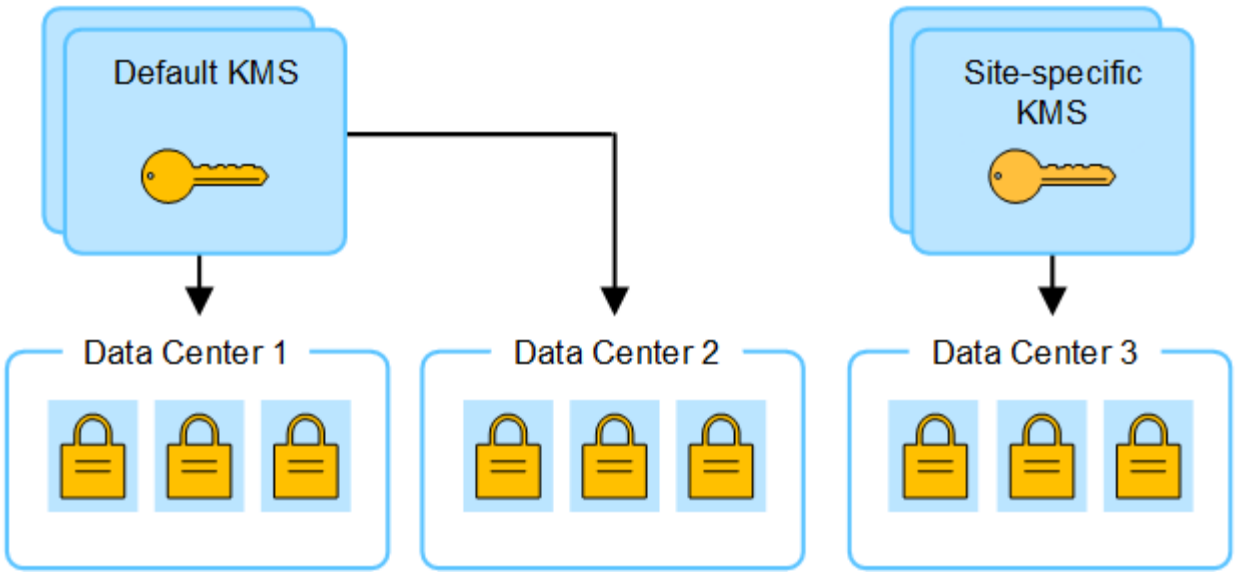
1. Sie konfigurieren zunächst ein Standard-KMS, das für alle Standorte gilt, die kein dediziertes KMS haben.
2. Wenn der KMS gespeichert wird, stellen alle Appliance-Nodes, deren **Node Encryption**-Einstellung aktiviert ist, eine Verbindung zum KMS her und fordern den Verschlüsselungsschlüssel an. Dieser Schlüssel wird verwendet, um die Appliance-Nodes an allen Standorten zu verschlüsseln. Dieser Schlüssel muss auch verwendet werden, um diese Geräte zu entschlüsseln.



3. Sie entscheiden, einen standortspezifischen KMS für einen Standort hinzuzufügen (Datacenter 3 in der Abbildung). Da die Appliance-Nodes jedoch bereits verschlüsselt sind, tritt ein Validierungsfehler auf, wenn Sie versuchen, die Konfiguration für den standortspezifischen KMS zu speichern. Der Fehler tritt auf, weil der standortspezifische KMS nicht über den korrekten Schlüssel verfügt, um die Knoten an diesem Standort zu entschlüsseln.



4. Um das Problem zu beheben, kopieren Sie die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS auf den neuen KMS. (Technisch kopieren Sie den Originalschlüssel in einen neuen Schlüssel mit dem gleichen Alias. Der ursprüngliche Schlüssel wird zu einer früheren Version des neuen Schlüssels.) Der standortspezifische KMS hat jetzt den richtigen Schlüssel zur Entschlüsselung der Appliance-Nodes in Datacenter 3, sodass er in StorageGRID gespeichert werden kann.



Anwendungsfälle für die Änderung, welcher KMS für eine Site verwendet wird

Die Tabelle fasst die erforderlichen Schritte für die häufigsten Fälle zur Änderung des KMS für einen Standort zusammen.

Anwendungsfall zum Ändern des KMS einer Site	Erforderliche Schritte
Sie haben einen oder mehrere Site-spezifische KMS-Einträge, und Sie möchten einen von ihnen als Standard-KMS verwenden.	Bearbeiten Sie den Site-spezifischen KMS. Wählen Sie im Feld **verwaltet Schlüssel für** die Option **Sites, die nicht von einem anderen KMS verwaltet werden (Standard KMS)**. Der Site-spezifische KMS wird jetzt als Standard-KMS verwendet. Sie gilt für alle Standorte, die kein dediziertes KMS haben. "Bearbeiten eines Verschlüsselungsmanagement-Servers (KMS)"
Sie haben einen Standard-KMS, und Sie fügen eine neue Site in einer Erweiterung hinzu. Sie möchten nicht das Standard-KMS für den neuen Standort verwenden.	1. Wenn die Appliance-Nodes auf dem neuen Standort bereits durch den Standard-KMS verschlüsselt wurden, kopieren Sie mithilfe der KMS-Software die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS auf einen neuen KMS. 2. Fügen Sie mithilfe des Grid-Managers den neuen KMS hinzu und wählen Sie die Site aus. "Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)"
Sie möchten, dass der KMS für eine Site einen anderen Server verwendet.	1. Wenn die Appliance-Nodes am Standort bereits durch den vorhandenen KMS verschlüsselt wurden, kopieren Sie mithilfe der KMS-Software die aktuelle Version des Verschlüsselungsschlüssels vom bestehenden KMS auf den neuen KMS. 2. Bearbeiten Sie mithilfe des Grid Manager die bestehende KMS-Konfiguration und geben Sie den neuen Hostnamen oder die neue IP-Adresse ein. "Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)"

Sie müssen StorageGRID als Client für jeden externen Verschlüsselungsmanagement-Server oder KMS-Cluster konfigurieren, bevor Sie den KMS StorageGRID hinzufügen können.

Über diese Aufgabe

Diese Anweisungen gelten für Thales CipherTrust Manager. Eine Liste der unterstützten Versionen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool (IMT)".

Schritte

1. Erstellen Sie von der KMS-Software einen StorageGRID-Client für jeden KMS- oder KMS-Cluster, den Sie verwenden möchten.

   Jeder KMS managt einen einzelnen Verschlüsselungsschlüssel für die Nodes der StorageGRID Appliances an einem einzelnen Standort oder einer Gruppe von Standorten.

2. Erstellen Sie von der KMS-Software einen AES-Verschlüsselungsschlüssel für jedes KMS- oder KMS-Cluster.

   Der Verschlüsselungsschlüssel muss mindestens 2,048 Bit haben und exportierbar sein.

3. Notieren Sie die folgenden Informationen für jeden KMS- oder KMS-Cluster.

   Diese Informationen benötigen Sie, wenn Sie den KMS StorageGRID hinzufügen.

   - Host-Name oder IP-Adresse für jeden Server.
   - Der vom KMS verwendete KMIP-Port.
   - Schlüsselalias für den Verschlüsselungsschlüssel im KMS.

   > Der Verschlüsselungsschlüssel muss bereits im KMS vorhanden sein. StorageGRID erstellt oder managt keine KMS-Schlüssel.

4. Beziehen Sie für jeden KMS- oder KMS-Cluster ein Serverzertifikat, das von einer Zertifizierungsstelle (CA) signiert wurde, oder ein Zertifikatbündel, das jede der PEM-kodierten CA-Zertifikatdateien enthält, die in der Reihenfolge der Zertifikatskette verkettet sind.

   Das Serverzertifikat ermöglicht es dem externen KMS, sich bei StorageGRID zu authentifizieren.

   - Das Zertifikat muss das mit Privacy Enhanced Mail (PEM) Base-64 codierte X.509-Format verwenden.
   - Das Feld für alternativen Servernamen (SAN) in jedem Serverzertifikat muss den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse enthalten, mit der StorageGRID eine Verbindung herstellt.

     > Wenn Sie den KMS in StorageGRID konfigurieren, müssen Sie dieselben FQDNs oder IP-Adressen im Feld **Hostname** eingeben.

   - Das Serverzertifikat muss mit dem Zertifikat übereinstimmen, das von der KMIP-Schnittstelle des KMS verwendet wird. In der Regel wird Port 5696 verwendet.

5. Holen Sie sich das öffentliche Clientzertifikat, das vom externen KMS an StorageGRID ausgestellt wurde, und den privaten Schlüssel für das Clientzertifikat.

Das Client-Zertifikat ermöglicht StorageGRID, sich am KMS zu authentifizieren.

Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)

Mithilfe des Assistenten für den StorageGRID-Verschlüsselungsmanagement-Server können Sie jeden KMS- oder KMS-Cluster hinzufügen.

Bevor Sie beginnen

- Sie haben die geprüft "Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers".
- Das ist schon "StorageGRID wurde als Client im KMS konfiguriert", Und Sie haben die erforderlichen Informationen für jeden KMS- oder KMS-Cluster.
- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die Root-Zugriffsberechtigung.

Über diese Aufgabe

Konfigurieren Sie, falls möglich, Site-spezifische Verschlüsselungsmanagement-Server, bevor Sie einen Standard-KMS konfigurieren, der für alle Standorte gilt, die nicht von einem anderen KMS gemanagt werden. Wenn Sie zuerst den Standard-KMS erstellen, werden alle Node-verschlüsselten Appliances im Grid durch den Standard-KMS verschlüsselt. Wenn Sie später einen Site-spezifischen KMS erstellen möchten, müssen Sie zuerst die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS auf den neuen KMS kopieren. Siehe "Überlegungen für das Ändern des KMS für einen Standort" Entsprechende Details.

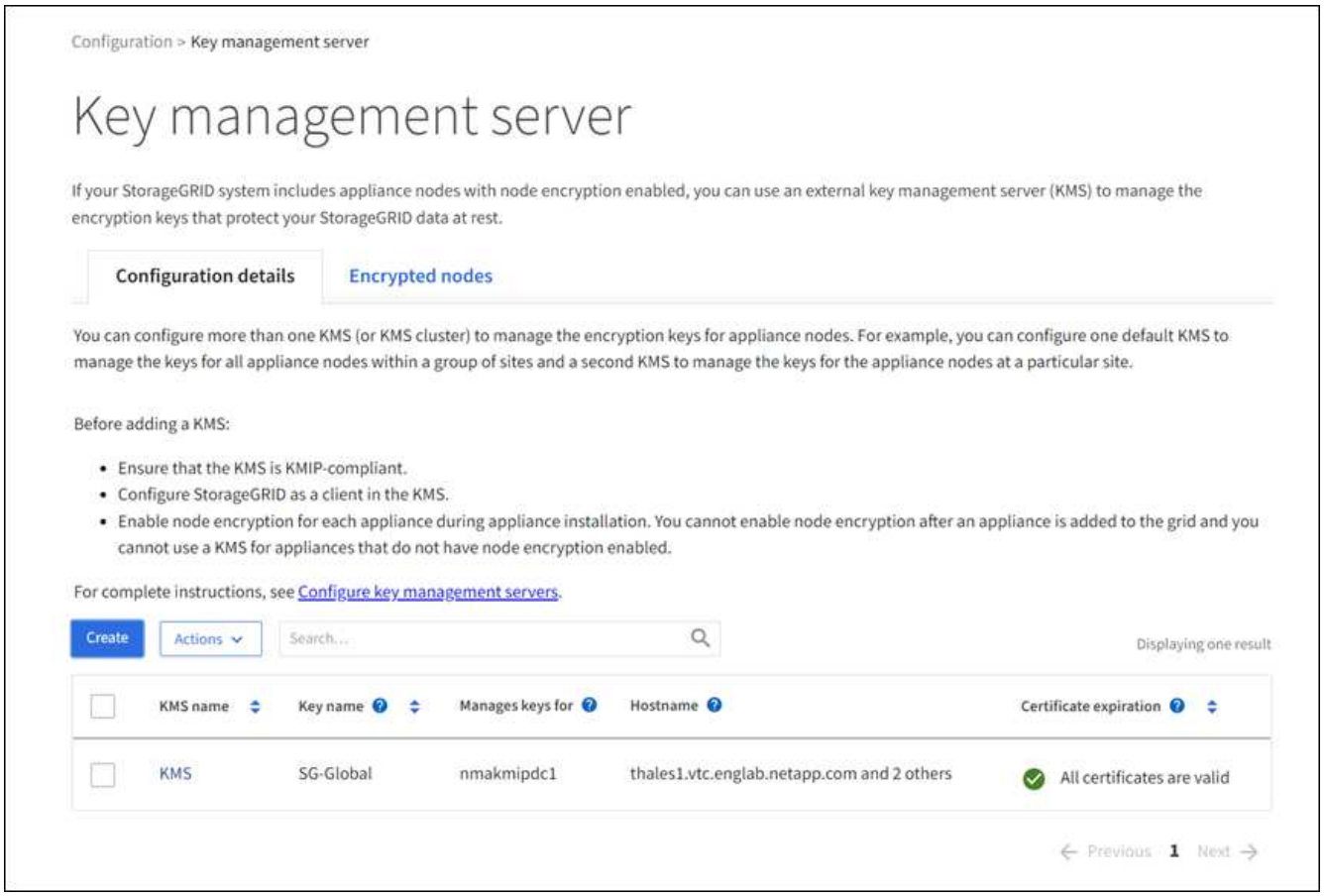
Schritt 1: KM Details

In Schritt 1 (KMS-Details) des Assistenten zum Hinzufügen eines Schlüsselverwaltungsservers geben Sie Details zum KMS- oder KMS-Cluster an.

Schritte

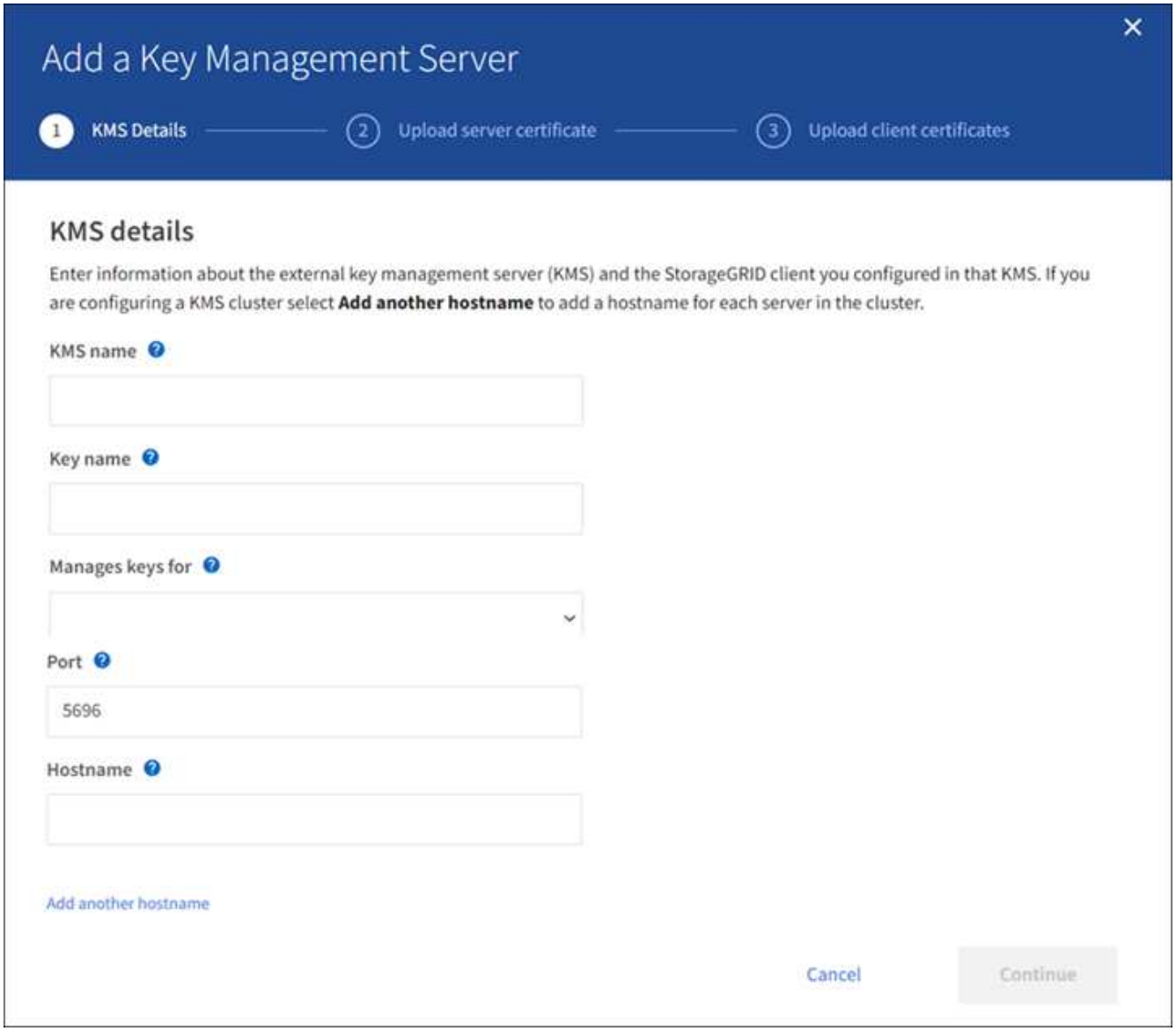
1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Schlüsselverwaltungsserver** aus.

   Die Seite Key Management Server wird angezeigt, und die Registerkarte Configuration Details ist ausgewählt.



2. Wählen Sie **Erstellen**.

   Schritt 1 (KMS-Details) des Assistenten zum Hinzufügen eines Schlüsselverwaltungsservers wird angezeigt.



3. Geben Sie die folgenden Informationen für den KMS und den StorageGRID-Client ein, den Sie in diesem KMS konfiguriert haben.

Feld	Beschreibung
KMS-Name	Einen beschreibenden Namen, der Ihnen bei der Identifizierung dieses KMS hilft. Muss zwischen 1 und 64 Zeichen liegen.
Schlüsselname	Der exakte Schlüssel-Alias für den StorageGRID-Client im KMS. Muss zwischen 1 und 255 Zeichen liegen.

Feld	Beschreibung
Verwaltet Schlüssel für	Der StorageGRID-Site, die diesem KMS zugeordnet wird. Wenn möglich, sollten Sie alle standortspezifischen Verschlüsselungsmanagement-Server konfigurieren, bevor Sie einen Standard-KMS konfigurieren, der für alle Standorte gilt, die nicht von einem anderen KMS verwaltet werden. • Wählen Sie einen Standort aus, wenn dieser KMS Verschlüsselungen für die Appliance-Nodes an einem bestimmten Standort managt. • Wählen Sie **Sites Not Managed by another KMS (default KMS)** aus, um ein Standard-KMS zu konfigurieren, das für alle Sites gilt, die kein dediziertes KMS haben, und für alle Sites, die Sie in nachfolgenden Erweiterungen hinzufügen. **Hinweis:** beim Speichern der KMS-Konfiguration Tritt Ein Validierungsfehler auf, wenn Sie eine Site auswählen, die zuvor durch den Standard-KMS verschlüsselt wurde, aber Sie haben die aktuelle Version des ursprünglichen Verschlüsselungsschlüssels nicht dem neuen KMS zur Verfügung gestellt.
Port	Der Port, den der KMS-Server für die KMIP-Kommunikation (Key Management Interoperability Protocol) verwendet. Die Standardeinstellung ist 5696, d. h. der KMIP-Standardport.
Hostname	Der vollständig qualifizierte Domänenname oder die IP-Adresse für den KMS. **Hinweis:** das Feld Subject Alternative Name (SAN) des Serverzertifikats muss den FQDN oder die IP-Adresse enthalten, die Sie hier eingeben. Andernfalls kann StorageGRID keine Verbindung zum KMS oder zu allen Servern eines KMS-Clusters herstellen.

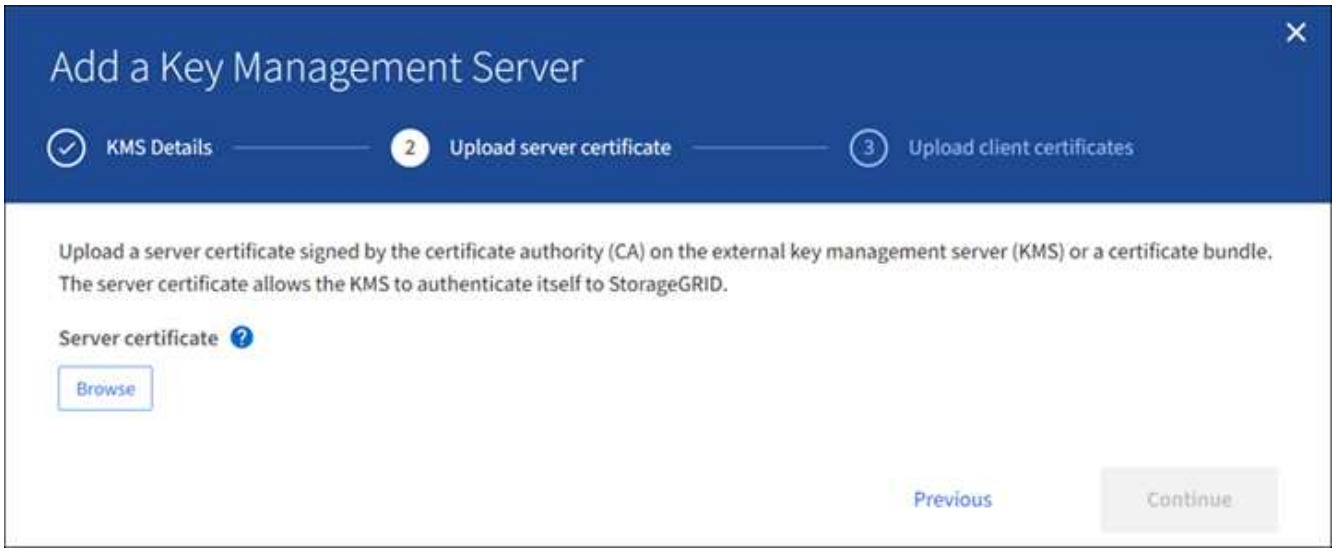
4. Wenn Sie einen KMS-Cluster konfigurieren, wählen Sie **Add another hostname**, um einen Hostnamen für jeden Server im Cluster hinzuzufügen.
5. Wählen Sie **Weiter**.

Schritt 2: Serverzertifikat hochladen

In Schritt 2 (Serverzertifikat hochladen) des Assistenten zum Hinzufügen eines Schlüsselverwaltungsservers laden Sie das Serverzertifikat (oder Zertifikatpaket) für das KMS hoch. Das Serverzertifikat ermöglicht es dem externen KMS, sich bei StorageGRID zu authentifizieren.

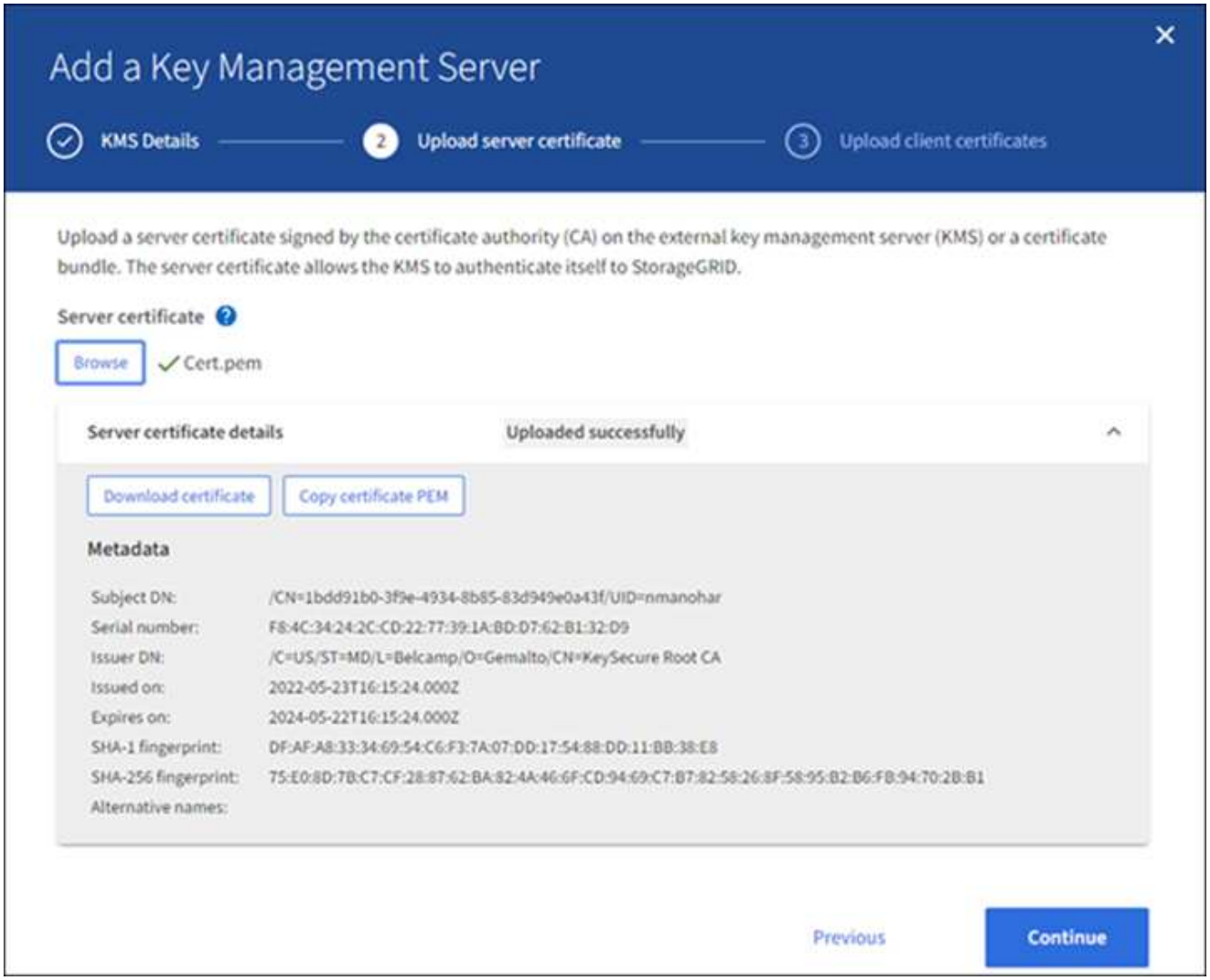
Schritte

1. Navigieren Sie aus **Schritt 2 (Serverzertifikat hochladen)** zum Speicherort des gespeicherten Serverzertifikats oder Zertifikatbündels.



2. Laden Sie die Zertifikatdatei hoch.

   Die Metadaten des Serverzertifikats werden angezeigt.



Wenn Sie ein Zertifikatbündel hochgeladen haben, werden die Metadaten für jedes Zertifikat auf der eigenen Registerkarte angezeigt.

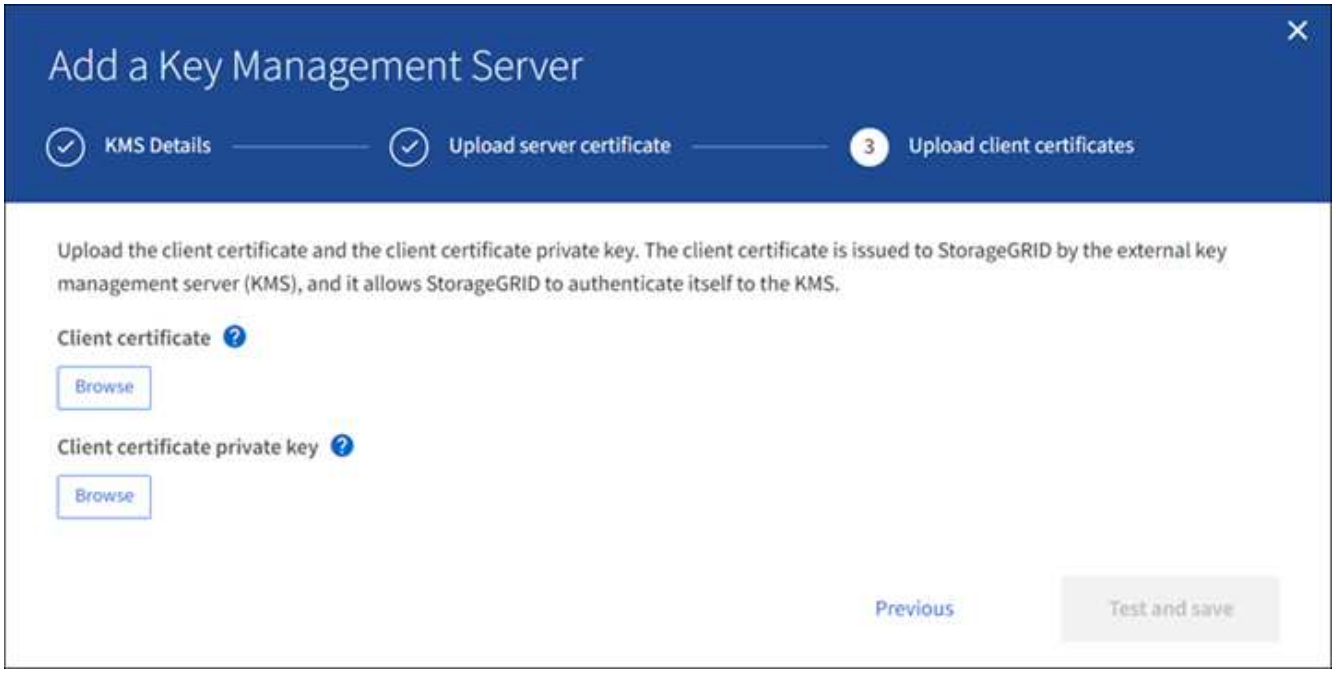
3. Wählen Sie **Weiter**.

Schritt 3: Laden Sie Clientzertifikate hoch

In Schritt 3 (Clientzertifikate hochladen) des Assistenten zum Hinzufügen eines Schlüsselverwaltungsservers laden Sie das Clientzertifikat und den privaten Schlüssel des Clientzertifikats hoch. Das Client-Zertifikat ermöglicht StorageGRID, sich am KMS zu authentifizieren.

Schritte

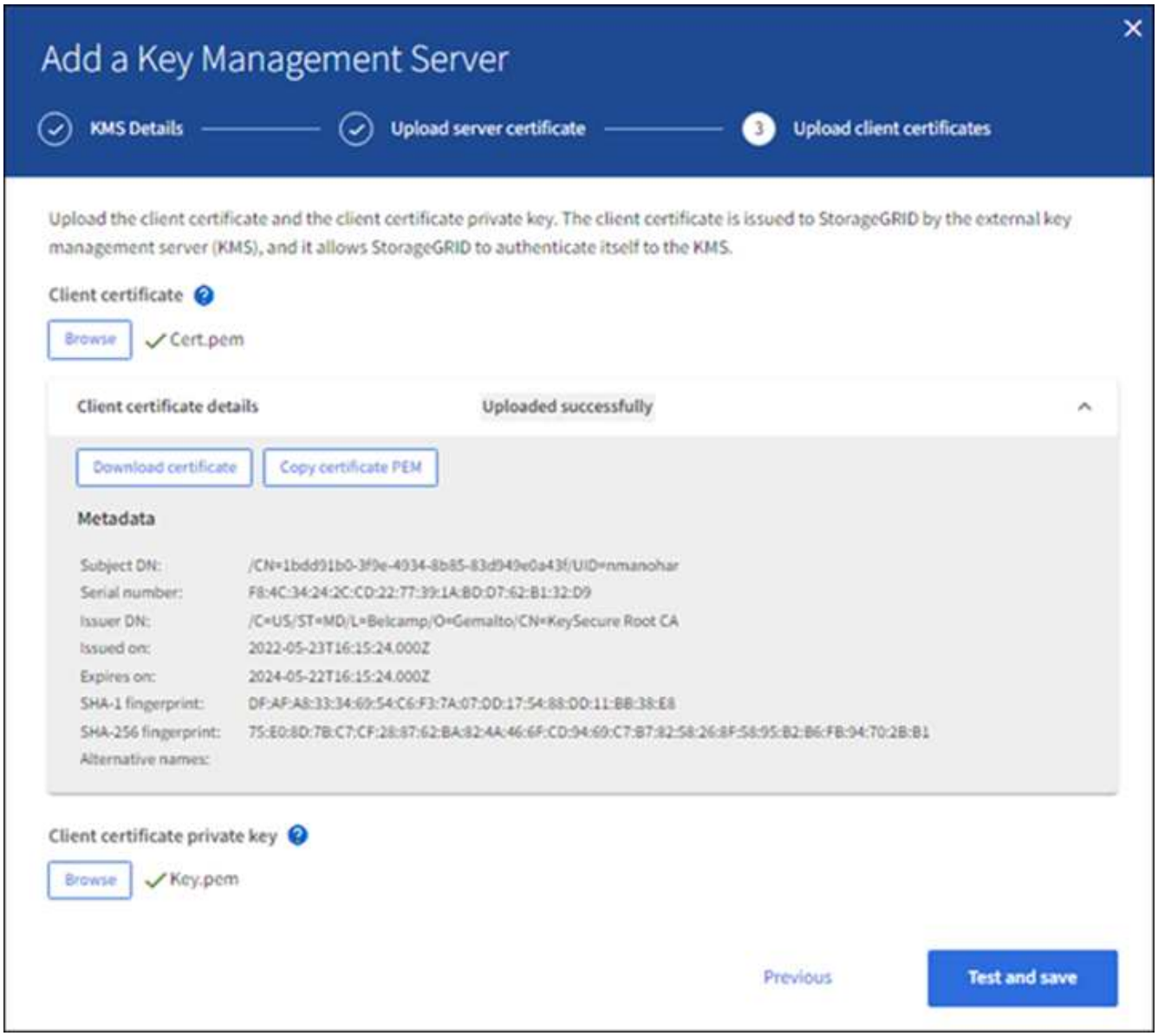
1. Navigieren Sie unter **Schritt 3 (Client-Zertifikate hochladen)** zum Speicherort des Client-Zertifikats.



2. Laden Sie die Clientzertifikatdatei hoch.

   Die Metadaten des Client-Zertifikats werden angezeigt.

3. Navigieren Sie zum Speicherort des privaten Schlüssels für das Clientzertifikat.
4. Laden Sie die Datei mit dem privaten Schlüssel hoch.



5. Wählen Sie **Test und Speichern**.

   Die Verbindungen zwischen dem Verschlüsselungsmanagement-Server und den Appliance-Nodes werden getestet. Wenn alle Verbindungen gültig sind und der korrekte Schlüssel auf dem KMS gefunden wird, wird der neue Schlüsselverwaltungsserver der Tabelle auf der Seite des Key Management Servers hinzugefügt.

   > Unmittelbar nach dem Hinzufügen eines KMS wird der Zertifikatsstatus auf der Seite Key Management Server als Unbekannt angezeigt. Es kann StorageGRID bis zu 30 Minuten dauern, bis der aktuelle Status eines jeden Zertifikats angezeigt wird. Sie müssen Ihren Webbrowser aktualisieren, um den aktuellen Status anzuzeigen.

6. Wenn bei der Auswahl von **Test und Speichern** eine Fehlermeldung angezeigt wird, überprüfen Sie die Nachrichtendetails und wählen Sie dann **OK** aus.

   Beispiel: Wenn ein Verbindungstest fehlgeschlagen ist, können Sie einen Fehler bei unbearbeitbarer Einheit mit 422: Nicht verarbeitbarer Einheit erhalten.

7. Wenn Sie die aktuelle Konfiguration speichern müssen, ohne die externe Verbindung zu testen, wählen Sie **Speichern erzwingen**.

Wenn Sie **Force save** auswählen, wird die KMS-Konfiguration gespeichert, aber die externe Verbindung von jedem Gerät zu diesem KMS wird nicht getestet. Wenn Probleme mit der Konfiguration bestehen, können Sie Appliance-Nodes, für die die Node-Verschlüsselung am betroffenen Standort aktiviert ist, möglicherweise nicht neu starten. Wenn der Zugriff auf Ihre Daten nicht mehr vollständig ist, können Sie diese Probleme beheben.

8. Überprüfen Sie die Bestätigungswarnung, und wählen Sie **OK**, wenn Sie sicher sind, dass Sie das Speichern der Konfiguration erzwingen möchten.

   Die KMS-Konfiguration wird gespeichert, die Verbindung zum KMS wird jedoch nicht getestet.

KMS-Details anzeigen

Sie können Informationen zu jedem Schlüsselverwaltungsserver (KMS) in Ihrem StorageGRID-System anzeigen, einschließlich des aktuellen Status des Servers und der Clientzertifikate.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Schlüsselverwaltungsserver** aus.

   Die Seite Key Management Server wird angezeigt. Auf der Registerkarte Konfigurationsdetails werden alle konfigurierten Schlüsselverwaltungsserver angezeigt.

2. Überprüfen Sie die Informationen in der Tabelle für jeden KMS.

Feld	Beschreibung
KMS-Name	Der beschreibende Name des KMS.
Schlüsselname	Der Schlüsselalias für den StorageGRID-Client im KMS.
Verwaltet Schlüssel für	Der dem KMS zugeordnete StorageGRID-Site. Dieses Feld zeigt den Namen einer bestimmten StorageGRID-Site oder **Sites an, die nicht von einem anderen KMS verwaltet werden (Standard-KMS).**

Feld	Beschreibung
Hostname	Der vollständig qualifizierte Domänenname oder die IP-Adresse des KMS. Wenn ein Cluster von zwei Schlüsselverwaltungsservern vorhanden ist, werden der vollständig qualifizierte Domänenname oder die IP-Adresse beider Server aufgelistet. Wenn mehr als zwei Schlüsselverwaltungsserver in einem Cluster vorhanden sind, wird der vollständig qualifizierte Domänenname oder die IP-Adresse des ersten KMS zusammen mit der Anzahl der zusätzlichen Schlüsselverwaltungsserver im Cluster aufgelistet. Beispiel: `10.10.10.10 and 10.10.10.11` Oder `10.10.10.10 and 2 others`. Um alle Hostnamen in einem Cluster anzuzeigen, öffnen Sie ein KMS und wählen **Bearbeiten** oder **Aktionen** > **Bearbeiten**.
Ablauf des Zertifikats	Aktueller Status des Serverzertifikats, des optionalen CA-Zertifikats und des Client-Zertifikats: Gültig, abgelaufen, bald abgelaufen oder unbekannt. **Hinweis:** Es kann StorageGRID so lange wie 30 Minuten dauern, bis Updates zum Ablauf des Zertifikats erhalten. Sie müssen Ihren Webbrowser aktualisieren, um die aktuellen Werte anzuzeigen.

3. Wenn der Ablauf des Zertifikats unbekannt ist, warten Sie bis zu 30 Minuten, und aktualisieren Sie dann Ihren Webbrowser.

> Unmittelbar nach dem Hinzufügen eines KMS wird der Ablauf des Zertifikats auf der Seite Key Management Server als Unbekannt angezeigt. Es kann StorageGRID bis zu 30 Minuten dauern, bis der aktuelle Status eines jeden Zertifikats angezeigt wird. Sie müssen Ihren Webbrowser aktualisieren, um den aktuellen Status anzuzeigen.

4. Wenn in der Spalte Zertifikatablauf angezeigt wird, dass ein Zertifikat abgelaufen ist oder kurz vor dem Ablaufdatum steht, beheben Sie das Problem so schnell wie möglich.

   Wenn die Warnungen **KMS CA Certificate Expiration**, **KMS Client Certificate Expiration** und **KMS Server Certificate Expiration** ausgelöst werden, notieren Sie sich die Beschreibung der einzelnen Warnungen und führen Sie die empfohlenen Aktionen durch.

> Sie müssen Probleme mit dem Zertifikat so schnell wie möglich beheben, um den Datenzugriff aufrechtzuerhalten.

5. Um die Zertifikatdetails für dieses KMS anzuzeigen, wählen Sie den KMS-Namen aus der Tabelle aus.
6. Überprüfen Sie auf der KMS-Übersichtsseite die Metadaten und das Zertifikat-PEM sowohl für das Serverzertifikat als auch für das Clientzertifikat. Wählen Sie bei Bedarf **Zertifikat bearbeiten**, um ein Zertifikat durch ein neues zu ersetzen.

Verschlüsselte Nodes anzeigen

Sie können Informationen zu den Appliance-Knoten in Ihrem StorageGRID-System anzeigen, bei denen die Einstellung **Node-Verschlüsselung** aktiviert ist.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Schlüsselverwaltungsserver** aus.

   Die Seite Key Management Server wird angezeigt. Auf der Registerkarte Konfigurationsdetails werden alle konfigurierten Schlüsselverwaltungsserver angezeigt.

2. Wählen Sie oben auf der Seite die Registerkarte **verschlüsselte Knoten** aus.

   Auf der Registerkarte Verschlüsselte Knoten werden die Geräteknoten in Ihrem StorageGRID-System aufgelistet, für die die Einstellung **Knotenverschlüsselung** aktiviert ist.

3. Überprüfen Sie die Informationen in der Tabelle für jeden Appliance-Node.

Spalte	Beschreibung
Node-Name	Der Name des Appliance-Node.
Node-Typ	Der Node-Typ: Storage, Admin oder Gateway.
Standort	Der Name der StorageGRID-Site, auf der der Node installiert ist.
KMS-Name	Der beschreibende Name des für den Knoten verwendeten KMS. Wenn kein KMS aufgeführt ist, wählen Sie die Registerkarte Konfigurationsdetails aus, um ein KMS hinzuzufügen. "Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)"
Schlüssel-UID	Die eindeutige ID des Verschlüsselungsschlüssels, der zur Verschlüsselung und Entschlüsselung von Daten auf dem Appliance-Node verwendet wird. Um eine gesamte Schlüssel-UID anzuzeigen, setzen Sie den Cursor über die Zelle. Ein Bindestrich (-) gibt an, dass die Schlüssel-UID unbekannt ist, möglicherweise wegen eines Verbindungsproblem zwischen dem Appliance-Node und dem KMS.
Status	Der Status der Verbindung zwischen dem KMS und dem Appliance-Node. Wenn der Knoten verbunden ist, wird der Zeitstempel alle 30 Minuten aktualisiert. Nach einer Änderung der KMS-Konfiguration kann es mehrere Minuten dauern, bis der Verbindungsstatus aktualisiert wird. **Hinweis:** Sie müssen Ihren Webbrowser aktualisieren, um die neuen Werte zu sehen.

4. Wenn in der Spalte Status ein KMS-Problem angezeigt wird, beheben Sie das Problem sofort.

Während normaler KMS-Vorgänge wird der Status **mit KMS** verbunden. Wenn ein Knoten von der Tabelle getrennt wird, wird der Verbindungsstatus des Knotens angezeigt (administrativ ausgefallen oder unbekannt).

Andere Statusmeldungen entsprechen StorageGRID Meldungen mit denselben Namen:

- KMS-Konfiguration konnte nicht geladen werden
- KMS-Verbindungsfehler
- DER VERSCHLÜSSELUNGSSCHLÜSSELNAME VON KMS wurde nicht gefunden
- DIE Drehung des VERSCHLÜSSELUNGSSCHLÜSSELS ist fehlgeschlagen
- KMS-Schlüssel konnte ein Appliance-Volume nicht entschlüsseln
- KM ist nicht konfiguriert

Führen Sie die empfohlenen Aktionen für diese Warnmeldungen aus.

Sämtliche Probleme müssen sofort behoben werden, um einen vollständigen Schutz Ihrer Daten zu gewährleisten.

Bearbeiten eines Verschlüsselungsmanagement-Servers (KMS)

Möglicherweise müssen Sie die Konfiguration eines Schlüsselverwaltungsservers bearbeiten, z. B. wenn ein Zertifikat kurz vor dem Ablauf steht.

Bevor Sie beginnen

- Sie haben die geprüft "Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers".
- Wenn Sie die für einen KMS ausgewählte Site aktualisieren möchten, haben Sie die geprüft "Überlegungen für das Ändern des KMS für einen Standort".
- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die Root-Zugriffsberechtigung.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Schlüsselverwaltungsserver** aus.

   Die Seite Key Management Server wird angezeigt und zeigt alle konfigurierten Key Management Server an.

2. Wählen Sie den KMS aus, den Sie bearbeiten möchten, und wählen Sie **actions** > **Edit**.

   Sie können einen KMS auch bearbeiten, indem Sie den KMS-Namen in der Tabelle auswählen und auf der KMS-Detailseite **Bearbeiten** auswählen.

3. Aktualisieren Sie optional die Details in **Schritt 1 (KMS-Details)** des Assistenten zum Bearbeiten eines Schlüsselverwaltungsservers.

Feld	Beschreibung
KMS-Name	Einen beschreibenden Namen, der Ihnen bei der Identifizierung dieses KMS hilft. Muss zwischen 1 und 64 Zeichen liegen.

Feld	Beschreibung
Schlüsselname	Der exakte Schlüssel-Alias für den StorageGRID-Client im KMS. Muss zwischen 1 und 255 Zeichen liegen. In seltenen Fällen müssen Sie nur den Schlüsselnamen bearbeiten. Sie müssen beispielsweise den Schlüsselnamen bearbeiten, wenn der Alias im KMS umbenannt wird oder alle Versionen des vorherigen Schlüssels in die Versionsgeschichte des neuen Alias kopiert wurden. Versuchen Sie niemals, einen Schlüssel zu drehen, indem Sie den Schlüsselnamen (Alias) für den KMS ändern. Drehen Sie stattdessen den Schlüssel, indem Sie die Schlüsselversion in der KMS-Software aktualisieren. Für StorageGRID müssen alle zuvor verwendeten Schlüsselversionen (sowie zukünftige Versionen) vom KMS mit demselben Schlüsselalias zugänglich sein. Wenn Sie den Schlüssel-Alias für einen konfigurierten KMS ändern, kann StorageGRID Ihre Daten möglicherweise nicht entschlüsseln. "Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers"
Verwaltet Schlüssel für	Wenn Sie ein standortspezifisches KMS bearbeiten und noch kein Standard-KMS haben, wählen Sie optional **Sites Not Managed by another KMS (default KMS)** aus. Diese Auswahl konvertiert ein standortspezifisches KMS in das Standard-KMS, das für alle Standorte gilt, die kein dediziertes KMS haben, und für alle Sites, die in einer Erweiterung hinzugefügt wurden. **Hinweis:** Wenn Sie eine Site-spezifische KMS bearbeiten, können Sie keine andere Site auswählen. Wenn Sie das Standard-KMS bearbeiten, können Sie keine bestimmte Site auswählen.
Port	Der Port, den der KMS-Server für die KMIP-Kommunikation (Key Management Interoperability Protocol) verwendet. Die Standardeinstellung ist 5696, d. h. der KMIP-Standardport.
Hostname	Der vollständig qualifizierte Domänenname oder die IP-Adresse für den KMS. **Hinweis:** das Feld Subject Alternative Name (SAN) des Serverzertifikats muss den FQDN oder die IP-Adresse enthalten, die Sie hier eingeben. Andernfalls kann StorageGRID keine Verbindung zum KMS oder zu allen Servern eines KMS-Clusters herstellen.

4. Wenn Sie einen KMS-Cluster konfigurieren, wählen Sie **Add another hostname**, um einen Hostnamen für jeden Server im Cluster hinzuzufügen.
5. Wählen Sie **Weiter**.

   Schritt 2 (Serverzertifikat hochladen) des Assistenten zum Bearbeiten eines Schlüsselverwaltungsservers wird angezeigt.

6. Wenn Sie das Serverzertifikat ersetzen müssen, wählen Sie **Durchsuchen** und laden Sie die neue Datei hoch.
7. Wählen Sie **Weiter**.

   Schritt 3 (Client-Zertifikate hochladen) des Assistenten zum Bearbeiten eines Schlüsselverwaltungsservers wird angezeigt.

8. Wenn Sie das Clientzertifikat und den privaten Schlüssel des Clientzertifikats ersetzen müssen, wählen Sie **Durchsuchen** und laden Sie die neuen Dateien hoch.
9. Wählen Sie **Test und Speichern**.

   Die Verbindungen zwischen dem Verschlüsselungsmanagement-Server und allen Node-verschlüsselten Appliance-Nodes an den betroffenen Standorten werden getestet. Wenn alle Knotenverbindungen gültig sind und der korrekte Schlüssel auf dem KMS gefunden wird, wird der Schlüsselverwaltungsserver der Tabelle auf der Seite des Key Management Servers hinzugefügt.

10. Wenn eine Fehlermeldung angezeigt wird, überprüfen Sie die Nachrichtendetails, und wählen Sie **OK**.

    Sie können beispielsweise einen Fehler bei der nicht verarbeitbaren Einheit von 422 erhalten, wenn die für diesen KMS ausgewählte Site bereits von einem anderen KMS verwaltet wird oder wenn ein Verbindungstest fehlgeschlagen ist.

11. Wenn Sie die aktuelle Konfiguration speichern müssen, bevor Sie die Verbindungsfehler beheben, wählen Sie **Speichern erzwingen**.

    > Wenn Sie **Force save** auswählen, wird die KMS-Konfiguration gespeichert, aber die externe Verbindung von jedem Gerät zu diesem KMS wird nicht getestet. Wenn Probleme mit der Konfiguration bestehen, können Sie Appliance-Nodes, für die die Node-Verschlüsselung am betroffenen Standort aktiviert ist, möglicherweise nicht neu starten. Wenn der Zugriff auf Ihre Daten nicht mehr vollständig ist, können Sie diese Probleme beheben.

    Die KMS-Konfiguration wird gespeichert.

12. Überprüfen Sie die Bestätigungswarnung, und wählen Sie **OK**, wenn Sie sicher sind, dass Sie das Speichern der Konfiguration erzwingen möchten.

    Die KMS-Konfiguration wird gespeichert, die Verbindung zum KMS wird jedoch nicht getestet.

Entfernen eines Verschlüsselungsmanagement-Servers (KMS)

In einigen Fällen möchten Sie einen Schlüsselverwaltungsserver entfernen. Sie können beispielsweise einen standortspezifischen KMS entfernen, wenn Sie den Standort deaktiviert haben.

Bevor Sie beginnen

- Sie haben die geprüft "Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers".
- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die Root-Zugriffsberechtigung.

Über diese Aufgabe

In diesen Fällen können Sie einen KMS entfernen:

- Wenn der Standort außer Betrieb genommen wurde oder wenn der Standort keine Appliance-Nodes mit aktivierter Node-Verschlüsselung enthält, können Sie einen standortspezifischen KMS entfernen.
- Der Standard-KMS kann entfernt werden, wenn für jeden Standort bereits ein standortspezifischer KMS vorhanden ist, bei dem Appliance-Nodes mit aktivierter Node-Verschlüsselung vorhanden sind.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Schlüsselverwaltungsserver** aus.

   Die Seite Key Management Server wird angezeigt und zeigt alle konfigurierten Key Management Server an.

2. Wählen Sie den KMS aus, den Sie entfernen möchten, und wählen Sie **Aktionen** > **Entfernen**.

   Sie können KMS auch entfernen, indem Sie den KMS-Namen in der Tabelle auswählen und auf der KMS-Detailseite **Entfernen** auswählen.

3. Bestätigen Sie, dass Folgendes zutrifft:
   - Sie entfernen ein standortspezifisches KMS für einen Standort, der keinen Appliance-Knoten mit aktivierter Knotenverschlüsselung hat.
   - Sie entfernen den Standard-KMS, aber für jeden Standort mit Knotenverschlüsselung ist bereits ein standortspezifisches KMS vorhanden.
4. Wählen Sie **Ja**.

   Die KMS-Konfiguration wurde entfernt.

Proxy-Einstellungen verwalten

Konfigurieren Sie Speicher-Proxy-Einstellungen

Wenn Sie Plattform-Services oder Cloud Storage-Pools verwenden, können Sie einen nicht transparenten Proxy zwischen Storage Nodes und den externen S3-Endpunkten konfigurieren. Beispielsweise benötigen Sie einen nicht transparenten Proxy, um Meldungen von Plattformdiensten an externe Endpunkte, z. B. einen Endpunkt im Internet, zu senden.

Bevor Sie beginnen

- Sie haben spezifische Zugriffsberechtigungen.
- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".

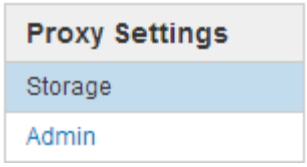
Über diese Aufgabe

Sie können die Einstellungen für einen einzelnen Speicherproxy konfigurieren.

Schritte

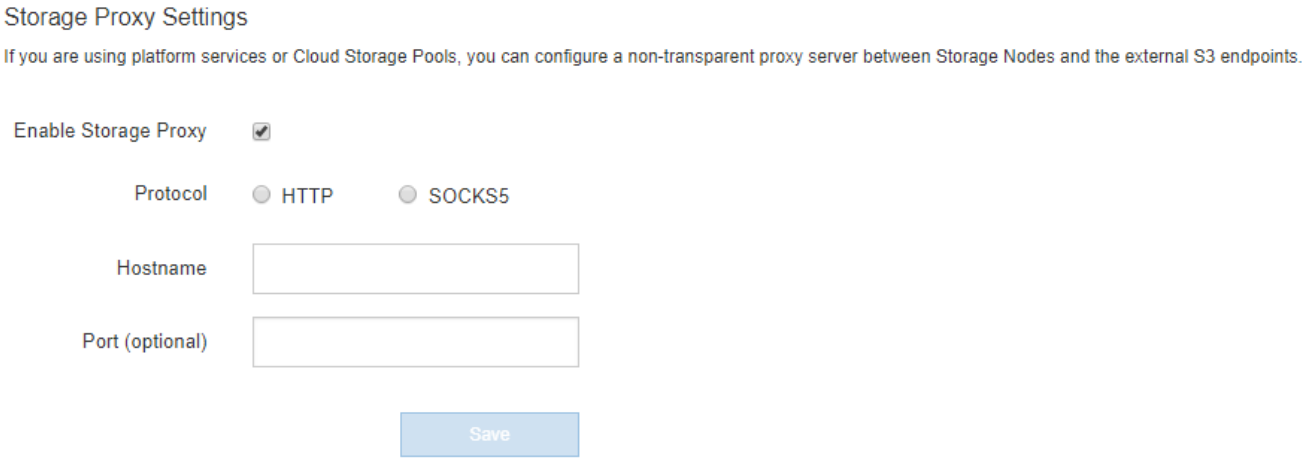
1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Proxy-Einstellungen**.

   Die Seite Speicher-Proxy-Einstellungen wird angezeigt. Standardmäßig ist **Storage** im Sidebar-Menü ausgewählt.



2. Aktivieren Sie das Kontrollkästchen **Speicher-Proxy aktivieren**.

   Die Felder zum Konfigurieren eines Speicher-Proxys werden angezeigt.



3. Wählen Sie das Protokoll für den nicht-transparenten Speicher-Proxy aus.
4. Geben Sie den Hostnamen oder die IP-Adresse des Proxy-Servers ein.
5. Geben Sie optional den Port ein, der für die Verbindung mit dem Proxyserver verwendet wird.

   Sie können dieses Feld leer lassen, wenn Sie den Standardport für das Protokoll verwenden: 80 für HTTP oder 1080 für SOCKS5.

6. Wählen Sie **Speichern**.

   Nach dem Speichern des Storage-Proxy können neue Endpunkte für Plattformservices oder Cloud-Storage-Pools konfiguriert und getestet werden.

   ⓘ Änderungen an Proxy können bis zu 10 Minuten in Anspruch nehmen.

7. Überprüfen Sie die Einstellungen Ihres Proxy-Servers, um sicherzustellen, dass für den Plattformdienst bezogene Nachrichten von StorageGRID nicht blockiert werden.

Nachdem Sie fertig sind

Wenn Sie einen Speicher-Proxy deaktivieren müssen, deaktivieren Sie das Kontrollkästchen **Speicher-Proxy aktivieren**, und wählen Sie **Speichern** aus.

Verwandte Informationen

- "Netzwerk und Ports für Plattformservices"
- "Objektmanagement mit ILM"

Konfigurieren Sie die Administrator-Proxy-Einstellungen

Wenn Sie AutoSupport-Meldungen über HTTP oder HTTPS senden (siehe "Konfigurieren

Sie AutoSupport") Können Sie einen nicht transparenten Proxy-Server zwischen Admin-Knoten und technischem Support (AutoSupport) konfigurieren.

Bevor Sie beginnen

- Sie haben spezifische Zugriffsberechtigungen.
- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".

Über diese Aufgabe

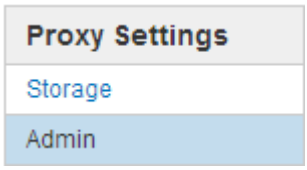
Sie können die Einstellungen für einen einzigen Admin-Proxy konfigurieren.

Schritte

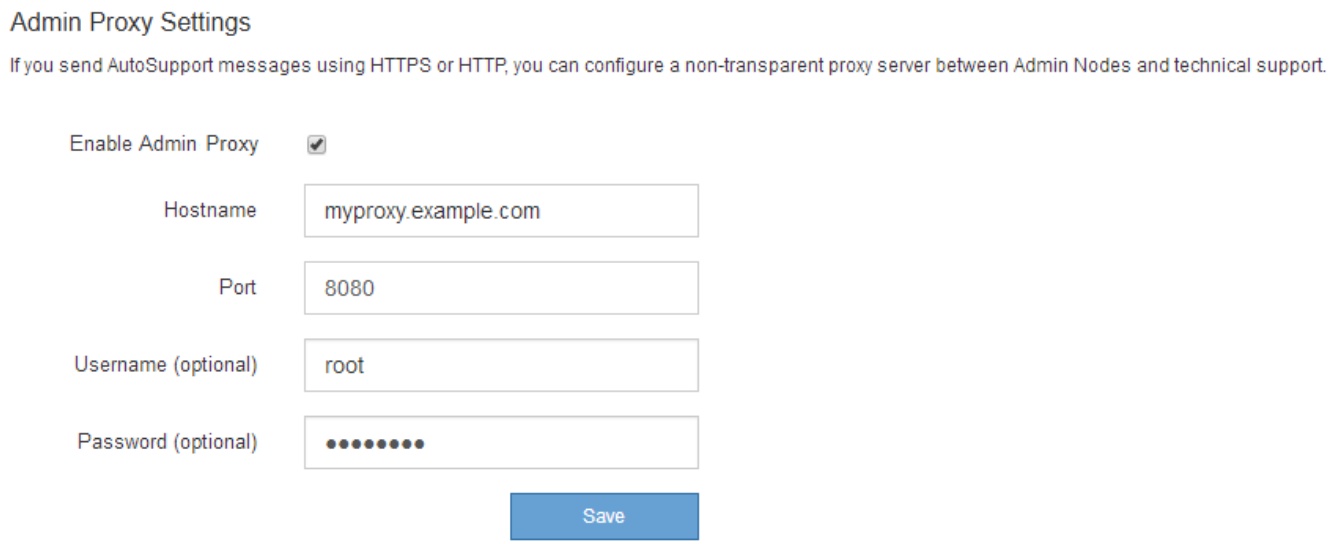
1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Proxy-Einstellungen**.

   Die Seite Admin Proxy Settings wird angezeigt. Standardmäßig ist **Storage** im Sidebar-Menü ausgewählt.

2. Wählen Sie im Sidebar-Menü die Option **Admin**.



3. Aktivieren Sie das Kontrollkästchen **Admin-Proxy aktivieren**.



4. Geben Sie den Hostnamen oder die IP-Adresse des Proxy-Servers ein.
5. Geben Sie den Port ein, der für die Verbindung mit dem Proxy-Server verwendet wird.
6. Geben Sie optional den Proxy-Benutzernamen ein.

   Lassen Sie dieses Feld leer, wenn Ihr Proxy-Server keinen Benutzernamen benötigt.

7. Geben Sie optional das Proxy-Kennwort ein.

   Lassen Sie dieses Feld leer, wenn Ihr Proxy-Server kein Passwort benötigt.

8. Wählen Sie **Speichern**.

   Nachdem der Admin-Proxy gespeichert wurde, wird der Proxy-Server zwischen Admin-Nodes und dem technischen Support konfiguriert.

   Änderungen an Proxy können bis zu 10 Minuten in Anspruch nehmen.

9. Wenn Sie den Proxy deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Admin Proxy aktivieren**, und wählen Sie **Save** aus.

Kontrollieren Sie Firewalls

Kontrolle des Zugriffs über externe Firewall

Sie können bestimmte Ports an der externen Firewall öffnen oder schließen.

Sie können den Zugriff auf die Benutzeroberflächen und APIs auf StorageGRID-Administratorknoten steuern, indem Sie bestimmte Ports an der externen Firewall öffnen oder schließen. Beispielsweise möchten Sie verhindern, dass Mandanten sich an der Firewall mit dem Grid Manager verbinden können, und zwar zusätzlich über andere Methoden zur Steuerung des Systemzugriffs.

Informationen zum Konfigurieren der internen StorageGRID-Firewall finden Sie unter "Konfigurieren Sie die interne Firewall".

Port	Beschreibung	Port offen…
443	Standard-HTTPS-Port für Admin-Nodes	Webbrowser und Management-API-Clients können auf den Grid Manager, die Grid Management API, den Mandanten-Manager und die Mandanten-Management-API zugreifen. **Hinweis:** Port 443 wird auch für einen internen Verkehr genutzt.
8443	Eingeschränkter Grid Manager-Port an Admin-Nodes	• Webbrowser und Management-API-Clients können mithilfe von HTTPS auf den Grid Manager und die Grid Management API zugreifen. • Webbrowser und Management-API-Clients können nicht auf den Tenant Manager oder die Mandanten-Management-API zugreifen. • Anfragen nach internen Inhalten werden abgelehnt.

Port	Beschreibung	Port offen…
9443	Eingeschränkter Mandantenmanager-Port an Admin-Nodes	• Webbrowser und Management-API-Clients können mithilfe von HTTPS auf den Mandanten-Manager und die Mandanten-Management-API zugreifen. • Webbrowser und Management-API-Clients können nicht auf den Grid Manager oder die Grid-Management-API zugreifen. • Anfragen nach internen Inhalten werden abgelehnt.

Single Sign-On (SSO) ist auf den Ports Restricted Grid Manager oder Tenant Manager nicht verfügbar. Sie müssen den Standard-HTTPS-Port (443) verwenden, wenn Benutzer sich mit Single Sign-On authentifizieren möchten.

Verwandte Informationen

- "Melden Sie sich beim Grid Manager an"
- "Erstellen eines Mandantenkontos"
- "Externe Kommunikation"

Interne Firewall-Kontrollen verwalten

StorageGRID verfügt über eine interne Firewall auf jedem Node, die die Sicherheit Ihres Grids erhöht, indem Sie den Netzwerkzugriff auf den Node kontrollieren können. Verwenden Sie die Firewall, um den Netzwerkzugriff auf allen Ports zu verhindern, außer den für Ihre spezifische Grid-Bereitstellung erforderlichen Ports. Die Konfigurationsänderungen, die Sie auf der Seite Firewall-Steuerung vornehmen, werden für jeden Knoten bereitgestellt.

Verwenden Sie die drei Registerkarten auf der Seite „Firewall-Steuerung“, um den für Ihr Raster erforderlichen Zugriff anzupassen.

- **Privilegierte Adressliste**: Verwenden Sie diese Registerkarte, um ausgewählten Zugriff auf geschlossene Ports zu ermöglichen. Sie können IP-Adressen oder Subnetze in CIDR-Notation hinzufügen, die über die Registerkarte externen Zugriff managen auf geschlossene Ports zugreifen können.
- **Externen Zugriff verwalten**: Verwenden Sie diese Registerkarte, um Ports zu schließen, die standardmäßig geöffnet sind, oder um zuvor geschlossene Ports wieder zu öffnen.
- **Nicht vertrauenswürdiges Client-Netzwerk**: Verwenden Sie diese Registerkarte, um anzugeben, ob ein Knoten eingehenden Datenverkehr vom Client-Netzwerk anvertraut.

  Auf dieser Registerkarte können Sie auch zusätzliche Ports angeben, die geöffnet werden sollen, wenn das nicht vertrauenswürdige Clientnetzwerk konfiguriert ist. Diese Ports können Zugriff auf den Grid Manager, den Tenant Manager oder beide ermöglichen.

  Die Einstellungen auf dieser Registerkarte überschreiben die Einstellungen auf der Registerkarte externen Zugriff verwalten.

  - Ein Knoten mit einem nicht vertrauenswürdigen Client-Netzwerk akzeptiert nur Verbindungen auf den

an diesem Knoten konfigurierten Load-Balancer-Endpunktports (global, Knotenschnittstelle und Knotentyp gebundene Endpunkte).

- Zusätzliche Ports, die auf der Registerkarte nicht vertrauenswürdiger Client-Netzwerk geöffnet werden, sind in allen nicht vertrauenswürdigen Client-Netzwerken geöffnet, auch wenn keine Load Balancer-Endpunkte konfiguriert sind.
- Load Balancer-Endpunkt-Ports und ausgewählte zusätzliche Ports *sind die einzigen offenen Ports* in nicht vertrauenswürdigen Client-Netzwerken, unabhängig von den Einstellungen auf der Registerkarte Externe Netzwerke verwalten.
- Wenn vertrauenswürdig, sind alle Ports, die auf der Registerkarte externen Zugriff managen geöffnet sind, sowie alle im Client-Netzwerk geöffneten Load Balancer-Endpunkte zugänglich.

> Die Einstellungen, die Sie auf einer Registerkarte vornehmen, können sich auf die Zugriffsänderungen auswirken, die Sie auf einer anderen Registerkarte vornehmen. Überprüfen Sie die Einstellungen auf allen Registerkarten, um sicherzustellen, dass sich Ihr Netzwerk wie erwartet verhält.

Informationen zum Konfigurieren der internen Firewall-Steuerelemente finden Sie unter "Konfigurieren Sie die Firewall-Steuerelemente".

Weitere Informationen zu externen Firewalls und Netzwerksicherheit finden Sie unter "Kontrolle des Zugriffs über externe Firewall".

Liste privilegierter Adressen und Verwaltung externer Zugriffsregisterkarten

Auf der Registerkarte Liste der privilegierten Adressen können Sie eine oder mehrere IP-Adressen registrieren, denen Zugriff auf geschlossene Grid-Ports gewährt wird. Auf der Registerkarte externen Zugriff verwalten können Sie den externen Zugriff auf ausgewählte externe Ports oder alle offenen externen Ports schließen (externe Ports sind Ports, auf die standardmäßig nicht-Grid-Nodes zugreifen können). Diese beiden Registerkarten können häufig zusammen verwendet werden, um den genauen Netzwerkzugriff anzupassen, den Sie für Ihr Raster benötigen.

> Privilegierte IP-Adressen haben standardmäßig keinen internen Grid-Port-Zugriff.

Beispiel 1: Verwenden Sie einen Jump-Host für Wartungsaufgaben

Angenommen, Sie möchten einen Jump-Host (einen sicherheitsgesicherten Host) für die Netzwerkadministration verwenden. Sie können die folgenden allgemeinen Schritte verwenden:

1. Verwenden Sie die Registerkarte Liste der privilegierten Adressen, um die IP-Adresse des Jump-Hosts hinzuzufügen.
2. Verwenden Sie die Registerkarte externen Zugriff verwalten, um alle Ports zu blockieren.

> Fügen Sie die privilegierte IP-Adresse hinzu, bevor Sie die Ports 443 und 8443 blockieren. Alle Benutzer, die derzeit mit einem blockierten Port verbunden sind, einschließlich Ihnen, verlieren den Zugriff auf Grid Manager, es sei denn, ihre IP-Adresse wurde der Liste der privilegierten Adressen hinzugefügt.

Nachdem Sie Ihre Konfiguration gespeichert haben, werden alle externen Ports auf dem Admin-Knoten in Ihrem Grid für alle Hosts außer dem Jump-Host gesperrt. Sie können dann den Jump-Host verwenden, um Wartungsarbeiten am Grid sicherer durchzuführen.

Beispiel 2: Beschränken Sie den Zugriff auf den Grid-Manager und den Tenant Manager

Angenommen, Sie möchten den Zugriff auf den Grid-Manager und den Mandantenmanager aus Sicherheitsgründen einschränken. Sie können die folgenden allgemeinen Schritte verwenden:

1. Verwenden Sie den Umschalter auf der Registerkarte externen Zugriff verwalten, um Port 443 zu blockieren.
2. Verwenden Sie die Umschalttaste auf der Registerkarte externen Zugriff verwalten, um den Zugriff auf Port 8443 zu ermöglichen.
3. Verwenden Sie die Umschalttaste auf der Registerkarte externen Zugriff verwalten, um den Zugriff auf Port 9443 zu ermöglichen.

Nachdem Sie Ihre Konfiguration gespeichert haben, können Hosts nicht auf Port 443 zugreifen, aber sie können dennoch über Port 8443 und den Tenant Manager über Port 9443 auf den Grid Manager zugreifen.

Beispiel 3: Sperren sensibler Ports

Angenommen, Sie möchten sensible Ports und den Dienst auf diesem Port sperren (z. B. SSH an Port 22). Sie können die folgenden allgemeinen Schritte verwenden:

1. Verwenden Sie die Registerkarte Liste der privilegierten Adressen, um nur den Hosts Zugriff zu gewähren, die Zugriff auf den Dienst benötigen.
2. Verwenden Sie die Registerkarte externen Zugriff verwalten, um alle Ports zu blockieren.

> Fügen Sie die privilegierte IP-Adresse hinzu, bevor Sie die Ports 443 und 8443 blockieren. Alle Benutzer, die derzeit mit einem blockierten Port verbunden sind, einschließlich Ihnen, verlieren den Zugriff auf Grid Manager, es sei denn, ihre IP-Adresse wurde der Liste der privilegierten Adressen hinzugefügt.

Nachdem Sie die Konfiguration gespeichert haben, stehen den Hosts auf der Liste der privilegierten Adressen Port 22 und SSH-Dienst zur Verfügung. Allen anderen Hosts wird der Zugriff auf den Dienst verweigert, unabhängig davon, von welcher Schnittstelle die Anforderung stammt.

Beispiel 4: Deaktivieren Sie den Zugriff auf nicht verwendete Dienste

Auf Netzwerkebene können Sie einige Dienste deaktivieren, die Sie nicht verwenden möchten. Wenn Sie beispielsweise keinen Swift-Zugriff bereitstellen, führen Sie die folgenden allgemeinen Schritte aus:

1. Verwenden Sie den Umschalter auf der Registerkarte externen Zugriff verwalten, um Port 18083 zu blockieren.
2. Verwenden Sie den Umschalter auf der Registerkarte externen Zugriff verwalten, um Port 18085 zu blockieren.

Nachdem Sie die Konfiguration gespeichert haben, lässt der Storage Node die Swift-Konnektivität nicht mehr zu, erlaubt aber weiterhin den Zugriff auf andere Dienste auf nicht blockierten Ports.

Registerkarte nicht vertrauenswürdige Client-Netzwerke

Wenn Sie ein Clientnetzwerk verwenden, können Sie StorageGRID vor feindlichen Angriffen schützen, indem Sie eingehenden Clientverkehr nur an explizit konfigurierten Endpunkten oder zusätzlichen Ports akzeptieren, die Sie auf dieser Registerkarte auswählen.

Standardmäßig ist das Client-Netzwerk auf jedem Grid-Knoten *Trusted*. Das heißt, standardmäßig vertraut

StorageGRID eingehende Verbindungen zu jedem Grid-Knoten auf allen "Verfügbare externe Ports".

Sie können die Bedrohung durch feindliche Angriffe auf Ihrem StorageGRID-System verringern, indem Sie angeben, dass das Client-Netzwerk auf jedem Knoten *unvertrauenswürdig* ist. Wenn das Client-Netzwerk eines Knotens nicht vertrauenswürdig ist, akzeptiert der Knoten nur eingehende Verbindungen an Ports, die explizit als Load Balancer-Endpunkte konfiguriert sind, und alle zusätzlichen Ports, die Sie über die Registerkarte nicht vertrauenswürdiges Client-Netzwerk auf der Seite Firewall-Steuerung festlegen. Siehe "Konfigurieren von Load Balancer-Endpunkten" Und "Konfigurieren Sie die Firewall-Steuerelemente".

Beispiel 1: Der Gateway-Node akzeptiert nur HTTPS-S3-Anforderungen

Angenommen, ein Gateway-Node soll den gesamten eingehenden Datenverkehr im Client-Netzwerk mit Ausnahme von HTTPS S3-Anforderungen ablehnen. Sie würden folgende allgemeine Schritte durchführen:

1. Von "Load Balancer-Endpunkte" Konfigurieren Sie einen Load Balancer-Endpunkt für S3 über HTTPS an Port 443.
2. Wählen Sie auf der Seite Firewall-Steuerung die Option nicht vertrauenswürdig aus, um anzugeben, dass das Client-Netzwerk auf dem Gateway-Knoten nicht vertrauenswürdig ist.

Nachdem Sie Ihre Konfiguration gespeichert haben, wird der gesamte eingehende Datenverkehr im Client-Netzwerk des Gateway-Knotens außer HTTPS-S3-Anfragen auf Port 443- und ICMP-Echo-(Ping-)Anfragen verworfen.

Beispiel 2: Storage-Node sendet Anforderungen von S3-Plattform-Services

Angenommen, Sie möchten den ausgehenden Datenverkehr der S3-Plattformdienste von einem Storage-Node aktivieren, möchten jedoch eingehende Verbindungen zu diesem Storage-Node im Client-Netzwerk verhindern. Sie würden diesen allgemeinen Schritt durchführen:

- Geben Sie auf der Registerkarte nicht vertrauenswürdige Client-Netzwerke der Seite Firewall-Steuerung an, dass das Client-Netzwerk auf dem Storage Node nicht vertrauenswürdig ist.

Nachdem Sie die Konfiguration gespeichert haben, akzeptiert der Storage Node keinen eingehenden Datenverkehr mehr im Client-Netzwerk, erlaubt jedoch weiterhin ausgehende Anfragen an konfigurierte Plattformdienstziele.

Beispiel 3: Zugriff auf Grid Manager auf ein Subnetz beschränken

Angenommen, Sie möchten den Zugriff des Grid-Managers nur auf ein bestimmtes Subnetz zulassen. Führen Sie die folgenden Schritte aus:

1. Verbinden Sie das Client-Netzwerk Ihrer Admin-Knoten mit dem Subnetz.
2. Verwenden Sie die Registerkarte nicht vertrauenswürdiges Clientnetzwerk, um das Clientnetzwerk als nicht vertrauenswürdig zu konfigurieren.
3. Fügen Sie im Abschnitt **zusätzliche Ports auf nicht vertrauenswürdigem Client-Netzwerk öffnen** der Registerkarte Port 443 oder 8443 hinzu.
4. Verwenden Sie die Registerkarte externen Zugriff verwalten, um alle externen Ports zu blockieren (mit oder ohne privilegierte IP-Adressen für Hosts außerhalb dieses Subnetzes).

Nachdem Sie die Konfiguration gespeichert haben, können nur Hosts in dem von Ihnen angegebenen Subnetz auf den Grid Manager zugreifen. Alle anderen Hosts sind blockiert.

Sie können die StorageGRID Firewall konfigurieren, um den Netzwerkzugriff auf bestimmte Ports auf Ihren StorageGRID Nodes zu steuern.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Das ist schon "Bestimmte Zugriffsberechtigungen".
- Sie haben die Informationen in geprüft "Management der Firewall-Kontrollen" Und "Netzwerkrichtlinien".
- Wenn ein Admin-Node oder Gateway-Node nur eingehenden Datenverkehr auf explizit konfigurierten Endpunkten annehmen soll, haben Sie die Load Balancer-Endpunkte definiert.

> Wenn Sie die Konfiguration des Client-Netzwerks ändern, können bestehende Clientverbindungen fehlschlagen, wenn die Load Balancer-Endpunkte nicht konfiguriert wurden.

Über diese Aufgabe

StorageGRID verfügt über eine interne Firewall auf jedem Node, über die Sie einige Ports an den Nodes des Grids öffnen oder schließen können. Sie können die Registerkarten für die Firewall-Steuerung verwenden, um Ports zu öffnen oder zu schließen, die standardmäßig im Grid-Netzwerk, im Admin-Netzwerk und im Client-Netzwerk geöffnet sind. Sie können auch eine Liste mit privilegierten IP-Adressen erstellen, die auf gesperrte Grid-Ports zugreifen können. Wenn Sie ein Client-Netzwerk verwenden, können Sie angeben, ob ein Knoten eingehenden Datenverkehr vom Client-Netzwerk anvertraut, und Sie können den Zugriff bestimmter Ports auf dem Client-Netzwerk konfigurieren.

Die Beschränkung der Anzahl der offenen Ports auf IP-Adressen außerhalb Ihres Grids auf nur die absolut notwendigen Ports erhöht die Sicherheit Ihres Grids. Mithilfe der Einstellungen auf den drei Registerkarten für die Firewall-Steuerung stellen Sie sicher, dass nur die erforderlichen Ports geöffnet sind.

Weitere Informationen zur Verwendung von Firewall-Kontrollen, einschließlich Beispiele, finden Sie unter "Management der Firewall-Kontrollen".

Weitere Informationen zu externen Firewalls und Netzwerksicherheit finden Sie unter "Kontrolle des Zugriffs über externe Firewall".

Firewall-Kontrollen für den Zugriff

Schritte

1. Wählen Sie **CONFIGURATION** > **Security** > **Firewall Control**.

   Die drei Registerkarten auf dieser Seite werden unter beschrieben "Management der Firewall-Kontrollen".

2. Wählen Sie eine beliebige Registerkarte aus, um die Firewall-Steuerelemente zu konfigurieren.

   Sie können diese Registerkarten in beliebiger Reihenfolge verwenden. Die Konfigurationen, die Sie auf einer Registerkarte festlegen, beschränken nicht, was Sie auf den anderen Registerkarten tun können. Konfigurationsänderungen, die Sie auf einer Registerkarte vornehmen, können jedoch das Verhalten der auf anderen Registerkarten konfigurierten Ports ändern.

Liste privilegierter Adressen

Sie verwenden die Registerkarte Liste der privilegierten Adressen, um Hosts Zugriff auf Ports zu gewähren, die standardmäßig geschlossen oder durch Einstellungen auf der Registerkarte externen Zugriff verwalten geschlossen sind.

Privilegierte IP-Adressen und Subnetze haben standardmäßig keinen internen Grid-Zugriff. Zudem sind die Load Balancer-Endpunkte und zusätzliche Ports, die auf der Registerkarte „privilegierte Adressen“ geöffnet wurden, auch dann verfügbar, wenn sie auf der Registerkarte „externen Zugriff verwalten“ gesperrt sind.

Einstellungen auf der Registerkarte „Liste privilegierter Adressen“ können die Einstellungen auf der Registerkarte „nicht vertrauenswürdiges Clientnetzwerk“ nicht außer Kraft setzen.

Schritte

1. Geben Sie auf der Registerkarte Liste der privilegierten Adressen die Adresse oder das IP-Subnetz ein, die Sie Zugriff auf geschlossene Ports gewähren möchten.
2. Wählen Sie optional **Add another IP address or subnet in CIDR Notation** aus, um weitere privilegierte Clients hinzuzufügen.

   Fügen Sie so wenig Adressen wie möglich zur Liste der privilegierten Adressen hinzu.

3. Wählen Sie optional **privilegierten IP-Adressen erlauben, auf interne StorageGRID-Ports zuzugreifen**. Siehe "Interne StorageGRID-Ports".

   Diese Option entfernt einige Schutzmaßnahmen für interne Dienste. Lassen Sie sie nach Möglichkeit deaktiviert.

4. Wählen Sie **Speichern**.

Management des externen Zugriffs

Wenn ein Port auf der Registerkarte externen Zugriff verwalten geschlossen wird, kann keine IP-Adresse ohne Grid auf den Port zugegriffen werden, es sei denn, Sie fügen die IP-Adresse der Liste privilegierter Adressen hinzu. Sie können nur Ports schließen, die standardmäßig geöffnet sind, und Sie können nur Ports öffnen, die Sie geschlossen haben.

Einstellungen auf der Registerkarte „externen Zugriff verwalten“ können die Einstellungen auf der Registerkarte „nicht vertrauenswürdiges Clientnetzwerk“ nicht außer Kraft setzen. Wenn ein Knoten beispielsweise nicht vertrauenswürdig ist, wird Port SSH/22 im Client-Netzwerk gesperrt, selbst wenn er auf der Registerkarte externen Zugriff verwalten geöffnet ist. Die Einstellungen auf der Registerkarte nicht vertrauenswürdiger Client-Netzwerk überschreiben geschlossene Ports (z. B. 443, 8443, 9443) im Client-Netzwerk.

Schritte

1. Wählen Sie **externen Zugriff verwalten**. Auf der Registerkarte wird eine Tabelle mit allen externen Ports (Ports, auf die standardmäßig nicht-Grid-Nodes zugreifen können) für die Nodes in Ihrem Grid angezeigt.
2. Konfigurieren Sie die Ports, die geöffnet und geschlossen werden sollen, mithilfe der folgenden Optionen:
   - Verwenden Sie den Umschalter neben jedem Port, um den ausgewählten Port zu öffnen oder zu schließen.
   - Wählen Sie **Alle angezeigten Ports öffnen**, um alle in der Tabelle aufgeführten Ports zu öffnen.

- Wählen Sie **Alle angezeigten Ports schließen**, um alle in der Tabelle aufgeführten Ports zu schließen.

> Wenn Sie die Grid-Manager-Ports 443 oder 8443 schließen, verlieren alle Benutzer, die derzeit an einem blockierten Port verbunden sind, einschließlich Ihnen, den Zugriff auf Grid Manager, es sei denn, ihre IP-Adresse wurde der Liste der privilegierten Adressen hinzugefügt.

> Verwenden Sie die Bildlaufleiste auf der rechten Seite der Tabelle, um sicherzustellen, dass Sie alle verfügbaren Ports angezeigt haben. Verwenden Sie das Suchfeld, um die Einstellungen für einen externen Port zu finden, indem Sie eine Portnummer eingeben. Sie können einen Teil der Portnummer eingeben. Wenn Sie beispielsweise einen **2** eingeben, werden alle Ports angezeigt, die den String "2" als Teil ihres Namens haben.

3. Wählen Sie **Speichern**

Nicht Vertrauenswürdiges Client-Netzwerk

Wenn das Client-Netzwerk für einen Knoten nicht vertrauenswürdig ist, akzeptiert der Knoten nur eingehenden Datenverkehr an Ports, die als Load Balancer-Endpunkte konfiguriert sind, und optional zusätzliche Ports, die Sie auf dieser Registerkarte auswählen. Auf dieser Registerkarte können Sie auch die Standardeinstellung für neue Knoten festlegen, die in einer Erweiterung hinzugefügt wurden.

> Vorhandene Client-Verbindungen können fehlschlagen, wenn die Load Balancer-Endpunkte nicht konfiguriert wurden.

Die Konfigurationsänderungen, die Sie auf der Registerkarte **nicht vertrauenswürdiges Client-Netzwerk** vornehmen, überschreiben die Einstellungen auf der Registerkarte **externen Zugriff verwalten**.

Schritte

1. Wählen Sie **Nicht Vertrauenswürdiges Client-Netzwerk**.
2. Geben Sie im Abschnitt „Standard für neuen Knoten festlegen“ an, welche Standardeinstellung verwendet werden soll, wenn in einem Erweiterungsverfahren neue Knoten zum Raster hinzugefügt werden.

   - **Trusted** (Standard): Wenn ein Knoten in einer Erweiterung hinzugefügt wird, wird sein Client-Netzwerk vertrauenswürdig.
   - **UnTrusted**: Wenn ein Knoten in einer Erweiterung hinzugefügt wird, ist sein Client-Netzwerk nicht vertrauenswürdig.

     Bei Bedarf können Sie zu dieser Registerkarte zurückkehren, um die Einstellung für einen bestimmten neuen Knoten zu ändern.

   > Diese Einstellung hat keine Auswirkung auf die vorhandenen Nodes im StorageGRID System.

3. Verwenden Sie die folgenden Optionen, um die Knoten auszuwählen, die Clientverbindungen nur an explizit konfigurierten Endpunkten des Lastausgleichs oder zusätzlichen ausgewählten Ports zulassen sollen:

   - Wählen Sie **Untrust on displayed Nodes** aus, um alle in der Tabelle angezeigten Knoten zur Liste UnTrusted Client Network hinzuzufügen.
   - Wählen Sie **Trust on displayed Nodes** aus, um alle in der Tabelle angezeigten Knoten aus der Liste

UnTrusted Client Network zu entfernen.

- Verwenden Sie den Umschalter neben den einzelnen Ports, um das Client-Netzwerk für den ausgewählten Knoten als vertrauenswürdig oder nicht vertrauenswürdig festzulegen.

  Sie können beispielsweise **Untrust on displayed Nodes** auswählen, um alle Knoten zur Liste UnTrusted Client Network hinzuzufügen, und dann den Umschalter neben einem einzelnen Knoten verwenden, um diesen einzelnen Knoten zur Liste Trusted Client Network hinzuzufügen.

> Verwenden Sie die Bildlaufleiste auf der rechten Seite der Tabelle, um sicherzustellen, dass Sie alle verfügbaren Knoten angezeigt haben. Verwenden Sie das Suchfeld, um die Einstellungen für jeden Knoten durch Eingabe des Knotennamens zu suchen. Sie können einen Teilnamen eingeben. Wenn Sie beispielsweise einen **GW** eingeben, werden alle Knoten angezeigt, die den String "GW" als Teil ihres Namens haben.

4. Wählen Sie optional alle zusätzlichen Ports aus, die im nicht vertrauenswürdigen Client-Netzwerk geöffnet werden sollen. Diese Ports können Zugriff auf den Grid Manager, den Tenant Manager oder beide ermöglichen.

   Sie können z. B. mit dieser Option sicherstellen, dass der Grid-Manager im Client-Netzwerk zu Wartungszwecken aufgerufen werden kann.

> Diese zusätzlichen Ports sind im Client-Netzwerk geöffnet, unabhängig davon, ob sie auf der Registerkarte externen Zugriff verwalten geschlossen sind.

5. Wählen Sie **Speichern**.

   Die neuen Firewall-Einstellungen werden sofort angewendet und durchgesetzt. Vorhandene Client-Verbindungen können fehlschlagen, wenn die Load Balancer-Endpunkte nicht konfiguriert wurden.

Verwalten von Mandanten

Mandanten managen: Übersicht

Als Grid-Administrator erstellen und managen Sie die Mandantenkonten, die S3 und Swift-Clients zum Speichern und Abrufen von Objekten verwenden.

> Die Unterstützung für Swift-Client-Anwendungen wurde veraltet und wird in einer zukünftigen Version entfernt.

Was sind Mandantenkonten?

Ein Mandantenkonto ermöglicht Ihnen, entweder die Simple Storage Service (S3) REST-API oder die Swift REST-API zu verwenden, um Objekte in einem StorageGRID System zu speichern und abzurufen.

Jedes Mandantenkonto verfügt über föderierte oder lokale Gruppen, Benutzer, S3 Buckets oder Swift Container und Objekte.

Mandantenkonten können verwendet werden, um gespeicherte Objekte durch verschiedene Einheiten zu trennen. Beispielsweise können für einen der folgenden Anwendungsfälle mehrere Mandantenkonten verwendet werden:

- **Anwendungsbeispiel für Unternehmen:** Wenn Sie ein StorageGRID-System in einer Enterprise-

Anwendung verwalten, sollten Sie den Objekt-Storage des Grid möglicherweise von den verschiedenen Abteilungen Ihres Unternehmens trennen. In diesem Fall können Sie Mandantenkonten für die Marketingabteilung, die Kundenbetreuung, die Personalabteilung usw. erstellen.

> Wenn Sie das S3-Client-Protokoll verwenden, können Sie S3-Buckets und Bucket-Richtlinien verwenden, um Objekte zwischen den Abteilungen eines Unternehmens zu trennen. Sie müssen keine Mandantenkonten verwenden. Siehe Anweisungen zur Implementierung "S3-Buckets und Bucket-Richtlinien" Finden Sie weitere Informationen.

- **Anwendungsbeispiel Service Provider:** Wenn Sie ein StorageGRID-System als Service-Provider verwalten, können Sie den Objekt-Storage des Grid durch die verschiedenen Entitäten verteilen, die den Storage auf Ihrem Grid leasen. In diesem Fall würden Sie Mandantenkonten für Unternehmen A, Unternehmen B, Unternehmen C usw. erstellen.

Weitere Informationen finden Sie unter "Verwenden Sie ein Mandantenkonto".

Wie erstelle ich ein Mandantenkonto?

Wenn Sie ein Mandantenkonto erstellen, geben Sie die folgenden Informationen an:

- Grundlegende Informationen, einschließlich Mandantenname, Client-Typ (S3 oder Swift) und optionalem Storage-Kontingent.
- Berechtigungen für das Mandantenkonto, z. B. ob das Mandantenkonto S3-Plattformservices verwenden, seine eigene Identitätsquelle konfigurieren, S3 Select verwenden oder eine Grid-Verbundverbindung verwenden kann.
- Der erste Root-Zugriff für den Mandanten basiert darauf, ob das StorageGRID System lokale Gruppen und Benutzer, Identitätsföderation oder Single Sign On (SSO) verwendet.

Darüber hinaus können Sie die S3-Objektsperrung für das StorageGRID-System aktivieren, wenn S3-Mandantenkonten gesetzliche Vorgaben erfüllen müssen. Wenn S3 Object Lock aktiviert ist, können alle S3-Mandantenkonten konforme Buckets erstellen und managen.

Wofür wird Tenant Manager verwendet?

Nachdem Sie das Mandantenkonto erstellt haben, können sich Mandantenbenutzer beim Tenant Manager anmelden, um Aufgaben wie die folgenden auszuführen:

- Identitätsföderation einrichten (es sei denn, die Identitätsquelle wird mit dem Grid gemeinsam genutzt)
- Verwalten von Gruppen und Benutzern
- Grid-Verbund für Account-Klone und Grid-übergreifende Replizierung verwenden
- Managen von S3-Zugriffsschlüsseln
- S3 Buckets erstellen und managen
- Verwenden Sie S3-Plattformservices
- Verwenden Sie S3 Select
- Monitoring der Storage-Auslastung

> Benutzer von S3-Mandanten können mit dem Tenant Manager S3-Zugriffsschlüssel und -Buckets erstellen und managen, müssen jedoch Objekte mit einer S3-Client-Applikation aufnehmen und managen. Siehe "S3-REST-API VERWENDEN" Entsprechende Details.

Swift-Benutzer müssen über die Root-Zugriffsberechtigung für den Zugriff auf den Mandanten-Manager verfügen. Die Berechtigung Root-Zugriff erlaubt Benutzern jedoch nicht, sich in der Swift REST-API zu authentifizieren, um Container zu erstellen und Objekte aufzunehmen. Benutzer müssen über die Swift-Administratorberechtigung verfügen, um sich bei der Swift-REST-API zu authentifizieren.

Erstellen Sie ein Mandantenkonto

Sie müssen mindestens ein Mandantenkonto erstellen, um den Zugriff auf den Storage in Ihrem StorageGRID-System zu kontrollieren.

Die Schritte zum Erstellen eines Mandantenkontos variieren je nachdem, ob "Identitätsföderation" Und "Single Sign On" Sind konfiguriert und ob das Grid Manager-Konto, das Sie zum Erstellen des Mandantenkontos verwenden, einer Admin-Gruppe mit Root-Zugriffsberechtigung angehört.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie verfügen über die Berechtigung Root-Zugriff oder Mandantenkonten.
- Wenn das Mandantenkonto die für den Grid Manager konfigurierte Identitätsquelle verwendet und Sie einer föderierten Gruppe Root-Zugriffsberechtigungen für das Mandantenkonto gewähren möchten, haben Sie diese föderierte Gruppe in den Grid Manager importiert. Sie müssen dieser Administratorgruppe keine Grid Manager-Berechtigungen zuweisen. Siehe "Managen von Admin-Gruppen".
- Wenn Sie einem S3-Mandanten das Klonen von Kontodaten und das Replizieren von Bucket-Objekten in einem anderen Grid über eine Grid-Federation-Verbindung ermöglichen möchten:
  - Das ist schon "Grid Federation-Verbindung konfiguriert".
  - Der Status der Verbindung lautet **connected**.
  - Sie haben Root-Zugriffsberechtigung.
  - Sie haben die Überlegungen für überprüft "Verwalten der zulässigen Mandanten für den Grid-Verbund".
  - Wenn das Mandantenkonto die Identitätsquelle verwendet, die für Grid Manager konfiguriert wurde, haben Sie dieselbe Verbundgruppe in Grid Manager auf beiden Grids importiert.

    Wenn Sie den Mandanten erstellen, wählen Sie diese Gruppe aus, um die anfängliche Root-Zugriffsberechtigung für die Quell- und Zielmandantenkonten zu erhalten.

    Wenn diese Administratorgruppe vor dem Erstellen des Mandanten nicht auf beiden Grids vorhanden ist, wird der Mandant nicht am Ziel repliziert.

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **MIETER**.
2. Wählen Sie **Erstellen**.

Geben Sie Details ein

Schritte

1. Geben Sie Details für die Serviceeinheit ein.

Feld	Beschreibung
Name	Ein Name für das Mandantenkonto. Mandantennamen müssen nicht eindeutig sein. Wenn das Mandantenkonto erstellt wird, erhält es eine eindeutige, 20-stellige Konto-ID.
Beschreibung (optional)	Eine Beschreibung zur Identifizierung des Mandanten. Wenn Sie einen Mandanten erstellen, der eine Grid-Federation-Verbindung verwendet, können Sie optional mithilfe dieses Felds ermitteln, welcher der Quell-Tenant ist und welcher der Zielmandant ist. Beispielsweise wird diese Beschreibung für einen Mandanten, der in Grid 1 erstellt wurde, auch für den Mandanten angezeigt, der in Grid 2 repliziert wurde: „Dieser Mandant wurde in Grid 1 erstellt.“
Client-Typ	Der Typ des Client-Protokolls, das dieser Mandant verwendet, entweder **S3** oder **Swift**. **Hinweis**: Die Unterstützung für Swift-Client-Anwendungen wurde veraltet und wird in einer zukünftigen Version entfernt.
Storage-Kontingent (optional)	Wenn Sie möchten, dass dieser Mandant über ein Speicherkontingent, einen numerischen Wert für das Kontingent und die Einheiten verfügt.

2. Wählen Sie **Weiter**.

Wählen Sie Berechtigungen aus

Schritte

1. Wählen Sie optional alle Berechtigungen aus, die dieser Tenant haben soll.

> Einige dieser Berechtigungen haben zusätzliche Anforderungen. Für Details wählen Sie das Hilfesymbol für jede Berechtigung aus.

Berechtigung	Wenn ausgewählt…
Unterstützung von Plattform-Services	Der Mandant kann S3-Plattformservices wie CloudMirror verwenden. Siehe "Management von Plattform-Services für S3-Mandantenkonten".
Eigene Identitätsquelle verwenden	Der Mandant kann seine eigene Identitätsquelle für verbundene Gruppen und Benutzer konfigurieren und verwalten. Diese Option ist deaktiviert, wenn Sie dies haben "SSO konfiguriert" Für Ihr StorageGRID-System.
S3 Select zulassen	Der Mandant kann S3 SelectObjectContent API-Anforderungen ausgeben, um Objektdaten zu filtern und abzurufen. Siehe "Management von S3 Select für Mandantenkonten". **Wichtig**: SelectObjectContent Requests können die Load Balancer Performance für alle S3 Clients und alle Tenants verringern. Aktivieren Sie diese Funktion nur bei Bedarf und nur für vertrauenswürdige Mandanten.

Berechtigung	Wenn ausgewählt…
Netzverbundverbindung verwenden	Der Mandant kann eine Grid Federation-Verbindung verwenden. Auswahl dieser Option: • Bewirkt, dass dieser Mandant und alle dem Konto hinzugefügten Mandantengruppen und Benutzer aus diesem Raster (das *source Grid*) in das andere Raster der ausgewählten Verbindung (das *Destination Grid*) geklont werden. • Ermöglicht diesem Mandanten, die Grid-übergreifende Replizierung zwischen entsprechenden Buckets in jedem Grid zu konfigurieren. Siehe "Verwalten Sie die zulässigen Mandanten für den Grid-Verbund". **Hinweis**: Sie können nur **Grid Federation connection** verwenden auswählen, wenn Sie einen neuen S3-Mandanten erstellen; Sie können diese Berechtigung nicht für einen vorhandenen Mandanten auswählen.

2. Wenn Sie **Grid Federation connection** verwenden ausgewählt haben, wählen Sie eine der verfügbaren Grid Federation-Verbindungen aus.

3. Wählen Sie **Weiter**.

Root-Zugriff definieren und Mandanten erstellen

Schritte

1. Definieren Sie den Root-Zugriff für das Mandantenkonto, je nachdem, ob Ihr StorageGRID-System Identitätsföderation, Single Sign-On (SSO) oder beides verwendet.

Option	Tun Sie das
Wenn die Identitätsföderation nicht aktiviert ist	Geben Sie das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.
Wenn die Identitätsföderation aktiviert ist	a. Wählen Sie eine vorhandene Verbundgruppe aus, um Root-Zugriffsberechtigungen für den Mandanten zu erhalten. b. Geben Sie optional das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.

Option	Tun Sie das
Wenn sowohl Identitätsföderation als auch Single Sign-On (SSO) aktiviert sind	Wählen Sie eine vorhandene Verbundgruppe aus, um Root-Zugriffsberechtigungen für den Mandanten zu erhalten. Keine lokalen Benutzer können sich anmelden.

2. Wählen Sie **Create Tenant**.

   Eine Erfolgsmeldung wird angezeigt, und die neue Serviceeinheit wird auf der Seite „Serviceeinheiten“ aufgeführt. Informationen zum Anzeigen von Mandantendetails und zum Überwachen der Mandantenaktivität finden Sie unter "Überwachen Sie die Mandantenaktivität".

3. Wenn Sie die Berechtigung **Grid Federation connection** für den Mieter verwenden ausgewählt haben:

   a. Vergewissern Sie sich, dass ein identischer Mandant auf das andere Grid in der Verbindung repliziert wurde. Die Mandanten in beiden Grids haben die gleiche 20-stellige Konto-ID, den gleichen Namen, die gleiche Beschreibung, das gleiche Kontingent und die gleichen Berechtigungen.

      Wenn die Fehlermeldung „`Tenant created without a Clone`,“ angezeigt wird, lesen Sie die Anweisungen in "Fehler beim Grid-Verbund beheben".

   b. Wenn Sie beim Definieren des Root-Zugriffs ein lokales Root-Benutzerpasswort angegeben haben, "Ändern Sie das Passwort für den lokalen Root-Benutzer" Für den replizierten Mandanten.

      Ein lokaler Root-Benutzer kann sich erst bei Tenant Manager im Zielraster anmelden, wenn das Passwort geändert wurde.

Beim Mandanten anmelden (optional)

Sie können sich nach Bedarf jetzt beim neuen Mandanten anmelden, um die Konfiguration abzuschließen, oder sich später beim Mandanten anmelden. Die Schritte zur Anmeldung hängen davon ab, ob Sie über den Standardport (443) oder einen eingeschränkten Port beim Grid Manager angemeldet sind. Siehe "Kontrolle des Zugriffs über externe Firewall".

Jetzt anmelden

Sie verwenden…	Tun Sie das…
Port 443 und Sie legen ein Passwort für den lokalen Root-Benutzer fest	1. Wählen Sie **als root anmelden**. Wenn Sie sich anmelden, werden Links zum Konfigurieren von Buckets, Identitätsverbünden, Gruppen und Benutzern angezeigt. 2. Wählen Sie die Links aus, um das Mandantenkonto zu konfigurieren. Jeder Link öffnet die entsprechende Seite im Tenant Manager. Informationen zum Ausfüllen der Seite finden Sie im "Anweisungen zur Verwendung von Mandantenkonten".

Sie verwenden…	Tun Sie das…
Port 443 und Sie haben kein Passwort für den lokalen Root-Benutzer festgelegt	Wählen Sie **Anmelden**, und geben Sie die Anmeldeinformationen für einen Benutzer in der Gruppe Root Access Federated ein.
Ein eingeschränkter Port	1. Wählen Sie **Fertig Stellen** 2. Wählen Sie **eingeschränkt** in der Tabelle Tenant aus, um mehr über den Zugriff auf dieses Mandantenkonto zu erfahren. Die URL für den Tenant Manager weist folgendes Format auf: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ *`FQDN_or_Admin_Node_IP`* Ist ein vollständig qualifizierter Domain-Name oder die IP-Adresse eines Admin-Knotens ◦ *`port`* Ist der reine Mandantenport ◦ *`20-digit-account-id`* Die eindeutige Account-ID des Mandanten

Melden Sie sich später an

Sie verwenden…	Führen Sie eine dieser…
Port 443	• Wählen Sie im Grid Manager **MIETERS** aus und wählen Sie **Anmelden** rechts neben dem Mieternamen aus. • Geben Sie die URL des Mandanten in einen Webbrowser ein: `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ *`FQDN_or_Admin_Node_IP`* Ist ein vollständig qualifizierter Domain-Name oder die IP-Adresse eines Admin-Knotens ◦ *`20-digit-account-id`* Die eindeutige Account-ID des Mandanten
Ein eingeschränkter Port	• Wählen Sie im Grid Manager die Option **MITERS** aus, und wählen Sie **eingeschränkt**. • Geben Sie die URL des Mandanten in einen Webbrowser ein: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ *`FQDN_or_Admin_Node_IP`* Ist ein vollständig qualifizierter Domain-Name oder die IP-Adresse eines Admin-Knotens ◦ *`port`* Ist der ausschließlich auf Mandanten beschränkte Port ◦ *`20-digit-account-id`* Die eindeutige Account-ID des Mandanten

Konfigurieren Sie den Mandanten

Befolgen Sie die Anweisungen unter "Verwenden Sie ein Mandantenkonto" Zum Management von Mandantengruppen und -Benutzern managen Sie S3-Zugriffsschlüssel, Buckets, Plattform-Services sowie Konto-Klone und Grid-Replizierung.

Mandantenkonto bearbeiten

Sie können ein Mandantenkonto bearbeiten, um den Anzeigenamen, das Speicherkontingent oder die Berechtigungen für Mandanten zu ändern.

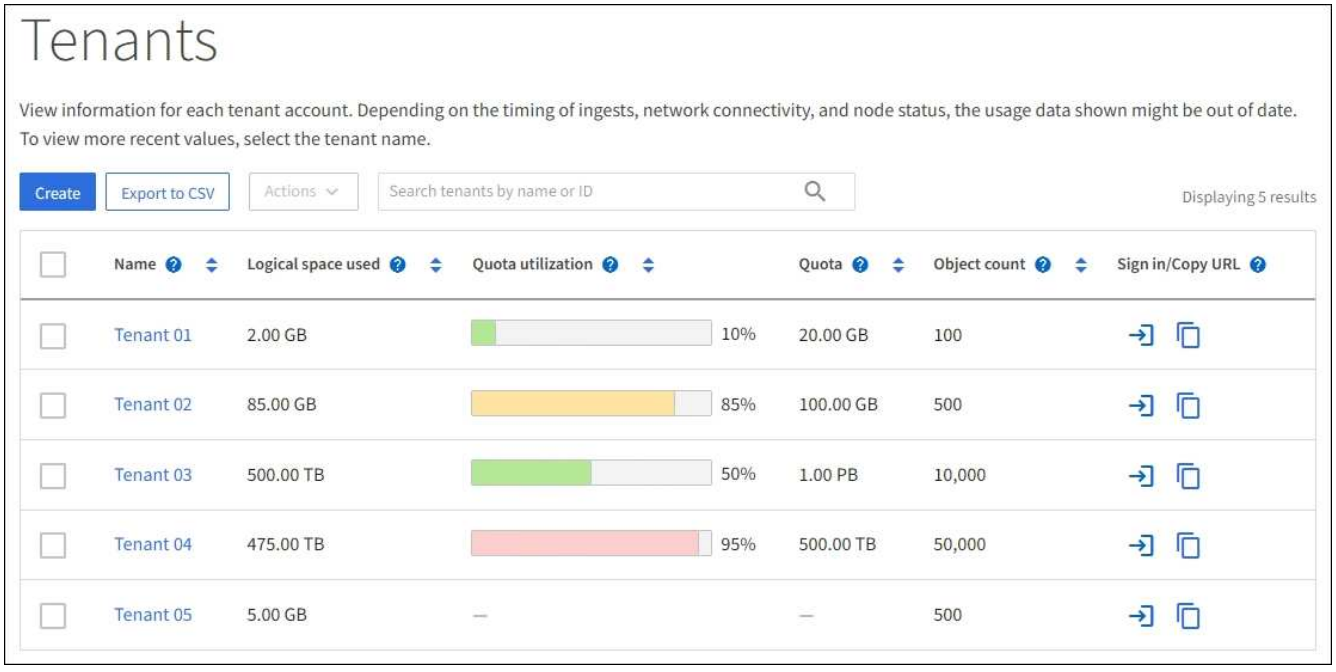
Wenn ein Mandant über die Berechtigung **Grid Federation connection** verwenden verfügt, können Sie die Mandantendetails von beiden Rastergittern in der Verbindung bearbeiten. Änderungen, die Sie an einem Raster in der Verbindung vornehmen, werden jedoch nicht in das andere Raster kopiert. Wenn Sie die Details der Serviceeinheit zwischen den Rastern exakt synchronisieren möchten, nehmen Sie die gleichen Änderungen an beiden Rastern vor. Siehe "Verwalten Sie die zulässigen Mandanten für die Grid Federation-Verbindung".

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie verfügen über die Berechtigung Root-Zugriff oder Mandantenkonten.

Schritte

1. Wählen Sie **MIETER**.



2. Suchen Sie das Mandantenkonto, das Sie bearbeiten möchten.

   Verwenden Sie das Suchfeld, um nach einem Mandanten anhand des Namens oder der Mandanten-ID zu suchen.

3. Wählen Sie den Mandanten aus. Sie können eine der folgenden Aktionen ausführen:
   - Aktivieren Sie das Kontrollkästchen für den Mandanten und wählen Sie **actions** > **Edit**.

- Wählen Sie den Namen des Mandanten aus, um die Detailseite anzuzeigen, und wählen Sie **Bearbeiten**.

4. Ändern Sie optional die Werte für diese Felder:
   - **Name**
   - **Beschreibung**
   - **Speicherquote**
5. Wählen Sie **Weiter**.
6. Wählen oder deaktivieren Sie die Berechtigungen für das Mandantenkonto.
   - Wenn Sie **Platform Services** für einen Mandanten deaktivieren, der diese bereits nutzt, werden die Dienste, die er für seine S3-Buckets konfiguriert hat, nicht mehr funktionieren. Es wird keine Fehlermeldung an den Mandanten gesendet. Wenn der Mandant beispielsweise die Replizierung von CloudMirror für einen S3-Bucket konfiguriert hat, können sie Objekte weiterhin im Bucket speichern, doch werden Kopien dieser Objekte nicht mehr im externen S3-Bucket erstellt, den sie als Endpunkt konfiguriert haben. Siehe "Management von Plattform-Services für S3-Mandantenkonten".
   - Ändern Sie die Einstellung **verwendet eigene Identitätsquelle**, um zu bestimmen, ob das Mandantenkonto seine eigene Identitätsquelle oder die für den Grid Manager konfigurierte Identitätsquelle verwendet.

     Wenn **eigene Identitätsquelle verwendet** ist:

     - Deaktiviert und ausgewählt, hat der Mandant bereits seine eigene Identitätsquelle aktiviert. Ein Mandant muss seine Identitätsquelle deaktivieren, bevor er die für den Grid Manager konfigurierte Identitätsquelle verwenden kann.
     - Deaktiviert und nicht ausgewählt, SSO ist für das StorageGRID-System aktiviert. Der Mandant muss die Identitätsquelle verwenden, die für den Grid Manager konfiguriert wurde.
   - Wählen oder deaktivieren Sie die Berechtigung **allow S3 Select** nach Bedarf. Siehe "Management von S3 Select für Mandantenkonten".
   - Um die Berechtigung **use Grid Federation connection** zu entfernen, folgen Sie den Anweisungen für "Entfernen der Berechtigung eines Mandanten zur Verwendung des Grid-Verbunds".

Ändern Sie das Passwort für den lokalen Root-Benutzer des Mandanten

Möglicherweise müssen Sie das Passwort für den lokalen Root-Benutzer eines Mandanten ändern, wenn der Root-Benutzer aus dem Konto gesperrt ist.

Bevor Sie beginnen

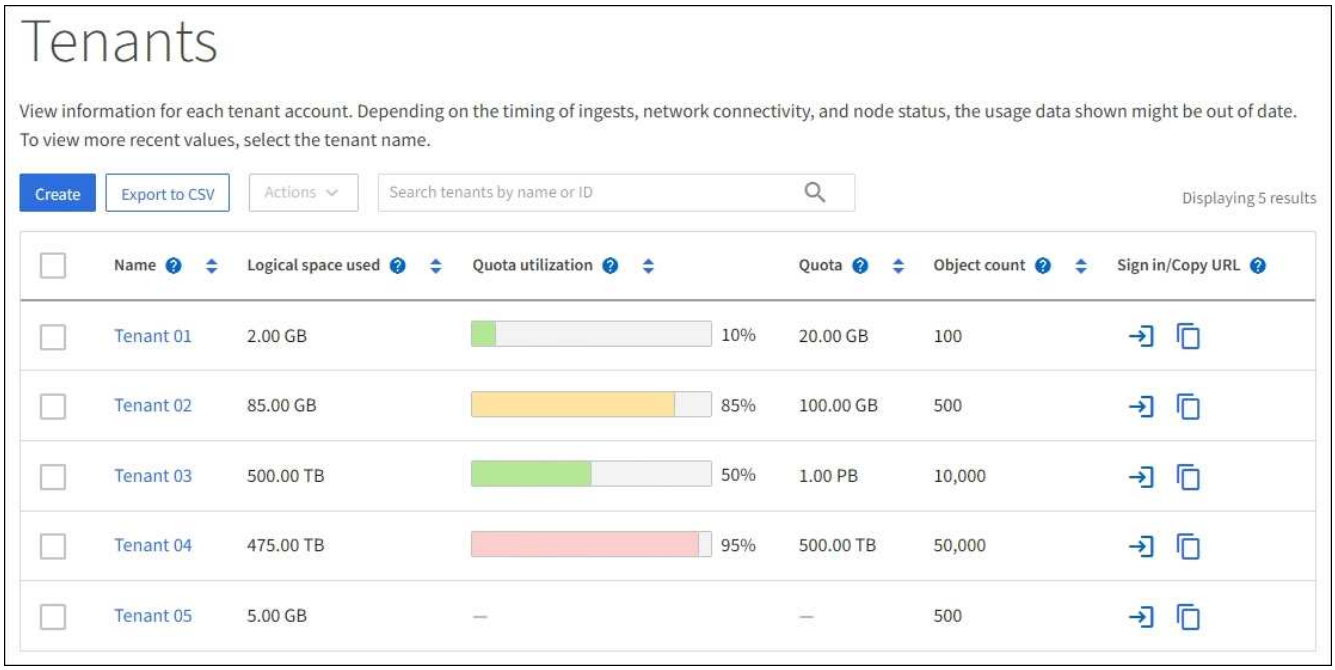
- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, kann sich der lokale Root-Benutzer nicht beim Mandanten-Konto anmelden. Um Root-Benutzeraufgaben auszuführen, müssen Benutzer einer föderierten Gruppe angehören, die über die Root-Zugriffsberechtigung für den Mandanten verfügt.

Schritte

1. Wählen Sie **MIETER**.



2. Wählen Sie das Mandantenkonto aus. Sie können eine der folgenden Aktionen ausführen:
   - Aktivieren Sie das Kontrollkästchen für den Mandanten, und wählen Sie **actions** > **root-Passwort ändern**.
   - Wählen Sie den Namen des Mandanten aus, um die Detailseite anzuzeigen, und wählen Sie **actions** > **root password ändern**.
3. Geben Sie das neue Kennwort für das Mandantenkonto ein.
4. Wählen Sie **Speichern**.

Mandantenkonto löschen

Sie können ein Mandantenkonto löschen, wenn Sie den Zugriff des Mandanten auf das System dauerhaft entfernen möchten.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben alle Buckets (S3), Container (Swift) und Objekte entfernt, die dem Mandantenkonto zugeordnet sind.
- Wenn der Mandant eine Grid Federation-Verbindung verwenden darf, haben Sie die Überlegungen für geprüft "Löschen eines Mandanten mit der Berechtigung Grid Federation verwenden".

Schritte

1. Wählen Sie **MIETER**.
2. Suchen Sie das oder die Konten, die Sie löschen möchten.

   Verwenden Sie das Suchfeld, um nach einem Mandanten anhand des Namens oder der Mandanten-ID zu suchen.

3. Um mehrere Mandanten zu löschen, aktivieren Sie die Kontrollkästchen und wählen **Aktionen** > **Löschen**.

4. Führen Sie einen der folgenden Schritte aus, um eine einzelne Serviceeinheit zu löschen:
   - Aktivieren Sie das Kontrollkästchen, und wählen Sie **Aktionen** > **Löschen**.
   - Wählen Sie den Namen des Mandanten aus, um die Detailseite anzuzeigen, und wählen Sie dann **actions** > **Delete** aus.
5. Wählen Sie **Ja**.

Management von Plattform-Services

Verwaltung von Plattformservices für Mandanten: Übersicht

Wenn Sie Plattformservices für S3-Mandantenkonten aktivieren, müssen Sie Ihr Grid so konfigurieren, dass Mandanten auf die externen Ressourcen zugreifen können, die für die Nutzung dieser Services erforderlich sind.

Was sind Plattform-Services?

Zu den Plattform-Services zählen die CloudMirror-Replizierung, Ereignisbenachrichtigungen und der Such-Integrationsservice.

Dank dieser Services können Mandanten die folgenden Funktionen mit ihren S3 Buckets nutzen:

- **CloudMirror Replikation**: Der StorageGRID CloudMirror Replikationsservice wird verwendet, um bestimmte Objekte von einem StorageGRID-Bucket auf ein bestimmtes externes Ziel zu spiegeln.

  So können Sie beispielsweise CloudMirror Replizierung verwenden, um spezifische Kundendaten in Amazon S3 zu spiegeln und anschließend AWS Services für Analysen Ihrer Daten nutzen.

  > Die CloudMirror-Replizierung weist einige wichtige Ähnlichkeiten und Unterschiede zur Grid-übergreifenden Replizierungsfunktion auf. Weitere Informationen finden Sie unter "Vergleichen Sie Grid-Replizierung und CloudMirror Replizierung".

  > Die CloudMirror-Replizierung wird nicht unterstützt, wenn im Quell-Bucket S3-Objektsperre aktiviert ist.

- **Benachrichtigungen**: Pro Bucket werden Ereignisbenachrichtigungen verwendet, um Benachrichtigungen über bestimmte Aktionen zu senden, die an Objekte an einen bestimmten externen Amazon Simple Notification Service™ (Amazon SNS) durchgeführt werden.

  Beispielsweise können Sie Warnmeldungen so konfigurieren, dass sie an Administratoren über jedes Objekt, das einem Bucket hinzugefügt wurde, gesendet werden, wo die Objekte Protokolldateien darstellen, die mit einem kritischen Systemereignis verbunden sind.

  > Obwohl die Ereignisbenachrichtigung für einen Bucket konfiguriert werden kann, bei dem S3 Object Lock aktiviert ist, werden die S3 Object Lock Metadaten (einschließlich „Aufbewahrung bis Datum“ und „Legal Hold“-Status) der Objekte in den Benachrichtigungsmeldungen nicht enthalten.

- **Suchintegrationsdienst**: Der Suchintegrationsdienst dient dazu, S3-Objektmetadaten an einen bestimmten Elasticsearch-Index zu senden, in dem die Metadaten mit dem externen Dienst durchsucht oder analysiert werden können.

Sie könnten beispielsweise die Buckets konfigurieren, um S3 Objekt-Metadaten an einen Remote-Elasticsearch-Service zu senden. Anschließend kann Elasticsearch verwendet werden, um nach Buckets zu suchen und um anspruchsvolle Analysen der Muster in den Objektmetadaten durchzuführen.

> Die Elasticsearch-Integration kann auf einem Bucket konfiguriert werden, bei dem die S3-Objektsperre aktiviert ist, aber die S3-Objektsperrmetadaten (einschließlich Aufbewahrung bis Datum und Status der Aufbewahrung) der Objekte werden nicht in die Benachrichtigungen einbezogen.

Dank Plattform-Services können Mandanten externe Storage-Ressourcen, Benachrichtigungsservices und Such- oder Analyseservices für ihre Daten nutzen. Da sich der Zielstandort für Plattformservices in der Regel außerhalb Ihrer StorageGRID-Implementierung befindet, müssen Sie entscheiden, ob die Nutzung dieser Services durch Mandanten gestattet werden soll. Wenn Sie dies tun, müssen Sie die Verwendung von Plattform-Services aktivieren, wenn Sie Mandantenkonten erstellen oder bearbeiten. Sie müssen auch Ihr Netzwerk so konfigurieren, dass die von Mandanten generierten Plattformservices Meldungen ihre Ziele erreichen können.

Empfehlungen für die Nutzung von Plattform-Services

Vor der Verwendung von Plattform-Services sollten Sie sich der folgenden Empfehlungen bewusst sein:

- Wenn in einem S3-Bucket im StorageGRID System sowohl die Versionierung als auch die CloudMirror-Replizierung aktiviert sind, sollten Sie für den Zielendpunkt auch die S3-Bucket-Versionierung aktivieren. So kann die CloudMirror-Replizierung ähnliche Objektversionen auf dem Endpunkt generieren.
- Sie sollten nicht mehr als 100 aktive Mandanten mit S3-Anfragen verwenden, die CloudMirror-Replizierung, Benachrichtigungen und Suchintegration erfordern. Mehr als 100 aktive Mandanten können zu einer langsameren S3-Client-Performance führen.
- Anforderungen an einen Endpunkt, die nicht abgeschlossen werden können, werden in die Warteschlange für maximal 500,000 Anfragen gestellt. Dieses Limit wird gleich von aktiven Mandanten gemeinsam genutzt. Neue Mandanten dürfen dieses Limit von 500,000 vorübergehend überschreiten, sodass neu erstellte Mandanten nicht unfair bestraft werden.

Verwandte Informationen

- "Verwenden Sie ein Mandantenkonto"
- "Konfigurieren Sie Speicher-Proxy-Einstellungen"
- "Monitoring von StorageGRID"

Netzwerk und Ports für Plattformservices

Wenn ein S3-Mandant Plattformservices verwendet, müssen Sie das Netzwerk für das Grid konfigurieren, um sicherzustellen, dass Plattformservices-Meldungen an seine Ziele gesendet werden können.

Sie können Plattformservices für ein S3-Mandantenkonto aktivieren, wenn Sie das Mandantenkonto erstellen oder aktualisieren. Wenn Plattformservices aktiviert sind, kann der Mandant Endpunkte erstellen, die als Ziel für die CloudMirror-Replizierung, Ereignisbenachrichtigungen oder Integrationsmeldungen aus seinen S3-Buckets dienen. Diese Plattform-Services-Meldungen werden von Storage-Nodes gesendet, die den ADC-Service an die Ziel-Endpunkte ausführen.

Beispielsweise können Mandanten die folgenden Typen von Ziel-Endpunkten konfigurieren:

- Ein lokal gehostetes Elasticsearch-Cluster ausführen
- Eine lokale Anwendung, die den Empfang von Amazon SNS-Nachrichten (Simple Notification Service) unterstützt
- Ein lokal gehosteter S3-Bucket auf derselben oder einer anderen Instanz von StorageGRID
- Einem externen Endpunkt wie einem Endpunkt auf Amazon Web Services

Um sicherzustellen, dass Meldungen von Plattformservices bereitgestellt werden können, müssen Sie das Netzwerk oder die Netzwerke mit den ADC-Speicherknoten konfigurieren. Sie müssen sicherstellen, dass die folgenden Ports zum Senden von Plattformservices-Meldungen an die Ziel-Endpunkte verwendet werden können.

Standardmäßig werden Plattform-Services-Meldungen an die folgenden Ports gesendet:

- **80**: Für Endpunkt-URIs, die mit http beginnen
- **443**: Für Endpunkt-URIs, die mit https beginnen

Mandanten können bei der Erstellung oder Bearbeitung eines Endpunkts einen anderen Port angeben.

> Wenn eine StorageGRID-Bereitstellung als Ziel für die CloudMirror-Replikation verwendet wird, können Replikationsmeldungen auf einem anderen Port als 80 oder 443 empfangen werden. Vergewissern Sie sich, dass der von der Ziel-StorageGRID-Implementierung für S3 verwendete Port im Endpunkt angegeben ist.

Wenn Sie einen nicht-transparenten Proxy-Server verwenden, müssen Sie auch "Konfigurieren Sie Speicher-Proxy-Einstellungen" Damit Nachrichten an externe Endpunkte gesendet werden können, z. B. an einem Endpunkt im Internet.

Verwandte Informationen

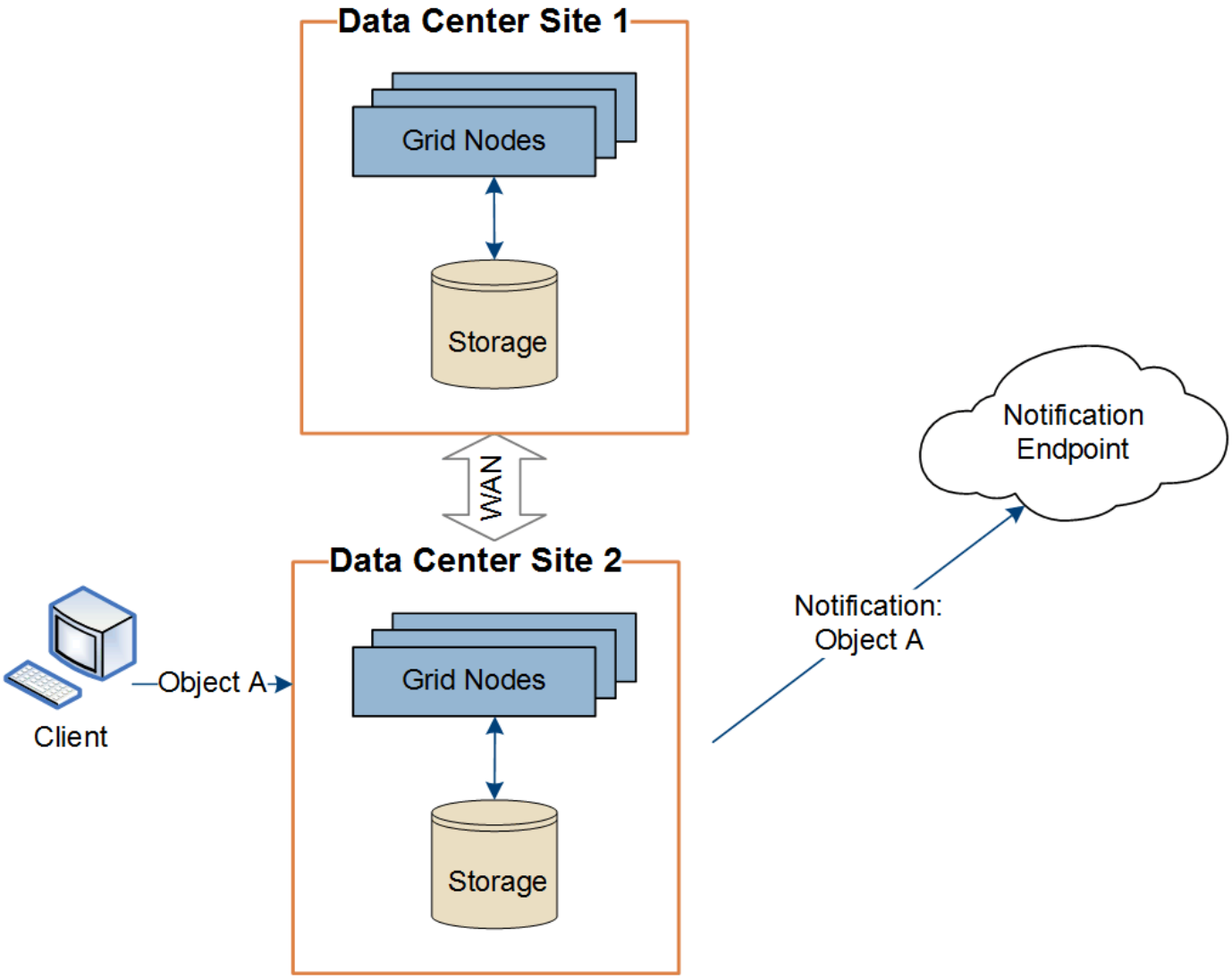
- "Verwenden Sie ein Mandantenkonto"

Bereitstellung von Plattform-Services am Standort

Alle Vorgänge von Plattform-Services werden am Standort durchgeführt.

Wenn ein Mandant einen Client verwendet, um einen S3 API Create-Vorgang für ein Objekt durch eine Verbindung zu einem Gateway-Node an Datacenter Standort 1 durchzuführen, wird die Benachrichtigung über diese Aktion von Datacenter Standort 1 ausgelöst und gesendet.

Wenn der Client anschließend einen S3-API-Löschvorgang auf demselben Objekt von Data Center Site 2 aus durchführt, wird die Benachrichtigung über die Löschaktion ausgelöst und von Data Center Site 2 gesendet.



Stellen Sie sicher, dass das Netzwerk an jedem Standort so konfiguriert ist, dass Plattformdienste-Meldungen an ihre Ziele gesendet werden können.

Fehlerbehebung bei Plattform-Services

Die in Plattform-Services verwendeten Endpunkte werden von Mandantenbenutzern im Mandanten-Manager erstellt und gewartet. Falls jedoch Probleme bei der Konfiguration oder Verwendung von Plattformservices bei einem Mandanten auftreten, können Sie das Problem mithilfe des Grid Manager beheben.

Probleme mit neuen Endpunkten

Bevor ein Mandant Plattform-Services nutzen kann, muss er mithilfe des Mandanten-Manager einen oder mehrere Endpunkte erstellen. Jeder Endpunkt stellt ein externes Ziel für einen Plattform-Service dar, wie einen StorageGRID S3 Bucket, einen Amazon Web Services Bucket, ein Thema „Simple Notification Service“ oder ein Elasticsearch-Cluster, der lokal oder in AWS gehostet wird. Jeder Endpunkt umfasst sowohl den Standort der externen Ressource als auch die für den Zugriff auf diese Ressource erforderlichen Zugangsdaten.

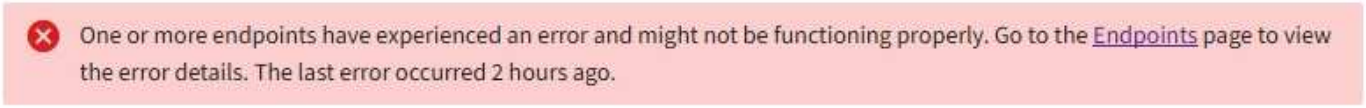
Wenn ein Mandant einen Endpunkt erstellt, überprüft das StorageGRID System, ob der Endpunkt vorhanden ist und ob er mit den angegebenen Zugangsdaten erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Node an jedem Standort validiert.

Wenn die Endpoint-Validierung fehlschlägt, erklärt eine Fehlermeldung, warum die Endpoint-Validierung fehlgeschlagen ist. Der Mandantenbenutzer sollte das Problem lösen, und versuchen Sie dann erneut, den Endpunkt zu erstellen.

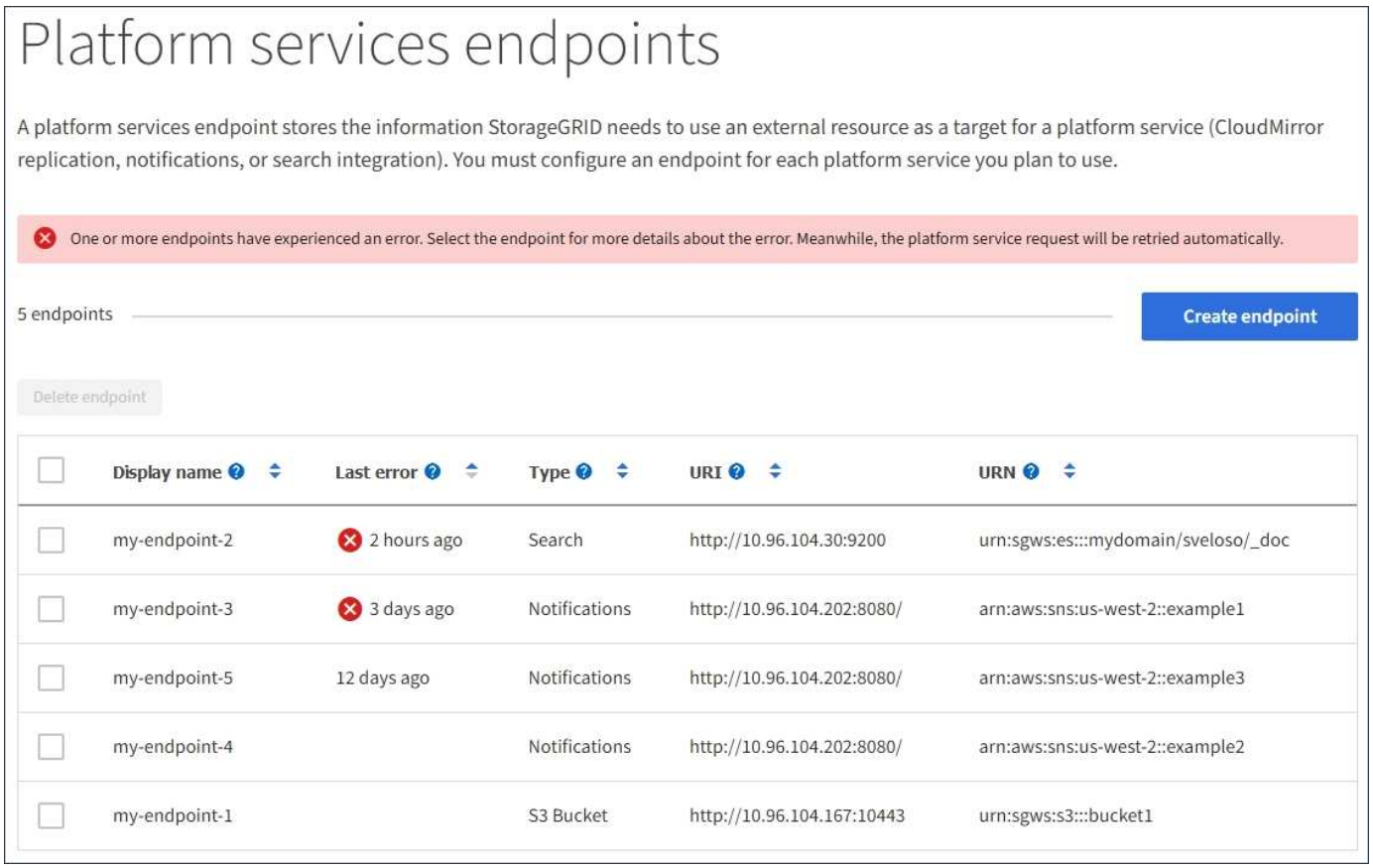
Die Erstellung von Endpunkten schlägt fehl, wenn Plattformdienste für das Mandantenkonto nicht aktiviert sind.

Probleme mit vorhandenen Endpunkten

Wenn ein Fehler auftritt, wenn StorageGRID versucht, einen vorhandenen Endpunkt zu erreichen, wird im Mandantenmanager eine Meldung auf dem Dashboard angezeigt.



Mandantenbenutzer können auf der Seite Endpunkte die aktuellste Fehlermeldung für jeden Endpunkt lesen und herausfinden, wie lange der Fehler bereits aufgetreten ist. Die Spalte **Letzter Fehler** zeigt die aktuellste Fehlermeldung für jeden Endpunkt an und gibt an, wie lange der Fehler aufgetreten ist. Fehler, die das enthalten Das Symbol trat innerhalb der letzten 7 Tage auf.



Einige Fehlermeldungen in der Spalte **Letzter Fehler** können eine LOGID in Klammern enthalten. Ein Grid-Administrator oder technischer Support kann diese ID verwenden, um ausführlichere Informationen über den Fehler im bycast.log zu finden.

Probleme im Zusammenhang mit Proxy-Servern

Wenn Sie einen konfiguriert haben "Storage-Proxy" Zwischen Storage-Nodes und Plattform-Service-Endpunkten können Fehler auftreten, wenn Ihr Proxy-Service keine Meldungen von StorageGRID zulässt. Um diese Probleme zu beheben, überprüfen Sie die Einstellungen Ihres Proxy-Servers, um sicherzustellen, dass keine Nachrichten im Zusammenhang mit dem Plattformdienst blockiert werden.

Ermitteln Sie, ob ein Fehler aufgetreten ist

Wenn in den letzten 7 Tagen Endpunktfehler aufgetreten sind, zeigt das Dashboard im Tenant Manager eine Warnmeldung an. Sie können die Seite Endpoints aufrufen, um weitere Details über den Fehler zu sehen.

Client-Betrieb schlägt fehl

Einige Probleme bei Plattform-Services können zum Ausfall von Client-Operationen auf dem S3-Bucket führen. Beispielsweise schlägt der S3-Client-Betrieb fehl, wenn der interne RSM-Service (Replicated State Machine) ausfällt oder es zu viele Plattformservices-Nachrichten in Warteschlange für die Lieferung gibt.

So überprüfen Sie den Status der Dienste:

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***site*** > ***Storage Node*** > **SSM** > **Services** aus.

Behebbare und nicht wiederherstellbare Endpunktfehler

Nach der Erstellung von Endpunkten können Fehler bei Plattformservice-Anfragen aus verschiedenen Gründen auftreten. Einige Fehler lassen sich durch Benutzereingriffe wiederherstellen. Beispielsweise können behebbare Fehler aus den folgenden Gründen auftreten:

- Die Anmeldedaten des Benutzers wurden gelöscht oder abgelaufen.
- Der Ziel-Bucket ist nicht vorhanden.
- Die Benachrichtigung kann nicht zugestellt werden.

Wenn bei StorageGRID ein wiederherstellbarer Fehler auftritt, wird die Serviceanfrage für die Plattform erneut versucht, bis sie erfolgreich ist.

Andere Fehler können nicht behoben werden. Beispielsweise tritt ein nicht behebbarer Fehler auf, wenn der Endpunkt gelöscht wird.

Wenn bei StorageGRID ein nicht behebbarer Endpunktfehler auftritt, wird im Grid Manager der alte Alarm „Total Events“ (SMTT) ausgelöst. So zeigen Sie den alten Alarm „Ereignisse insgesamt“ an:

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***site*** > ***Node*** > **SSM** > **Events** aus.
3. Letztes Ereignis oben in der Tabelle anzeigen.

   Ereignismeldungen sind auch in aufgeführt `/var/local/log/bycast-err.log`.

4. Befolgen Sie die Anweisungen im SMTT-Alarminhalt, um das Problem zu beheben.
5. Wählen Sie die Registerkarte **Konfiguration**, um die Ereignisanzahl zurückzusetzen.
6. Benachrichtigen Sie den Mieter über die Objekte, deren Plattform-Services-Nachrichten nicht geliefert wurden.

7. Weisen Sie den Mandanten an, die fehlgeschlagene Replikation oder Benachrichtigung durch Aktualisieren der Metadaten oder Tags des Objekts erneut auszulösen.

   Der Mieter kann die vorhandenen Werte erneut einreichen, um unerwünschte Änderungen zu vermeiden.

Nachrichten zu Plattform-Services können nicht bereitgestellt werden

Wenn im Ziel ein Problem auftritt, das verhindert, dass Plattformdienste-Meldungen akzeptiert werden, wird der Client-Vorgang auf dem Bucket erfolgreich ausgeführt, die Plattform-Services-Meldung wird jedoch nicht geliefert. Dieser Fehler kann z. B. auftreten, wenn die Anmeldeinformationen auf dem Ziel aktualisiert werden, sodass sich StorageGRID nicht mehr beim Ziel-Service authentifizieren kann.

Wenn Meldungen zu Plattformdiensten aufgrund eines nicht behebbaren Fehlers nicht zugestellt werden können, wird der Legacy-Alarm „Total Events (SMTT)“ im Grid Manager ausgelöst.

Langsamere Performance für Plattform-Service-Anfragen

StorageGRID kann eingehende S3-Anfragen für einen Bucket drosseln, wenn die Rate, mit der die Anforderungen gesendet werden, die Rate übersteigt, mit der der Zielendpunkt die Anforderungen empfangen kann. Eine Drosselung tritt nur auf, wenn ein Rückstand von Anfragen besteht, die auf den Zielendpunkt warten.

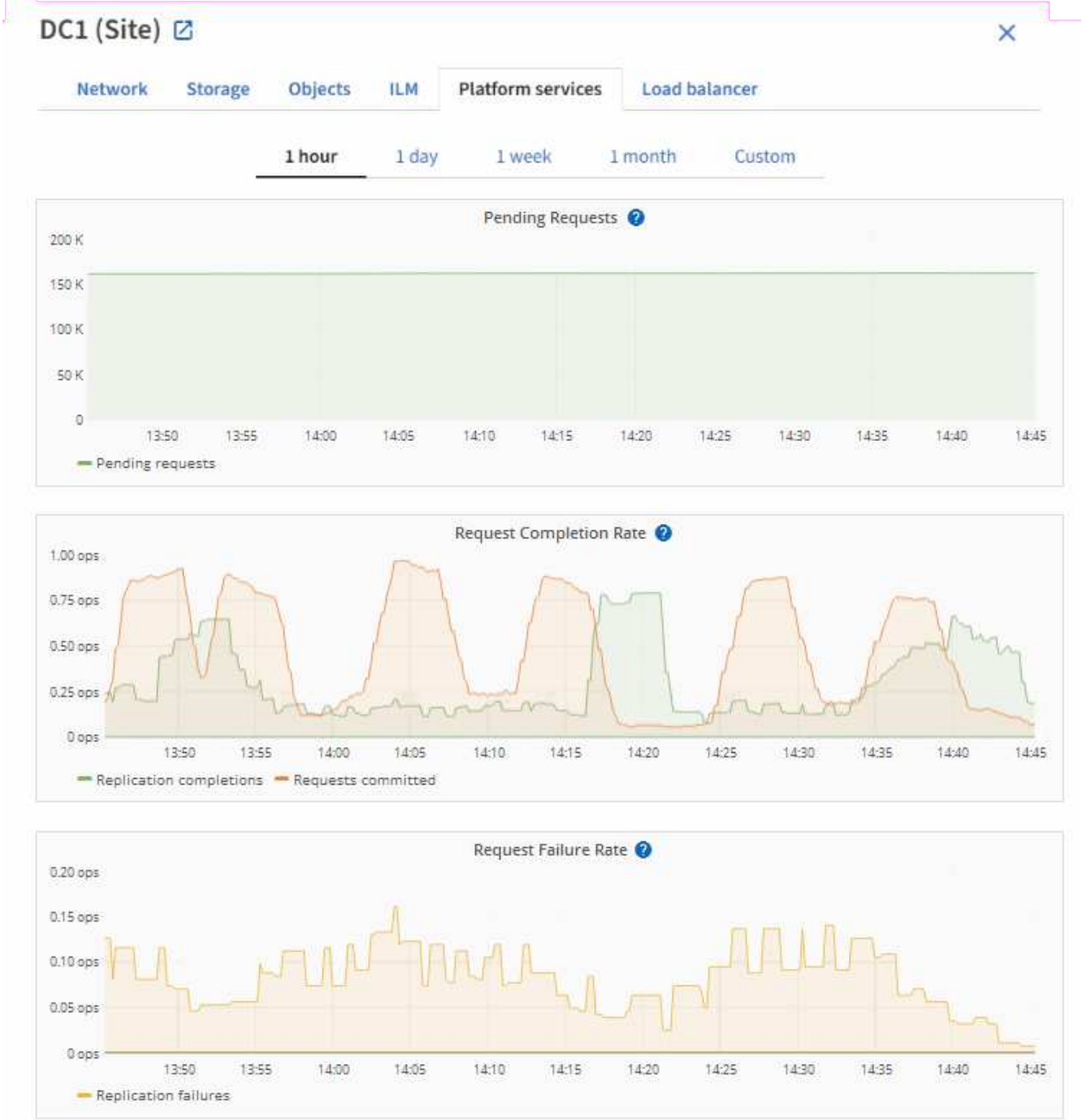
Der einzige sichtbare Effekt besteht darin, dass die eingehenden S3-Anforderungen länger in Anspruch nehmen. Wenn Sie die Performance deutlich schlechter erkennen, sollten Sie die Aufnahmerate reduzieren oder einen Endpunkt mit höherer Kapazität verwenden. Falls der Rückstand von Anforderungen weiterhin wächst, scheitern Client-S3-Vorgänge (wie Z. B. PUT-Anforderungen) letztendlich.

CloudMirror-Anforderungen sind wahrscheinlicher von der Performance des Zielendpunkts betroffen, da diese Anfragen in der Regel mehr Datentransfer beinhalten als Anfragen zur Suchintegration oder Ereignisbenachrichtigung.

Plattformdienstanfragen schlagen fehl

So zeigen Sie die Ausfallrate der Anfrage für Plattformdienste an:

1. Wählen Sie **KNOTEN**.
2. Wählen Sie ***site*** > **Platform Services**.
3. Zeigen Sie das Diagramm Fehlerrate anfordern an.



Plattformdienste – Warnung nicht verfügbar

Die Warnmeldung **Platform Services nicht verfügbar** zeigt an, dass an einem Standort keine Plattformservicevorgänge ausgeführt werden können, da zu wenige Speicherknoten mit dem RSM-Dienst ausgeführt oder verfügbar sind.

Der RSM-Dienst stellt sicher, dass Plattformserviceanforderungen an die jeweiligen Endpunkte gesendet werden.

Um diese Warnmeldung zu beheben, legen Sie fest, welche Speicherknoten am Standort den RSM-Service enthalten. (Der RSM-Service ist auf Speicherknoten vorhanden, die auch den ADC-Service enthalten.) Stellen Sie anschließend sicher, dass ein einfacher Großteil dieser Speicherknoten ausgeführt und verfügbar ist.

Wenn mehr als ein Speicherknoten, der den RSM-Dienst enthält, an einem Standort ausfällt, verlieren Sie alle ausstehenden Plattformserviceanforderungen für diesen Standort.

Zusätzliche Anleitung zur Fehlerbehebung für Endpunkte von Plattformservices

Weitere Informationen finden Sie unter **Verwenden Sie ein Mandantenkonto › Troubleshooting der Endpunkte für Plattformservices**.

Verwandte Informationen

- "Fehlerbehebung für das StorageGRID-System"

Management von S3 Select für Mandantenkonten

Bestimmte S3-Mandanten können S3 Select verwenden, um SelectObjectContent-Anfragen für einzelne Objekte auszulösen.

S3 Select bietet eine effiziente Möglichkeit, große Datenmengen zu durchsuchen, ohne eine Datenbank und zugehörige Ressourcen bereitstellen zu müssen, um die Suche zu ermöglichen. Es senkt auch die Kosten und die Latenz beim Abrufen der Daten.

Was ist S3 Select?

Mit S3 Select können S3-Clients SelectObjectContent-Anfragen verwenden, um nur die von einem Objekt benötigten Daten zu filtern und abzurufen. Die StorageGRID Implementierung von S3 Select enthält eine Untergruppe von S3 Select-Befehlen und -Funktionen.

Überlegungen und Anforderungen bei der Verwendung von S3 Select

Grid-Administrationsanforderungen

Der Grid-Administrator muss Mandanten die Möglichkeit S3 Select erteilen. Wählen Sie **S3-Auswahl zulassen** aus, wann "Erstellen eines Mandanten" Oder "Bearbeiten eines Mandanten".

Anforderungen an das Objektformat

Das Objekt, das Sie abfragen möchten, muss eines der folgenden Formate aufweisen:

- **CSV**. Kann wie ist verwendet oder in GZIP- oder BZIP2-Archiven komprimiert werden.
- **Parkett**. Zusätzliche Anforderungen an Parkett-Objekte:
  - S3 Select unterstützt nur Spaltenkomprimierung mit GZIP oder Snappy. S3 Select unterstützt keine Komprimierung ganzer Objekte für Parkett-Objekte.
  - S3 Select unterstützt keine Parkett-Ausgabe. Sie müssen das Ausgabeformat als CSV oder JSON angeben.
  - Die maximale Größe der nicht komprimierten Zeilengruppe beträgt 512 MB.
  - Sie müssen die im Objektschema angegebenen Datentypen verwenden.
  - Sie können KEINE logischen TYPEN VON INTERVALL, JSON, LISTE, ZEIT oder UUID verwenden.

Anforderungen an Endpunkte

Die SelectObjectContent-Anforderung muss an ein gesendet werden "Endpunkt des StorageGRID-Load-

Balancer".

Die vom Endpunkt verwendeten Admin- und Gateway-Nodes müssen einen der folgenden sein:

- Ein SG100- oder SG1000-Appliance-Node
- Ein auf VMware basierender Software-Node
- Ein Bare-Metal-Knoten, auf dem ein Kernel mit aktivierter cgroup v2 ausgeführt wird

Allgemeine Überlegungen

Abfragen können nicht direkt an Storage-Nodes gesendet werden.

> SelectObjectContent-Anforderungen können die Load Balancer-Performance für alle S3-Clients und alle Mandanten reduzieren. Aktivieren Sie diese Funktion nur bei Bedarf und nur für vertrauenswürdige Mandanten.

Siehe "Anweisungen zur Verwendung von S3 Select".

Um sie anzuzeigen "Grafana-Diagramme" Für S3 Wählen Sie im Grid Manager Operationen über die Zeit aus, wählen Sie im Grid Manager * SUPPORT* > **Tools** > **Metriken**.

Client-Verbindungen konfigurieren

Konfigurieren Sie S3- und Swift-Client-Verbindungen: Übersicht

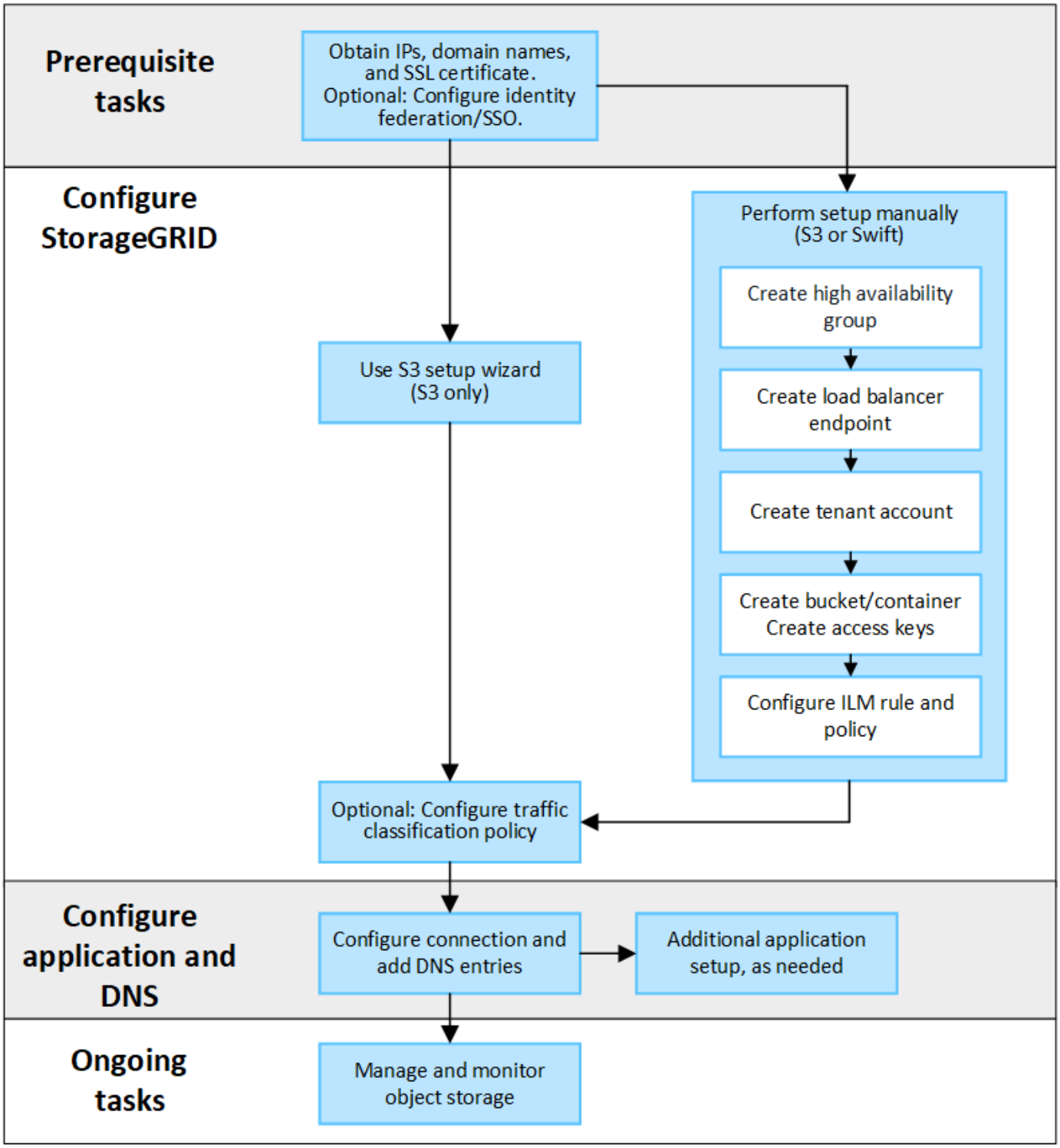
Als Grid-Administrator managen Sie die Konfigurationsoptionen, die steuern, wie sich S3 und Swift Client-Applikationen mit dem StorageGRID System verbinden, um Daten zu speichern und abzurufen.

> Die Unterstützung für Swift-Client-Anwendungen wurde veraltet und wird in einer zukünftigen Version entfernt.

Konfigurationsworkflow

Wie im Workflow-Diagramm dargestellt, gibt es vier primäre Schritte für die Verbindung von StorageGRID mit einer beliebigen S3- oder Swift-Applikation:

1. Führen Sie erforderliche Aufgaben in StorageGRID aus, je nachdem, wie die Clientanwendung eine Verbindung zu StorageGRID herstellt.
2. Verwenden Sie StorageGRID, um die Werte abzurufen, die die Anwendung für die Verbindung mit dem Grid benötigt. Sie können entweder den S3-Einrichtungsassistenten verwenden oder jede StorageGRID-Einheit manuell konfigurieren.
3. Verwenden Sie die S3- oder Swift-Applikation, um die Verbindung zu StorageGRID abzuschließen. Erstellen Sie DNS-Einträge, um IP-Adressen mit beliebigen Domänennamen zu verknüpfen, die Sie verwenden möchten.
4. Laufende Aufgaben in der Applikation und in StorageGRID werden durchgeführt, um Objekt-Storage über einen längeren Zeitraum zu managen und zu überwachen.



Informationen, die zum Anhängen von StorageGRID an eine Client-Applikation erforderlich sind

Bevor Sie StorageGRID an eine S3- oder Swift-Client-Applikation anhängen können, müssen Sie die Konfigurationsschritte in StorageGRID ausführen und einen bestimmten Wert erhalten.

Welche Werte brauche ich?

Die folgende Tabelle zeigt die Werte, die Sie in StorageGRID konfigurieren müssen und wo diese Werte von der S3- oder Swift-Anwendung und dem DNS-Server verwendet werden.

Wert	Wobei der Wert konfiguriert ist	Wo Wert verwendet wird
Virtuelle IP-Adressen (VIP)	StorageGRID > HA-Gruppe	DNS-Eintrag
Port	StorageGRID > Endpunkt des Load Balancer	Client-Anwendung
SSL-Zertifikat	StorageGRID > Endpunkt des Load Balancer	Client-Anwendung
Servername (FQDN)	StorageGRID > Endpunkt des Load Balancer	• Client-Anwendung • DNS-Eintrag
S3 Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel	StorageGRID > Mandant und Bucket	Client-Anwendung
Bucket/Container-Name	StorageGRID > Mandant und Bucket	Client-Anwendung

Wie erhalte ich diese Werte?

Je nach Ihren Anforderungen können Sie eine der folgenden Möglichkeiten nutzen, um die benötigten Informationen zu erhalten:

- **Verwenden Sie die "S3-Einrichtungsassistent"**. Der S3-Einrichtungsassistent unterstützt Sie beim schnellen Konfigurieren der erforderlichen Werte in StorageGRID und gibt eine oder zwei Dateien aus, die Sie bei der Konfiguration der S3-Anwendung verwenden können. Der Assistent führt Sie durch die erforderlichen Schritte und stellt sicher, dass Ihre Einstellungen den StorageGRID Best Practices entsprechen.

  Wenn Sie eine S3-Applikation konfigurieren, wird die Verwendung des S3-Setup-Assistenten von empfohlen, es sei denn, Sie verfügen über besondere Anforderungen oder Ihre Implementierung erfordert eine umfangreiche Anpassung.

- **Verwenden Sie die "FabricPool Setup-Assistent"**. Ähnlich wie der S3-Einrichtungsassistent unterstützt Sie der FabricPool-Einrichtungsassistent bei der schnellen Konfiguration der erforderlichen Werte und gibt eine Datei aus, die Sie bei der Konfiguration eines FabricPool-Cloud-Tiers in ONTAP verwenden können.

  Wenn Sie StorageGRID als Objekt-Storage-System für eine FabricPool Cloud-Tier nutzen möchten, empfiehlt sich die Verwendung des FabricPool Setup-Assistenten, es sei denn, Sie haben besondere Anforderungen oder Ihre Implementierung erfordert erhebliche Anpassungen.

- **Elemente manuell konfigurieren**. Wenn Sie eine Verbindung zu einer Swift-Anwendung herstellen (oder eine Verbindung zu einer S3-Anwendung herstellen und den S3-Einrichtungsassistenten nicht verwenden möchten), können Sie die erforderlichen Werte abrufen, indem Sie die Konfiguration manuell durchführen. Führen Sie hierzu folgende Schritte aus:

  a. Konfigurieren Sie die HA-Gruppe (High Availability, Hochverfügbarkeit), die Sie für die S3- oder Swift-Applikation verwenden möchten. Siehe "Konfigurieren Sie Hochverfügbarkeitsgruppen".

b. Erstellen Sie den Load Balancer-Endpunkt, den die S3- oder Swift-Applikation verwenden wird. Siehe "Konfigurieren von Load Balancer-Endpunkten".

c. Erstellen Sie das Mandantenkonto, das die S3- oder Swift-Applikation verwenden wird. Siehe "Erstellen Sie ein Mandantenkonto".

d. Melden Sie sich für einen S3-Mandanten beim Mandantenkonto an und generieren Sie für jeden Benutzer, der auf die Applikation zugreift, eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel. Siehe "Erstellen Sie Ihre eigenen Zugriffsschlüssel".

e. Erstellen Sie einen oder mehrere S3-Buckets oder Swift-Container im Mandantenkonto. Informationen zu S3 finden Sie unter "S3-Bucket erstellen". Verwenden Sie für Swift die "Container-Anforderung SETZEN".

f. Um Anweisungen zur Platzierung von Objekten, die zu dem neuen Mandanten oder Bucket/Container gehören, hinzuzufügen, erstellen Sie eine neue ILM-Regel und aktivieren Sie zur Verwendung dieser Regel eine neue ILM-Richtlinie. Siehe "ILM-Regel erstellen" Und "ILM-Richtlinie erstellen".

Verwenden Sie den S3-Einrichtungsassistenten

Überlegungen und Anforderungen im S3-Setup-Assistenten

Sie können mit dem S3-Einrichtungsassistenten StorageGRID als Objekt-Storage-System für eine S3-Applikation konfigurieren.

Wann der S3-Einrichtungsassistent verwendet werden soll

Der S3-Einrichtungsassistent führt Sie durch jeden Schritt bei der Konfiguration von StorageGRID für die Verwendung mit einer S3-Applikation. Im Rahmen der Ausführung des Assistenten laden Sie Dateien herunter, mit denen Sie Werte in die S3-Anwendung eingeben können. Mit dem Assistenten konfigurieren Sie Ihr System schneller und stellen sicher, dass Ihre Einstellungen den StorageGRID Best Practices entsprechen.

Wenn Sie über die Berechtigung für den Root-Zugriff verfügen, können Sie den S3-Einrichtungsassistenten abschließen, wenn Sie den StorageGRID-Grid-Manager verwenden. Sie können aber auch jederzeit auf den Assistenten zugreifen und ihn abschließen. Je nach Ihren Anforderungen können Sie auch einige oder alle erforderlichen Elemente manuell konfigurieren und dann mithilfe des Assistenten die Werte zusammenstellen, die eine S3-Anwendung benötigt.

Bevor Sie den Assistenten verwenden

Vergewissern Sie sich vor der Verwendung des Assistenten, dass Sie diese Voraussetzungen erfüllt haben.

Beziehen Sie IP-Adressen, und richten Sie VLAN-Schnittstellen ein

Wenn Sie eine HA-Gruppe (High Availability, Hochverfügbarkeit) konfigurieren, wissen Sie, mit welchen Nodes die S3-Applikation eine Verbindung herstellen und welches StorageGRID-Netzwerk verwendet wird. Sie wissen auch, welche Werte für das Subnetz CIDR, die Gateway-IP-Adresse und die virtuelle IP (VIP)-Adresse eingegeben werden sollen.

Wenn Sie planen, einen virtuellen LAN zur Trennung des Datenverkehrs von der S3-Anwendung zu verwenden, haben Sie die VLAN-Schnittstelle bereits konfiguriert. Siehe "Konfigurieren Sie die VLAN-Schnittstellen".

Konfigurieren Sie Identity Federation und SSO

Wenn Sie planen, Identity Federation oder Single Sign-On (SSO) für Ihr StorageGRID-System zu verwenden,

haben Sie diese Funktionen aktiviert. Sie wissen auch, welche föderierte Gruppe Root-Zugriff für das Mandantenkonto haben soll, das die S3-Anwendung verwenden wird. Siehe "Verwenden Sie den Identitätsverbund" Und "Konfigurieren Sie Single Sign-On".

Abrufen und Konfigurieren von Domänennamen

Sie wissen, welcher vollständig qualifizierte Domänenname (FQDN) für StorageGRID verwendet werden soll. DNS-Einträge (Domain Name Server) weisen diesen FQDN den virtuellen IP-Adressen (VIP) der HA-Gruppe zu, die Sie mit dem Assistenten erstellen.

Wenn Sie Anforderungen im virtuellen Hosted-Stil von S3 verwenden möchten, sollten Sie dies beachten "Domänennamen des S3-Endpunkts wurden konfiguriert". Die Verwendung von Anforderungen im virtuellen Hosted-Stil wird empfohlen.

Anforderungen für Load Balancer und Sicherheitszertifikate prüfen

Wenn Sie den StorageGRID Load Balancer einsetzen möchten, haben Sie die allgemeinen Überlegungen zum Lastausgleich besprochen. Sie verfügen über die hochgeladenen Zertifikate oder die Werte, die Sie zum Generieren eines Zertifikats benötigen.

Wenn Sie einen externen (Drittanbieter-)Load Balancer-Endpunkt verwenden möchten, verfügen Sie über den vollständig qualifizierten Domänennamen (FQDN), den Port und das Zertifikat für diesen Load Balancer.

Konfigurieren Sie alle Verbindungen des Grid-Verbunds

Wenn Sie es dem S3-Mandanten erlauben möchten, Kontodaten zu klonen und Bucket-Objekte mithilfe einer Grid-Federation-Verbindung in ein anderes Grid zu replizieren, bestätigen Sie Folgendes, bevor Sie den Assistenten starten:

- Das ist schon "Grid Federation-Verbindung konfiguriert".
- Der Status der Verbindung lautet **connected**.
- Sie haben Root-Zugriffsberechtigung.

Rufen Sie den S3-Setup-Assistenten auf und vervollständigen Sie sie

Sie können den S3-Einrichtungsassistenten verwenden, um StorageGRID für die Verwendung mit einer S3-Applikation zu konfigurieren. Der Einrichtungsassistent bietet die Werte, die die Anwendung benötigt, um auf einen StorageGRID-Bucket zuzugreifen und Objekte zu speichern.

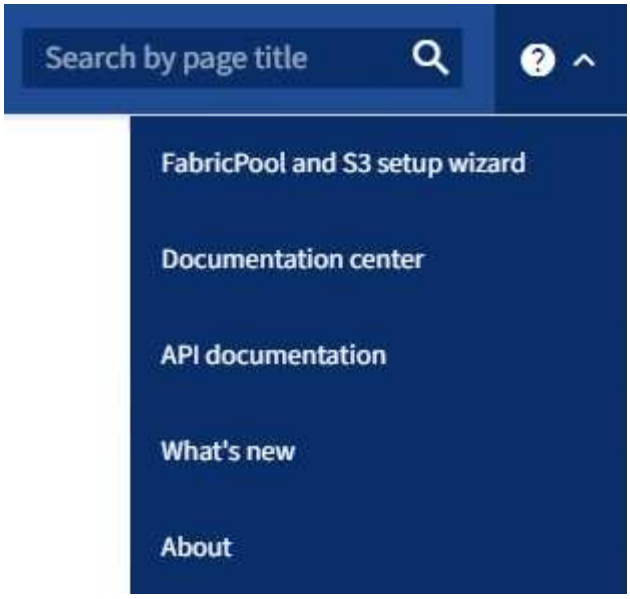
Bevor Sie beginnen

- Sie haben die "Root-Zugriffsberechtigung".
- Sie haben die geprüft "Überlegungen und Anforderungen" Zur Verwendung des Assistenten.

Greifen Sie auf den Assistenten zu

Schritte

1. Melden Sie sich mit einem bei Grid Manager an "Unterstützter Webbrowser".
2. Wenn das Banner **FabricPool and S3 Setup Wizard** auf dem Dashboard angezeigt wird, wählen Sie den Link im Banner aus. Wenn das Banner nicht mehr angezeigt wird, wählen Sie in der Kopfzeile des Grid-Managers das Hilfesymbol aus und wählen Sie **FabricPool und S3-Setup-Assistent** aus.



3. Wählen Sie im Abschnitt S3-Anwendung der Seite FabricPool und S3-Setup-Assistent **Jetzt konfigurieren** aus.

Schritt 1 von 6: Konfigurieren Sie die HA-Gruppe

Eine HA-Gruppe ist eine Sammlung von Nodes, die jeweils den StorageGRID Lastausgleich enthalten. Eine HA-Gruppe kann Gateway-Nodes, Admin-Nodes oder beides enthalten.

Sie können eine HA-Gruppe verwenden, um die S3 Datenverbindungen verfügbar zu halten. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle den Workload mit geringen Auswirkungen auf den S3-Betrieb managen.

Weitere Informationen zu dieser Aufgabe finden Sie unter "Management von Hochverfügbarkeitsgruppen".

Schritte

1. Wenn Sie einen externen Load Balancer verwenden möchten, müssen Sie keine HA-Gruppe erstellen. Wählen Sie **diesen Schritt überspringen** und gehen Sie zu Schritt 2 von 6: Konfigurieren Sie den Load Balancer-Endpunkt.
2. Um den StorageGRID Load Balancer zu verwenden, können Sie eine neue HA-Gruppe erstellen oder eine vorhandene HA-Gruppe verwenden.

Erstellen Sie eine HA-Gruppe

a. Um eine neue HA-Gruppe zu erstellen, wählen Sie **HA-Gruppe erstellen**.

b. Füllen Sie für den Schritt **Enter Details** die folgenden Felder aus.

Feld	Beschreibung
Name DER HA-Gruppe	Ein eindeutiger Anzeigename für diese HA-Gruppe.
Beschreibung (optional)	Die Beschreibung dieser HA-Gruppe.

c. Wählen Sie im Schritt **Schnittstellen hinzufügen** die Knotenschnittstellen aus, die Sie in dieser HA-Gruppe verwenden möchten.

Verwenden Sie die Spaltenüberschriften, um die Zeilen zu sortieren, oder geben Sie einen Suchbegriff ein, um Schnittstellen schneller zu finden.

Sie können einen oder mehrere Nodes auswählen, aber Sie können nur eine Schnittstelle für jeden Node auswählen.

d. Bestimmen Sie für den Schritt **priorisiere Schnittstellen** die primäre Schnittstelle und alle Backup-Schnittstellen für diese HA-Gruppe.

Ziehen Sie Zeilen, um die Werte in der Spalte **Priority order** zu ändern.

Die erste Schnittstelle in der Liste ist die primäre Schnittstelle. Die primäre Schnittstelle ist die aktive Schnittstelle, sofern kein Fehler auftritt.

Wenn die HA-Gruppe mehr als eine Schnittstelle enthält und die aktive Schnittstelle ausfällt, werden die virtuellen IP-Adressen (VIP-Adressen) zur ersten Backup-Schnittstelle in der Prioritätsreihenfolge verschoben. Wenn diese Schnittstelle ausfällt, wechseln die VIP-Adressen zur nächsten Backup-Schnittstelle usw. Wenn Fehler behoben sind, werden die VIP-Adressen auf die Schnittstelle mit der höchsten Priorität zurückverschoben.

e. Füllen Sie für den Schritt **IP-Adressen eingeben** die folgenden Felder aus.

Feld	Beschreibung
Subnetz-CIDR	Die Adresse des VIP-Subnetzes in CIDR-Notation — eine IPv4-Adresse gefolgt von einem Schrägstrich und der Subnetz-Länge (0-32). Die Netzwerkadresse darf keine Host-Bits festgelegt haben. Beispiel: `192.16.0.0/22`.
Gateway-IP-Adresse (optional)	Wenn sich die S3-IP-Adressen für den Zugriff auf StorageGRID nicht im selben Subnetz wie die StorageGRID-VIP-Adressen befinden, geben Sie die lokale StorageGRID-VIP-Gateway-IP-Adresse ein. Die IP-Adresse des lokalen Gateways muss sich im VIP-Subnetz befinden.

Feld	Beschreibung
Virtuelle IP-Adresse	Geben Sie mindestens eine und nicht mehr als zehn VIP-Adressen für die aktive Schnittstelle in der HA-Gruppe ein. Alle VIP-Adressen müssen sich innerhalb des VIP-Subnetzes befinden. Mindestens eine Adresse muss IPv4 sein. Optional können Sie weitere IPv4- und IPv6-Adressen angeben.

f. Wählen Sie **HA-Gruppe erstellen** und dann **Fertig stellen**, um zum S3-Setup-Assistenten zurückzukehren.

g. Wählen Sie **Weiter**, um zum Schritt Load Balancer zu gelangen.

Verwenden Sie die vorhandene HA-Gruppe

a. Um eine vorhandene HA-Gruppe zu verwenden, wählen Sie den Namen der HA-Gruppe aus **Select an HA Group** aus.

b. Wählen Sie **Weiter**, um zum Schritt Load Balancer zu gelangen.

Schritt 2 von 6: Konfigurieren Sie den Load Balancer-Endpunkt

StorageGRID verwendet einen Load Balancer für das Management des Workloads aus Client-Applikationen. Load Balancing maximiert Geschwindigkeit und Verbindungskapazität über mehrere Storage Nodes hinweg.

Sie können den StorageGRID Load Balancer-Dienst verwenden, der auf allen Gateway- und Admin-Nodes vorhanden ist, oder eine Verbindung zu einem externen Load Balancer (Drittanbieter) herstellen. Die Verwendung des StorageGRID Load Balancer wird empfohlen.

Weitere Informationen zu dieser Aufgabe finden Sie unter "Überlegungen zum Lastausgleich".

Um den StorageGRID Load Balancer Service zu verwenden, wählen Sie die Registerkarte **StorageGRID Load Balancer** aus und erstellen oder wählen Sie dann den gewünschten Load Balancer-Endpunkt aus. Um einen externen Load Balancer zu verwenden, wählen Sie die Registerkarte **External Load Balancer** und geben Sie Details zum System an, das Sie bereits konfiguriert haben.

Endpunkt erstellen

Schritte

1. Um einen Load Balancer-Endpunkt zu erstellen, wählen Sie **Endpunkt erstellen**.
2. Füllen Sie für den Schritt **Enter Endpoint Details** die folgenden Felder aus.

Feld	Beschreibung
Name	Ein beschreibender Name für den Endpunkt.
Port	Der StorageGRID-Port, den Sie für den Lastausgleich verwenden möchten. Dieses Feld ist für den ersten erstellten Endpunkt standardmäßig auf 10433 eingestellt, Sie können jedoch jeden nicht verwendeten externen Port eingeben. Wenn Sie 80 oder 443 eingeben, wird der Endpunkt nur auf Gateway-Nodes konfiguriert, da diese Ports auf Admin-Nodes reserviert sind. **Hinweis:** von anderen Netzdiensten verwendete Ports sind nicht erlaubt. Siehe"Referenz für Netzwerk-Ports".
Client-Typ	Muss **S3** sein.
Netzwerkprotokoll	Wählen Sie **HTTPS**. **Hinweis**: Die Kommunikation mit StorageGRID ohne TLS-Verschlüsselung wird unterstützt, aber nicht empfohlen.

3. Geben Sie für den Schritt **Bindungsmodus auswählen** den Bindungsmodus an. Der Bindungsmodus steuert, wie auf den Endpunkt zugegriffen wird—Verwendung einer beliebigen IP-Adresse oder Verwendung bestimmter IP-Adressen und Netzwerkschnittstellen.

Option	Beschreibung
Global (Standard)	Clients können über die IP-Adresse eines beliebigen Gateway-Node oder Admin-Node, die virtuelle IP-Adresse (VIP) einer beliebigen HA-Gruppe in einem beliebigen Netzwerk oder einen entsprechenden FQDN auf den Endpunkt zugreifen. Verwenden Sie die **Global**-Einstellung (Standard), es sei denn, Sie müssen die Zugriffsmöglichkeiten dieses Endpunkts einschränken.
Virtuelle IPs von HA-Gruppen	Clients müssen eine virtuelle IP-Adresse (oder einen entsprechenden FQDN) einer HA-Gruppe verwenden, um auf diesen Endpunkt zuzugreifen. Endpunkte mit diesem Bindungsmodus können alle dieselbe Portnummer verwenden, solange sich die für die Endpunkte ausgewählten HA-Gruppen nicht überlappen.

Option	Beschreibung
Node-Schnittstellen	Clients müssen die IP-Adressen (oder entsprechende FQDNs) der ausgewählten Knotenschnittstellen verwenden, um auf diesen Endpunkt zuzugreifen.
Node-Typ	Basierend auf dem von Ihnen ausgewählten Knotentyp müssen Clients entweder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Admin-Knotens oder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Gateway-Knotens verwenden, um auf diesen Endpunkt zuzugreifen.

4. Wählen Sie für den Schritt Tenant Access eine der folgenden Optionen aus:

Feld	Beschreibung
Alle Mandanten zulassen (Standard)	Alle Mandantenkonten können diesen Endpunkt verwenden, um auf ihre Buckets zuzugreifen.
Ausgewählte Mandanten zulassen	Nur die ausgewählten Mandantenkonten können diesen Endpunkt für den Zugriff auf ihre Buckets verwenden.
Ausgewählte Mandanten blockieren	Die ausgewählten Mandantenkonten können diesen Endpunkt nicht für den Zugriff auf ihre Buckets verwenden. Dieser Endpunkt kann von allen anderen Mandanten verwendet werden.

5. Wählen Sie für den Schritt **Zertifikat anhängen** eine der folgenden Optionen aus:

Feld	Beschreibung
Zertifikat hochladen (empfohlen)	Verwenden Sie diese Option, um ein CA-signiertes Serverzertifikat, einen privaten Zertifikatschlüssel und ein optionales CA-Paket hochzuladen.
Zertifikat wird generiert	Verwenden Sie diese Option, um ein selbstsigniertes Zertifikat zu generieren. Siehe "Konfigurieren von Load Balancer-Endpunkten" Für Details, was eingegeben werden soll.
StorageGRID S3 und Swift-Zertifikat verwenden	Verwenden Sie diese Option nur, wenn Sie bereits eine benutzerdefinierte Version des globalen StorageGRID-Zertifikats hochgeladen oder generiert haben. Siehe "Konfigurieren von S3- und Swift-API-Zertifikaten" Entsprechende Details.

6. Wählen Sie **Finish**, um zum S3-Setup-Assistenten zurückzukehren.
7. Wählen Sie **Weiter**, um zum Mandanten- und Bucket-Schritt zu gelangen.

Änderungen an einem Endpunktzertifikat können bis zu 15 Minuten dauern, bis sie auf alle Knoten angewendet werden können.

Verwenden Sie den vorhandenen Endpunkt des Load Balancer

Schritte

1. Um einen vorhandenen Endpunkt zu verwenden, wählen Sie seinen Namen aus dem **Select a Load Balancer Endpunkt** aus.
2. Wählen Sie **Weiter**, um zum Mandanten- und Bucket-Schritt zu gelangen.

Externen Load Balancer verwenden

Schritte

1. Um einen externen Load Balancer zu verwenden, füllen Sie die folgenden Felder aus.

Feld	Beschreibung
FQDN	Der vollständig qualifizierte Domänenname (FQDN) des externen Load Balancer.
Port	Die Portnummer, die die S3-Anwendung für die Verbindung mit dem externen Load Balancer verwendet.
Zertifikat	Kopieren Sie das Serverzertifikat für den externen Load Balancer und fügen Sie es in dieses Feld ein.

2. Wählen Sie **Weiter**, um zum Mandanten- und Bucket-Schritt zu gelangen.

Schritt 3 von 6: Erstellen Sie einen Mandanten und Bucket

Ein Mandant ist eine Einheit, die S3-Applikationen zum Speichern und Abrufen von Objekten in StorageGRID verwenden kann. Jeder Mandant verfügt über eigene Benutzer, Zugriffsschlüssel, Buckets, Objekte und bestimmte Funktionen. Sie müssen den Mandanten erstellen, bevor Sie den Bucket erstellen können, den die S3-Applikation zum Speichern ihrer Objekte verwendet.

Ein Bucket ist ein Container, mit dem die Objekte und Objektmetadaten eines Mandanten gespeichert werden können. Obwohl einige Mandanten möglicherweise über viele Buckets verfügen, hilft Ihnen der Assistent dabei, auf schnelle und einfache Weise einen Mandanten und einen Bucket zu erstellen. Sie können den Tenant Manager später verwenden, um zusätzliche Buckets hinzuzufügen, die Sie benötigen.

Sie können einen neuen Mandanten für diese S3-Anwendung erstellen. Optional können Sie auch einen Bucket für den neuen Mandanten erstellen. Schließlich können Sie zulassen, dass der Assistent die S3-Zugriffsschlüssel für den Root-Benutzer des Mandanten erstellt.

Weitere Informationen zu dieser Aufgabe finden Sie unter "Erstellen eines Mandantenkontos" Und"S3-Bucket erstellen".

Schritte

1. Wählen Sie **Create Tenant**.
2. Geben Sie für die Schritte zum Eingeben von Details die folgenden Informationen ein.

Feld	Beschreibung
Name	Ein Name für das Mandantenkonto. Mandantennamen müssen nicht eindeutig sein. Wenn das Mandantenkonto erstellt wird, erhält es eine eindeutige, numerische Konto-ID.
Beschreibung (optional)	Eine Beschreibung zur Identifizierung des Mandanten.
Client-Typ	Der Typ des Clientprotokolls, das von diesem Mandanten verwendet wird. Für den S3-Setup-Assistenten ist **S3** ausgewählt und das Feld deaktiviert.
Storage-Kontingent (optional)	Wenn Sie möchten, dass dieser Mandant über ein Speicherkontingent, einen numerischen Wert für das Kontingent und die Einheiten verfügt.

3. Wählen Sie **Weiter**.
4. Wählen Sie optional alle Berechtigungen aus, die dieser Tenant haben soll.

> Einige dieser Berechtigungen haben zusätzliche Anforderungen. Für Details wählen Sie das Hilfesymbol für jede Berechtigung aus.

Berechtigung	Wenn ausgewählt…
Unterstützung von Plattform-Services	Der Mandant kann S3-Plattformservices wie CloudMirror verwenden. Siehe "Management von Plattform-Services für S3-Mandantenkonten".
Eigene Identitätsquelle verwenden	Der Mandant kann seine eigene Identitätsquelle für verbundene Gruppen und Benutzer konfigurieren und verwalten. Diese Option ist deaktiviert, wenn Sie dies haben "SSO konfiguriert" Für Ihr StorageGRID-System.
S3 Select zulassen	Der Mandant kann S3 SelectObjectContent API-Anforderungen ausgeben, um Objektdaten zu filtern und abzurufen. Siehe "Management von S3 Select für Mandantenkonten". **Wichtig**: SelectObjectContent Requests können die Load Balancer Performance für alle S3 Clients und alle Tenants verringern. Aktivieren Sie diese Funktion nur bei Bedarf und nur für vertrauenswürdige Mandanten.

Berechtigung	Wenn ausgewählt…
Netzverbundverbindung verwenden	Der Mandant kann eine Grid Federation-Verbindung verwenden. Auswahl dieser Option: • Bewirkt, dass dieser Mandant und alle dem Konto hinzugefügten Mandantengruppen und Benutzer aus diesem Raster (das *source Grid*) in das andere Raster der ausgewählten Verbindung (das *Destination Grid*) geklont werden. • Ermöglicht diesem Mandanten, die Grid-übergreifende Replizierung zwischen entsprechenden Buckets in jedem Grid zu konfigurieren. Siehe "Verwalten Sie die zulässigen Mandanten für den Grid-Verbund". **Hinweis**: Sie können nur **Grid Federation connection** verwenden auswählen, wenn Sie einen neuen S3-Mandanten erstellen; Sie können diese Berechtigung nicht für einen vorhandenen Mandanten auswählen.

5. Wenn Sie **Grid Federation connection** verwenden ausgewählt haben, wählen Sie eine der verfügbaren Grid Federation-Verbindungen aus.
6. Definieren Sie den Root-Zugriff für das Mandantenkonto, je nachdem, ob Ihr StorageGRID-System verwendet "Identitätsföderation", "Single Sign On (SSO)"Oder beides.

Option	Tun Sie das
Wenn die Identitätsföderation nicht aktiviert ist	Geben Sie das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.
Wenn die Identitätsföderation aktiviert ist	a. Wählen Sie eine vorhandene Verbundgruppe aus, um Root-Zugriffsberechtigungen für den Mandanten zu erhalten. b. Geben Sie optional das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.
Wenn sowohl Identitätsföderation als auch Single Sign-On (SSO) aktiviert sind	Wählen Sie eine vorhandene Verbundgruppe aus, um Root-Zugriffsberechtigungen für den Mandanten zu erhalten. Keine lokalen Benutzer können sich anmelden.

7. Wenn Sie möchten, dass der Assistent die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel für den Root-Benutzer erstellt, wählen Sie **Root-Benutzer S3-Zugriffsschlüssel automatisch erstellen**.

Wählen Sie diese Option aus, wenn der einzige Benutzer für den Mandanten der Root-Benutzer ist. Wenn andere Benutzer diesen Mandanten verwenden, konfigurieren Sie mit Tenant Manager Schlüssel und Berechtigungen.

8. Wählen Sie **Weiter**.
9. Erstellen Sie für den Schritt „Bucket erstellen“ optional einen Bucket für die Objekte des Mandanten. Andernfalls wählen Sie **Create Tenant without bucket**, um zum zu gelangen Datenschritt herunterladen.

Wenn S3 Object Lock für das Raster aktiviert ist, ist für den in diesem Schritt erstellten Bucket die S3 Object Lock nicht aktiviert. Wenn Sie einen S3 Object Lock Bucket für diese S3-Anwendung verwenden müssen, wählen Sie **Create Tenant without Bucket** aus. Verwenden Sie anschließend Tenant Manager für "Erstellen Sie den Bucket" Stattdessen.

a. Geben Sie den Namen des Buckets ein, den die S3-Applikation verwendet. Beispiel: `S3-bucket`.

   Sie können den Bucket-Namen nach dem Erstellen des Buckets nicht ändern.

b. Wählen Sie die **Region** für diesen Bucket aus.

   Verwenden Sie die Standardregion (US-East-1), es sei denn, Sie möchten ILM zukünftig verwenden, um Objekte basierend auf der Region des Buckets zu filtern.

c. Wählen Sie **enable object Versioning** aus, wenn Sie jede Version jedes Objekts in diesem Bucket speichern möchten.

d. Wählen Sie **Create Tenant and bucket** und gehen Sie zum Download Data Step.

Schritt 4 von 6: Daten herunterladen

Im Schritt zum Herunterladen von Daten können Sie eine oder zwei Dateien herunterladen, um die Details zu dem zu speichern, was Sie gerade konfiguriert haben.

Schritte

1. Wenn Sie **Root-Benutzer S3-Zugriffsschlüssel automatisch erstellen** ausgewählt haben, führen Sie einen oder beide der folgenden Schritte aus:
   - Wählen Sie **Download Access keys**, um einen herunterzuladen `.csv` Datei mit dem Kontonamen des Mandanten, der Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel.
   - Wählen Sie das Symbol Kopieren ( ) Um die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel in die Zwischenablage zu kopieren.
2. Wählen Sie **Konfigurationswerte herunterladen**, um einen herunterzuladen `.txt` Datei mit den Einstellungen für den Load Balancer-Endpunkt, den Mandanten, den Bucket und den Root-Benutzer.
3. Speichern Sie diese Informationen an einem sicheren Ort.

   Schließen Sie diese Seite erst, wenn Sie beide Zugriffsschlüssel kopiert haben. Die Tasten sind nach dem Schließen dieser Seite nicht mehr verfügbar. Speichern Sie diese Informationen an einem sicheren Ort, da sie zum Abrufen von Daten von Ihrem StorageGRID-System verwendet werden können.

4. Wenn Sie dazu aufgefordert werden, aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Schlüssel heruntergeladen oder kopiert haben.
5. Wählen Sie **Weiter**, um zur ILM-Regel und zum Richtlinienschritt zu gelangen.

Schritt 5 von 6: Prüfen Sie die ILM-Regel und die ILM-Richtlinie für S3

Informationen Lifecycle Management-Regeln (ILM) steuern die Platzierung, Dauer und das Aufnahmeverhalten aller Objekte in Ihrem StorageGRID System. Mit der bei StorageGRID enthaltenen ILM-Richtlinie werden zwei replizierte Kopien aller Objekte erstellt. Diese Richtlinie ist gültig, bis Sie eine neue vorgeschlagene Richtlinie erstellen und aktivieren.

Schritte

1. Überprüfen Sie die Informationen auf der Seite.
2. Wenn Sie bestimmte Anweisungen für die Objekte hinzufügen möchten, die zum neuen Mandanten oder Bucket gehören, erstellen Sie eine neue Regel und eine neue Richtlinie. Siehe "ILM-Regel erstellen" Und "ILM-Richtlinie erstellen: Übersicht".
3. Wählen Sie * Ich habe diese Schritte überprüft und verstehe, was ich tun muss*.
4. Aktivieren Sie das Kontrollkästchen, um anzugeben, dass Sie die nächsten Schritte verstehen.
5. Wählen Sie **Weiter**, um zu **Zusammenfassung** zu gelangen.

Schritt 6 von 6: Zusammenfassung überprüfen

Schritte

1. Überprüfen Sie die Zusammenfassung.
2. Notieren Sie sich in den nächsten Schritten die Details, die die zusätzliche Konfiguration beschreiben, die möglicherweise erforderlich ist, bevor Sie eine Verbindung zum S3-Client herstellen. Wenn Sie beispielsweise **als root anmelden** auswählen, gelangen Sie zum Tenant Manager, wo Sie Mandantenbenutzer hinzufügen, zusätzliche Buckets erstellen und Bucket-Einstellungen aktualisieren können.
3. Wählen Sie **Fertig**.
4. Konfigurieren Sie die Anwendung mit der Datei, die Sie von StorageGRID heruntergeladen haben, oder mit den manuell erhaltenen Werten.

Managen von HA-Gruppen

Verwaltung von Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen): Übersicht

Die Netzwerkschnittstellen mehrerer Admin- und Gateway-Nodes können in einer HA-Gruppe (High Availability, Hochverfügbarkeit) gruppieren. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle den Workload verwalten.

Was ist eine HA-Gruppe?

Darüber hinaus können HA-Gruppen (High Availability, Hochverfügbarkeit) für hochverfügbare Datenverbindungen für S3 und Swift Clients verwendet oder hochverfügbare Verbindungen mit dem Grid Manager und dem Mandanten Manager hergestellt werden.

Jede HA-Gruppe bietet Zugriff auf die Shared Services auf den ausgewählten Nodes.

- HA-Gruppen, die Gateway-Nodes, Admin-Nodes oder beide umfassen, bieten hochverfügbare Datenverbindungen für S3- und Swift-Clients.
- HA-Gruppen, die nur Admin-Nodes enthalten, bieten hochverfügbare Verbindungen zum Grid Manager und dem Mandanten-Manager.
- Eine HA-Gruppe, die nur SG100- oder SG1000-Appliances und VMware-basierte Software-Nodes enthält, kann für hochverfügbare Verbindungen bereitstellen "S3-Mandanten, die S3 Select nutzen". HA-Gruppen werden empfohlen, wenn S3 Select verwendet wird, jedoch nicht erforderlich.

Wie erstellen Sie eine HA-Gruppe?

1. Sie wählen eine Netzwerkschnittstelle für einen oder mehrere Admin-Nodes oder Gateway-Knoten aus.

Sie können eine Grid Network (eth0)-Schnittstelle, eine eth2-Schnittstelle (Client Network), eine VLAN-Schnittstelle oder eine Access-Interface verwenden, die Sie dem Node hinzugefügt haben.

> Sie können einer HA-Gruppe keine Schnittstelle hinzufügen, wenn ihr eine DHCP-zugewiesene IP-Adresse zugewiesen ist.

2. Sie geben an, dass die primäre Schnittstelle sein soll. Die primäre Schnittstelle ist die aktive Schnittstelle, sofern kein Fehler auftritt.
3. Sie bestimmen die Prioritätsreihenfolge für alle Backup-Schnittstellen.
4. Sie weisen der Gruppe eine bis 10 virtuelle IP-Adressen (VIP) zu. Client-Anwendungen können eine dieser VIP-Adressen verwenden, um eine Verbindung zu StorageGRID herzustellen.

Anweisungen hierzu finden Sie unter "Konfigurieren Sie Hochverfügbarkeitsgruppen".

Was ist die aktive Schnittstelle?

Im normalen Betrieb werden alle VIP-Adressen für die HA-Gruppe der primären Schnittstelle hinzugefügt, die die erste Schnittstelle in der Prioritätsreihenfolge ist. Solange die primäre Schnittstelle verfügbar bleibt, wird sie verwendet, wenn sich Clients mit einer beliebigen VIP-Adresse für die Gruppe verbinden. Das heißt, während des normalen Betriebs ist die primäre Schnittstelle die Schnittstelle „`Active`“ für die Gruppe.

Ebenso fungieren alle Schnittstellen mit niedriger Priorität für die HA-Gruppe im normalen Betrieb als „`Backup`“-Schnittstellen. Diese Backup-Schnittstellen werden nur dann verwendet, wenn die primäre (derzeit aktive) Schnittstelle nicht mehr verfügbar ist.

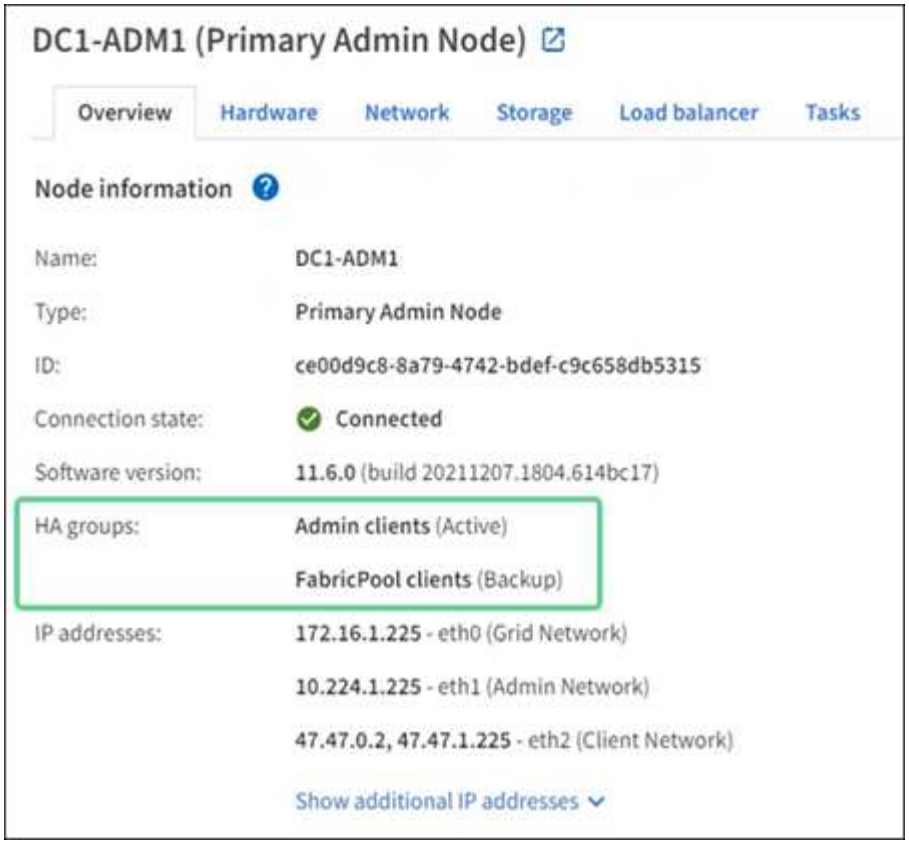
Anzeigen des aktuellen HA-Gruppen-Status eines Node

Um zu ermitteln, ob ein Node einer HA-Gruppe zugewiesen ist und seinen aktuellen Status ermittelt, wählen Sie **NODES** > ***Node*** aus.

Wenn die Registerkarte **Übersicht** einen Eintrag für **HA-Gruppen** enthält, wird der Knoten den aufgeführten HA-Gruppen zugewiesen. Der Wert nach dem Gruppennamen ist der aktuelle Status des Node in der HA-Gruppe:

- **Aktiv**: Die HA-Gruppe wird derzeit auf diesem Knoten gehostet.
- **Backup**: Die HA-Gruppe benutzt derzeit nicht diesen Knoten; dies ist ein Backup Interface.
- **Angehalten**: Die HA-Gruppe kann nicht auf diesem Knoten gehostet werden, da der Dienst hohe Verfügbarkeit (keepalibed) manuell angehalten wurde.
- **Fault**: Die HA-Gruppe kann nicht auf diesem Knoten gehostet werden, weil einer oder mehrere der folgenden:
  - Der Lastverteilungsservice (nginx-gw) wird auf dem Knoten nicht ausgeführt.
  - Die eth0- oder VIP-Schnittstelle des Node ist nicht aktiv.
  - Der Node ist ausgefallen.

In diesem Beispiel wurde der primäre Admin-Node zwei HA-Gruppen hinzugefügt. Dieser Knoten ist derzeit die aktive Schnittstelle für die Gruppe Admin-Clients und eine Sicherungsschnittstelle für die Gruppe FabricPool-Clients.



Was geschieht, wenn die aktive Schnittstelle ausfällt?

Die Schnittstelle, die derzeit die VIP-Adressen hostet, ist die aktive Schnittstelle. Wenn die HA-Gruppe mehrere Schnittstellen umfasst und die aktive Schnittstelle ausfällt, verschieben sich die VIP-Adressen auf die erste verfügbare Backup-Schnittstelle in der Prioritätsreihenfolge. Wenn diese Schnittstelle ausfällt, wechseln die VIP-Adressen zur nächsten verfügbaren Backup-Schnittstelle usw.

Ein Failover kann aus einem der folgenden Gründe ausgelöst werden:

- Der Node, auf dem die Schnittstelle konfiguriert ist, schaltet sich aus.
- Der Node, auf dem die Schnittstelle konfiguriert ist, verliert mindestens 2 Minuten lang die Verbindung zu allen anderen Nodes.
- Die aktive Schnittstelle ausfällt.
- Der Lastverteiler-Dienst wird angehalten.
- Der High Availability Service stoppt.

> Der Failover wird möglicherweise nicht durch Netzwerkausfälle außerhalb des Node ausgelöst, der die aktive Schnittstelle hostet. Ebenso wird Failover nicht von den Diensten für den Grid Manager oder den Tenant Manager ausgelöst.

Der Failover-Prozess dauert in der Regel nur wenige Sekunden und ist schnell genug, dass Client-Applikationen nur geringe Auswirkungen haben und sich auf normale Wiederholungsmuster verlassen können, um den Betrieb fortzusetzen.

Wenn ein Fehler behoben ist und eine Schnittstelle mit höherer Priorität wieder verfügbar wird, werden die VIP-Adressen automatisch auf die verfügbare Schnittstelle mit der höchsten Priorität verschoben.

Wie werden HA-Gruppen verwendet?

Es können HA-Gruppen (High Availability, Hochverfügbarkeit) verwendet werden, um hochverfügbare Verbindungen zu StorageGRID für Objektdaten und zur Verwendung durch den Administrator zur Verfügung zu stellen.

- Eine HA-Gruppe kann hochverfügbare administrative Verbindungen mit dem Grid Manager oder dem Mandanten Manager bereitstellen.
- Eine HA-Gruppe kann hochverfügbare Datenverbindungen für S3 und Swift Clients bieten.
- Eine HA-Gruppe, die nur eine Schnittstelle enthält, ermöglicht es Ihnen, viele VIP-Adressen bereitzustellen und explizit IPv6-Adressen festzulegen.

Eine HA-Gruppe kann nur Hochverfügbarkeit bieten, wenn alle Nodes in der Gruppe dieselben Services bereitstellen. Wenn Sie eine HA-Gruppe erstellen, fügen Sie Schnittstellen von den Typen von Nodes hinzu, die die erforderlichen Services bereitstellen.

- **Admin Nodes**: Schließen Sie den Load Balancer Service ein und ermöglichen Sie den Zugriff auf den Grid Manager oder den Tenant Manager.
- **Gateway Nodes**: Fügen Sie den Load Balancer Service ein.

Zweck der HA-Gruppe	Fügen Sie diesem Typ Nodes der HA-Gruppe hinzu
Zugriff auf Grid Manager	• Primärer Admin-Node (**Primär**) • Nicht primäre Admin-Nodes **Hinweis:** der primäre Admin-Knoten muss die primäre Schnittstelle sein. Einige Wartungsvorgänge können nur vom primären Admin-Node ausgeführt werden.
Zugriff nur auf Tenant Manager	• Primäre oder nicht primäre Admin-Nodes
S3- oder Swift-Client-Zugriff – Load Balancer Service	• Admin-Nodes • Gateway-Nodes
S3-Client-Zugriff für "S3 Select"	• SG100- oder SG1000-Appliances • VMware-basierte Software-Nodes **Hinweis**: HA-Gruppen werden bei der Verwendung von S3 Select empfohlen, aber nicht erforderlich.

Einschränkungen bei der Verwendung von HA-Gruppen mit Grid Manager oder Tenant Manager

Wenn ein Grid Manager oder der Tenant Manager-Dienst ausfällt, wird das Failover von HA-Gruppen nicht ausgelöst.

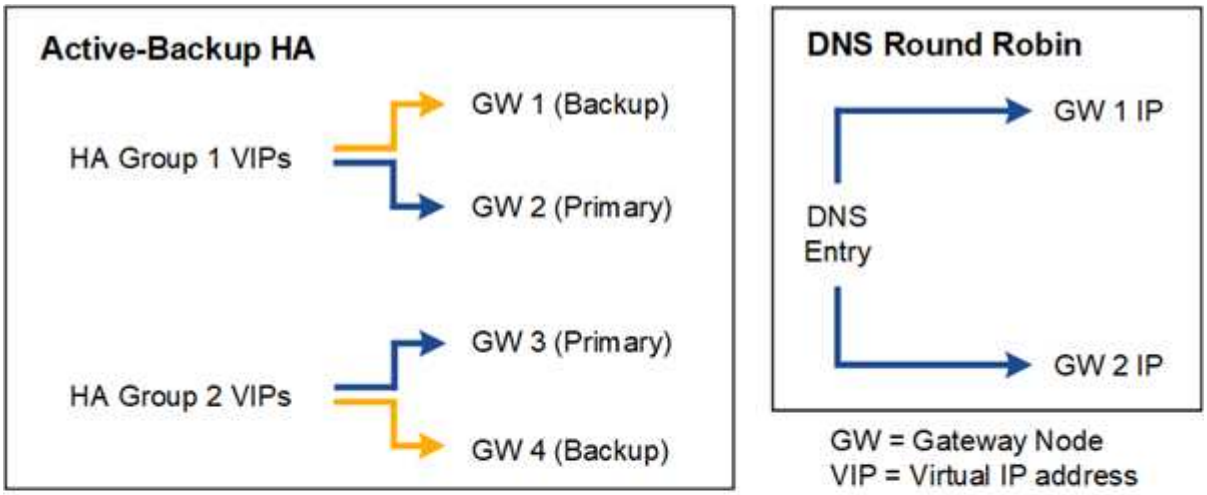
Wenn Sie sich bei einem Failover beim Grid Manager oder beim Tenant Manager angemeldet haben, werden Sie abgemeldet und müssen sich erneut anmelden, um Ihre Aufgabe fortzusetzen.

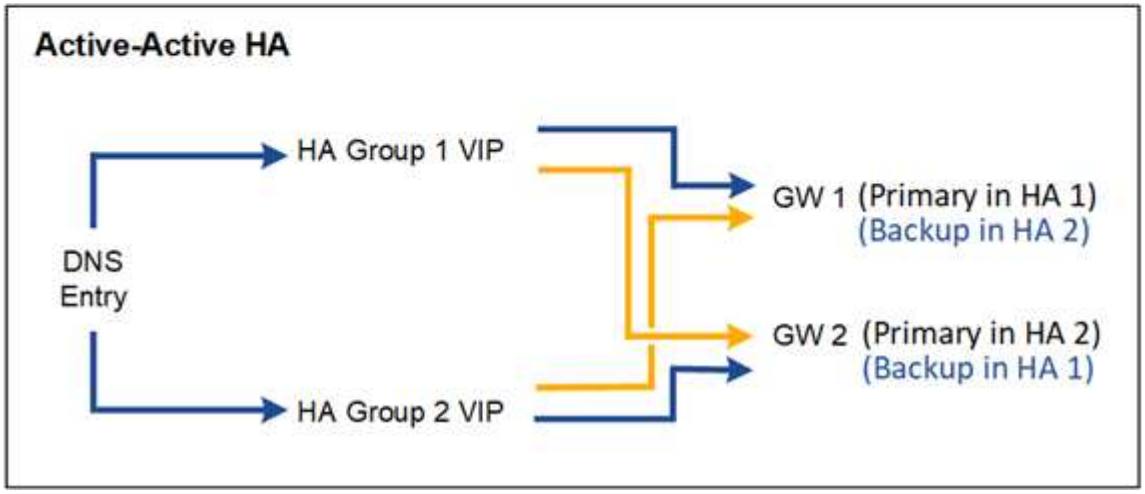
Einige Wartungsverfahren können nicht durchgeführt werden, wenn der primäre Admin-Node nicht verfügbar ist. Während des Failovers können Sie Ihr StorageGRID-System mit dem Grid-Manager überwachen.

Konfigurationsoptionen für HA-Gruppen

Die folgenden Diagramme bieten Beispiele für verschiedene Möglichkeiten zum Konfigurieren von HA-Gruppen. Jede Option hat vor- und Nachteile.

In den Diagrammen zeigt blau die primäre Schnittstelle in der HA-Gruppe an und gelb gibt die Backup-Schnittstelle in der HA-Gruppe an.





Die Tabelle enthält eine Zusammenfassung der Vorteile der einzelnen HA-Konfigurationen, die in der Abbildung dargestellt sind.

Konfiguration	Vorteile	Nachteile
Aktiv/Backup HA	• Management über StorageGRID ohne externe Abhängigkeiten • Schnelles Failover.	• In einer HA-Gruppe ist nur ein Node aktiv. Mindestens ein Node pro HA-Gruppe bleibt im Ruhezustand.

Konfiguration	Vorteile	Nachteile
DNS Round Robin	• Erhöhter Aggregatdurchsatz: • Keine leerlaufenden Hosts	• Langsamer Failover, der vom Client-Verhalten abhängen kann. • Konfiguration von Hardware außerhalb von StorageGRID erforderlich • Benötigt eine vom Kunden implementierte Zustandsprüfung.
Aktiv/aktiv-HA	• Der Datenverkehr wird über mehrere HA-Gruppen verteilt. • Hoher Aggregatdurchsatz, der mit der Anzahl der HA-Gruppen skaliert werden kann • Schnelles Failover.	• Komplexer zu konfigurieren. • Konfiguration von Hardware außerhalb von StorageGRID erforderlich • Benötigt eine vom Kunden implementierte Zustandsprüfung.

Konfigurieren Sie Hochverfügbarkeitsgruppen

Sie können Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen) konfigurieren, um hochverfügbaren Zugriff auf die Services in Admin-Nodes oder Gateway-Nodes bereitzustellen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die Root-Zugriffsberechtigung.
- Wenn Sie eine VLAN-Schnittstelle in einer HA-Gruppe verwenden möchten, haben Sie die VLAN-Schnittstelle erstellt. Siehe "Konfigurieren Sie die VLAN-Schnittstellen".
- Wenn Sie eine Zugriffsoberfläche für einen Node in einer HA-Gruppe verwenden möchten, haben Sie die Schnittstelle erstellt:
  - **Red hat Enterprise Linux oder CentOS (vor der Installation des Knotens)**: "Erstellen von Node-Konfigurationsdateien"
  - **Ubuntu oder Debian (vor der Installation des Knotens)**: "Erstellen von Node-Konfigurationsdateien"
  - **Linux (nach der Installation des Knotens)**: "Linux: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node"
  - **VMware (nach der Installation des Knotens)**: "VMware: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node"

Erstellen Sie eine Hochverfügbarkeitsgruppe

Wenn Sie eine Hochverfügbarkeitsgruppe erstellen, wählen Sie eine oder mehrere Schnittstellen aus und organisieren sie in Prioritätsreihenfolge. Anschließend weisen Sie der Gruppe eine oder mehrere VIP-Adressen zu.

Eine Schnittstelle muss lauten, damit ein Gateway-Node oder ein Admin-Node in einer HA-Gruppe enthalten sein kann. Eine HA-Gruppe kann nur eine Schnittstelle für jeden angegebenen Node verwenden. Jedoch können andere Schnittstellen für denselben Node in anderen HA-Gruppen verwendet werden.

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **CONFIGURATION** > **Network** > **High Availability groups**.
2. Wählen Sie **Erstellen**.

Geben Sie Details für die HA-Gruppe ein

Schritte

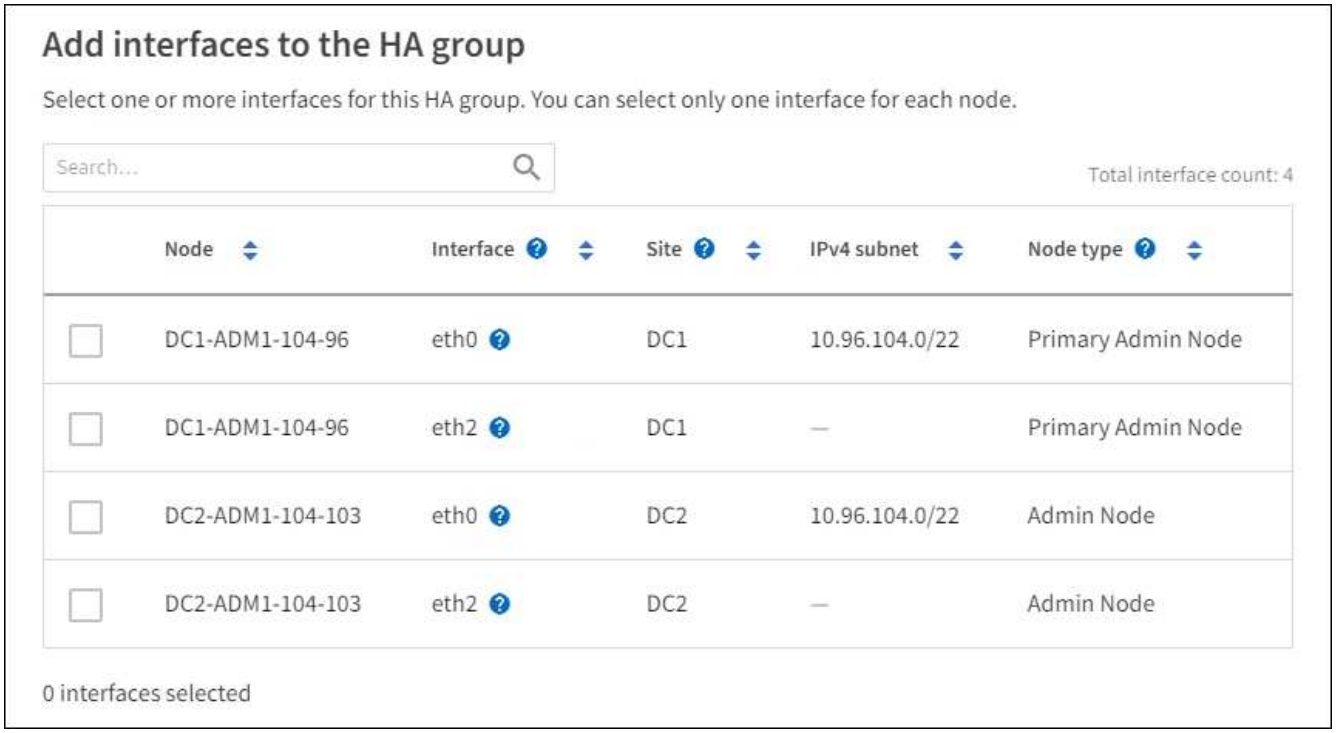
1. Geben Sie einen eindeutigen Namen für die HA-Gruppe ein.
2. Geben Sie optional eine Beschreibung für die HA-Gruppe ein.
3. Wählen Sie **Weiter**.

Fügen Sie der HA-Gruppe Schnittstellen hinzu

Schritte

1. Wählen Sie eine oder mehrere Schnittstellen aus, die dieser HA-Gruppe hinzugefügt werden sollen.

   Verwenden Sie die Spaltenüberschriften, um die Zeilen zu sortieren, oder geben Sie einen Suchbegriff ein, um Schnittstellen schneller zu finden.

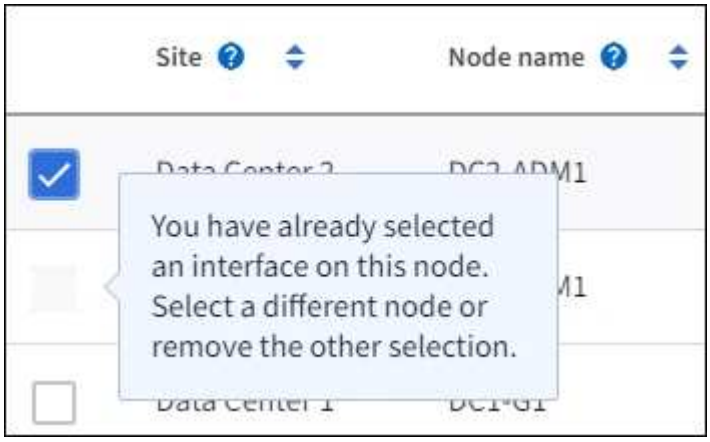


> Warten Sie nach dem Erstellen einer VLAN-Schnittstelle bis zu 5 Minuten, bis die neue Schnittstelle in der Tabelle angezeigt wird.

Richtlinien für die Auswahl von Schnittstellen

- Sie müssen mindestens eine Schnittstelle auswählen.
- Sie können nur eine Schnittstelle für einen Node auswählen.
- Wenn die HA-Gruppe den HA-Schutz von Admin Node-Services bietet, zu denen der Grid Manager und der MandantenManager gehören, wählen Sie nur Schnittstellen zu Admin-Nodes aus.

- Wenn die HA-Gruppe einen HA-Schutz für den Client-Datenverkehr von S3 oder Swift bietet, wählen Sie Schnittstellen an Admin-Nodes, Gateway Nodes oder beiden.
- Wenn Sie Schnittstellen für verschiedene Node-Typen auswählen, wird ein Informationshinweis angezeigt. Sie werden daran erinnert, dass bei einem Failover Dienste, die vom zuvor aktiven Knoten bereitgestellt werden, möglicherweise auf dem neu aktiven Knoten nicht verfügbar sind. Ein Backup-Gateway-Node kann beispielsweise keinen HA-Schutz für Admin-Node-Services bereitstellen. Ebenso kann ein Backup-Admin-Node nicht alle Wartungsverfahren durchführen, die der primäre Admin-Node bereitstellen kann.
- Wenn Sie keine Schnittstelle auswählen können, ist das Kontrollkästchen deaktiviert. Der QuickInfo enthält weitere Informationen.



- Eine Schnittstelle kann nicht ausgewählt werden, wenn ihr Subnetzwert oder Gateway mit einer anderen ausgewählten Schnittstelle in Konflikt steht.
- Sie können keine konfigurierte Schnittstelle auswählen, wenn diese keine statische IP-Adresse hat.

2. Wählen Sie **Weiter**.

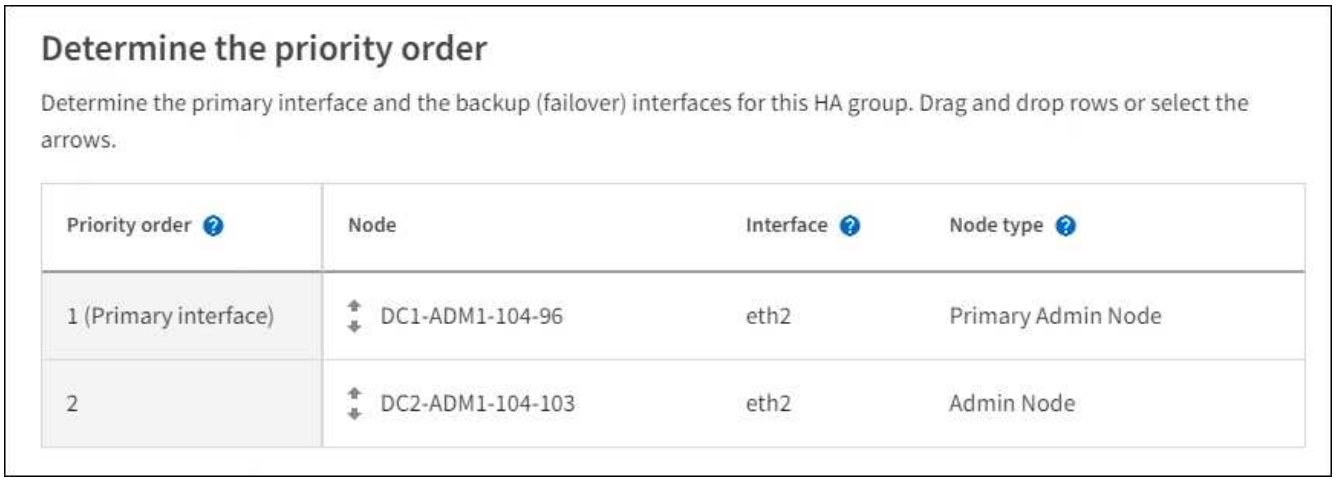
Legen Sie die Prioritätsreihenfolge fest

Wenn die HA-Gruppe mehr als eine Schnittstelle umfasst, können Sie feststellen, welche primäre Schnittstelle und welche Backup-Schnittstellen (Failover) sind. Wenn die primäre Schnittstelle fehlschlägt, werden die VIP-Adressen zur Schnittstelle mit der höchsten Priorität verschoben, die verfügbar ist. Wenn diese Schnittstelle ausfällt, werden die VIP-Adressen zur nächsten verfügbaren Schnittstelle mit der höchsten Priorität usw. verschoben.

Schritte

1. Ziehen Sie Zeilen in die Spalte **Priority order**, um die primäre Schnittstelle und alle Backup-Schnittstellen zu bestimmen.

   Die erste Schnittstelle in der Liste ist die primäre Schnittstelle. Die primäre Schnittstelle ist die aktive Schnittstelle, sofern kein Fehler auftritt.



Wenn die HA-Gruppe Zugriff auf den Grid Manager bietet, müssen Sie eine Schnittstelle am primären Admin-Node als primäre Schnittstelle auswählen. Einige Wartungsvorgänge können nur vom primären Admin-Node ausgeführt werden.

2. Wählen Sie **Weiter**.

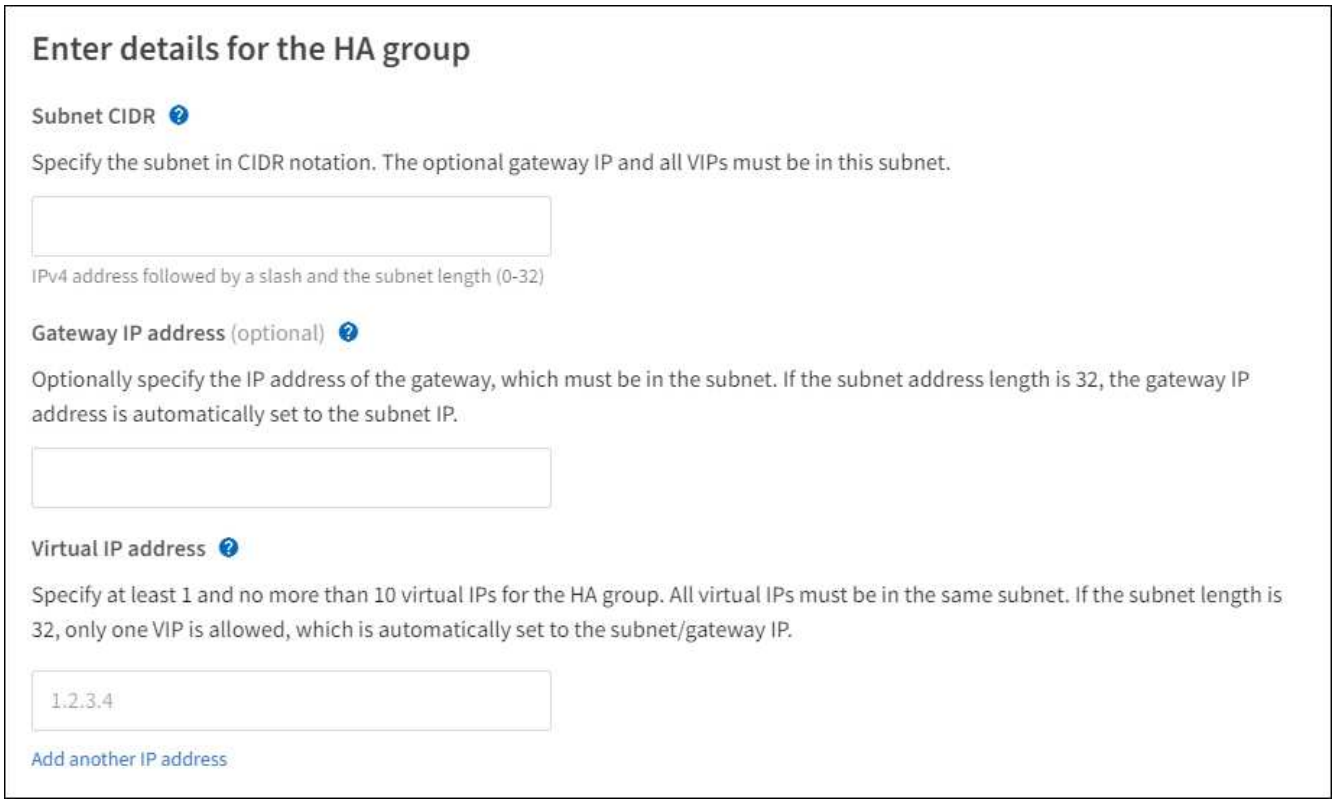
Geben Sie die IP-Adressen ein

Schritte

1. Geben Sie im Feld **Subnetz CIDR** das VIP-Subnetz in CIDR-Notation an - eine IPv4-Adresse gefolgt von einem Schrägstrich und der Subnetz-Länge (0-32).

   Die Netzwerkadresse darf keine Host-Bits festgelegt haben. Beispiel: `192.16.0.0/22`.

   Wenn Sie ein 32-Bit-Präfix verwenden, dient die VIP-Netzwerkadresse auch als Gateway-Adresse und VIP-Adresse.



2. Wenn auf diese VIP-Adressen von S3-, Swift-, Administrations- oder Mandantenclients aus einem anderen Subnetz zugegriffen wird, geben Sie die **Gateway IP-Adresse** ein. Die Gateway-Adresse muss sich im VIP-Subnetz befinden.

   Client- und Admin-Benutzer verwenden dieses Gateway, um auf die virtuellen IP-Adressen zuzugreifen.

3. Geben Sie mindestens eine und nicht mehr als zehn VIP-Adressen für die aktive Schnittstelle in der HA-Gruppe ein. Alle VIP-Adressen müssen sich innerhalb des VIP-Subnetzes befinden, und alle müssen gleichzeitig auf der aktiven Schnittstelle aktiv sein.

   Sie müssen mindestens eine IPv4-Adresse angeben. Optional können Sie weitere IPv4- und IPv6-Adressen angeben.

4. Wählen Sie **HA-Gruppe erstellen** und wählen Sie **Fertig**.

   Die HA-Gruppe wird erstellt. Sie können jetzt die konfigurierten virtuellen IP-Adressen verwenden.

> Warten Sie bis zu 15 Minuten, bis Änderungen an einer HA-Gruppe auf alle Nodes angewendet werden.

Nächste Schritte

Wenn Sie diese HA-Gruppe zum Lastausgleich verwenden möchten, erstellen Sie einen Endpunkt zum Load Balancer, um den Port und das Netzwerkprotokoll zu ermitteln und die erforderlichen Zertifikate anzuschließen. Siehe "Konfigurieren von Load Balancer-Endpunkten".

Bearbeiten Sie eine Hochverfügbarkeitsgruppe

Sie können eine HA-Gruppe (High Availability, Hochverfügbarkeit) bearbeiten, um ihren Namen und ihre Beschreibung zu ändern, Schnittstellen hinzuzufügen oder zu entfernen, die Prioritätsreihenfolge zu ändern

oder virtuelle IP-Adressen hinzuzufügen oder zu aktualisieren.

Beispielsweise müssen Sie möglicherweise eine HA-Gruppe bearbeiten, wenn Sie den Node, der einer ausgewählten Schnittstelle zugeordnet ist, entfernen möchten, wenn Sie ihn an einem Standort ausmustern oder einem Node entfernen möchten.

Schritte

1. Wählen Sie **CONFIGURATION** > **Network** > **High Availability groups**.

   Auf der Seite „Hochverfügbarkeitsgruppen“ werden alle vorhandenen HA-Gruppen angezeigt.

2. Aktivieren Sie das Kontrollkästchen für die HA-Gruppe, die Sie bearbeiten möchten.
3. Führen Sie einen der folgenden Schritte aus, je nachdem, was Sie aktualisieren möchten:
   - Wählen Sie **Aktionen** > **virtuelle IP-Adresse bearbeiten**, um VIP-Adressen hinzuzufügen oder zu entfernen.
   - Wählen Sie **Aktionen** > **HA-Gruppe bearbeiten** aus, um den Namen oder die Beschreibung der Gruppe zu aktualisieren, Schnittstellen hinzuzufügen oder zu entfernen, die Prioritätsreihenfolge zu ändern oder VIP-Adressen hinzuzufügen oder zu entfernen.
4. Wenn Sie **virtuelle IP-Adresse bearbeiten** ausgewählt haben:
   a. Aktualisieren Sie die virtuellen IP-Adressen für die HA-Gruppe.
   b. Wählen Sie **Speichern**.
   c. Wählen Sie **Fertig**.
5. Wenn Sie **HA-Gruppe bearbeiten** ausgewählt haben:
   a. Optional können Sie den Namen oder die Beschreibung der Gruppe aktualisieren.
   b. Aktivieren oder deaktivieren Sie optional die Kontrollkästchen, um Schnittstellen hinzuzufügen oder zu entfernen.

      Wenn die HA-Gruppe Zugriff auf den Grid Manager bietet, müssen Sie eine Schnittstelle am primären Admin-Node als primäre Schnittstelle auswählen. Einige Wartungsvorgänge können nur vom primären Admin-Node ausgeführt werden

   c. Optional können Sie Zeilen ziehen, um die Prioritätsreihenfolge der primären Schnittstelle und aller Backup-Schnittstellen für diese HA-Gruppe zu ändern.
   d. Optional können Sie die virtuellen IP-Adressen aktualisieren.
   e. Wählen Sie **Speichern** und dann **Fertig stellen**.

Warten Sie bis zu 15 Minuten, bis Änderungen an einer HA-Gruppe auf alle Nodes angewendet werden.

Entfernen Sie eine Hochverfügbarkeitsgruppe

Sie können eine oder mehrere HA-Gruppen (High Availability, Hochverfügbarkeit) gleichzeitig entfernen.

Sie können eine HA-Gruppe nicht entfernen, wenn sie an einen Load Balancer-Endpunkt gebunden ist. Zum Löschen einer HA-Gruppe müssen Sie sie von allen Endpunkten der Load Balancer entfernen, die sie verwenden.

Um Client-Unterbrechungen zu vermeiden, aktualisieren Sie die betroffenen S3- oder Swift-Client-Applikationen, bevor Sie eine HA-Gruppe entfernen. Aktualisieren Sie jeden Client, um eine Verbindung über eine andere IP-Adresse herzustellen, z. B. die virtuelle IP-Adresse einer anderen HA-Gruppe oder die IP-Adresse, die während der Installation für eine Schnittstelle konfiguriert wurde.

Schritte

1. Wählen Sie **CONFIGURATION** > **Network** > **High Availability groups**.
2. Überprüfen Sie die Spalte **Load Balancer Endpunkte** für jede HA-Gruppe, die Sie entfernen möchten. Wenn Load Balancer-Endpunkte aufgeführt sind:
   a. Gehen Sie zu **CONFIGURATION** > **Network** > **Load Balancer Endpunkte**.
   b. Aktivieren Sie das Kontrollkästchen für den Endpunkt.
   c. Wählen Sie **Aktionen** > **Endpunktbindungsmodus bearbeiten**.
   d. Aktualisieren Sie den Bindungsmodus, um die HA-Gruppe zu entfernen.
   e. Wählen Sie **Änderungen speichern**.
3. Wenn keine Load Balancer-Endpunkte aufgeführt sind, aktivieren Sie das Kontrollkästchen für jede HA-Gruppe, die Sie entfernen möchten.
4. Wählen Sie **actions** > **Remove HA Group**.
5. Überprüfen Sie die Nachricht und wählen Sie **HA-Gruppe löschen**, um Ihre Auswahl zu bestätigen.

   Alle von Ihnen ausgewählten HA-Gruppen werden entfernt. Ein grünes Banner wird auf der Seite „Hochverfügbarkeitsgruppen“ angezeigt.

Managen Sie den Lastausgleich

Überlegungen zum Lastausgleich

Mit Lastausgleich können Workloads bei der Aufnahme und dem Abruf von S3 und Swift Clients genutzt werden.

Was ist Load Balancing?

Wenn eine Client-Applikation Daten eines StorageGRID Systems speichert oder abruft, verwendet StorageGRID einen Load Balancer, um den Aufnahme- und Abruf-Workload zu managen. Load Balancing maximiert die Geschwindigkeit und die Verbindungskapazität, indem der Workload auf mehrere Storage Nodes verteilt wird.

Der StorageGRID Load Balancer-Service wird auf allen Admin-Nodes und allen Gateway-Knoten installiert und bietet Layer 7-Lastausgleich. Sie beendet die TLS-Beendigung von Client-Anforderungen, prüft die Anforderungen und stellt neue sichere Verbindungen zu den Storage-Nodes her.

Der Load Balancer-Service auf jedem Node wird unabhängig ausgeführt, wenn der Client-Datenverkehr an die Storage Nodes weitergeleitet wird. Durch eine Gewichtung leitet der Load Balancer-Service mehr Anfragen an Storage-Nodes mit höherer CPU-Verfügbarkeit weiter.

> Obwohl der StorageGRID Load Balancer-Service der empfohlene Load-Balancing-Mechanismus ist, können Sie stattdessen einen Load Balancer eines Drittanbieters integrieren. Weitere Informationen erhalten Sie von Ihrem NetApp Ansprechpartner oder unter "TR-4626: StorageGRID Anbieter- und Global Load Balancer".

Wie viele Nodes für Lastausgleich benötige ich?

Als allgemeine Best Practice sollte jeder Standort in Ihrem StorageGRID-System zwei oder mehr Nodes mit dem Load Balancer Service umfassen. Ein Standort kann beispielsweise zwei Gateway-Nodes oder einen Admin-Node und einen Gateway-Node umfassen. Vergewissern Sie sich, dass für jeden Load-Balancing-Node eine entsprechende Netzwerk-, Hardware- oder Virtualisierungsinfrastruktur vorhanden ist, unabhängig davon, ob Sie SG100- oder SG1000-Servicegeräte, Bare Metal-Nodes oder VM-basierte Nodes verwenden.

Was ist ein Endpunkt eines Load Balancers?

Ein Load Balancer-Endpunkt definiert den Port und das Netzwerkprotokoll (HTTPS oder HTTP), über das eingehende und ausgehende Client-Anwendungsanforderungen auf die Knoten zugreifen, die den Load Balancer-Dienst enthalten. Der Endpunkt definiert außerdem den Client-Typ (S3 oder Swift), den Bindungsmodus und optional eine Liste zulässiger oder blockierter Mandanten.

Um einen Load Balancer-Endpunkt zu erstellen, wählen Sie entweder **CONFIGURATION** > **Network** > **Load Balancer-Endpunkte** oder schließen Sie den FabricPool- und S3-Setup-Assistenten ab. Weitere Informationen:

- "Konfigurieren von Load Balancer-Endpunkten"
- "Verwenden Sie den S3-Einrichtungsassistenten"
- "Verwenden Sie den FabricPool-Einrichtungsassistenten"

Überlegungen zum Port

Der Port für einen Load Balancer-Endpunkt ist für den ersten erstellten Endpunkt standardmäßig auf 10433 gesetzt. Sie können jedoch einen beliebigen nicht verwendeten externen Port zwischen 1 und 65535 angeben. Wenn Sie Port 80 oder 443 verwenden, verwendet der Endpunkt nur den Load Balancer-Dienst auf Gateway-Nodes. Diese Ports sind für Admin-Nodes reserviert. Wenn Sie denselben Port für mehr als einen Endpunkt verwenden, müssen Sie für jeden Endpunkt einen anderen Bindungsmodus angeben.

Von anderen Netzdiensten verwendete Ports sind nicht zulässig. Siehe "Referenz für Netzwerk-Ports".

Überlegungen zum Netzwerkprotokoll

In den meisten Fällen sollte für die Verbindungen zwischen Client-Anwendungen und StorageGRID die TLS-Verschlüsselung (Transport Layer Security) verwendet werden. Eine Verbindung mit StorageGRID ohne TLS-Verschlüsselung wird unterstützt, aber nicht empfohlen, insbesondere in Produktionsumgebungen. Wenn Sie das Netzwerkprotokoll für den StorageGRID Load Balancer-Endpunkt auswählen, sollten Sie **HTTPS** auswählen.

Überlegungen für Load Balancer-Endpunktzertifikate

Wenn Sie **HTTPS** als Netzwerkprotokoll für den Load Balancer-Endpunkt auswählen, müssen Sie ein Sicherheitszertifikat angeben. Beim Erstellen des Load Balancer-Endpunkts können Sie eine der folgenden drei Optionen verwenden:

- **Laden Sie ein signiertes Zertifikat hoch (empfohlen)**. Dieses Zertifikat kann entweder von einer öffentlich vertrauenswürdigen oder einer privaten Zertifizierungsstelle (CA) signiert werden. Die Verwendung eines öffentlich vertrauenswürdigen CA-Serverzertifikats zum Sichern der Verbindung ist die beste Methode. Im Gegensatz zu generierten Zertifikaten können von einer CA signierte Zertifikate unterbrechungsfrei gedreht werden, was dazu beitragen kann, Ablaufprobleme zu vermeiden.

  Sie müssen die folgenden Dateien abrufen, bevor Sie den Load Balancer-Endpunkt erstellen:

- Die Zertifikatdatei des benutzerdefinierten Servers.
- Die Datei mit dem privaten Schlüssel des benutzerdefinierten Serverzertifikats.
- Optional ein CA-Bündel der Zertifikate jeder zwischengeschalteten Zertifizierungsstelle.

- **Generieren Sie ein selbst signiertes Zertifikat**.
- **Verwenden Sie das globale StorageGRID S3 und Swift Zertifikat**. Sie müssen eine benutzerdefinierte Version dieses Zertifikats hochladen oder generieren, bevor Sie es für den Load Balancer-Endpunkt auswählen können. Siehe "Konfigurieren von S3- und Swift-API-Zertifikaten".

Welche Werte brauche ich?

Zum Erstellen des Zertifikats müssen Sie alle Domänennamen und IP-Adressen kennen, die von S3- oder Swift-Client-Anwendungen für den Zugriff auf den Endpunkt verwendet werden.

Der Eintrag **Subject DN** (Distinguished Name) für das Zertifikat muss den vollständig qualifizierten Domänennamen enthalten, den die Client-Anwendung für StorageGRID verwendet. Beispiel:

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

Bei Bedarf kann das Zertifikat Platzhalter verwenden, um die vollständig qualifizierten Domänennamen aller Admin-Nodes und Gateway-Nodes darzustellen, auf denen der Load Balancer-Dienst ausgeführt wird. Beispiel: `*.storagegrid.example.com` Verwendet den Platzhalter * für die Darstellung `adm1.storagegrid.example.com` Und `gn1.storagegrid.example.com`.

Wenn Sie S3 Virtual Hosted-Style-Anfragen verwenden möchten, muss das Zertifikat für jeden Eintrag auch einen **Alternative Name**-Eintrag enthalten "Der Domänenname des S3-Endpunkts" Sie haben konfiguriert, einschließlich aller Platzhalternamen. Beispiel:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

Wenn Sie Platzhalter für Domänennamen verwenden, lesen Sie die "Härtungsrichtlinien für Serverzertifikate".

Außerdem müssen Sie für jeden Namen im Sicherheitszertifikat einen DNS-Eintrag definieren.

Wie verwalte ich auslaufende Zertifikate?

Wenn das Zertifikat, mit dem die Verbindung zwischen der S3-Anwendung und StorageGRID gesichert wird, abläuft, kann die Applikation möglicherweise vorübergehend den Zugriff auf StorageGRID verlieren.

Befolgen Sie die folgenden Best Practices, um Probleme mit dem Ablauf von Zertifikaten zu vermeiden:

- Überwachen Sie sorgfältig alle Warnungen, die darauf hinweisen, dass sich das Ablaufdatum des Zertifikats nähert, z. B. das Endpunktzertifikat **Ablauf des Load Balancer** und **Ablauf des globalen Serverzertifikats für S3- und Swift-API**-Warnungen.
- Halten Sie die Versionen des Zertifikats für die StorageGRID- und S3-Anwendung immer synchron. Wenn

Sie das für einen Load Balancer-Endpunkt verwendete Zertifikat ersetzen oder erneuern, müssen Sie das von der S3-Anwendung verwendete entsprechende Zertifikat ersetzen oder erneuern.

- Ein öffentlich signiertes CA-Zertifikat verwenden. Wenn Sie ein von einer Zertifizierungsstelle signiertes Zertifikat verwenden, können Sie bald abgelaufene Zertifikate unterbrechungsfrei ersetzen.
- Wenn Sie ein selbstsigniertes StorageGRID-Zertifikat generiert haben und dieses Zertifikat kurz vor dem Ablauf steht, müssen Sie das Zertifikat sowohl in StorageGRID als auch in der S3-Anwendung manuell ersetzen, bevor das vorhandene Zertifikat abläuft.

Überlegungen zum Bindungsmodus

Im Bindungsmodus können Sie festlegen, welche IP-Adressen für den Zugriff auf einen Load Balancer-Endpunkt verwendet werden können. Wenn ein Endpunkt einen Bindungsmodus verwendet, können Clientanwendungen nur auf den Endpunkt zugreifen, wenn sie eine zulässige IP-Adresse oder den entsprechenden vollständig qualifizierten Domänennamen (FQDN) verwenden. Client-Anwendungen, die eine andere IP-Adresse oder FQDN verwenden, können nicht auf den Endpunkt zugreifen.

Sie können einen der folgenden Bindungsmodi festlegen:

- **Global** (Standard): Client-Anwendungen können über die IP-Adresse eines beliebigen Gateway-Knotens oder Admin-Knotens, die virtuelle IP-Adresse (VIP) einer HA-Gruppe in einem beliebigen Netzwerk oder einen entsprechenden FQDN auf den Endpunkt zugreifen. Verwenden Sie diese Einstellung, es sei denn, Sie müssen den Zugriff auf einen Endpunkt einschränken.
- **Virtuelle IPs von HA-Gruppen**. Client-Anwendungen müssen eine virtuelle IP-Adresse (oder einen entsprechenden FQDN) einer HA-Gruppe verwenden.
- **Knotenschnittstellen**. Clients müssen die IP-Adressen (oder entsprechende FQDNs) der ausgewählten Knotenschnittstellen verwenden.
- **Knotentyp**. Basierend auf dem von Ihnen ausgewählten Knotentyp müssen Clients entweder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Admin-Knotens oder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Gateway-Knotens verwenden.

Überlegungen für den Mandantenzugriff

Der Mandantenzugriff ist eine optionale Sicherheitsfunktion, mit der Sie steuern können, welche StorageGRID-Mandantenkonten einen Load-Balancer-Endpunkt für den Zugriff auf ihre Buckets verwenden können. Sie können allen Mandanten den Zugriff auf einen Endpunkt erlauben (Standard), oder Sie können eine Liste der zulässigen oder blockierten Mandanten für jeden Endpunkt festlegen.

Sie können diese Funktion nutzen, um eine bessere Sicherheitsisolierung zwischen Mandanten und ihren Endpunkten zu ermöglichen. Mit dieser Funktion können Sie beispielsweise sicherstellen, dass die streng geheimen oder streng klassifizierten Materialien eines Mandanten für andere Mieter nicht zugänglich sind.

> Für die Zugriffssteuerung wird der Mandant aus den Zugriffsschlüsseln ermittelt, die in der Client-Anfrage verwendet werden. Wenn im Rahmen der Anfrage keine Zugriffsschlüssel angegeben werden (z. B. mit anonymem Zugriff), wird der Bucket-Eigentümer zur Ermittlung des Mandanten verwendet.

Beispiel für Mandantenzugriff

Um zu verstehen, wie diese Sicherheitsfunktion funktioniert, betrachten Sie das folgende Beispiel:

1. Sie haben zwei Lastausgleichsendpunkte wie folgt erstellt:

- **Öffentlicher** Endpunkt: Nutzt Port 10443 und erlaubt den Zugriff auf alle Mandanten.
- **Top secret** Endpunkt: Verwendet Port 10444 und erlaubt nur den Zugriff auf den **Top secret** Mieter. Alle anderen Mandanten werden für den Zugriff auf diesen Endpunkt gesperrt.

2. Der `top-secret.pdf` Befindet sich in einem Eimer im Besitz des **Top Secret** Mieters.

Um auf den zuzugreifen `top-secret.pdf`Ein Benutzer im **`Top Secret`**-Mieter kann eine GET-Anfrage an ausstellen `\https://w.x.y.z:10444/top-secret.pdf`. Da dieser Mandant den Endpunkt 10444 verwenden darf, kann der Benutzer auf das Objekt zugreifen. Wenn ein Benutzer eines anderen Mandanten jedoch dieselbe Anforderung an dieselbe URL ausgibt, erhält er eine Meldung über „Zugriff verweigert“. Der Zugriff wird verweigert, selbst wenn die Anmeldeinformationen und die Signatur gültig sind.

CPU-Verfügbarkeit

Der Load Balancer Service läuft auf jedem Admin-Node und Gateway-Node unabhängig, wenn der S3- oder Swift-Datenverkehr zu den Storage-Nodes weitergeleitet wird. Durch eine Gewichtung leitet der Load Balancer-Service mehr Anfragen an Storage-Nodes mit höherer CPU-Verfügbarkeit weiter. Die Informationen zur CPU-Auslastung des Knotens werden alle paar Minuten aktualisiert. Die Gewichtung kann jedoch häufiger aktualisiert werden. Allen Storage-Nodes wird ein Mindestwert für das Basisgewicht zugewiesen, selbst wenn ein Node eine Auslastung von 100 % meldet oder seine Auslastung nicht meldet.

In manchen Fällen sind die Informationen zur CPU-Verfügbarkeit auf den Standort beschränkt, an dem sich der Load Balancer Service befindet.

Konfigurieren von Load Balancer-Endpunkten

Load Balancer-Endpunkte bestimmen die Ports und Netzwerkprotokolle S3 und Swift-Clients können beim Herstellen einer Verbindung zum StorageGRID Load Balancer auf Gateway und Admin-Nodes verwendet werden.

> Die Unterstützung für Swift-Client-Anwendungen wurde veraltet und wird in einer zukünftigen Version entfernt.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die Root-Zugriffsberechtigung.
- Sie haben die geprüft "Überlegungen zum Lastausgleich".
- Wenn Sie zuvor einen Port neu zugeordnet haben, den Sie für den Load Balancer-Endpunkt verwenden möchten, haben Sie diesen "Port-Remap wurde entfernt".
- Sie haben alle Hochverfügbarkeitsgruppen (High Availability groups, die Sie verwenden möchten, erstellt. HA-Gruppen werden empfohlen, jedoch nicht erforderlich. Siehe "Management von Hochverfügbarkeitsgruppen".
- Wenn der Endpunkt des Load Balancer von verwendet wird "S3 Mandanten für S3 Select", Es darf die IP-Adressen oder FQDNs von Bare-Metal-Knoten nicht verwenden. Für die bei S3 Select verwendeten Load Balancer-Endpunkte sind nur SG100- oder SG1000-Appliances und VMware-basierte Software-Nodes zulässig.
- Sie haben alle VLAN-Schnittstellen konfiguriert, die Sie verwenden möchten. Siehe "Konfigurieren Sie die VLAN-Schnittstellen".

- Wenn Sie einen HTTPS-Endpunkt erstellen (empfohlen), haben Sie die Informationen für das Serverzertifikat.

> Änderungen an einem Endpunktzertifikat können bis zu 15 Minuten dauern, bis sie auf alle Knoten angewendet werden können.

  - Zum Hochladen eines Zertifikats benötigen Sie das Serverzertifikat, den privaten Zertifikatschlüssel und optional ein CA-Bundle.
  - Zum Generieren eines Zertifikats benötigen Sie alle Domain-Namen und IP-Adressen, die S3- oder Swift-Clients für den Zugriff auf den Endpunkt verwenden. Sie müssen auch das Thema (Distinguished Name) kennen.
  - Wenn Sie das StorageGRID S3- und Swift-API-Zertifikat verwenden möchten (das auch für direkte Verbindungen zu Speicherknoten verwendet werden kann), haben Sie das Standardzertifikat bereits durch ein benutzerdefiniertes Zertifikat ersetzt, das von einer externen Zertifizierungsstelle signiert ist. Siehe"Konfigurieren von S3- und Swift-API-Zertifikaten".

Erstellen Sie einen Endpunkt für den Load Balancer

Jeder Load Balancer-Endpunkt gibt einen Port, einen Client-Typ (S3 oder Swift) und ein Netzwerkprotokoll (HTTP oder HTTPS) an.

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **CONFIGURATION** > **Network** > **Load Balancer Endpunkte**.
2. Wählen Sie **Erstellen**.

Geben Sie Details zu Endpunkten ein

Schritte

1. Geben Sie Details für den Endpunkt ein.

Feld	Beschreibung
Name	Ein beschreibbarer Name für den Endpunkt, der in der Tabelle auf der Seite Load Balancer Endpunkte angezeigt wird.
Port	Der StorageGRID-Port, den Sie für den Lastausgleich verwenden möchten. Dieses Feld ist für den ersten erstellten Endpunkt standardmäßig auf 10433 eingestellt. Sie können jedoch einen beliebigen nicht verwendeten externen Port zwischen 1 und 65535 eingeben. Wenn Sie **80** oder **443** eingeben, wird der Endpunkt nur auf Gateway-Knoten konfiguriert. Diese Ports sind für Admin-Nodes reserviert.
Client-Typ	Der Typ der Client-Anwendung, die diesen Endpunkt verwenden wird, entweder **S3** oder **Swift**.

Feld	Beschreibung
Netzwerkprotokoll	Das Netzwerkprotokoll, das Clients bei der Verbindung mit diesem Endpunkt verwenden werden. • Wählen Sie **HTTPS** für sichere, TLS verschlüsselte Kommunikation (empfohlen). Sie müssen ein Sicherheitszertifikat anhängen, bevor Sie den Endpunkt speichern können. • Wählen Sie **HTTP** für eine weniger sichere, unverschlüsselte Kommunikation. Verwenden Sie HTTP nur für ein Grid, das nicht produktionsbereit ist.

2. Wählen Sie **Weiter**.

Wählen Sie einen Bindungsmodus aus

Schritte

1. Wählen Sie einen Bindungsmodus für den Endpunkt aus, um zu steuern, wie auf den Endpunkt zugegriffen wird—Verwenden einer beliebigen IP-Adresse oder Verwenden bestimmter IP-Adressen und Netzwerkschnittstellen.

Option	Beschreibung
Global (Standard)	Clients können über die IP-Adresse eines beliebigen Gateway-Node oder Admin-Node, die virtuelle IP-Adresse (VIP) einer beliebigen HA-Gruppe in einem beliebigen Netzwerk oder einen entsprechenden FQDN auf den Endpunkt zugreifen. Verwenden Sie die **Global**-Einstellung (Standard), es sei denn, Sie müssen die Zugriffsmöglichkeiten dieses Endpunkts einschränken.
Virtuelle IPs von HA-Gruppen	Clients müssen eine virtuelle IP-Adresse (oder einen entsprechenden FQDN) einer HA-Gruppe verwenden, um auf diesen Endpunkt zuzugreifen. Endpunkte mit diesem Bindungsmodus können alle dieselbe Portnummer verwenden, solange sich die für die Endpunkte ausgewählten HA-Gruppen nicht überlappen.
Node-Schnittstellen	Clients müssen die IP-Adressen (oder entsprechende FQDNs) der ausgewählten Knotenschnittstellen verwenden, um auf diesen Endpunkt zuzugreifen.
Node-Typ	Basierend auf dem von Ihnen ausgewählten Knotentyp müssen Clients entweder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Admin-Knotens oder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Gateway-Knotens verwenden, um auf diesen Endpunkt zuzugreifen.

Wenn mehr als ein Endpunkt denselben Port verwendet, verwendet StorageGRID diese Prioritätsreihenfolge, um zu entscheiden, welcher Endpunkt verwendet werden soll: **Virtuelle IPs von HA-Gruppen** > **Knotenschnittstellen** > **Knotentyp** > **global**.

2. Wenn Sie **virtuelle IPs von HA-Gruppen** ausgewählt haben, wählen Sie eine oder mehrere HA-Gruppen aus.
3. Wenn Sie **Node-Schnittstellen** ausgewählt haben, wählen Sie für jeden Admin-Node oder Gateway-Node eine oder mehrere Node-Schnittstellen aus, die mit diesem Endpunkt verknüpft werden sollen.
4. Wenn Sie **Node type** ausgewählt haben, wählen Sie entweder Admin-Nodes aus, die sowohl den primären Admin-Node als auch alle nicht-primären Admin-Nodes enthalten, oder Gateway-Nodes.

Kontrolle des Mandantenzugriffs

Schritte

1. Wählen Sie für den Schritt **Tenant Access** eine der folgenden Optionen aus:

Feld	Beschreibung
Alle Mandanten zulassen (Standard)	Alle Mandantenkonten können diesen Endpunkt verwenden, um auf ihre Buckets zuzugreifen. Sie müssen diese Option auswählen, wenn Sie noch keine Mandantenkonten erstellt haben. Nachdem Sie Mandantenkonten hinzugefügt haben, können Sie den Load Balancer-Endpunkt bearbeiten, um bestimmte Konten zuzulassen oder zu blockieren.
Ausgewählte Mandanten zulassen	Nur die ausgewählten Mandantenkonten können diesen Endpunkt für den Zugriff auf ihre Buckets verwenden.
Ausgewählte Mandanten blockieren	Die ausgewählten Mandantenkonten können diesen Endpunkt nicht für den Zugriff auf ihre Buckets verwenden. Dieser Endpunkt kann von allen anderen Mandanten verwendet werden.

2. Wenn Sie einen **HTTP**-Endpunkt erstellen, müssen Sie kein Zertifikat anhängen. Wählen Sie **Erstellen**, um den neuen Load Balancer-Endpunkt hinzuzufügen. Fahren Sie dann mit fort Nachdem Sie fertig sind. Andernfalls wählen Sie **Weiter**, um das Zertifikat anzuhängen.

Zertifikat anhängen

Schritte

1. Wenn Sie einen **HTTPS**-Endpunkt erstellen, wählen Sie den Typ des Sicherheitszertifikats aus, das Sie an den Endpunkt anhängen möchten.

   Das Zertifikat sichert die Verbindungen zwischen S3- und Swift-Clients und dem Load Balancer-Service auf Admin-Node oder Gateway-Nodes.

   - **Zertifikat hochladen**. Wählen Sie diese Option aus, wenn Sie über benutzerdefinierte Zertifikate zum Hochladen verfügen.
   - **Zertifikat generieren**. Wählen Sie diese Option aus, wenn Sie über die Werte verfügen, die zum Generieren eines benutzerdefinierten Zertifikats erforderlich sind.

- **Verwenden Sie StorageGRID S3 und Swift Zertifikat**. Wählen Sie diese Option aus, wenn Sie das globale S3- und Swift-API-Zertifikat verwenden möchten, das auch für direkte Verbindungen zu Storage-Nodes verwendet werden kann.

  Sie können diese Option nur auswählen, wenn Sie das von der Grid-CA signierte Standard-API-Zertifikat S3 und Swift durch ein benutzerdefiniertes Zertifikat ersetzt haben, das von einer externen Zertifizierungsstelle signiert wurde. Siehe"Konfigurieren von S3- und Swift-API-Zertifikaten".

2. Wenn Sie das StorageGRID S3- und Swift-Zertifikat nicht verwenden, laden Sie das Zertifikat hoch oder generieren Sie es.

Zertifikat hochladen

a. Wählen Sie **Zertifikat hochladen**.

b. Laden Sie die erforderlichen Serverzertifikatdateien hoch:

- **Server-Zertifikat**: Die benutzerdefinierte Server-Zertifikatdatei in PEM-Kodierung.
- **Zertifikat privater Schlüssel**: Die benutzerdefinierte Server Zertifikat private Schlüssel Datei (`.key`).

> Private EC-Schlüssel müssen 224 Bit oder größer sein. RSA Private Keys müssen mindestens 2048 Bit groß sein.

- **CA-Paket**: Eine einzelne optionale Datei, die die Zertifikate jeder Intermediate-Zertifizierungsstelle (CA) enthält. Die Datei sollte alle PEM-kodierten CA-Zertifikatdateien enthalten, die in der Reihenfolge der Zertifikatskette verkettet sind.

c. Erweitern Sie **Zertifikatdetails**, um die Metadaten für jedes hochgeladene Zertifikat anzuzeigen. Wenn Sie ein optionales CA-Paket hochgeladen haben, wird jedes Zertifikat auf seiner eigenen Registerkarte angezeigt.

- Wählen Sie **Zertifikat herunterladen**, um die Zertifikatdatei zu speichern, oder wählen Sie **CA-Paket herunterladen**, um das Zertifikatspaket zu speichern.

  Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung `.pem`.

  Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Zertifikat kopieren PEM** oder **CA-Paket kopieren PEM** aus, um den Zertifikatinhalt zum Einfügen an eine andere Stelle zu kopieren.

d. Wählen Sie **Erstellen**. + der Endpunkt des Load Balancer wird erstellt. Das individuelle Zertifikat wird für alle nachfolgenden neuen Verbindungen zwischen S3 und Swift Clients und dem Endpunkt verwendet.

Zertifikat wird generiert

a. Wählen Sie **Zertifikat erstellen**.

b. Geben Sie die Zertifikatsinformationen an:

Feld	Beschreibung
Domain-Name	Mindestens ein vollständig qualifizierter Domänenname, der in das Zertifikat aufgenommen werden soll. Verwenden Sie ein * als Platzhalter, um mehrere Domain-Namen darzustellen.
IP	Mindestens eine IP-Adresse, die in das Zertifikat aufgenommen werden soll.

Feld	Beschreibung
Betreff (optional)	X.509 Subject oder Distinguished Name (DN) des Zertifikateigentümers. Wenn in diesem Feld kein Wert eingegeben wird, verwendet das generierte Zertifikat den ersten Domänennamen oder die IP-Adresse als allgemeinen Studienteilnehmer (CN).
Tage gültig	Anzahl der Tage nach Erstellung, nach denen das Zertifikat abläuft.
Fügen Sie wichtige Nutzungserweiterungen hinzu	Wenn diese Option ausgewählt ist (Standard und empfohlen), werden die Schlüsselnutzung und die erweiterten Schlüsselnutzungserweiterungen dem generierten Zertifikat hinzugefügt. Diese Erweiterungen definieren den Zweck des Schlüssels, der im Zertifikat enthalten ist. **Hinweis**: Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, Sie haben Verbindungsprobleme mit älteren Clients, wenn Zertifikate diese Erweiterungen enthalten.

c. Wählen Sie **Erzeugen**.

d. Wählen Sie **Zertifikatdetails** aus, um die Metadaten für das generierte Zertifikat anzuzeigen.

   - Wählen Sie **Zertifikat herunterladen**, um die Zertifikatdatei zu speichern.

     Geben Sie den Namen der Zertifikatdatei und den Speicherort für den Download an. Speichern Sie die Datei mit der Erweiterung `.pem`.

   Beispiel: `storagegrid_certificate.pem`

   - Wählen Sie **Zertifikat kopieren PEM** aus, um den Zertifikatinhalt zum Einfügen an eine andere Stelle zu kopieren.

e. Wählen Sie **Erstellen**.

   Der Endpunkt des Load Balancer wird erstellt. Das individuelle Zertifikat wird für alle nachfolgenden neuen Verbindungen zwischen S3 und Swift Clients und diesem Endpunkt verwendet.

Nachdem Sie fertig sind

Schritte

1. Wenn Sie einen DNS verwenden, stellen Sie sicher, dass der DNS einen Datensatz enthält, mit dem der vollständig qualifizierte StorageGRID-Domänenname (FQDN) jeder IP-Adresse zugeordnet wird, die Clients zum Verbindungsaufbau verwenden.

   Die IP-Adresse, die Sie im DNS-Datensatz eingeben, hängt davon ab, ob Sie eine HA-Gruppe von Load-Balancing-Nodes verwenden:

- Wenn Sie eine HA-Gruppe konfiguriert haben, stellen Clients eine Verbindung zu den virtuellen IP-Adressen dieser HA-Gruppe her.
- Wenn Sie keine HA-Gruppe verwenden, stellen Clients mithilfe der IP-Adresse eines Gateway-Node oder Admin-Node eine Verbindung zum StorageGRID Load Balancer-Service her.

  Außerdem müssen Sie sicherstellen, dass der DNS-Datensatz alle erforderlichen Endpunkt-Domain-Namen referenziert, einschließlich Platzhalternamen.

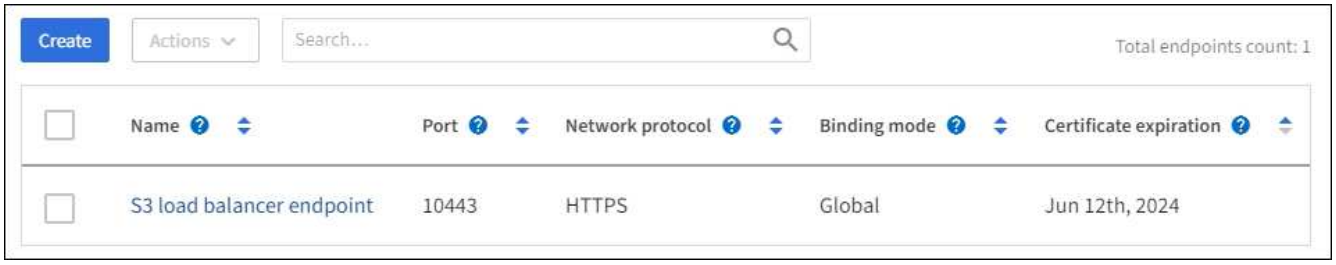
2. S3- und Swift-Clients erhalten die für die Verbindung mit dem Endpunkt erforderlichen Informationen:
   - Port-Nummer
   - Vollständig qualifizierter Domain-Name oder IP-Adresse
   - Alle erforderlichen Zertifikatsdetails

Load Balancer-Endpunkte anzeigen und bearbeiten

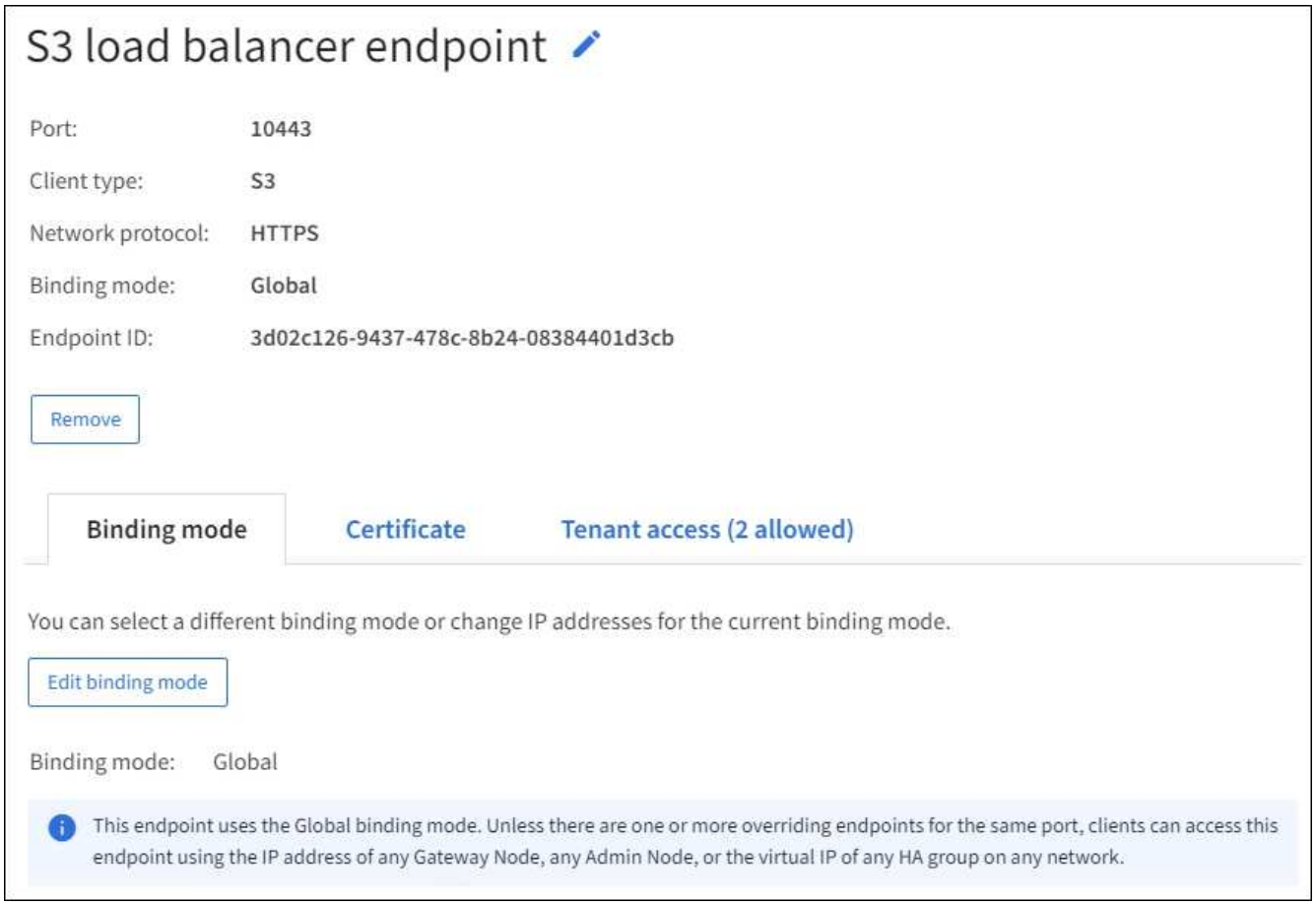
Sie können Details zu vorhandenen Load Balancer-Endpunkten anzeigen, einschließlich der Zertifikatmetadaten für einen gesicherten Endpunkt. Sie können auch den Namen oder den Bindungsmodus eines Endpunkts ändern und alle zugehörigen Zertifikate aktualisieren.

Sie können den Servicetyp (S3 oder Swift), den Port oder das Protokoll (HTTP oder HTTPS) nicht ändern.

- Um grundlegende Informationen für alle Load Balancer-Endpunkte anzuzeigen, lesen Sie die Tabelle auf der Seite Load Balancer Endpunkte durch.



- Um alle Details zu einem bestimmten Endpunkt einschließlich Zertifikatmetadaten anzuzeigen, wählen Sie in der Tabelle den Namen des Endpunkts aus.



- Um einen Endpunkt zu bearbeiten, verwenden Sie das Menü **Aktionen** auf der Seite Load Balancer Endpoints oder die Detailseite für einen bestimmten Endpunkt.

> Nach dem Bearbeiten eines Endpunkts müssen Sie möglicherweise bis zu 15 Minuten warten, bis Ihre Änderungen auf alle Nodes angewendet werden.

Aufgabe	Menü „Aktionen“	Detailseite
Endpunktname bearbeiten	a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie **Aktionen** > **Endpunktname bearbeiten** aus. c. Geben Sie den neuen Namen ein. d. Wählen Sie **Speichern**.	a. Wählen Sie den Endpunktnamen aus, um die Details anzuzeigen. b. Wählen Sie das Bearbeitungssymbol . c. Geben Sie den neuen Namen ein. d. Wählen Sie **Speichern**.

Aufgabe	Menü „Aktionen“	Detailseite
Endpunktbindungsmodus bearbeiten	a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie **Aktionen** > **Endpunktbindungsmodus bearbeiten**. c. Aktualisieren Sie den Bindungsmodus, falls erforderlich. d. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Endpunktnamen aus, um die Details anzuzeigen. b. Wählen Sie **Bindungsmodus bearbeiten**. c. Aktualisieren Sie den Bindungsmodus, falls erforderlich. d. Wählen Sie **Änderungen speichern**.
Endpunktzertifikat bearbeiten	a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie **Aktionen** > **Endpunktzertifikat bearbeiten** aus. c. Laden Sie ein neues benutzerdefiniertes Zertifikat hoch oder erstellen Sie es, falls erforderlich, mit der Verwendung des globalen S3- und Swift-Zertifikats. d. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Endpunktnamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte **Zertifikat** aus. c. Wählen Sie **Zertifikat bearbeiten**. d. Laden Sie ein neues benutzerdefiniertes Zertifikat hoch oder erstellen Sie es, falls erforderlich, mit der Verwendung des globalen S3- und Swift-Zertifikats. e. Wählen Sie **Änderungen speichern**.
Bearbeiten Sie den Mandantenzugriff	a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie **actions** > **Edit Tenant Access**. c. Wählen Sie eine andere Zugriffsoption aus, wählen Sie Mandanten aus der Liste aus oder entfernen Sie sie aus oder führen Sie beides aus. d. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Endpunktnamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte **Tenant Access**. c. Wählen Sie **Mandantenzugriff bearbeiten**. d. Wählen Sie eine andere Zugriffsoption aus, wählen Sie Mandanten aus der Liste aus oder entfernen Sie sie aus oder führen Sie beides aus. e. Wählen Sie **Änderungen speichern**.

Entfernen Sie Load Balancer-Endpunkte

Sie können einen oder mehrere Endpunkte über das Menü **Aktionen** entfernen oder einen einzelnen Endpunkt von der Detailseite entfernen.

> Um Client-Unterbrechungen zu vermeiden, aktualisieren Sie die betroffenen S3- oder Swift-Client-Applikationen, bevor Sie einen Load Balancer-Endpunkt entfernen. Aktualisieren Sie jeden Client, um eine Verbindung über einen Port herzustellen, der einem anderen Load Balancer-Endpunkt zugewiesen ist. Aktualisieren Sie auch die erforderlichen Zertifikatsinformationen.

- So entfernen Sie einen oder mehrere Endpunkte:
  a. Aktivieren Sie auf der Seite Load Balancer das Kontrollkästchen für jeden Endpunkt, den Sie entfernen möchten.
  b. Wählen Sie **Aktionen** > **Entfernen**.
  c. Wählen Sie **OK**.
- So entfernen Sie einen Endpunkt auf der Detailseite:
  a. Auf der Seite Load Balancer. Wählen Sie den Endpunktnamen aus.
  b. Wählen Sie auf der Detailseite * Entfernen.
  c. Wählen Sie **OK**.

Konfigurieren Sie die Domänennamen des S3-Endpunkts

Um Anforderungen im virtuellen Hosted-Stil von S3 zu unterstützen, müssen Sie die Liste der S3-Endpunkt-Domänennamen, mit denen S3-Clients eine Verbindung herstellen, mit dem Grid Manager konfigurieren.

> Die Verwendung einer IP-Adresse für einen Domänennamen des Endpunkts wird nicht unterstützt. Zukünftige Versionen verhindern diese Konfiguration.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Das ist schon "Bestimmte Zugriffsberechtigungen".
- Sie haben bestätigt, dass ein Grid-Upgrade nicht ausgeführt wird.

> Nehmen Sie keine Änderungen an der Domänennamenkonfiguration vor, wenn ein Grid-Upgrade durchgeführt wird.

Über diese Aufgabe

Um Clients die Verwendung von S3-Endpunkt-Domain-Namen zu ermöglichen, müssen Sie folgende Aktionen durchführen:

- Verwenden Sie den Grid-Manager, um dem StorageGRID System die S3-Endpunkt-Domain-Namen hinzuzufügen.
- Stellen Sie das sicher "Zertifikat, das der Client für HTTPS-Verbindungen zu StorageGRID verwendet" Ist für alle Domänennamen signiert, die der Client benötigt.

  Beispiel: Wenn der Endpunkt lautet `s3.company.com`, Sie müssen sicherstellen, dass das Zertifikat verwendet für HTTPS-Verbindungen enthält die `s3.company.com` endpunkt und Wildcard-alternativer Name (SAN) des Endpunkts: `*.s3.company.com`.

- Konfigurieren Sie den vom Client verwendeten DNS-Server. Fügen Sie DNS-Datensätze für die IP-Adressen ein, die Clients zum Verbindungsaufbau verwenden, und stellen Sie sicher, dass die Datensätze auf alle erforderlichen S3-Endpunkt-Domänennamen verweisen, einschließlich aller Platzhalternamen.

Clients können sich mit StorageGRID über die IP-Adresse eines Gateway-Node, eines Admin-Nodes oder eines Storage-Nodes oder durch Verbindung mit der virtuellen IP-Adresse einer Hochverfügbarkeitsgruppe verbinden. Sie sollten verstehen, wie Client-Anwendungen eine Verbindung zum Raster herstellen, sodass Sie die richtigen IP-Adressen in die DNS-Einträge aufnehmen können.

Clients, die HTTPS-Verbindungen (empfohlen) zum Raster verwenden, können eines der folgenden Zertifikate verwenden:

- Clients, die eine Verbindung zu einem Load Balancer-Endpunkt herstellen, können für diesen Endpunkt ein benutzerdefiniertes Zertifikat verwenden. Jeder Load Balancer-Endpunkt kann so konfiguriert werden, dass er unterschiedliche S3-Endpunkt-Domänennamen erkennt.
- Clients, die sich mit einem Load-Balancer-Endpunkt oder direkt mit einem Storage-Node verbinden, können das globale S3- und Swift-API-Zertifikat so anpassen, dass alle erforderlichen S3-Endpunkt-Domänennamen enthalten sind.

Wenn Sie keine S3-Endpunkt-Domänennamen hinzufügen und die Liste leer ist, wird die Unterstützung für Anforderungen im virtuellen Hosted-Stil von S3 deaktiviert.

Fügen Sie einen S3-Endpunkt-Domänennamen hinzu

Schritte

1. Wählen Sie **CONFIGURATION** > **Network** > **S3-Endpunkt-Domänennamen**.
2. Geben Sie den Domainnamen in das Feld **Domain Name 1** ein. Wählen Sie **Add another Domain Name**, um weitere Domainnamen hinzuzufügen.
3. Wählen Sie **Speichern**.
4. Stellen Sie sicher, dass die von Clients verwendeten Serverzertifikate mit den erforderlichen S3-Endpunkt-Domänennamen übereinstimmen.
   - Wenn Clients eine Verbindung zu einem Load Balancer-Endpunkt herstellen, der ein eigenes Zertifikat verwendet, "Aktualisieren Sie das dem Endpunkt zugeordnete Zertifikat".
   - Wenn Clients eine Verbindung zu einem Load Balancer-Endpunkt herstellen, der das globale S3- und Swift-API-Zertifikat verwendet oder direkt mit Storage-Nodes verbunden ist, "Aktualisieren Sie das globale S3- und Swift-API-Zertifikat".
5. Fügen Sie die erforderlichen DNS-Einträge hinzu, um sicherzustellen, dass die Anforderungen für den Domänennamen des Endpunkts aufgelöst werden können.

Ergebnis

Wenn Clients nun den Endpunkt verwenden `bucket.s3.company.com`, Der DNS-Server löst sich auf den richtigen Endpunkt und das Zertifikat authentifiziert den Endpunkt wie erwartet.

Benennen Sie einen S3-Endpunkt-Domänennamen um

Wenn Sie einen Namen ändern, der von S3-Anwendungen verwendet wird, schlagen Anforderungen im virtuellen Hosted-Stil fehl.

Schritte

1. Wählen Sie **CONFIGURATION** > **Network** > **S3-Endpunkt-Domänennamen**.
2. Wählen Sie das Feld für den Domänennamen aus, das Sie bearbeiten möchten, und nehmen Sie die erforderlichen Änderungen vor.

3. Wählen Sie **Speichern**.
4. Wählen Sie **Ja**, um Ihre Änderung zu bestätigen.

Löschen Sie einen S3-Endpunkt-Domänennamen

Wenn Sie einen Namen entfernen, der von S3-Anwendungen verwendet wird, schlagen Anforderungen im virtuellen Hosted-Stil fehl.

Schritte

1. Wählen Sie **CONFIGURATION** > **Network** > **S3-Endpunkt-Domänennamen**.
2. Klicken Sie auf das Löschsymbol ✕ Neben dem Domänennamen.
3. Wählen Sie **Ja**, um den Löschvorgang zu bestätigen.

Verwandte Informationen

- "S3-REST-API VERWENDEN"
- "Zeigen Sie IP-Adressen an"
- "Konfigurieren Sie Hochverfügbarkeitsgruppen"

Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen

Zum Speichern oder Abrufen von Objekten verbinden sich S3- und Swift-Client-Anwendungen mit dem Load Balancer-Dienst, der auf allen Admin-Knoten und Gateway-Knoten enthalten ist, oder mit dem Local Distribution Router (LDR)-Dienst, der auf allen Storage-Knoten enthalten ist.

Client-Applikationen können mithilfe der IP-Adresse eines Grid-Node und der Portnummer des Service auf diesem Node eine Verbindung zu StorageGRID herstellen. Optional können Sie Gruppen für Hochverfügbarkeit (High Availability, HA) von Load-Balancing-Nodes erstellen, um hochverfügbare Verbindungen bereitzustellen, die virtuelle IP-Adressen (VIP) verwenden. Wenn Sie eine Verbindung zu StorageGRID über einen vollständig qualifizierten Domänennamen (FQDN) anstelle einer IP- oder VIP-Adresse herstellen möchten, können Sie DNS-Einträge konfigurieren.

In dieser Tabelle sind die verschiedenen Verbindungsmethoden aufgeführt, mit denen Clients eine Verbindung zu StorageGRID herstellen können, sowie die für den jeweiligen Verbindungstyp verwendeten IP-Adressen und Ports. Wenn Sie bereits Load Balancer-Endpunkte und Hochverfügbarkeitsgruppen (HA-Gruppen) erstellt haben, finden Sie weitere Informationen unter Wo finden Sie IP-Adressen Um diese Werte im Grid-Manager zu finden.

Wo eine Verbindung hergestellt wird	Dienst, mit dem der Client verbunden ist	IP-Adresse	Port
HA-Gruppe	Lastausgleich	Virtuelle IP-Adresse einer HA-Gruppe	Port, der dem Endpunkt des Lastausgleichs zugewiesen ist
Admin-Node	Lastausgleich	IP-Adresse des Admin-Knotens	Port, der dem Endpunkt des Lastausgleichs zugewiesen ist

Wo eine Verbindung hergestellt wird	Dienst, mit dem der Client verbunden ist	IP-Adresse	Port
Gateway-Node	Lastausgleich	IP-Adresse des Gateway-Node	Port, der dem Endpunkt des Lastausgleichs zugewiesen ist
Storage-Node	LDR	IP-Adresse des Speicherknoten	S3-Standard-Ports: • HTTPS: 18082 • HTTP: 18084 Swift-Standardports: • HTTPS: 18083 • HTTP:18085

Beispiel-URLs

Um eine Client-Applikation mit dem Endpunkt Load Balancer einer HA-Gruppe von Gateway Nodes zu verbinden, verwenden Sie eine wie unten gezeigt strukturierte URL:

`https://VIP-of-HA-group:LB-endpoint-port`

Wenn beispielsweise die virtuelle IP-Adresse der HA-Gruppe 192.0.2.5 lautet und die Portnummer des Endpunkts des Load Balancer 10443 lautet, könnte eine Applikation die folgende URL verwenden, um eine Verbindung zum StorageGRID herzustellen:

`https://192.0.2.5:10443`

Wo finden Sie IP-Adressen

1. Melden Sie sich mit einem bei Grid Manager an "Unterstützter Webbrowser".
2. So suchen Sie die IP-Adresse eines Grid-Knotens:
   a. Wählen Sie **KNOTEN**.
   b. Wählen Sie den Admin-Node, Gateway-Node oder Storage-Node aus, mit dem Sie eine Verbindung herstellen möchten.
   c. Wählen Sie die Registerkarte **Übersicht**.
   d. Notieren Sie im Abschnitt Node-Informationen die IP-Adressen für den Node.
   e. Wählen Sie **Mehr anzeigen**, um IPv6-Adressen und Schnittstellen-Zuordnungen anzuzeigen.

      Sie können Verbindungen von Client-Anwendungen zu einer beliebigen IP-Adresse in der Liste herstellen:

      - **Eth0:** Grid Network
      - **Eth1:** Admin-Netzwerk (optional)
      - **Eth2:** Client-Netzwerk (optional)

Wenn ein Admin-Node oder ein Gateway-Node angezeigt wird und dieser in einer Hochverfügbarkeitsgruppe der aktive Node ist, wird auf eth2 die virtuelle IP-Adresse der HA-Gruppe angezeigt.

3. So finden Sie die virtuelle IP-Adresse einer Hochverfügbarkeitsgruppe:
   a. Wählen Sie **CONFIGURATION** > **Network** > **High Availability groups**.
   b. Notieren Sie in der Tabelle die virtuelle IP-Adresse der HA-Gruppe.
4. So finden Sie die Portnummer eines Load Balancer-Endpunkts:
   a. Wählen Sie **CONFIGURATION** > **Network** > **Load Balancer Endpunkte**.
   b. Notieren Sie sich die Portnummer für den zu verwendenden Endpunkt.

   Wenn die Portnummer 80 oder 443 ist, wird der Endpunkt nur auf Gateway-Nodes konfiguriert, da diese Ports auf Admin-Nodes reserviert sind. Alle anderen Ports werden sowohl an Gateway-Knoten als auch an Admin-Nodes konfiguriert.

   c. Wählen Sie den Namen des Endpunkts aus der Tabelle aus.
   d. Bestätigen Sie, dass der **Client-Typ** (S3 oder Swift) mit der Client-Anwendung übereinstimmt, die den Endpunkt verwendet.

Netzwerke und Verbindungen verwalten

Netzwerkeinstellungen konfigurieren: Übersicht

Sie können verschiedene Netzwerkeinstellungen vom Grid Manager konfigurieren, um den Betrieb Ihres StorageGRID Systems zu optimieren.

Konfigurieren Sie die VLAN-Schnittstellen

Das können Sie "Erstellung von Virtual LAN-Schnittstellen (VLAN" Isolieren und partitionieren Sie den Datenverkehr für Sicherheit, Flexibilität und Performance. Jede VLAN-Schnittstelle ist einer oder mehreren übergeordneten Schnittstellen auf Admin-Nodes und Gateway-Nodes zugeordnet. Die VLAN-Schnittstellen können in HA-Gruppen und in Load Balancer Endpunkten eingesetzt werden, um den Client- oder Admin-Datenverkehr nach Applikation oder Mandanten zu trennen.

Richtlinien für die Verkehrsklassifizierung

Verwenden Sie können "Richtlinien zur Verkehrsklassifizierung" Zur Identifizierung und Verarbeitung verschiedener Arten von Netzwerkverkehr, einschließlich des Datenverkehrs in Bezug auf bestimmte Buckets, Mandanten, Client-Subnetze oder Lastausgleichsendpunkte. Diese Richtlinien unterstützen die Begrenzung und das Monitoring des Datenverkehrs.

Richtlinien für StorageGRID-Netzwerke

Mit dem Grid Manager können Sie StorageGRID-Netzwerke und -Verbindungen konfigurieren und verwalten.

Siehe "Konfiguration von S3- und Swift-Client-Verbindungen" Informationen zum Verbinden von S3 oder Swift Clients

Standard-StorageGRID-Netzwerke

Standardmäßig unterstützt StorageGRID drei Netzwerkschnittstellen pro Grid Node. So können Sie das Netzwerk für jeden einzelnen Grid Node so konfigurieren, dass er Ihren Sicherheits- und Zugriffsanforderungen entspricht.

Weitere Informationen zur Netzwerktopologie finden Sie unter "Netzwerkrichtlinien".

Grid-Netzwerk

Erforderlich. Das Grid-Netzwerk wird für den gesamten internen StorageGRID-Datenverkehr verwendet. Das System bietet Konnektivität zwischen allen Nodes im Grid und allen Standorten und Subnetzen.

Admin-Netzwerk

Optional Das Admin-Netzwerk wird in der Regel für die Systemadministration und -Wartung verwendet. Sie kann auch für den Zugriff auf das Client-Protokoll verwendet werden. Das Admin-Netzwerk ist in der Regel ein privates Netzwerk und muss nicht zwischen Standorten routingfähig sein.

Client-Netzwerk

Optional Das Client-Netzwerk ist ein offenes Netzwerk, das normalerweise für den Zugriff auf S3- und Swift-Client-Applikationen verwendet wird, sodass das Grid-Netzwerk isoliert und gesichert werden kann. Das Client-Netzwerk kann mit jedem Subnetz kommunizieren, das über das lokale Gateway erreichbar ist.

Richtlinien

- Jeder StorageGRID Grid Node benötigt für jedes ihm zugewiesene Netzwerk eine dedizierte Netzwerkschnittstelle, eine IP-Adresse, eine Subnetzmaske und ein Gateway.
- Ein Grid-Knoten kann nicht mehr als eine Schnittstelle in einem Netzwerk haben.
- Es wird ein einzelnes Gateway pro Netzwerk und pro Grid-Node unterstützt, das sich im gleichen Subnetz wie der Node befindet. Sie können bei Bedarf komplexere Routing-Lösungen im Gateway implementieren.
- Auf jedem Node ist jedes Netzwerk einer bestimmten Netzwerkschnittstelle zugeordnet.

Netzwerk	Schnittstellenname
Raster	Eth0
Admin (optional)	Eth1
Client (optional)	Eth2

- Wenn der Node mit einer StorageGRID Appliance verbunden ist, werden für jedes Netzwerk bestimmte Ports verwendet. Weitere Informationen finden Sie in den Installationsanweisungen für Ihr Gerät.
- Die Standardroute wird automatisch pro Knoten generiert. Wenn eth2 aktiviert ist, verwendet 0.0.0.0/0 das Client-Netzwerk auf eth2. Wenn eth2 nicht aktiviert ist, verwendet 0.0.0.0/0 das Grid-Netzwerk auf eth0.
- Das Client-Netzwerk ist erst betriebsbereit, wenn der Grid-Node dem Grid beigetreten ist
- Das Admin-Netzwerk kann während der Bereitstellung des Grid-Knotens konfiguriert werden, um den Zugriff auf die Installations-Benutzeroberfläche zu ermöglichen, bevor das Grid vollständig installiert ist.

Optionale Schnittstellen

Optional können Sie einem Node zusätzliche Schnittstellen hinzufügen. Beispielsweise möchten Sie einem Admin- oder Gateway-Node eine Trunk-Schnittstelle hinzufügen, sodass Sie verwenden können "VLAN-Schnittstellen" Zur Trennung des Datenverkehrs von unterschiedlichen Applikationen oder Mandanten. Oder Sie möchten möglicherweise eine Zugriffsschnittstelle hinzufügen, die in A verwendet werden soll "Hochverfügbarkeitsgruppe (High Availability Group, HA-Gruppe".

Informationen zum Hinzufügen von Trunk- oder Access-Schnittstellen finden Sie unter:

- **VMware (nach der Installation des Knotens)**: "VMware: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node"
  - **RHEL oder CentOS (vor dem Installieren des Knotens)**: "Erstellen von Node-Konfigurationsdateien"
  - **Ubuntu oder Debian (vor der Installation des Knotens)**: "Erstellen von Node-Konfigurationsdateien"
  - **RHEL, CentOS, Ubuntu oder Debian (nach der Installation des Knotens)**: "Linux: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node"

Zeigen Sie IP-Adressen an

Sie können die IP-Adresse für jeden Grid-Node im StorageGRID System anzeigen. Sie können sich dann mithilfe dieser IP-Adresse am Grid Node an der Befehlszeile anmelden und verschiedene Wartungsverfahren durchführen.

Bevor Sie beginnen

Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".

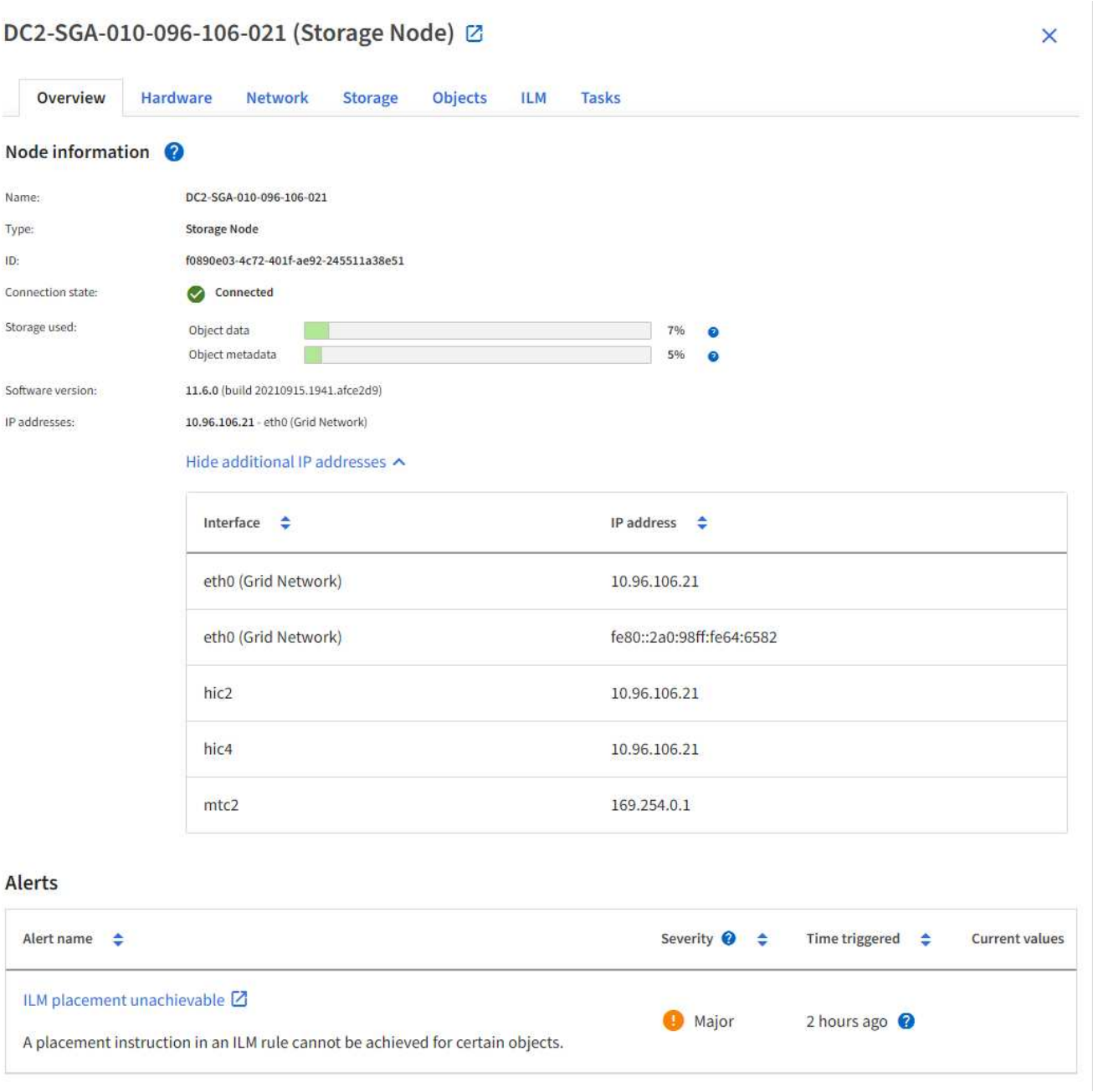
Über diese Aufgabe

Informationen zum Ändern von IP-Adressen finden Sie unter "Konfigurieren Sie IP-Adressen".

Schritte

1. Wählen Sie **NODES** > ***Grid Node*** > **Übersicht** aus.
2. Wählen Sie **Mehr anzeigen** rechts neben dem Titel der IP-Adressen.

   Die IP-Adressen für diesen Grid-Node werden in einer Tabelle aufgeführt.



Unterstützte Chiffren für ausgehende TLS-Verbindungen

Das StorageGRID System unterstützt eine begrenzte Anzahl von Verschlüsselungssuiten für TLS-Verbindungen (Transport Layer Security) zu den externen Systemen, die für Identitätsföderation und Cloud-Storage-Pools verwendet werden.

Unterstützte Versionen von TLS

StorageGRID unterstützt TLS 1.2 und TLS 1.3 für Verbindungen zu externen Systemen, die für Identitätsföderation und Cloud-Storage-Pools verwendet werden.

Die zur Verwendung mit externen Systemen unterstützten TLS-Chiffren wurden ausgewählt, um die Kompatibilität mit verschiedenen externen Systemen sicherzustellen. Die Liste ist größer als die Liste der Chiffren, die zur Verwendung mit S3- oder Swift-Client-Applikationen unterstützt werden. Um Chiffren zu konfigurieren, gehen Sie zu **CONFIGURATION** > **Security** > **Security settings** und wählen **TLS und SSH**

Policies aus.

> TLS-Konfigurationsoptionen wie Protokollversionen, Chiffren, Schlüsselaustauschalgorithmen und MAC-Algorithmen sind in StorageGRID nicht konfigurierbar. Wenden Sie sich an Ihren NetApp Ansprechpartner, wenn Sie spezifische Anfragen zu diesen Einstellungen haben.

Konfigurieren Sie die VLAN-Schnittstellen

Sie können virtuelle LAN-Schnittstellen (VLAN) auf Admin-Nodes und Gateway-Nodes erstellen und diese in HA-Gruppen und Load Balancer-Endpunkten verwenden, um den Datenverkehr für Sicherheit, Flexibilität und Performance zu isolieren und zu partitionieren.

Überlegungen zu VLAN-Schnittstellen

- Sie erstellen eine VLAN-Schnittstelle, indem Sie eine VLAN-ID eingeben und eine übergeordnete Schnittstelle auf einem oder mehreren Nodes auswählen.
- Eine übergeordnete Schnittstelle muss als Trunk-Schnittstelle am Switch konfiguriert sein.
- Eine übergeordnete Schnittstelle kann das Grid-Netzwerk (eth0), das Client-Netzwerk (eth2) oder eine zusätzliche Trunk-Schnittstelle für die VM oder Bare-Metal-Host (z. B. ens256) sein.
- Sie können für jede VLAN-Schnittstelle nur eine übergeordnete Schnittstelle für einen bestimmten Node auswählen. Beispielsweise können Sie nicht sowohl die Grid-Netzwerkschnittstelle als auch die Client-Netzwerkschnittstelle auf demselben Gateway-Node wie die übergeordnete Schnittstelle für dasselbe VLAN verwenden.
- Wenn die VLAN-Schnittstelle für den Admin-Node-Datenverkehr dient, der Datenverkehr zum Grid-Manager und dem Mandanten-Manager enthält, wählen Sie nur Schnittstellen auf Admin-Nodes aus.
- Wenn die VLAN-Schnittstelle für S3- oder Swift-Client-Datenverkehr dient, wählen Sie Schnittstellen entweder auf Admin-Nodes oder Gateway-Nodes aus.
- Wenn Sie Leitungsbündelschnittstellen hinzufügen müssen, lesen Sie die folgenden Informationen:
  - **VMware (nach der Installation des Knotens)**: "VMware: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node"
  - **RHEL oder CentOS (vor dem Installieren des Knotens)**: "Erstellen von Node-Konfigurationsdateien"
  - **Ubuntu oder Debian (vor der Installation des Knotens)**: "Erstellen von Node-Konfigurationsdateien"
  - **RHEL, CentOS, Ubuntu oder Debian (nach der Installation des Knotens)**: "Linux: Hinzufügen von Trunk- oder Zugriffsschnittstellen zu einem Node"

Erstellen einer VLAN-Schnittstelle

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die Root-Zugriffsberechtigung.
- Im Netzwerk wurde eine Trunk-Schnittstelle konfiguriert und mit dem VM- oder Linux-Node verbunden. Sie kennen den Namen der Trunk-Schnittstelle.
- Sie kennen die ID des zu konfigurierende VLANs.

Über diese Aufgabe

Ihr Netzwerkadministrator hat möglicherweise eine oder mehrere Trunk-Schnittstellen und ein oder mehrere

VLANs konfiguriert, um den Client- oder Admin-Datenverkehr verschiedener Applikationen oder Mandanten zu trennen. Jedes VLAN wird durch eine numerische ID oder ein Tag identifiziert. Beispielsweise könnte Ihr Netzwerk VLAN 100 für FabricPool-Datenverkehr und VLAN 200 für eine Archivierungsanwendung verwenden.

Sie können den Grid-Manager verwenden, um VLAN-Schnittstellen zu erstellen, die Clients den Zugriff auf StorageGRID in einem bestimmten VLAN ermöglichen. Wenn Sie VLAN-Schnittstellen erstellen, geben Sie die VLAN-ID an und wählen Sie übergeordnete Schnittstellen (Trunk) auf einem oder mehreren Nodes aus.

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **VLAN-Schnittstellen**.
2. Wählen Sie **Erstellen**.

Geben Sie Details zu den VLAN-Schnittstellen ein

Schritte

1. Geben Sie die ID des VLANs in Ihrem Netzwerk an. Sie können einen beliebigen Wert zwischen 1 und 4094 eingeben.

   VLAN-IDs müssen nicht eindeutig sein. Beispielsweise können Sie die VLAN-ID 200 für den Admin-Datenverkehr an einem Standort und dieselbe VLAN-ID für den Client-Datenverkehr an einem anderen Standort verwenden. Sie können separate VLAN-Schnittstellen mit verschiedenen Gruppen von übergeordneten Schnittstellen an jedem Standort erstellen. Zwei VLAN-Schnittstellen mit derselben ID können jedoch nicht dieselbe Schnittstelle auf einem Node gemeinsam nutzen. Wenn Sie eine ID angeben, die bereits verwendet wurde, wird eine Meldung angezeigt.

2. Geben Sie optional eine kurze Beschreibung für die VLAN-Schnittstelle ein.
3. Wählen Sie **Weiter**.

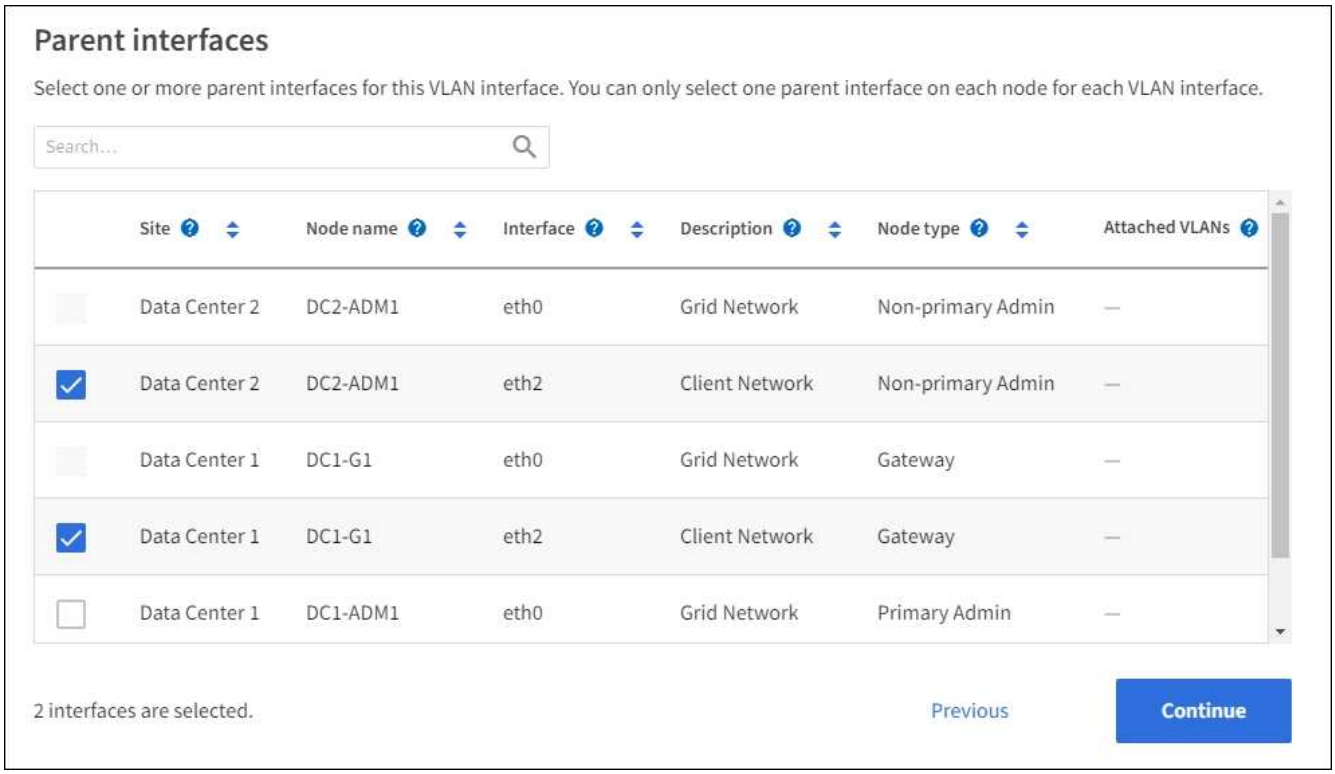
Wählen Sie übergeordnete Schnittstellen

In der Tabelle sind die verfügbaren Schnittstellen für alle Admin-Nodes und Gateway-Nodes an jedem Standort im Raster aufgeführt. Schnittstellen des Admin-Netzwerks (eth1) können nicht als übergeordnete Schnittstellen verwendet werden und werden nicht angezeigt.

Schritte

1. Wählen Sie eine oder mehrere übergeordnete Schnittstellen aus, an die dieses VLAN angeschlossen werden soll.

   Sie möchten beispielsweise ein VLAN an die Schnittstelle „Client Network“ (eth2) für einen Gateway-Node und einen Admin-Node anschließen.



2. Wählen Sie **Weiter**.

Bestätigen Sie die Einstellungen

Schritte

1. Überprüfen Sie die Konfiguration und nehmen Sie alle Änderungen vor.
   - Wenn Sie die VLAN-ID oder Beschreibung ändern möchten, wählen Sie oben auf der Seite **VLAN-Details eingeben** aus.
   - Wenn Sie eine übergeordnete Schnittstelle ändern möchten, wählen Sie oben auf der Seite die Option **übergeordnete Schnittstellen auswählen** aus, oder wählen Sie **Zurück**.
   - Wenn Sie eine übergeordnete Schnittstelle entfernen müssen, wählen Sie den Papierkorb aus .
2. Wählen Sie **Speichern**.
3. Warten Sie bis zu 5 Minuten, bis die neue Schnittstelle auf der Seite Hochverfügbarkeitsgruppen als Auswahl angezeigt wird und in der Tabelle **Netzwerkschnittstellen** für den Knoten (**NODES** > ***Parent Interface Node*** > **Network**) aufgelistet wird.

Bearbeiten Sie eine VLAN-Schnittstelle

Wenn Sie eine VLAN-Schnittstelle bearbeiten, können Sie die folgenden Arten von Änderungen vornehmen:

- Ändern Sie die VLAN-ID oder -Beschreibung.
- Übergeordnete Schnittstellen hinzufügen oder entfernen.

Sie möchten beispielsweise eine übergeordnete Schnittstelle von einer VLAN-Schnittstelle entfernen, wenn Sie den zugeordneten Node außer Betrieb setzen möchten.

Beachten Sie Folgendes:

- Sie können keine VLAN-ID ändern, wenn die VLAN-Schnittstelle in einer HA-Gruppe verwendet wird.
- Sie können eine übergeordnete Schnittstelle nicht entfernen, wenn diese übergeordnete Schnittstelle in einer HA-Gruppe verwendet wird.

  Nehmen Sie beispielsweise an, dass VLAN 200 an den übergeordneten Schnittstellen auf den Nodes A und B. angeschlossen ist Wenn eine HA-Gruppe die VLAN 200-Schnittstelle für Node A und die eth2-Schnittstelle für Node B verwendet, können Sie die nicht verwendete übergeordnete Schnittstelle für Node B entfernen, Sie können jedoch die verwendete übergeordnete Schnittstelle für Node A nicht entfernen

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **VLAN-Schnittstellen**.
2. Aktivieren Sie das Kontrollkästchen für die VLAN-Schnittstelle, die Sie bearbeiten möchten. Wählen Sie dann **Aktionen** > **Bearbeiten** aus.
3. Optional können Sie die VLAN-ID oder die Beschreibung aktualisieren. Wählen Sie anschließend **Weiter**.

   Sie können keine VLAN-ID aktualisieren, wenn das VLAN in einer HA-Gruppe verwendet wird.

4. Aktivieren oder deaktivieren Sie optional die Kontrollkästchen, um übergeordnete Schnittstellen hinzuzufügen oder nicht verwendete Schnittstellen zu entfernen. Wählen Sie anschließend **Weiter**.
5. Überprüfen Sie die Konfiguration und nehmen Sie alle Änderungen vor.
6. Wählen Sie **Speichern**.

Entfernen Sie eine VLAN-Schnittstelle

Sie können eine oder mehrere VLAN-Schnittstellen entfernen.

Sie können eine VLAN-Schnittstelle nicht entfernen, wenn sie derzeit in einer HA-Gruppe verwendet wird. Sie müssen die VLAN-Schnittstelle aus der HA-Gruppe entfernen, bevor Sie sie entfernen können.

Um Unterbrechungen des Client-Traffic zu vermeiden, sollten Sie einen der folgenden Schritte in Betracht ziehen:

- Fügen Sie einer neuen VLAN-Schnittstelle zur HA-Gruppe hinzu, bevor Sie diese VLAN-Schnittstelle entfernen.
- Erstellen Sie eine neue HA-Gruppe, die diese VLAN-Schnittstelle nicht verwendet.
- Wenn die VLAN-Schnittstelle, die Sie entfernen möchten, derzeit die aktive Schnittstelle ist, bearbeiten Sie die HA-Gruppe. Verschieben Sie die VLAN-Schnittstelle, die Sie entfernen möchten, auf die Unterseite der Prioritätenliste. Warten Sie, bis die Kommunikation auf der neuen primären Schnittstelle eingerichtet ist, und entfernen Sie dann die alte Schnittstelle aus der HA-Gruppe. Schließlich, löschen Sie die VLAN-Schnittstelle auf diesem Knoten.

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **VLAN-Schnittstellen**.
2. Aktivieren Sie das Kontrollkästchen für jede VLAN-Schnittstelle, die Sie entfernen möchten. Wählen Sie dann **Aktionen** > **Löschen** aus.
3. Wählen Sie **Ja**, um Ihre Auswahl zu bestätigen.

   Alle ausgewählten VLAN-Schnittstellen werden entfernt. Auf der Seite VLAN-Schnittstellen wird ein grünes Erfolgsbanner angezeigt.

Verwalten von Richtlinien zur Verkehrsklassifizierung

Managen von Richtlinien zur Verkehrsklassifizierung: Übersicht

Zur Verbesserung Ihrer QoS-Angebote (Quality of Service) können Sie Richtlinien zur Traffic-Klassifizierung erstellen, um verschiedene Arten von Netzwerkverkehr zu identifizieren und zu überwachen. Diese Richtlinien unterstützen die Begrenzung und das Monitoring des Datenverkehrs.

Richtlinien zur Traffic-Klassifizierung werden auf Endpunkte im StorageGRID Load Balancer Service für Gateway-Knoten und Admin-Nodes angewendet. Zum Erstellen von Richtlinien für die Verkehrsklassifizierung müssen Sie bereits Load Balancer Endpunkte erstellt haben.

Übereinstimmungsregeln

Jede Traffic-Klassifizierungsrichtlinie enthält mindestens eine übereinstimmende Regel, um den Netzwerkverkehr zu identifizieren, der mit einer oder mehreren der folgenden Einheiten in Verbindung steht:

- Buckets
- Subnetz
- Mandant
- Load Balancer-Endpunkte

StorageGRID überwacht den Datenverkehr, der mit allen Regeln innerhalb der Richtlinie im Einklang mit den Zielen der Regel steht. Jeder Traffic, der einer Richtlinie entspricht, wird von dieser Richtlinie übernommen. Umgekehrt können Sie Regeln festlegen, die mit dem gesamten Verkehr übereinstimmen, außer einer angegebenen Einheit.

Traffic-Beschränkung

Optional können Sie einer Richtlinie die folgenden Begrenzungstypen hinzufügen:

- Aggregatbandbreite
- Bandbreite pro Anforderung
- Gleichzeitige Anfragen
- Anforderungsrate

Grenzwerte werden pro Load Balancer erzwungen. Wenn der Datenverkehr gleichzeitig auf mehrere Load Balancer verteilt wird, sind die maximalen Raten ein Vielfaches der von Ihnen angegebenen Ratenlimits.

> Sie können Richtlinien erstellen, um die aggregierte Bandbreite zu begrenzen oder die Bandbreite nach Bedarf zu begrenzen. StorageGRID kann jedoch nicht beide Bandbreitenarten gleichzeitig einschränken. Eine Einschränkung der Bandbreite im Aggregat kann eine zusätzliche geringfügige Auswirkung auf die Performance des nicht begrenzten Datenverkehrs haben.

Bei Bandbreitenbeschränkungen oder -Anforderungen werden die Anforderungen mit der von Ihnen festgelegten Rate in- oder Out-Streaming übertragen. StorageGRID kann nur eine Geschwindigkeit erzwingen. Daher ist die jeweils spezifischste Richtlinienabgleiche nach Matcher-Typ erzwungen. Die von der Anforderung verbrauchte Bandbreite wird nicht mit anderen weniger spezifischen übereinstimmenden Richtlinien verglichen, die Richtlinien zur Gesamtbandbreite enthalten. Bei allen anderen Grenzwerttypen werden

Clientanforderungen um 250 Millisekunden verzögert und bei Anfragen, die die übereinstimmende Richtlinienbegrenzung überschreiten, eine langsame Antwort von 503 erhalten.

Im Grid Manager können Sie Traffic-Diagramme anzeigen und überprüfen, ob die Richtlinien die von Ihnen erwarteten Verkehrsgrenzen durchsetzen.

Richtlinien für die Verkehrsklassifizierung mit SLAs

Sie können Richtlinien für die Traffic-Klassifizierung in Verbindung mit Kapazitätsgrenzen und Datensicherung verwenden, um Service Level Agreements (SLAs) durchzusetzen, die Besonderheiten bei Kapazität, Datensicherung und Performance bieten.

Das folgende Beispiel zeigt drei SLA-Tiers. Sie können Traffic-Klassifizierungsrichtlinien erstellen, um die Performance-Ziele jeder SLA-Ebene zu erreichen.

Service Level-Ebene	Kapazität	Datensicherung	Maximal zulässige Leistung	Kosten
Gold	1 PB Speicherplatz zulässig	3 ILM-Regel für Kopien	25 K Anfragen/Sek. 5 GB/s (40 Gbit/s) Bandbreite	Kosten pro Monat
Silber	250 TB Speicherplatz zulässig	ILM-Regel für 2 Kopien	10 K Anfragen/Sek. 1.25 GB/s (10 Gbit/s) Bandbreite	Kosten pro Monat
Bronze	100 TB Speicherplatz zulässig	ILM-Regel für 2 Kopien	5 K Anfragen/Sek. 1 GB/s (8 Gbit/s) Bandbreite	Kosten pro Monat

Richtlinien für die Verkehrsklassifizierung erstellen

Sie können Richtlinien zur Verkehrsklassifizierung erstellen, wenn Sie den Netzwerk-Traffic nach Bucket, Bucket-Regex, CIDR, Load-Balancer-Endpunkt oder Mandant überwachen und optional begrenzen möchten. Optional können Sie Obergrenzen für eine Richtlinie basierend auf der Bandbreite, der Anzahl gleichzeitiger Anfragen oder der Anfragerate festlegen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die Root-Zugriffsberechtigung.
- Sie haben alle Load Balancer-Endpunkte erstellt, die übereinstimmen sollen.
- Sie haben alle Mandanten erstellt, denen Sie entsprechen möchten.

Schritte

1. Wählen Sie **CONFIGURATION** > **Network** > **traffic classification**.
2. Wählen Sie **Erstellen**.

3. Geben Sie einen Namen und eine Beschreibung (optional) für die Richtlinie ein und wählen Sie **Weiter**.

   Beschreiben Sie beispielsweise, auf welche Weise diese Richtlinie zur Klassifizierung von Verkehrsdaten zutrifft und welche Begrenzung sie hat.

4. Wählen Sie **Regel hinzufügen** und geben Sie die folgenden Details an, um eine oder mehrere übereinstimmende Regeln für die Richtlinie zu erstellen. Jede Richtlinie, die Sie erstellen, sollte mindestens eine übereinstimmende Regel haben. Wählen Sie **Weiter**.

Feld	Beschreibung
Typ	Wählen Sie die Verkehrstypen aus, für die die entsprechende Regel gilt. Traffic-Typen sind Bucket, Bucket-Regex, CIDR, Load Balancer-Endpunkt und Mandant.
Match-Wert	Geben Sie den Wert ein, der dem ausgewählten Typ entspricht. • Bucket: Geben Sie einen oder mehrere Bucket-Namen ein. • Bucket-regex: Geben Sie einen oder mehrere reguläre Ausdrücke ein, die für einen Satz von Bucket-Namen verwendet werden. Der reguläre Ausdruck ist nicht verankert. Verwenden Sie den Anker ^, um am Anfang des Bucket-Namens zu übereinstimmen, und verwenden Sie den Anker €, um am Ende des Namens zu übereinstimmen. Die Übereinstimmung mit regulären Ausdrücken unterstützt eine Teilmenge der PCRE-Syntax (Perl Compatible Regular Expression). • CIDR: Geben Sie ein oder mehrere IPv4-Subnetze in CIDR-Notation ein, die mit dem gewünschten Subnetz übereinstimmen. • Load-Balancer-Endpunkt: Wählen Sie einen Endpunktnamen aus. Dies sind die Lastausgleichsendpunkte, die Sie auf dem definiert haben "Konfigurieren von Load Balancer-Endpunkten". • Tenant: Tenant Matching verwendet die Zugriffsschlüssel-ID. Wenn die Anforderung keine Zugriffsschlüssel-ID enthält (z. B. anonymer Zugriff), wird die Eigentümerschaft des abgerufenen Buckets verwendet, um den Mandanten zu bestimmen.
Umgekehrtes Match	Wenn Sie den gesamten Netzwerkverkehr *except* mit dem gerade definierten Typ und Match-Wert abstimmen möchten, aktivieren Sie das Kontrollkästchen **inverse Übereinstimmung**. Andernfalls lassen Sie das Kontrollkästchen deaktiviert. Wenn Sie beispielsweise möchten, dass diese Richtlinie auf alle Endpunkte mit Ausnahme eines Lastausgleichs angewendet wird, geben Sie den auszuschließenden Lastausgleichsendpunkt an, und wählen Sie **inverse Übereinstimmung** aus. Bei einer Richtlinie, die mehrere Matriken enthält, bei denen mindestens eine inverse Matrix ist, sollten Sie darauf achten, keine Richtlinie zu erstellen, die allen Anforderungen entspricht.

5. Wählen Sie optional **Limit hinzufügen** und wählen Sie die folgenden Details aus, um eine oder mehrere

Grenzwerte hinzuzufügen, um den Netzwerkverkehr zu steuern, der von einer Regel abgeglichen wird.

StorageGRID sammelt Kennzahlen, auch wenn Sie keine Limits hinzufügen, sodass Sie Verkehrstrends besser verstehen können.

Feld	Beschreibung
Typ	Die Art der Begrenzung, die auf den Netzwerkverkehr angewendet werden soll, der der Regel entspricht. Beispielsweise können Sie die Bandbreite oder die Anforderungsrate begrenzen. **Hinweis**: Sie können Richtlinien erstellen, um die Gesamtbandbreite zu begrenzen oder die Bandbreite pro Anfrage zu begrenzen. StorageGRID kann jedoch nicht beide Bandbreitenarten gleichzeitig einschränken. Wenn die aggregierte Bandbreite verwendet wird, ist die Bandbreite pro Anforderung nicht verfügbar. Umgekehrt ist die aggregierte Bandbreite nicht verfügbar, wenn die Bandbreite pro Anforderung verwendet wird. Eine Einschränkung der Bandbreite im Aggregat kann eine zusätzliche geringfügige Auswirkung auf die Performance des nicht begrenzten Datenverkehrs haben. Bei Bandbreitenbeschränkungen wendet StorageGRID die Richtlinie an, die der jeweils festgelegten Grenzwertart am besten entspricht. Wenn Sie beispielsweise eine Richtlinie haben, die Datenverkehr in nur eine Richtung begrenzt, ist der Datenverkehr in die entgegengesetzte Richtung unbegrenzt, selbst wenn der Datenverkehr mit zusätzlichen Richtlinien mit Bandbreitenbeschränkungen übereinstimmt. StorageGRID implementiert die „besten“ Matches für Bandbreitenlimits in der folgenden Reihenfolge: • Exakte IP-Adresse (/32-Maske) • Exakter Bucket-Name • Eimer-Regex • Mandant • Endpunkt • Nicht exakte CIDR-Übereinstimmungen (nicht /32) • Umgekehrte Übereinstimmungen
Gilt für	Gibt an, ob diese Begrenzung auf Client-Leseanforderungen (GET oder HEAD) oder Schreibanforderungen (PUT, POST oder DELETE) zutrifft.
Wert	Der Wert, auf den der Netzwerkverkehr begrenzt wird, abhängig von der ausgewählten Einheit. Geben Sie beispielsweise 10 ein, und wählen Sie MiB/s aus, um zu verhindern, dass der Netzwerkverkehr, der dieser Regel entspricht, 10 MiB/s überschreitet **Hinweis**: Je nach Einstellung der Einheiten sind die verfügbaren Einheiten entweder binär (z. B. gib) oder dezimal (z. B. GB). Um die Einstellung Einheiten zu ändern, wählen Sie oben rechts im Grid-Manager das Dropdown-Menü Benutzer aus, und wählen Sie dann **Benutzereinstellungen** aus.

Feld	Beschreibung
Einheit	Die Einheit, die den eingegebenen Wert beschreibt.

Wenn Sie beispielsweise eine Bandbreitenbegrenzung von 40 GB/s für eine SLA-Ebene erstellen möchten, erstellen Sie zwei aggregierte Bandbreitenlimits: GET/HEAD bei 40 GB/s und PUT/POST/DELETE bei 40 GB/s.

6. Wählen Sie **Weiter**.
7. Lesen und prüfen Sie die Richtlinie zur Verkehrsklassifizierung. Verwenden Sie die Schaltfläche * Zurück*, um zurückzugehen und Änderungen vorzunehmen. Wenn Sie mit der Richtlinie zufrieden sind, wählen Sie **Speichern und fortfahren**.

   Der S3- und Swift-Client-Traffic wird nun gemäß der Traffic-Klassifizierungsrichtlinie behandelt.

Nachdem Sie fertig sind

"Zeigen Sie Metriken zum Netzwerkverkehr an" Um zu überprüfen, ob die Richtlinien die von Ihnen erwarteten Verkehrsgrenzwerte durchsetzen.

Richtlinie zur Verkehrsklassifizierung bearbeiten

Sie können eine Traffic-Klassifizierungsrichtlinie bearbeiten, um ihren Namen oder ihre Beschreibung zu ändern oder um Regeln oder Grenzen für die Richtlinie zu erstellen, zu bearbeiten oder zu löschen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die Root-Zugriffsberechtigung.

Schritte

1. Wählen Sie **CONFIGURATION** > **Network** > **traffic classification**.

   Die Seite für die Verkehrsklassifizierungsrichtlinien wird angezeigt, und die vorhandenen Richtlinien werden in einer Tabelle aufgeführt.

2. Bearbeiten Sie die Richtlinie über das Menü Aktionen oder die Detailseite. Siehe "Erstellen von Richtlinien zur Verkehrsklassifizierung" Für das, was zu betreten ist.

   Menü „Aktionen“

   a. Aktivieren Sie das Kontrollkästchen für die Richtlinie.

   b. Wählen Sie **Actions** > **Edit**.

   Detailseite

   a. Wählen Sie den Richtliniennamen aus.

   b. Klicken Sie neben dem Richtliniennamen auf die Schaltfläche **Bearbeiten**.

3. Bearbeiten Sie für den Schritt Richtliniennamen eingeben optional den Richtliniennamen oder die Beschreibung, und wählen Sie **Weiter** aus.

4. Fügen Sie für den Schritt übereinstimmende Regeln hinzufügen optional eine Regel hinzu oder bearbeiten Sie die Werte **Typ** und **Match** der bestehenden Regel und wählen Sie **Weiter**.
5. Für den Schritt Grenzen festlegen können Sie optional ein Limit hinzufügen, bearbeiten oder löschen und dann **Weiter** auswählen.
6. Überprüfen Sie die aktualisierte Richtlinie, und wählen Sie **Speichern und fortfahren**.

   Die an der Richtlinie vorgenommenen Änderungen werden gespeichert, und der Netzwerkverkehr wird nun gemäß den Richtlinien zur Klassifizierung von Verkehrsmeldungen verarbeitet. Sie können Verkehrsdiagramme anzeigen und überprüfen, ob die Richtlinien die von Ihnen erwarteten Verkehrsgrenzwerte durchsetzen.

Löschen einer Traffic-Klassifizierungsrichtlinie

Sie können eine Verkehrsklassifizierungsrichtlinie löschen, wenn Sie sie nicht mehr benötigen. Achten Sie darauf, die richtige Richtlinie zu löschen, da eine Richtlinie beim Löschen nicht abgerufen werden kann.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die Root-Zugriffsberechtigung.

Schritte

1. Wählen Sie **CONFIGURATION** > **Network** > **traffic classification**.

   Die Seite für die Verkehrsklassifizierungsrichtlinien wird mit den vorhandenen Richtlinien in einer Tabelle angezeigt.

2. Löschen Sie die Richtlinie über das Menü Aktionen oder die Detailseite.

   Menü „Aktionen“

   a. Aktivieren Sie das Kontrollkästchen für die Richtlinie.
   b. Wählen Sie **Aktionen** > **Entfernen**.

   Seite mit den Details der Richtlinie

   a. Wählen Sie den Richtliniennamen aus.
   b. Klicken Sie neben dem Richtliniennamen auf die Schaltfläche **Entfernen**.

3. Wählen Sie **Ja**, um zu bestätigen, dass Sie die Richtlinie löschen möchten.

   Die Richtlinie wird gelöscht.

Zeigen Sie Metriken zum Netzwerkverkehr an

Sie können den Netzwerkverkehr überwachen, indem Sie die Diagramme anzeigen, die auf der Seite für die Verkehrsklassifizierungsrichtlinien verfügbar sind.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie verfügen über die Root-Zugriffsberechtigung oder die Berechtigung für die Mandantenkonten.

Über diese Aufgabe

Für alle vorhandenen Richtlinien zur Verkehrsklassifizierung können Sie Metriken für den Load Balancer-Dienst anzeigen, um zu ermitteln, ob die Richtlinie den Datenverkehr im Netzwerk erfolgreich einschränkt. Anhand der Daten in den Diagrammen können Sie feststellen, ob Sie die Richtlinie anpassen müssen.

Auch wenn für eine Richtlinie zur Klassifizierung von Datenverkehr keine Grenzen gesetzt wurden, werden Kennzahlen erfasst und die Diagramme bieten nützliche Informationen zum Verständnis von Verkehrstrends.

Schritte

1. Wählen Sie **CONFIGURATION** > **Network** > **traffic classification**.

   Die Seite für die Verkehrsklassifizierungsrichtlinien wird angezeigt, und die vorhandenen Richtlinien werden in der Tabelle aufgeführt.

2. Wählen Sie den Richtliniennamen für die Verkehrsklassifizierung aus, für den Sie Metriken anzeigen möchten.
3. Wählen Sie die Registerkarte **Metriken**.

   Die Richtliniendiagramme für die Verkehrsklassifizierung werden angezeigt. Die Diagramme zeigen Metriken nur für den Datenverkehr an, der mit der ausgewählten Richtlinie übereinstimmt.

   Die folgenden Diagramme sind auf der Seite enthalten.

   - Anforderungsrate: Dieses Diagramm zeigt die Bandbreite an, die dieser Richtlinie entspricht, die von allen Load Balancern verarbeitet wird. Die empfangenen Daten umfassen Anforderungskopfzeilen für alle Anfragen und die Körperdatengröße für Antworten mit Körperdaten. „Gesendet“ enthält Antwortkopfzeilen für alle Anfragen und die Größe der Antwortkörperdaten für Anforderungen, die Körperdaten in die Antwort einschließen.

     > Wenn die Anforderungen abgeschlossen sind, zeigt dieses Diagramm nur die Bandbreitennutzung an. Bei langsamen oder großen Objektanforderungen kann die tatsächliche unmittelbare Bandbreite von den in diesem Diagramm gemeldeten Werten abweichen.

   - Fehlerreaktionsrate: Dieses Diagramm bietet eine ungefähre Rate, mit der Anfragen, die dieser Richtlinie entsprechen, Fehler (HTTP-Statuscode >= 400) an Clients zurückgeben.
   - Durchschnittliche Anforderungsdauer (kein Fehler): Diese Grafik bietet eine durchschnittliche Dauer erfolgreicher Anfragen, die dieser Richtlinie entsprechen.
   - Verwendung der Richtlinienbandbreite: Dieses Diagramm gibt die Bandbreite an, die dieser Richtlinie entspricht, die von allen Lastverteilern verarbeitet wird. Die empfangenen Daten umfassen Anforderungskopfzeilen für alle Anfragen und die Körperdatengröße für Antworten mit Körperdaten. „Gesendet“ enthält Antwortkopfzeilen für alle Anfragen und die Größe der Antwortkörperdaten für Anforderungen, die Körperdaten in die Antwort einschließen.
4. Positionieren Sie den Cursor über einem Liniendiagramm, um ein Popup-Fenster mit Werten für einen bestimmten Teil des Diagramms anzuzeigen.
5. Wählen Sie **Grafana Dashboard** direkt unter dem Metrics-Titel, um alle Diagramme für eine Richtlinie anzuzeigen. Zusätzlich zu den vier Diagrammen aus der Registerkarte **Metriken** können Sie zwei weitere Diagramme anzeigen:

- Schreibanforderungsrate nach Objektgröße: Die Rate für PUT/POST/DELETE-Anfragen, die dieser Richtlinie entsprechen. Die Positionierung auf einer einzelnen Zelle zeigt die Raten pro Sekunde an. Die in der Hover-Ansicht angezeigten Raten werden auf Ganzzahlen gekürzt und können 0 melden, wenn im Bucket Anfragen ohne Null angezeigt werden.
- Leseanforderungsrate nach Objektgröße: Die Rate für GET/HEAD-Anfragen, die dieser Richtlinie entsprechen. Die Positionierung auf einer einzelnen Zelle zeigt die Raten pro Sekunde an. Die in der Hover-Ansicht angezeigten Raten werden auf Ganzzahlen gekürzt und können 0 melden, wenn im Bucket Anfragen ohne Null angezeigt werden.

6. Alternativ können Sie über das Menü * SUPPORT* auf die Diagramme zugreifen.
   a. Wählen Sie **SUPPORT** > **Tools** > **Metriken**.
   b. Wählen Sie im Abschnitt **Grafana** die Option **Richtlinie zur Traffic-Klassifizierung** aus.
   c. Wählen Sie die Richtlinie aus dem Menü oben links auf der Seite aus.
   d. Positionieren Sie den Cursor über einem Diagramm, um ein Popup-Fenster anzuzeigen, in dem Datum und Uhrzeit der Probe, Objektgrößen, die in der Anzahl zusammengefasst werden, und die Anzahl der Anfragen pro Sekunde in diesem Zeitraum angezeigt werden.

      Richtlinien für die Verkehrsklassifizierung werden anhand ihrer ID identifiziert. Richtlinien-IDs werden auf der Seite für die Verkehrsklassifizierungsrichtlinien aufgeführt.

7. Analysieren Sie die Diagramme, um zu ermitteln, wie oft die Richtlinie den Datenverkehr einschränkt und ob Sie die Richtlinie anpassen müssen.

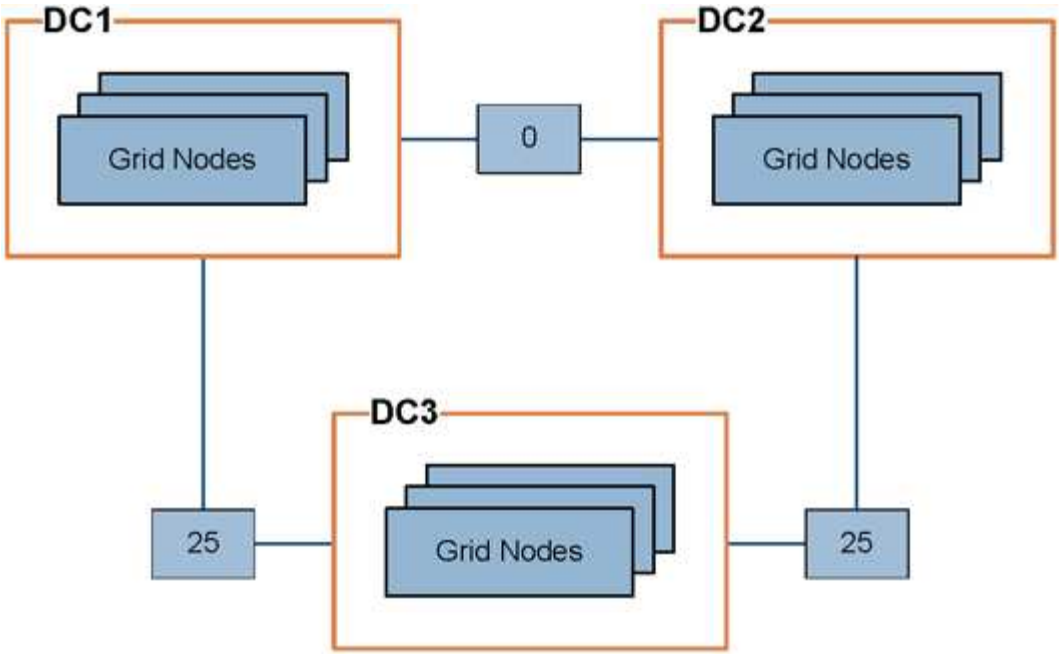
Verwalten Sie Verbindungskosten

Durch die Verbindungskosten können Sie festlegen, welcher Datacenter-Standort einen angeforderten Service bereitstellt, wenn zwei oder mehr Datacenter-Standorte vorhanden sind. Sie können die Verbindungskosten anpassen, um die Latenz zwischen Standorten reflektieren.

Was sind Verbindungskosten?

- Die Link-Kosten werden verwendet, um Prioritäten zu setzen, welche Objektkopie für die Bearbeitung von Objektabrufungen verwendet wird.
- Die Link-Kosten werden von der Grid-Management-API und der Mandanten-Management-API verwendet, um festzustellen, welche internen StorageGRID-Services verwendet werden sollen.
- Verbindungskosten werden vom Load Balancer-Service auf Admin-Nodes und Gateway-Nodes zum direkten Client-Verbindungen verwendet. Siehe "Überlegungen zum Lastausgleich".

Das Diagramm zeigt ein drei Standortraster mit Verbindungskosten, die zwischen Standorten konfiguriert sind:



- Der Load Balancer auf Admin-Nodes und Gateway-Nodes verteilt Client-Verbindungen zu allen Storage-Nodes am selben Datacenter-Standort und zu allen Datacenter-Standorten, für die keine Linkkosten anfallen.

  Im Beispiel verteilt ein Gateway-Node am Datacenter-Standort 1 (DC1) Client-Verbindungen gleichmäßig auf Storage-Nodes an DC1 und Storage Nodes an DC2. Ein Gateway-Node bei DC3 sendet Client-Verbindungen nur zu Storage-Nodes an DC3.

- Beim Abrufen eines Objekts, das als mehrere replizierte Kopien vorhanden ist, ruft StorageGRID die Kopie im Datacenter ab, das die niedrigsten Verbindungskosten bietet.

  Wenn in dem Beispiel eine Client-Anwendung bei DC2 ein Objekt abruft, das sowohl bei DC1 als auch bei DC3 gespeichert ist, wird das Objekt von DC1 abgerufen, da die Verbindungskosten von DC1 zu DC2 0 sind, was niedriger ist als die Verbindungskosten von DC3 zu DC2 (25).

Verbindungskosten sind willkürliche relative Zahlen ohne spezifische Maßeinheit. So werden beispielsweise die Linkkosten von 50 weniger bevorzugt genutzt als eine Linkkosten von 25. In der Tabelle sind die häufig verwendeten Verbindungskosten aufgeführt.

Verlinken	Verbindungskosten	Hinweise
Zwischen physischen Datacenter-Standorten zu wechseln	25 (Standard)	Über WAN-Verbindung verbundene Datacenter.
Zwischen logischen Datacenter-Standorten am selben physischen Standort	0	Logische Rechenzentren befinden sich in demselben physischen Gebäude oder Campus, das über ein LAN verbunden ist.

Verbindungskosten aktualisieren

Sie können die Verbindungskosten zwischen Datacenter-Standorten aktualisieren, um die Latenz zwischen

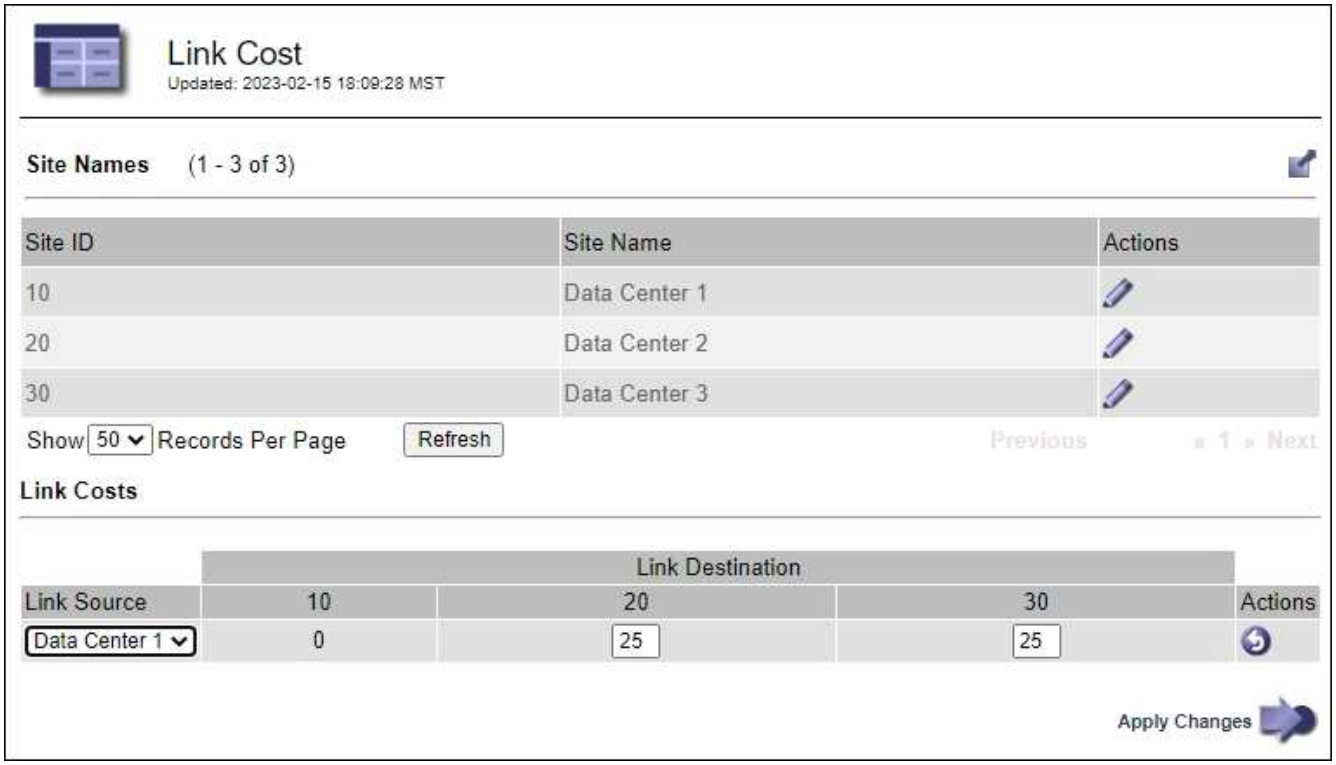
Standorten wiederzugeben.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Berechtigung zur Konfiguration der Grid-Topologie-Seite".

Schritte

1. Wählen Sie **SUPPORT** > **Other** > **Link Cost**.



2. Wählen Sie eine Website unter **Link Source** aus, und geben Sie unter **Link Destination** einen Kostenwert zwischen 0 und 100 ein.

   Sie können die Verbindungskosten nicht ändern, wenn die Quelle mit dem Ziel identisch ist.

   Um Änderungen abzubrechen, wählen Sie „ **Zurücksetzen**.

3. Wählen Sie **Änderungen Anwenden**.

Verwenden Sie AutoSupport

Verwenden Sie AutoSupport: Übersicht

Die AutoSupport-Funktion ermöglicht es Ihrem StorageGRID System, Gesundheits- und Statusmeldungen an den technischen Support zu senden.

Durch den Einsatz von AutoSupport werden die Problembestimmung und -Behebung erheblich beschleunigt. Der technische Support überwacht auch den Storage-Bedarf Ihres Systems und hilft Ihnen dabei zu ermitteln, ob Sie neue Nodes oder Standorte hinzufügen müssen. Optional können Sie AutoSupport Meldungen so konfigurieren, dass sie an ein zusätzliches Ziel gesendet werden.

Sie sollten StorageGRID AutoSupport nur auf dem primären Admin-Knoten konfigurieren. Sie müssen jedoch konfigurieren Hardware-AutoSupport Auf jedem Gerät.

Informationen, die in AutoSupport Meldungen enthalten sind

AutoSupport Meldungen enthalten Informationen, z. B. die folgenden:

- StorageGRID Softwareversion
- Betriebssystemversion
- Attributinformationen auf System- und Standortebene
- Aktuelle Warnmeldungen und Alarme (Altsystem)
- Aktueller Status aller Grid-Aufgaben, einschließlich historischer Daten
- Verwendung der Admin-Node-Datenbank
- Anzahl der verlorenen oder fehlenden Objekte
- Grid-Konfigurationseinstellungen
- NMS-Einheiten
- Aktive ILM-Richtlinie
- Bereitgestellte Grid-Spezifikations-Datei
- Diagnostische Metriken

Sie können die AutoSupport-Funktion und die einzelnen AutoSupport-Optionen bei der Erstinstallation von StorageGRID aktivieren oder später aktivieren. Wenn AutoSupport nicht aktiviert ist, wird im Grid Manager-Dashboard eine Meldung angezeigt. Die Meldung enthält einen Link zur AutoSupport-Konfigurationsseite.

Wenn Sie die Nachricht schließen, wird sie erst wieder angezeigt, wenn Ihr Browser-Cache gelöscht wird, auch wenn AutoSupport deaktiviert bleibt.

Was ist Digital Advisor?

Digital Advisor ist Cloud-basiert und nutzt prädiktive Analysen und Community-Wissen der installierten Basis von NetApp. Kontinuierliche Risikobewertungen, prädiktive Warnungen, beschreibende Tipps und automatisierte Aktionen helfen Ihnen, Probleme zu vermeiden, bevor sie auftreten. Dies führt zu verbesserter Systemintegrität und höherer Systemverfügbarkeit.

Sie müssen AutoSupport aktivieren, wenn Sie die Digital Advisor Dashboards und Funktionen auf der NetApp Support-Website verwenden möchten.

"Digital Advisor-Dokumentation"

Protokolle zum Senden von AutoSupport Meldungen

Sie können eines von drei Protokollen zum Senden von AutoSupport Meldungen wählen:

- HTTPS

- HTTP
- SMTP

Wenn Sie SMTP als Protokoll für AutoSupport-Meldungen verwenden, müssen Sie einen SMTP-Mail-Server konfigurieren.

AutoSupport-Optionen

Sie können eine beliebige Kombination der folgenden Optionen verwenden, um AutoSupport Meldungen an den technischen Support zu senden:

- **Wöchentlich**: Senden Sie automatisch einmal pro Woche AutoSupport-Nachrichten. Standardeinstellung: Aktiviert.
- **Event-triggered**: Sendet automatisch AutoSupport jede Stunde oder wenn wichtige Systemereignisse auftreten. Standardeinstellung: Aktiviert.
- **Auf Anfrage**: Technischen Support erlauben, um zu verlangen, dass Ihr StorageGRID-System AutoSupport-Nachrichten automatisch sendet, was nützlich ist, wenn sie aktiv an einem Problem arbeiten (erfordert HTTPS AutoSupport Übertragungsprotokoll). Standardeinstellung: Deaktiviert.
- **Vom Benutzer ausgelöst**: Senden Sie AutoSupport-Nachrichten jederzeit manuell.

AutoSupport für Appliances

AutoSupport für Appliances meldet StorageGRID-Hardwareprobleme, während StorageGRID AutoSupport StorageGRID-Softwareprobleme meldet (mit Ausnahme von SGF6112, bei denen StorageGRID AutoSupport sowohl Hardware- als auch Softwareprobleme meldet). Sie müssen AutoSupport auf jeder Appliance konfigurieren, mit Ausnahme der SGF6112, für die keine zusätzliche Konfiguration erforderlich ist. AutoSupport wird für Services und Storage Appliances unterschiedlich implementiert.

Sie müssen AutoSupport in SANtricity für jede Storage Appliance aktivieren. Sie können SANtricity AutoSupport während der ersten Appliance-Einrichtung oder nach der Installation einer Appliance konfigurieren:

- Für SG6000 und SG5700 Appliances, "Konfigurieren Sie AutoSupport in SANtricity System Manager"

AutoSupport Meldungen von E-Series Appliances können in StorageGRID AutoSupport enthalten sein, wenn Sie die AutoSupport-Bereitstellung als Proxy in konfigurieren "SANtricity System Manager".

StorageGRID AutoSupport meldet keine Hardwareprobleme, z. B. DIMM- oder HIC-Fehler (Host Interface Card). Einige Komponentenfehler können jedoch ausgelöst werden "Warnmeldungen zu Hardware". Bei StorageGRID Appliances mit einem Baseboard Management Controller (BMC) wie SG100, SG1000, SG6060 oder SGF6024 können Sie E-Mail- und SNMP-Traps konfigurieren, um Hardwareausfälle zu melden:

- "Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein"
- "Konfigurieren Sie die SNMP-Einstellungen" Für den SG6000-CN Controller oder die Service Appliances SG100 und SG1000

Verwandte Informationen

"NetApp Support"

Konfigurieren Sie AutoSupport

Sie können die AutoSupport-Funktion und die einzelnen AutoSupport-Optionen bei der

Erstinstallation von StorageGRID aktivieren oder später aktivieren.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die Berechtigung Root-Zugriff oder andere Grid-Konfigurationen.
- Wenn Sie HTTPS zum Senden von AutoSupport-Nachrichten verwenden, haben Sie den ausgehenden Internetzugang auf den primären Admin-Knoten entweder direkt oder bereitgestellt "Verwenden eines Proxy-Servers" (Eingehende Verbindungen sind nicht erforderlich).
- Wenn HTTP auf der Seite StorageGRID AutoSupport ausgewählt ist, haben Sie einen Proxyserver für die Weiterleitung von AutoSupport-Nachrichten als HTTPS konfiguriert. Die AutoSupport Server von NetApp lehnen über HTTP gesendete Nachrichten ab.

  "Erfahren Sie mehr über das Konfigurieren von Administrator-Proxy-Einstellungen".

- Wenn Sie SMTP als Protokoll für AutoSupport-Meldungen verwenden, haben Sie einen SMTP-Mail-Server konfiguriert. Die gleiche E-Mail-Serverkonfiguration wird für Benachrichtigungen über Alarm E-Mails verwendet (altes System).

Geben Sie das Protokoll für AutoSupport Meldungen an

Sie können eines der folgenden Protokolle zum Senden von AutoSupport Meldungen verwenden:

- **HTTPS**: Dies ist die Standard-Einstellung und wird für Neuinstallationen empfohlen. Dieses Protokoll verwendet Port 443. Wenn Sie möchten Aktivieren Sie die Funktion „AutoSupport On Demand“, Müssen Sie HTTPS verwenden.
- **HTTP**: Wenn Sie HTTP auswählen, müssen Sie einen Proxyserver konfigurieren, um AutoSupport-Nachrichten als HTTPS weiterzuleiten. Die AutoSupport Server von NetApp lehnen über HTTP gesendete Nachrichten ab. Dieses Protokoll verwendet Port 80.
- **SMTP**: Verwenden Sie diese Option, wenn Sie AutoSupport-Nachrichten per E-Mail versenden möchten. Wenn Sie SMTP als Protokoll für AutoSupport-Meldungen verwenden, müssen Sie auf der Seite Legacy E-Mail-Einrichtung einen SMTP-Mail-Server konfigurieren (**SUPPORT** > **Alarme (alt)** > **Legacy E-Mail-Setup**).

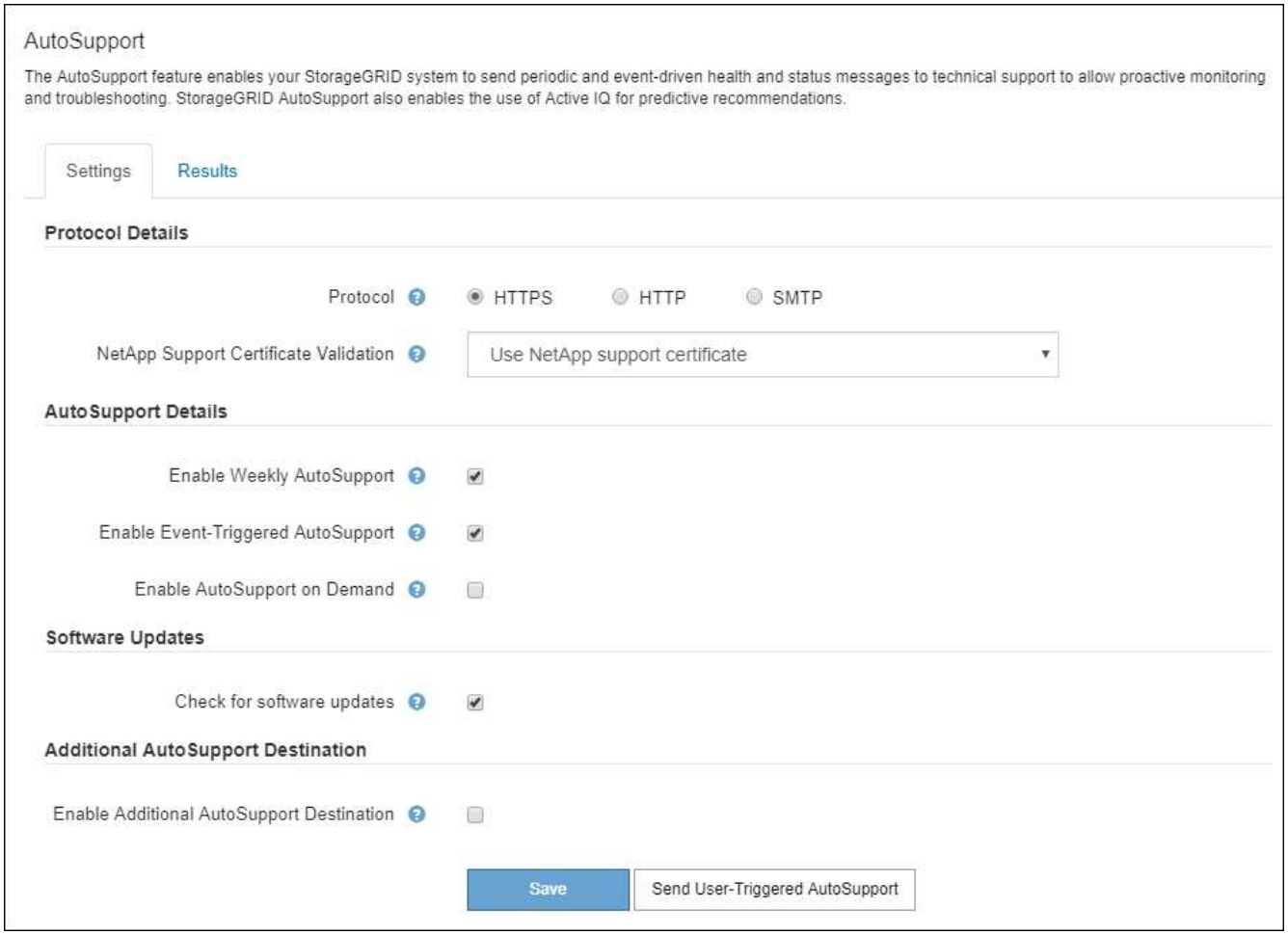
> ⓘ SMTP war das einzige Protokoll, das vor der StorageGRID 11.2-Version für AutoSupport-Meldungen verfügbar war. Wenn Sie zunächst eine frühere Version von StorageGRID installiert haben, ist SMTP möglicherweise das ausgewählte Protokoll.

Das von Ihnen festgelegte Protokoll wird für das Senden aller Typen von AutoSupport Meldungen verwendet.

Schritte

1. Wählen Sie **SUPPORT** > **Werkzeuge** > **AutoSupport**.

   Die Seite AutoSupport wird angezeigt, und die Registerkarte **Einstellungen** ist ausgewählt.



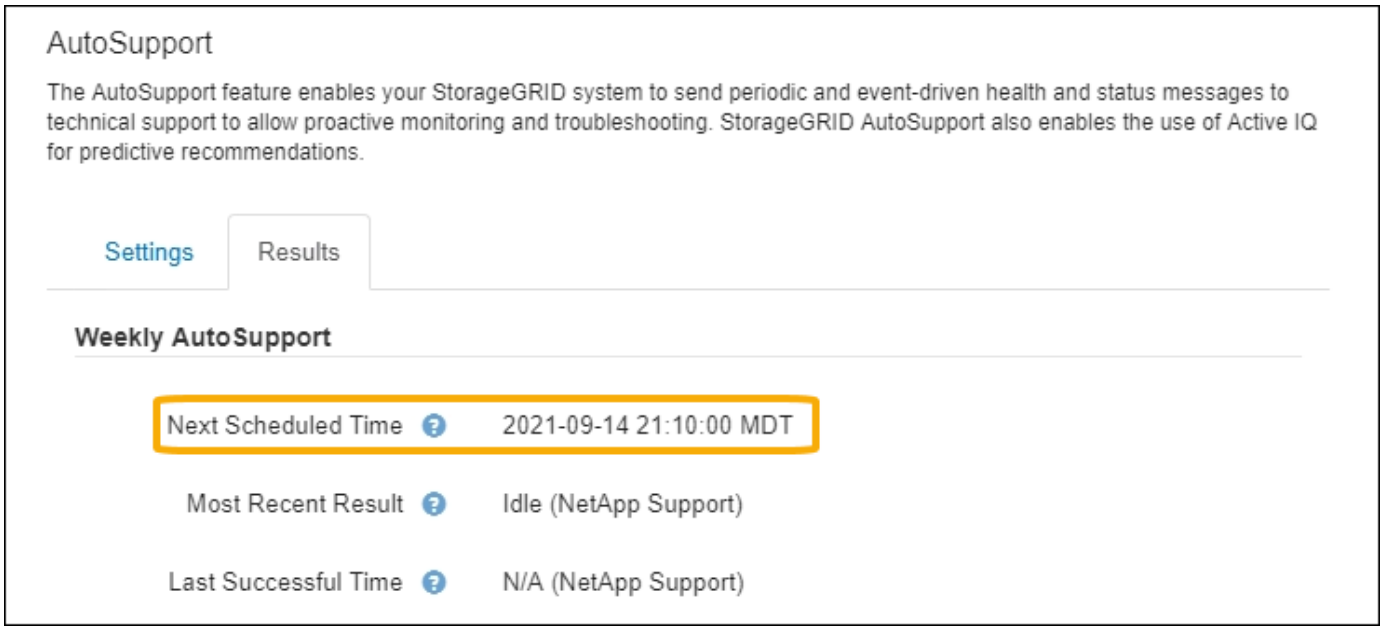
2. Wählen Sie das Protokoll aus, das Sie zum Senden von AutoSupport Meldungen verwenden möchten.
3. Wenn Sie **HTTPS** ausgewählt haben, wählen Sie aus, ob die Verbindung zum NetApp Support Server mit einem TLS-Zertifikat gesichert werden soll.
   - **NetApp Supportzertifikat verwenden** (Standard): Die Zertifikatvalidierung stellt sicher, dass die Übertragung von AutoSupport Meldungen sicher ist. Das NetApp Supportzertifikat ist bereits mit der StorageGRID Software installiert.
   - **Zertifikat nicht überprüfen**: Wählen Sie diese Option nur aus, wenn Sie einen guten Grund haben, keine Zertifikatvalidierung zu verwenden, z.B. wenn es ein vorübergehendes Problem mit einem Zertifikat gibt.
4. Wählen Sie **Speichern**.

   Alle wöchentlichen, vom Benutzer ausgelösten und von Ereignissen ausgelösten Meldungen werden über das ausgewählte Protokoll gesendet.

Deaktivieren Sie wöchentliche AutoSupport-Meldungen

Standardmäßig wird das StorageGRID System so konfiguriert, dass einmal pro Woche eine AutoSupport Meldung an den NetApp Support gesendet wird.

Um zu bestimmen, wann die wöchentliche AutoSupport-Nachricht gesendet wird, gehen Sie auf die Registerkarte **AutoSupport** > **Results**. Sehen Sie im Abschnitt **Wöchentliche AutoSupport** den Wert für **Nächste geplante Zeit** an.



Sie können das automatische Senden von wöchentlichen AutoSupport Meldungen jederzeit deaktivieren.

Schritte

1. Wählen Sie **SUPPORT** > **Werkzeuge** > **AutoSupport**.
2. Deaktivieren Sie das Kontrollkästchen **Weekly AutoSupport** aktivieren.
3. Wählen Sie **Speichern**.

Deaktivieren Sie ereignisgesteuerte AutoSupport Meldungen

Standardmäßig wird das StorageGRID System so konfiguriert, dass es eine AutoSupport Meldung an den NetApp Support sendet, wenn eine wichtige Meldung oder ein anderes bedeutendes Systemereignis auftritt.

Sie können AutoSupport Meldungen, bei denen Ereignisse ausgelöst wurden, jederzeit deaktivieren.

Schritte

1. Wählen Sie **SUPPORT** > **Werkzeuge** > **AutoSupport**.
2. Deaktivieren Sie das Kontrollkästchen **Event-Triggered AutoSupport** aktivieren.
3. Wählen Sie **Speichern**.

AutoSupport-on-Demand aktivieren

AutoSupport On Demand kann Ihnen bei der Lösung von Problemen helfen, an denen der technische Support aktiv arbeitet.

AutoSupport-on-Demand ist standardmäßig deaktiviert. Wenn Sie diese Funktion aktivieren, kann der technische Support von Ihrem StorageGRID System automatisch AutoSupport Meldungen senden. Der technische Support kann auch das Abfrageintervall für AutoSupport-on-Demand-Abfragen festlegen.

Der technische Support kann AutoSupport On Demand nicht aktivieren oder deaktivieren.

Schritte

1. Wählen Sie **SUPPORT** > **Werkzeuge** > **AutoSupport**.
2. Wählen Sie **HTTPS** für das Protokoll aus.

3. Aktivieren Sie das Kontrollkästchen **Weekly AutoSupport** aktivieren.
4. Aktivieren Sie das Kontrollkästchen **AutoSupport on Demand aktivieren**.
5. Wählen Sie **Speichern**.

   AutoSupport-on-Demand ist aktiviert, und der technische Support kann AutoSupport-on-Demand-Anfragen an StorageGRID senden.

Deaktivieren Sie die Prüfung auf Softwareupdates

Standardmäßig wendet sich StorageGRID an NetApp, um zu ermitteln, ob Software-Updates für Ihr System verfügbar sind. Wenn ein StorageGRID-Hotfix oder eine neue Version verfügbar ist, wird die neue Version auf der Seite StorageGRID-Aktualisierung angezeigt.

Bei Bedarf können Sie optional die Prüfung auf Softwareupdates deaktivieren. Wenn Ihr System beispielsweise keinen WAN-Zugriff hat, sollten Sie die Prüfung deaktivieren, um Download-Fehler zu vermeiden.

Schritte

1. Wählen Sie **SUPPORT** > **Werkzeuge** > **AutoSupport**.
2. Deaktivieren Sie das Kontrollkästchen **nach Softwareupdates suchen**.
3. Wählen Sie **Speichern**.

Fügen Sie ein weiteres AutoSupport Ziel hinzu

Wenn Sie AutoSupport aktivieren, werden Zustandsmeldungen und Statusmeldungen an den NetApp Support gesendet. Sie können ein zusätzliches Ziel für alle AutoSupport Meldungen angeben.

Informationen zum Überprüfen oder Ändern des Protokolls zum Senden von AutoSupport Meldungen finden Sie in den Anweisungen an Geben Sie das Protokoll für AutoSupport Meldungen an.

> Sie können das SMTP-Protokoll nicht zum Senden von AutoSupport Meldungen an ein weiteres Ziel verwenden.

Schritte

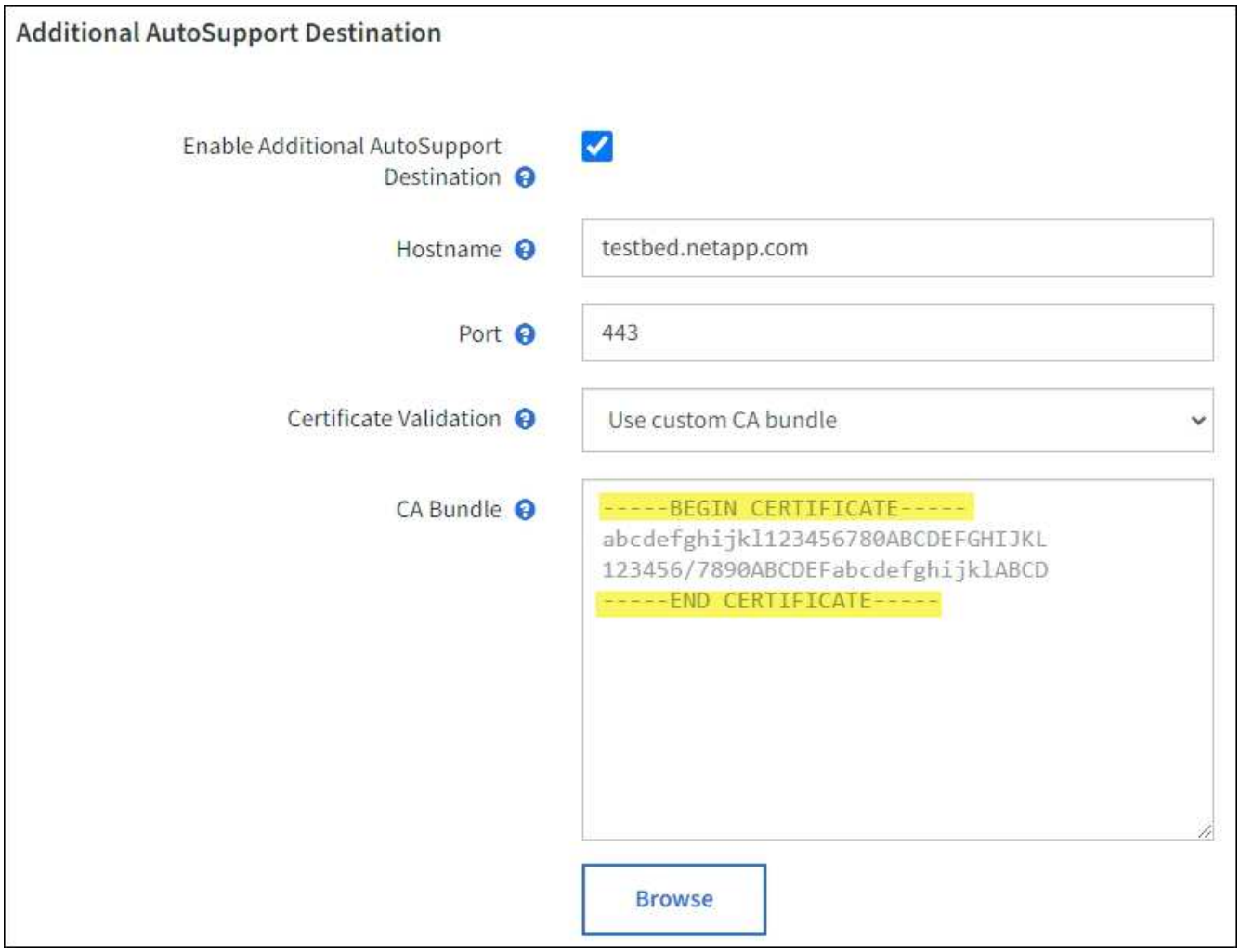
1. Wählen Sie **SUPPORT** > **Werkzeuge** > **AutoSupport**.
2. Wählen Sie **Zusätzliches AutoSupport-Ziel aktivieren**.
3. Geben Sie Folgendes an:

Feld	Beschreibung
Hostname	Der Hostname oder die IP-Adresse des Servers eines zusätzlichen AutoSupport-Zielservers. **Hinweis**: Sie können nur ein zusätzliches Ziel eingeben.
Port	Der Port, über den eine Verbindung zu einem zusätzlichen AutoSupport-Zielserver hergestellt wird. Der Standardwert ist Port 80 für HTTP oder Port 443 für HTTPS.

Feld	Beschreibung
Zertifizierungsvalidierung	Ob ein TLS-Zertifikat verwendet wird, um die Verbindung zum zusätzlichen Ziel zu sichern. • Wählen Sie **Zertifikat nicht verifizieren**, um Ihre AutoSupport-Nachrichten ohne Zertifikatvalidierung zu senden. Wählen Sie diese Option nur aus, wenn Sie einen guten Grund haben, die Zertifikatvalidierung nicht zu verwenden, z. B. wenn ein vorübergehendes Problem mit einem Zertifikat vorliegt. • Wählen Sie **Benutzerdefiniertes CA-Paket verwenden**, um die Zertifikatvalidierung zu verwenden.

4. Wenn Sie **benutzerdefiniertes CA-Paket verwenden** ausgewählt haben, führen Sie einen der folgenden Schritte aus:
   - Wählen Sie **Durchsuchen**, navigieren Sie zu der Datei mit den Zertifikaten und wählen Sie dann **Öffnen**, um die Datei hochzuladen.
   - Verwenden Sie ein Bearbeitungswerkzeug, um alle Inhalte der einzelnen PEM-kodierten CA-Zertifikatdateien in das Feld **CA Bundle** zu kopieren und einzufügen, das in der Zertifikatskette verknüpft ist.

     Sie müssen Folgendes einschließen `----BEGIN CERTIFICATE----` Und `----END CERTIFICATE----` Wählen Sie aus.



5. Wählen Sie **Speichern**.

   Alle zukünftigen wöchentlichen, ereignisgesteuert und vom Benutzer ausgelösten AutoSupport Meldungen werden an das zusätzliche Ziel gesendet.

Senden Sie manuell eine AutoSupport Meldung aus

Um den technischen Support bei der Fehlerbehebung bei Problemen mit Ihrem StorageGRID System zu unterstützen, können Sie manuell eine AutoSupport Meldung auslösen, die gesendet werden soll.

Bevor Sie beginnen

- Sie müssen mit einem beim Grid Manager angemeldet sein "Unterstützter Webbrowser".
- Sie müssen über die Berechtigung Root-Zugriff oder andere Grid-Konfiguration verfügen.

Schritte

1. Wählen Sie **SUPPORT** > **Werkzeuge** > **AutoSupport**.
2. Wählen Sie auf der Registerkarte **Einstellungen** die Option **vom Benutzer ausgelöste AutoSupport** senden.

   StorageGRID versucht, eine AutoSupport Nachricht an den technischen Support zu senden. Wenn der Versuch erfolgreich ist, werden die **aktuellsten Ergebnisse** und **Letzte erfolgreiche Zeit** Werte auf der

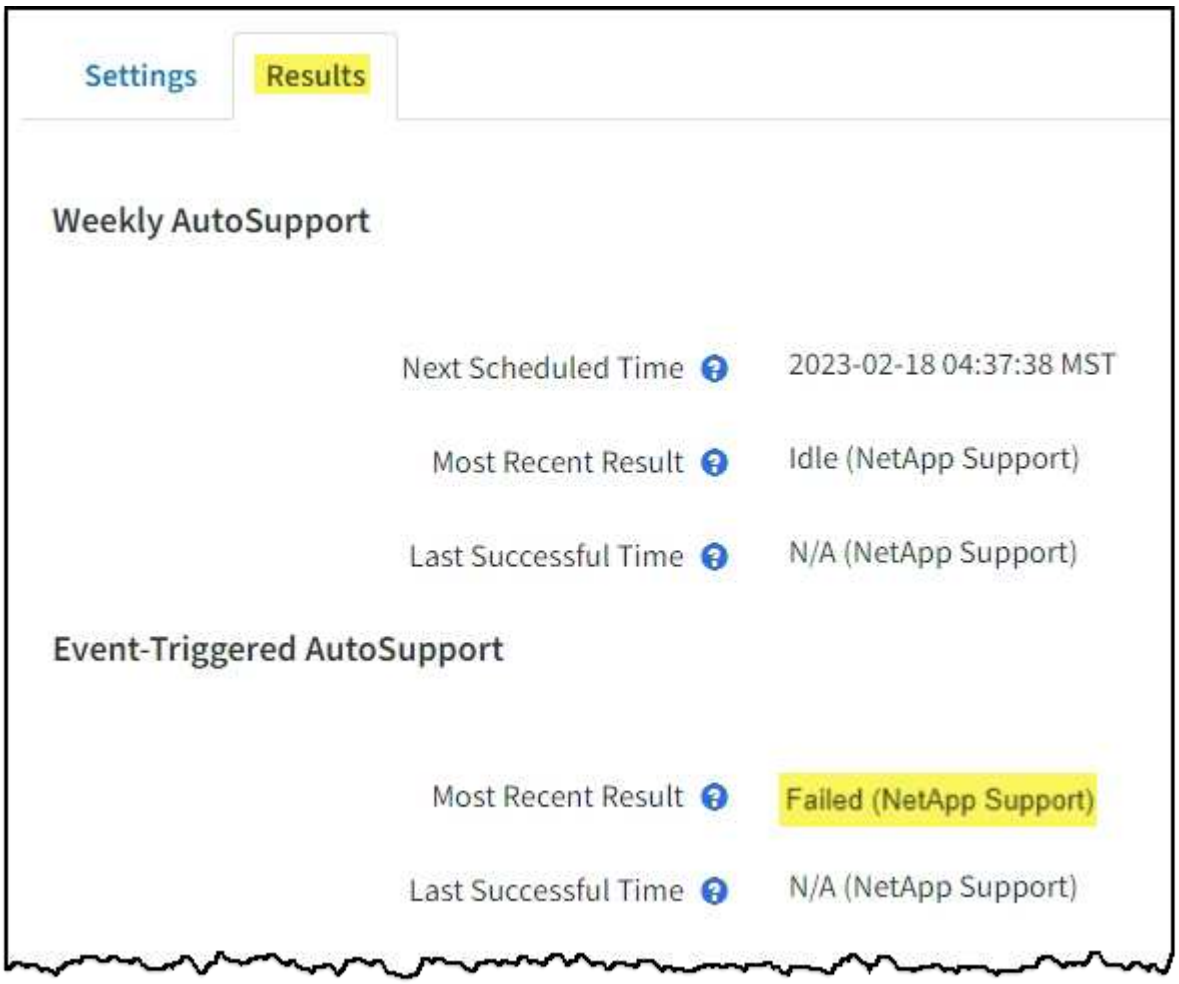
Registerkarte **Ergebnisse** aktualisiert. Wenn ein Problem auftritt, werden die **neuesten Ergebnisse**-Werte auf „Fehlgeschlagen“ aktualisiert, und StorageGRID versucht nicht, die AutoSupport-Nachricht erneut zu senden.

> Nachdem Sie eine vom Benutzer ausgelöste AutoSupport-Nachricht gesendet haben, aktualisieren Sie die AutoSupport-Seite im Browser nach 1 Minute, um auf die neuesten Ergebnisse zuzugreifen.

Fehlerbehebung für AutoSupport Meldungen

Wenn das Senden einer AutoSupport Meldung fehlschlägt, führt das StorageGRID System abhängig vom Typ der AutoSupport Meldung unterschiedliche Aktionen durch. Sie können den Status von AutoSupport-Meldungen überprüfen, indem Sie **SUPPORT** > **Werkzeuge** > **AutoSupport** > **Ergebnisse** auswählen.

Wenn die AutoSupport-Meldung nicht gesendet wird, wird „`failed`“ auf der Registerkarte **Results** der Seite **AutoSupport** angezeigt.



> Wenn Sie einen Proxyserver für die Weiterleitung von AutoSupport-Nachrichten an NetApp konfiguriert haben, sollten Sie dies tun "Überprüfen Sie, ob die Konfigurationseinstellungen des Proxy-Servers korrekt sind".

Wöchentlicher AutoSupport-Nachrichtenfehler

Wenn eine wöchentliche AutoSupport-Meldung nicht gesendet werden kann, werden im StorageGRID System folgende Aktionen ausgeführt:

1. Aktualisiert das Attribut für das aktuellste Ergebnis, um es erneut zu versuchen.
2. Versucht, die AutoSupport Meldung alle vier Minuten für eine Stunde 15 Mal erneut zu senden.
3. Nach einer Stunde des Sendefehlens aktualisiert das Attribut „Aktuelles Ergebnis“ auf „Fehlgeschlagen“.
4. Versucht, eine AutoSupport-Nachricht zum nächsten geplanten Zeitpunkt erneut zu senden.
5. Behält den regulären AutoSupport-Zeitplan bei, wenn die Meldung fehlschlägt, weil der NMS-Dienst nicht verfügbar ist und wenn eine Meldung vor sieben Tagen gesendet wird.
6. Wenn der NMS-Dienst wieder verfügbar ist, sendet sofort eine AutoSupport-Nachricht, wenn eine Nachricht für sieben Tage oder länger nicht gesendet wurde.

Vom Benutzer ausgelöste oder ereignisgesteuerte AutoSupport-Meldung ist fehlgeschlagen

Wenn eine vom Benutzer ausgelöste oder eine AutoSupport Meldung, die aufgrund eines Ereignisses ausgelöst wird, nicht gesendet wird, ergreift das StorageGRID System folgende Maßnahmen:

1. Zeigt eine Fehlermeldung an, wenn der Fehler bekannt ist. Wenn z. B. ein Benutzer das SMTP-Protokoll auswählt, ohne korrekte E-Mail-Konfigurationseinstellungen vorzunehmen, wird der folgende Fehler angezeigt: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. Versucht nicht, die Nachricht erneut zu senden.
3. Protokolliert den Fehler in `nms.log`.

Wenn ein Fehler auftritt und SMTP das ausgewählte Protokoll ist, überprüfen Sie, ob der E-Mail-Server des StorageGRID-Systems korrekt konfiguriert ist und Ihr E-Mail-Server ausgeführt wird (**SUPPORT** > **Alarme (alt)** > **> Legacy E-Mail-Setup**). Die folgende Fehlermeldung kann auf der AutoSupport-Seite angezeigt werden: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Erfahren Sie, wie Sie "Konfigurieren Sie die E-Mail-Servereinstellungen".

Korrigieren Sie einen Fehler bei der AutoSupport-Meldung

Wenn ein Fehler auftritt und SMTP das ausgewählte Protokoll ist, überprüfen Sie, ob der E-Mail-Server des StorageGRID-Systems korrekt konfiguriert ist und Ihr E-Mail-Server ausgeführt wird. Die folgende Fehlermeldung kann auf der AutoSupport-Seite angezeigt werden: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Senden Sie AutoSupport Nachrichten aus der E-Series über StorageGRID

Sie können AutoSupport Meldungen von E-Series SANtricity System Manager über einen StorageGRID Admin-Node anstelle des Storage Appliance Management-Ports an den technischen Support senden.

Siehe "E-Series Hardware AutoSupport" Weitere Informationen zur Verwendung von AutoSupport mit E-Series Appliances

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet "Unterstützter Webbrowser".
- Sie verfügen über Administratorrechte oder Root-Zugriffsberechtigungen für die Storage-Appliance.
- Sie haben SANtricity AutoSupport konfiguriert:
  - Für SG6000 und SG5700 Appliances, "Konfigurieren Sie AutoSupport in SANtricity System Manager"

> Sie müssen über SANtricity-Firmware 8.70 oder höher verfügen, um mit dem Grid Manager auf SANtricity System Manager zuzugreifen.

Über diese Aufgabe

E-Series AutoSupport-Meldungen enthalten Details zur Storage Hardware und sind spezifischer als andere AutoSupport-Meldungen, die vom StorageGRID System gesendet werden.

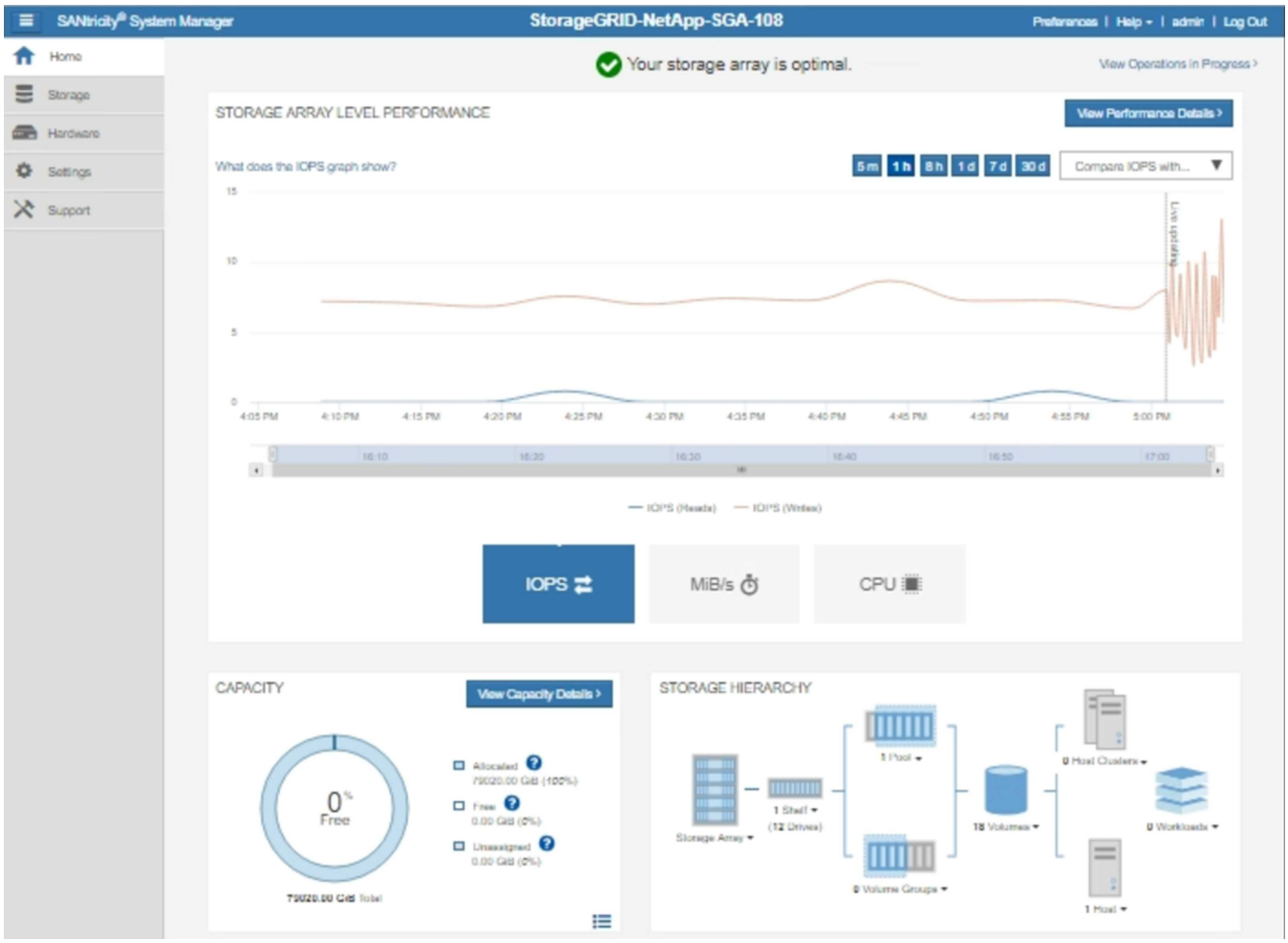
Sie können eine spezielle Proxy-Server-Adresse in SANtricity System Manager konfigurieren, um AutoSupport-Meldungen über einen StorageGRID-Admin-Knoten ohne Verwendung des Management-Ports der Appliance zu übertragen. AutoSupport-Nachrichten, die auf diese Weise übertragen werden, werden vom gesendet "Administratorknoten des bevorzugten Absenders", Und sie verwenden jede "Administrator-Proxy-Einstellungen" Die im Grid Manager konfiguriert wurden.

> Dieses Verfahren dient nur zur Konfiguration eines StorageGRID-Proxyservers für AutoSupport-Meldungen der E-Serie. Weitere Informationen zur Konfiguration der E-Series AutoSupport finden Sie unter "NetApp E-Series und SANtricity Dokumentation".

Schritte

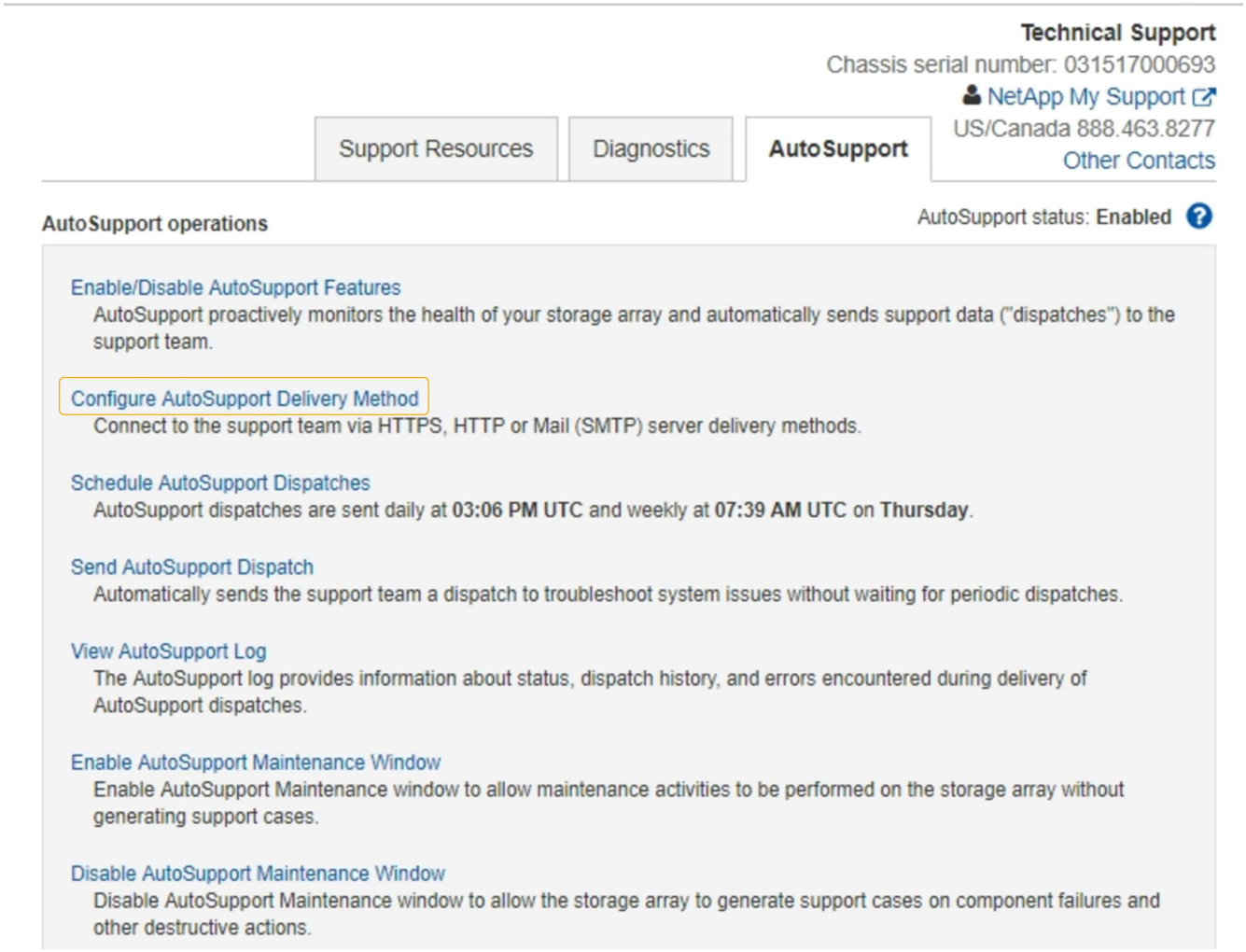
1. Wählen Sie im Grid Manager die Option **NODES** aus.
2. Wählen Sie in der Liste der Knoten links den Speicher-Appliance-Node aus, den Sie konfigurieren möchten.
3. Wählen Sie **SANtricity System Manager**.

   Die Startseite von SANtricity System Manager wird angezeigt.



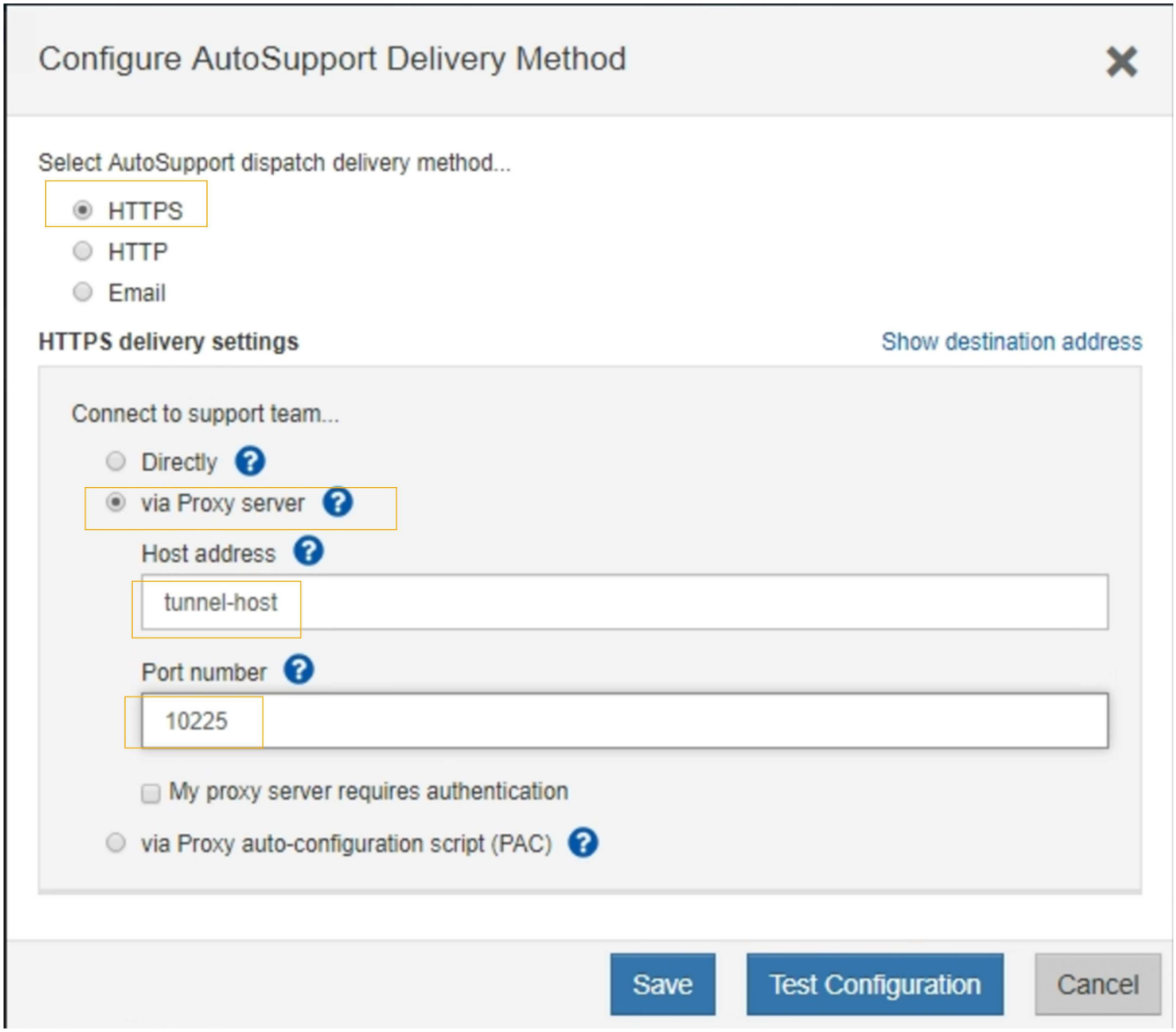
4. Wählen Sie **SUPPORT** > **Support Center** > **AutoSupport**.

   Die Seite AutoSupport-Vorgänge wird angezeigt.



5. Wählen Sie **AutoSupport-Bereitstellungsmethode konfigurieren**.

   Die Seite AutoSupport-Bereitstellungsmethode konfigurieren wird angezeigt.



6. Wählen Sie **HTTPS** für die Liefermethode aus.

   Das Zertifikat, das HTTPS aktiviert, ist vorinstalliert.

7. Wählen Sie **über Proxy-Server**.
8. Eingabe `tunnel-host` Für die **Host-Adresse**.

   `tunnel-host` Hat die besondere Adresse, um einen Admin-Node zum Senden von E-Series AutoSupport Meldungen zu verwenden.

9. Eingabe `10225` Für die * Portnummer*.

   `10225` Ist die Portnummer auf dem StorageGRID Proxy-Server, der AutoSupport Meldungen vom E-Series Controller in der Appliance empfängt.

10. Wählen Sie **Testkonfiguration** aus, um die Routing- und Konfigurationseinstellungen Ihres AutoSupport Proxy-Servers zu testen.

Falls richtig, erscheint eine Meldung in einem grünen Banner: „`Ihre AutoSupport-Konfiguration wurde verifiziert.`“

Wenn der Test fehlschlägt, wird eine Fehlermeldung in einem roten Banner angezeigt. Überprüfen Sie Ihre StorageGRID-DNS-Einstellungen und Netzwerk, stellen Sie sicher, dass die "Administratorknoten des bevorzugten Absenders" Kann eine Verbindung zur NetApp Support Site herstellen und den Test erneut versuchen.

11. Wählen Sie **Speichern**.

    Die Konfiguration wird gespeichert, und es wird eine Bestätigungsmeldung angezeigt: „`AutoSupport-Bereitstellungsmethode wurde konfiguriert.`“

Managen Sie Storage-Nodes

Storage-Nodes Verwalten: Übersicht

Storage-Nodes stellen Festplattenkapazität und Services zur Verfügung. Das Verwalten von Storage-Nodes umfasst Folgendes:

- Management der Storage-Optionen
- Um zu verstehen, welche Wasserzeichen für das Storage-Volume sind und wie Sie mit Wasserzeichen-Überschreibungen steuern können, wann Storage-Nodes schreibgeschützt sind
- Monitoring und Management des Speicherplatzes, der für Objektmetadaten verwendet wird
- Globale Einstellungen für gespeicherte Objekte konfigurieren
- Konfigurationseinstellungen für Speicherknoten werden angewendet
- Verwalten vollständiger Speicherknoten

Was ist ein Storage-Node?

Storage-Nodes managen und speichern Objektdaten und Metadaten. Jedes StorageGRID System muss mindestens drei Storage-Nodes aufweisen. Wenn Sie über mehrere Standorte verfügen, muss jeder Standort im StorageGRID System auch drei Storage-Nodes aufweisen.

Ein Storage Node umfasst die Services und Prozesse, die zum Speichern, Verschieben, Überprüfen und Abrufen von Objektdaten und Metadaten auf der Festplatte erforderlich sind. Auf der Seite **NODES** können Sie detaillierte Informationen zu den Speicherknoten anzeigen.

Was ist der ADC-Dienst?

Der Dienst Administrative Domain Controller (ADC) authentifiziert Grid-Knoten und ihre Verbindungen miteinander. Der ADC-Service wird auf jedem der ersten drei Storage-Nodes an einem Standort gehostet.

Der ADC-Dienst verwaltet Topologiedaten, einschließlich Standort und Verfügbarkeit von Diensten. Wenn ein Grid-Knoten Informationen von einem anderen Grid-Knoten benötigt oder eine Aktion von einem anderen Grid-Knoten ausgeführt werden muss, kontaktiert er einen ADC-Service, um den besten Grid-Knoten für die Bearbeitung seiner Anforderung zu finden. Darüber hinaus behält der ADC-Dienst eine Kopie der Konfigurationspakete der StorageGRID-Bereitstellung bei, sodass jeder Grid-Knoten aktuelle Konfigurationsinformationen abrufen kann.ADC-Informationen für einen Speicherknoten können Sie auf der

Seite Grid Topology anzeigen (**SUPPORT** > **Grid Topology**).

Zur Erleichterung von verteilten und isanded-Operationen synchronisiert jeder ADC-Dienst Zertifikate, Konfigurationspakete und Informationen über Services und Topologie mit den anderen ADC-Diensten im StorageGRID-System.

Im Allgemeinen unterhalten alle Rasterknoten eine Verbindung zu mindestens einem ADC-Dienst. So wird sichergestellt, dass die Grid-Nodes immer auf die neuesten Informationen zugreifen. Wenn Grid-Nodes verbunden sind, speichern sie Zertifikate anderer Grid-Nodes`, sodass die Systeme auch dann weiterhin mit bekannten Grid-Nodes funktionieren können, wenn ein ADC-Service nicht verfügbar ist. Neue Grid-Knoten können nur Verbindungen über einen ADC-Dienst herstellen.

Durch die Verbindung jedes Grid-Knotens kann der ADC-Service Topologiedaten erfassen. Die Informationen zu diesem Grid-Node umfassen die CPU-Last, den verfügbaren Festplattenspeicher (wenn der Storage vorhanden ist), unterstützte Services und die Standort-ID des Grid-Node. Andere Dienste fragen den ADC-Service nach Topologiedaten durch Topologieabfragen. Der ADC-Dienst reagiert auf jede Abfrage mit den neuesten Informationen, die vom StorageGRID-System empfangen wurden.

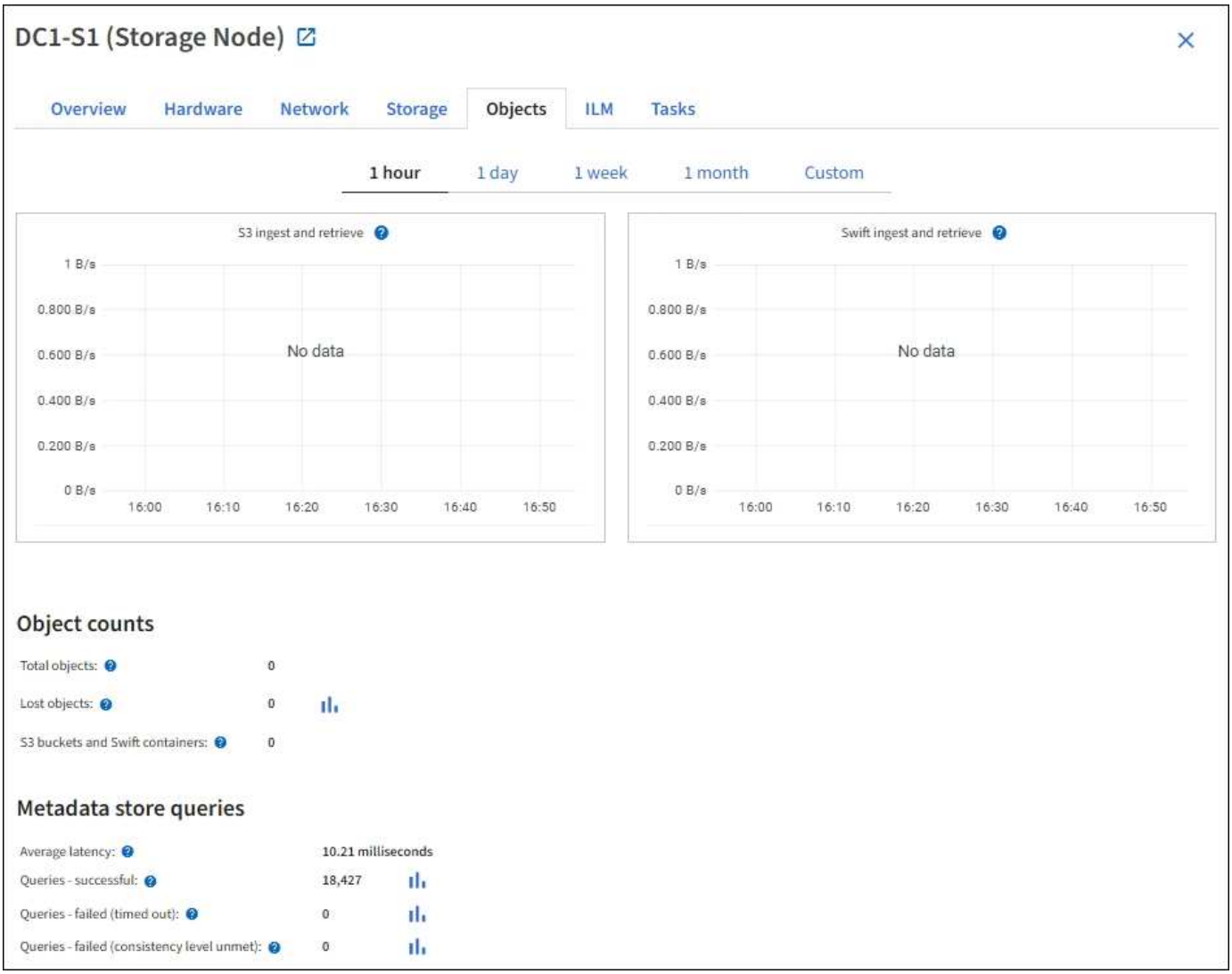
Was ist der DDS-Service?

Der DDS-Service (Distributed Data Store) wird von einem Storage-Node gehostet und führt Hintergrundaufgaben zu den im StorageGRID-System gespeicherten Objektmetadaten durch.

Anzahl der Objekte

Der DDS-Dienst verfolgt die Gesamtzahl der im StorageGRID-System aufgenommenen Objekte sowie die Gesamtzahl der über die unterstützten Schnittstellen (S3 oder Swift) des Systems aufgenommenen Objekte.

Die Anzahl der Objekte insgesamt wird auf der Seite Nodes > Registerkarte Objekte für jeden Storage Node angezeigt.



Abfragen

Sie können die durchschnittliche Zeit für die Ausführung einer Abfrage zum Metadatenspeicher durch den spezifischen DDS-Dienst, die Gesamtzahl der erfolgreichen Abfragen und die Gesamtanzahl der fehlgeschlagenen Abfragen für ein Timeout-Problem identifizieren.

Vielleicht möchten Sie nach Abfrageinformationen suchen, um den Zustand des Metadatenspeichers, Cassandra, zu überwachen. Dies hat Auswirkungen auf die Aufnahme- und Abrufleistung des Systems. Wenn beispielsweise die Latenz für eine durchschnittliche Abfrage langsam ist und die Anzahl fehlgeschlagener Abfragen aufgrund von Timeouts hoch ist, kann der Metadatenspeicher zu einer höheren Last führen oder einen anderen Vorgang ausführen.

Sie können auch die Gesamtzahl der Abfragen anzeigen, die aufgrund von Konsistenzfehlern fehlgeschlagen sind. Fehler auf Konsistenzebene resultieren aus einer unzureichenden Anzahl von verfügbaren Metadatenspeichern zum Zeitpunkt der Durchführung einer Abfrage durch den spezifischen DDS-Service.

Auf der Diagnoseseite erhalten Sie zusätzliche Informationen über den aktuellen Zustand Ihres Rasters. Siehe "Führen Sie eine Diagnose aus".

Konsistenzgarantien und -Kontrollen

StorageGRID garantiert die Konsistenz zwischen Lese- und Schreibvorgängen bei neu erstellten Objekten.

Jeder GET-Vorgang nach einem erfolgreich abgeschlossenen PUT-Vorgang kann die neu geschriebenen Daten lesen. Überschreibungen vorhandener Objekte, Metadatenaktualisierungen und -Löschungen bleiben irgendwann konsistent.

Was ist der LDR-Service?

Der Service Local Distribution Router (LDR) wird von jedem Speicherknoten gehostet und übernimmt den Content-Transport des StorageGRID-Systems. Der Content-Transport umfasst viele Aufgaben, einschließlich Datenspeicherung, Routing und Bearbeitung von Anfragen. Der LDR-Dienst erledigt die meiste harte Arbeit des StorageGRID-Systems durch die Verarbeitung von Datenübertragungslasten und Datenverkehrsfunktionen.

Der LDR-Service übernimmt folgende Aufgaben:

- Abfragen
- Information Lifecycle Management-Aktivitäten (ILM
- Löschen von Objekten
- Objekt-Storage
- Objektdatenübertragung von einem anderen LDR-Service (Storage Node)
- Datenspeicher-Management
- Protokollschnittstellen (S3 und Swift)

Der LDR-Service managt auch die Zuordnung von S3- und Swift-Objekten zu den eindeutigen „`Content Handles`“ (UUIDs), die das StorageGRID System jedem aufgenommene Objekt zuweist.

Abfragen

LDR-Abfragen umfassen Abfragen zum Objektspeicherort während Abruf- und Archivierungsvorgängen. Sie können die durchschnittliche Zeit zum Ausführen einer Abfrage, die Gesamtzahl der erfolgreichen Abfragen und die Gesamtzahl der Abfragen, die aufgrund eines Timeout-Problems fehlgeschlagen sind, identifizieren.

Sie können Abfrageinformationen prüfen, um den Zustand des Metadatenspeichers zu überwachen und die Aufnahme- und Abrufleistung des Systems zu beeinträchtigen. Wenn beispielsweise die Latenz für eine durchschnittliche Abfrage langsam ist und die Anzahl fehlgeschlagener Abfragen aufgrund von Timeouts hoch ist, kann der Metadatenspeicher zu einer höheren Last führen oder einen anderen Vorgang ausführen.

Sie können auch die Gesamtzahl der Abfragen anzeigen, die aufgrund von Konsistenzfehlern fehlgeschlagen sind. Fehler auf Konsistenzebene resultieren aus einer unzureichenden Anzahl an verfügbaren Metadatenspeichern zum Zeitpunkt einer Abfrage durch den spezifischen LDR-Service.

Auf der Diagnoseseite erhalten Sie zusätzliche Informationen über den aktuellen Zustand Ihres Rasters. Siehe "Führen Sie eine Diagnose aus".

ILM-Aktivität

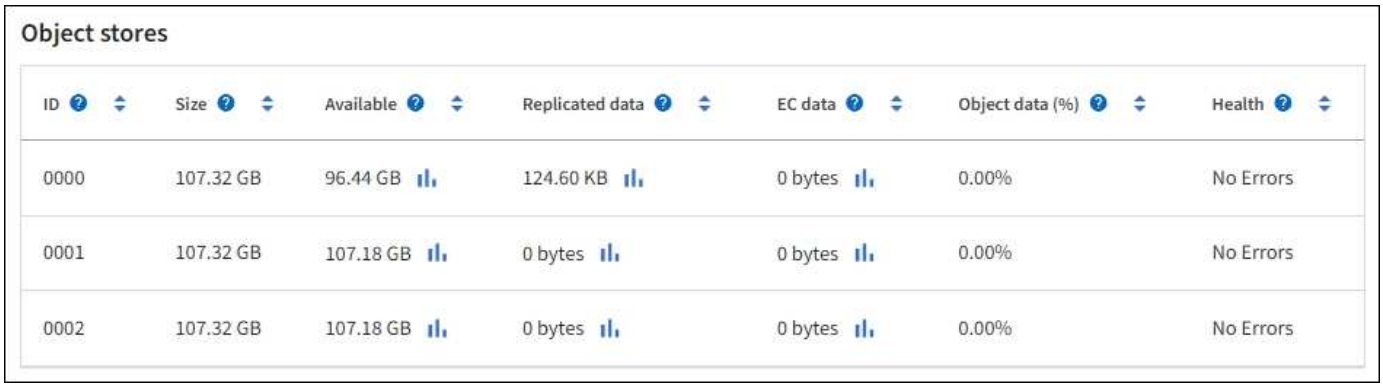
Mithilfe der ILM-Metriken (Information Lifecycle Management) können Sie die Bewertung von Objekten für die ILM-Implementierung durchführen. Sie können diese Metriken im Dashboard oder unter **NODES** > ***Storage Node*** > **ILM** anzeigen.

Objektspeicher

Der zugrunde liegende Datenspeicher eines LDR-Service wird in eine feste Anzahl an Objektspeichern (auch

Storage-Volumes genannt) unterteilt. Jeder Objektspeicher ist ein separater Bereitstellungspunkt.

Auf der Seite Knoten > Speicher werden die Objektspeicher für einen Speicherknoten angezeigt.



Das Objekt speichert in einem Storage-Node werden durch eine Hexadezimalzahl zwischen 0000 und 002F identifiziert, die als Volume-ID bezeichnet wird. Der Speicherplatz ist im ersten Objektspeicher (Volume 0) für Objekt-Metadaten in einer Cassandra-Datenbank reserviert. Für Objektdaten werden alle verbleibenden Speicherplatz auf diesem Volume verwendet. Alle anderen Objektspeichern werden ausschließlich für Objektdaten verwendet, zu denen replizierte Kopien und nach dem Erasure-Coding-Verfahren Fragmente gehören.

Um sicherzustellen, dass selbst der Speicherplatz für replizierte Kopien genutzt wird, werden Objektdaten für ein bestimmtes Objekt auf Basis des verfügbaren Storage in einem Objektspeicher gespeichert. Wenn ein oder mehrere Objektspeichern die Kapazität voll haben, speichern die übrigen Objektspeicher weiterhin Objekte, bis kein Platz mehr auf dem Speicherknoten vorhanden ist.

Metadatensicherung

Objektmetadaten sind Informationen mit oder eine Beschreibung eines Objekts, z. B. Änderungszeit des Objekts oder der Storage-Standort. StorageGRID speichert Objekt-Metadaten in einer Cassandra-Datenbank, die über eine Schnittstelle zum LDR-Service verfügt.

Um Redundanz sicherzustellen und so vor Verlust zu schützen, werden an jedem Standort drei Kopien von Objekt-Metadaten aufbewahrt. Diese Replikation ist nicht konfigurierbar und wird automatisch ausgeführt.

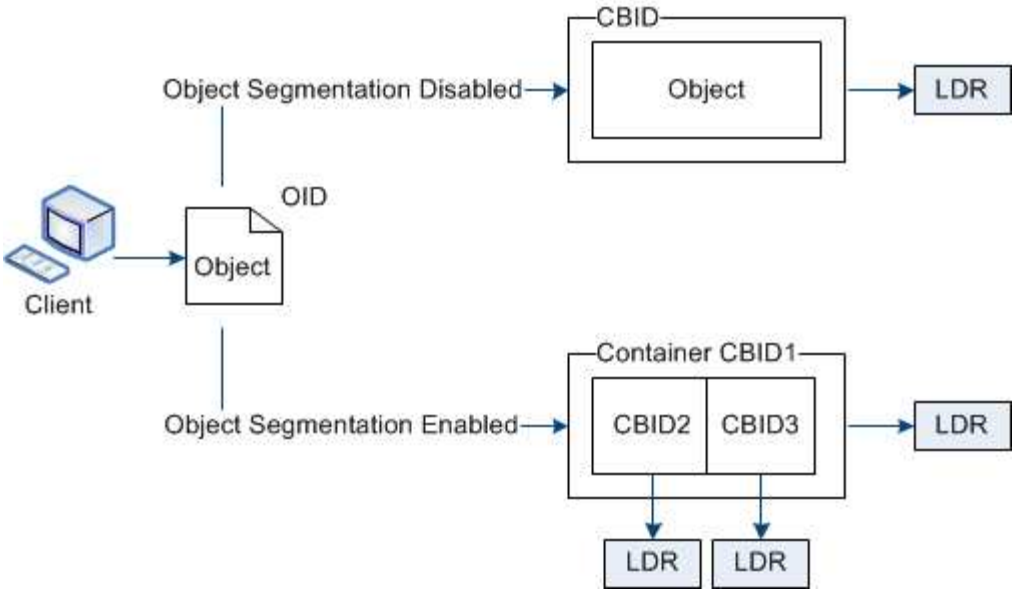
"Management von Objekt-Metadaten-Storage"

Verwenden Sie Speicheroptionen

Was ist Objektsegmentierung?

Bei der Objektsegmentierung wird ein Objekt in eine Sammlung kleinerer Objekte fester Größe aufgeteilt, um die Storage- und Ressourcennutzung für große Objekte zu optimieren. Auch beim S3-Multi-Part-Upload werden segmentierte Objekte erstellt, wobei ein Objekt die einzelnen Teile darstellt.

Wenn ein Objekt in das StorageGRID-System aufgenommen wird, teilt der LDR-Service das Objekt in Segmente auf und erstellt einen Segment-Container, der die Header-Informationen aller Segmente als Inhalt auflistet.



Beim Abruf eines Segment-Containers fasst der LDR-Service das ursprüngliche Objekt aus seinen Segmenten zusammen und gibt das Objekt dem Client zurück.

Der Container und die Segmente werden nicht unbedingt auf demselben Storage Node gespeichert. Container und Segmente können auf jedem Storage-Node innerhalb des in der ILM-Regel angegebenen Speicherpools gespeichert werden.

Jedes Segment wird vom StorageGRID System unabhängig behandelt und trägt zur Anzahl der Attribute wie verwaltete Objekte und gespeicherte Objekte bei. Wenn ein im StorageGRID System gespeichertes Objekt beispielsweise in zwei Segmente aufgeteilt wird, erhöht sich der Wert von verwalteten Objekten nach Abschluss der Aufnahme um drei Segmente:

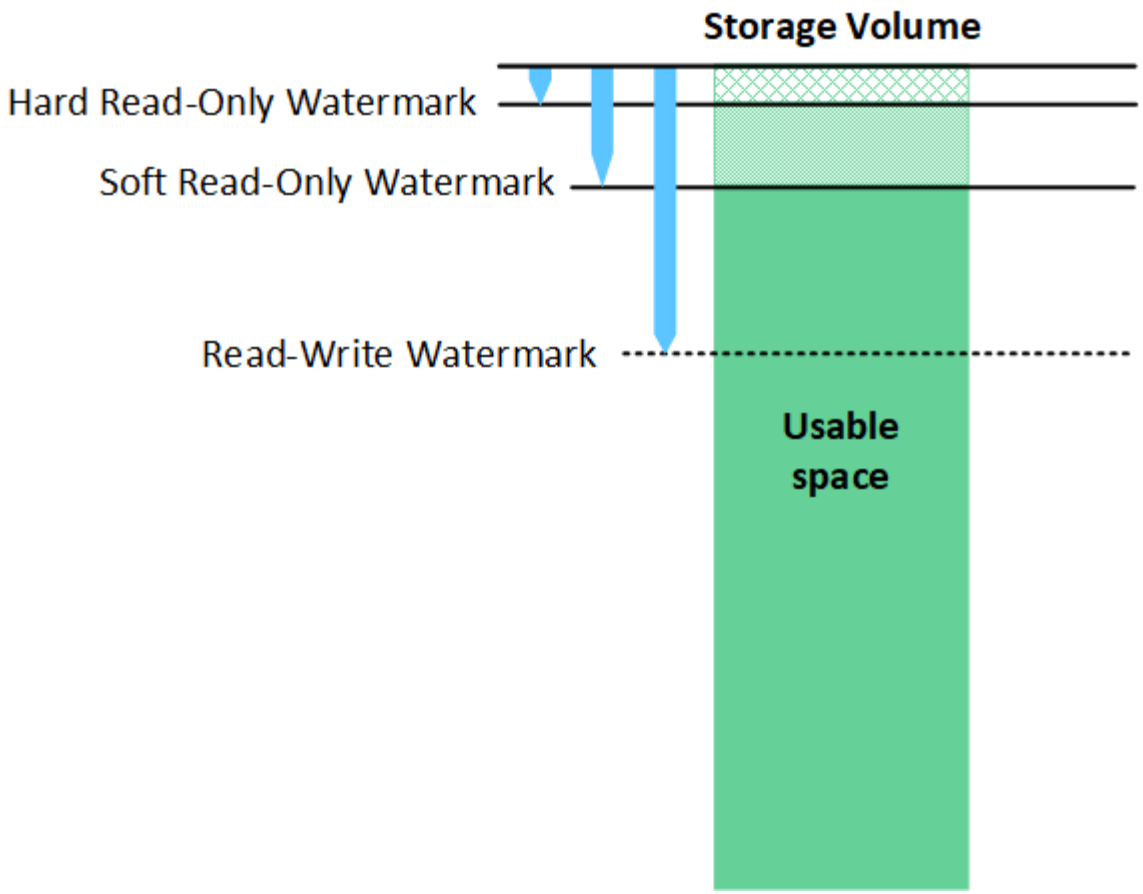
```
segment container + segment 1 + segment 2 = three stored objects
```

Die Performance beim Umgang mit großen Objekten lässt sich verbessern, indem Folgendes sichergestellt wird:

- Jedes Gateway und jeder Storage-Node verfügt über eine ausreichende Netzwerkbandbreite für den erforderlichen Durchsatz. Konfigurieren Sie beispielsweise separate Grid- und Client-Netzwerke auf 10-Gbit/s-Ethernet-Schnittstellen.
- Für den erforderlichen Durchsatz werden ausreichend Gateway und Storage-Nodes implementiert.
- Jeder Storage-Node verfügt über eine ausreichende Festplatten-I/O-Performance für den erforderlichen Durchsatz.

Was sind Wasserzeichen für Storage-Volumes?

StorageGRID verwendet drei Storage-Volume-Wasserzeichen, um sicherzustellen, dass Storage-Nodes sicher in einen schreibgeschützten Zustand überführt werden, bevor deren Speicherplatz kritisch knapp wird. Damit können Storage-Nodes, die aus einem schreibgeschützten Zustand migriert wurden, erneut Lese- und Schreibvorgänge werden.



Storage Volume-Wasserzeichen gelten nur für den Speicherplatz, der für replizierte und nach Datenkonsistenz (Erasure Coding) verwendet wird. Weitere Informationen über den Speicherplatz, der für Objekt-Metadaten auf Volume 0 reserviert ist, finden Sie unter"Management von Objekt-Metadaten-Storage".

Was ist das Soft Read-Only Watermark?

Das **Speichervolumen Soft Read-Only Watermark** ist das erste Wasserzeichen, das angibt, dass der für Objektdaten nutzbare Speicherplatz eines Speicherknoten voll wird.

Wenn jedes Volume in einem Storage-Node weniger freien Speicherplatz als das Soft Read-Only-Wasserzeichen dieses Volumes besitzt, wechselt der Storage-Node in den Modus *read-only*. Schreibgeschützter Modus bedeutet, dass der Storage Node für den Rest des StorageGRID Systems schreibgeschützte Dienste anbietet, aber alle ausstehenden Schreibanforderungen erfüllt.

Angenommen, jedes Volume in einem Speicherknoten hat einen Soft Read-Only-Wasserzeichen von 10 GB. Sobald jedes Volume weniger als 10 GB freien Speicherplatz hat, wechselt der Storage-Node in den Modus „Soft Read“.

Was ist die Hard Read-Only Watermark?

Das **Speichervolumen Hard Read-Only Watermark** ist das nächste Wasserzeichen, um anzuzeigen, dass der nutzbare Speicherplatz eines Knotens für Objektdaten voll wird.

Wenn der freie Speicherplatz auf einem Volume kleiner ist als das harte Read-Only-Wasserzeichen dieses Volumes, schlägt das Schreiben auf das Volume fehl. Schreibvorgänge auf anderen Volumes können jedoch fortgesetzt werden, bis der freie Speicherplatz auf diesen Volumes kleiner als ihre Hard Read-Only-

Wasserzeichen ist.

Angenommen, jedes Volume in einem Speicherknoten hat einen Hard Read-Only-Wasserzeichen von 5 GB. Sobald jedes Volume weniger als 5 GB freien Speicherplatz hat, akzeptiert der Speicherknoten keine Schreibanforderungen mehr.

Der Hard Read-Only-Wasserzeichen ist immer kleiner als der Soft Read-Only-Wasserzeichen.

Was ist der Read-Write-Wasserzeichen?

Das **Storage Volume Read-Write Watermark** gilt nur für Storage-Nodes, die in den schreibgeschützten Modus gewechselt sind. Er bestimmt, wann der Node wieder Lese-/Schreibzugriff werden kann. Wenn der freie Speicherplatz auf einem Speichervolumen in einem Speicherknoten größer ist als das Read-Write-Wasserzeichen dieses Volumes, wechselt der Knoten automatisch zurück in den Lese-Schreib-Zustand.

Angenommen, der Storage-Node ist in den schreibgeschützten Modus migriert. Nehmen Sie auch an, dass jedes Volume ein Read-Write-Wasserzeichen von 30 GB hat. Sobald der freie Speicherplatz eines beliebigen Volumes auf 30 GB ansteigt, wird der Node erneut zum Lesen/Schreiben.

Der Read-Write-Wasserzeichen ist immer größer als der Soft Read-Only-Wasserzeichen und der Hard Read-Only-Wasserzeichen.

Anzeigen von Wasserzeichen für Speichervolumen

Sie können die aktuellen Einstellungen für Wasserzeichen und die systemoptimierten Werte anzeigen. Wenn keine optimierten Wasserzeichen verwendet werden, können Sie festlegen, ob Sie die Einstellungen anpassen können oder sollten.

Bevor Sie beginnen

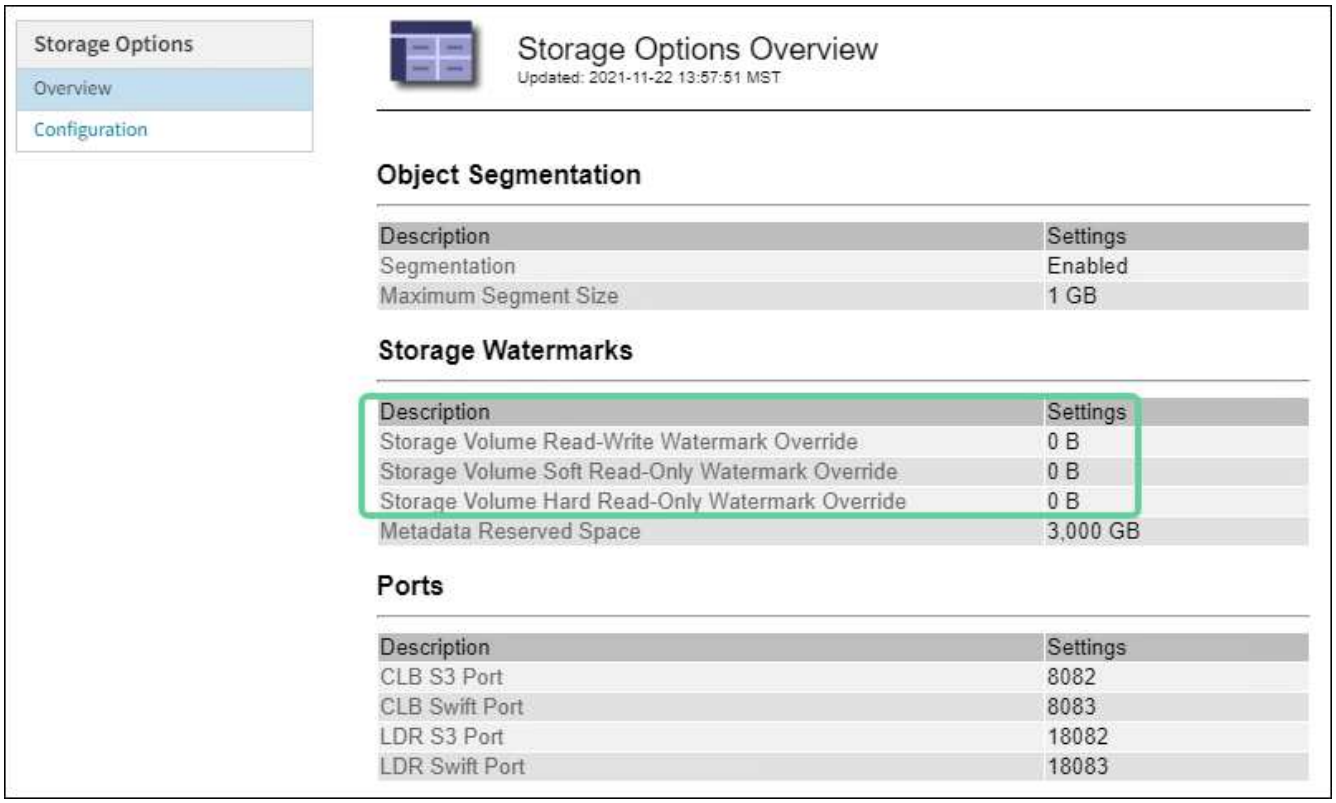
- Sie haben das Upgrade auf StorageGRID 11.6 oder höher abgeschlossen.
- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die Root-Zugriffsberechtigung.

Aktuelle Wasserzeichen-Einstellungen anzeigen

Im Grid Manager können Sie die aktuellen Einstellungen für Speicherwasserzeichen anzeigen.

Schritte

1. Wählen Sie **KONFIGURATION** > **System** > **Speicheroptionen**.
2. Sehen Sie sich im Abschnitt Speicherwasserzeichen die Einstellungen für die drei Überschreibungen der Speichervolumen an.



- Wenn die Wasserzeichen **0** überschreiben, sind alle drei Wasserzeichen für jedes Speichervolumen auf jedem Speicherknoten optimiert, basierend auf der Größe des Speicherknoten und der relativen Kapazität des Volumes.

  Dies ist die Standardeinstellung und die empfohlene Einstellung. Sie sollten diese Werte nicht aktualisieren. Nach Bedarf können Sie optional Anzeigen optimierter Speicherabdrücke.

- Wenn es sich bei den Wasserzeichen um nicht-0-Werte handelt, werden benutzerdefinierte (nicht optimierte) Wasserzeichen verwendet. Es wird nicht empfohlen, benutzerdefinierte Wasserzeichen zu verwenden. Befolgen Sie die Anweisungen für "Fehlerbehebung Warnungen bei niedriger Schreibschutzmarke überschreiben" Um zu bestimmen, ob Sie die Einstellungen anpassen können oder sollen.

Anzeigen optimierter Speicherabdrücke

StorageGRID verwendet zwei Prometheus-Kennzahlen, um die optimierten Werte anzuzeigen, die es für das **Speichervolumen Soft Read-Only Watermark** berechnet hat. Sie können die minimalen und maximalen optimierten Werte für jeden Speicherknoten in Ihrem Raster anzeigen.

1. Wählen Sie **SUPPORT** > **Tools** > **Metriken**.
2. Wählen Sie im Abschnitt Prometheus den Link aus, um auf die Benutzeroberfläche von Prometheus zuzugreifen.
3. Um das empfohlene Mindestwasserzeichen für weichen, schreibgeschützten Wert anzuzeigen, geben Sie die folgende Prometheus-Metrik ein, und wählen Sie **Ausführen**:

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   In der letzten Spalte wird der mindestens optimierte Wert des „Soft Read-Only“-Wasserzeichens für alle Storage-Volumes auf jedem Storage-Node angezeigt. Wenn dieser Wert größer ist als die benutzerdefinierte Einstellung für das **Speichervolumen-Soft-Read-Only-Wasserzeichen**, wird für den

Speicherknoten die Warnung **Low read-only Watermark override** ausgelöst.

4. Um das empfohlene maximale Softread-only-Wasserzeichen anzuzeigen, geben Sie die folgende Prometheus-Metrik ein und wählen Sie **Ausführen**:

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   In der letzten Spalte wird der maximal optimierte Wert des „Soft Read-Only“-Wasserzeichens für alle Storage-Volumes auf jedem Storage-Node angezeigt.

Management von Objekt-Metadaten-Storage

Die Kapazität der Objektmetadaten eines StorageGRID Systems steuert die maximale Anzahl an Objekten, die auf diesem System gespeichert werden können. Um sicherzustellen, dass Ihr StorageGRID System über ausreichend Platz zum Speichern neuer Objekte verfügt, müssen Sie wissen, wo und wie StorageGRID Objekt-Metadaten speichert.

Was sind Objekt-Metadaten?

Objektmetadaten sind alle Informationen, die ein Objekt beschreiben. StorageGRID verwendet Objektmetadaten, um die Standorte aller Objekte im Grid zu verfolgen und den Lebenszyklus eines jeden Objekts mit der Zeit zu managen.

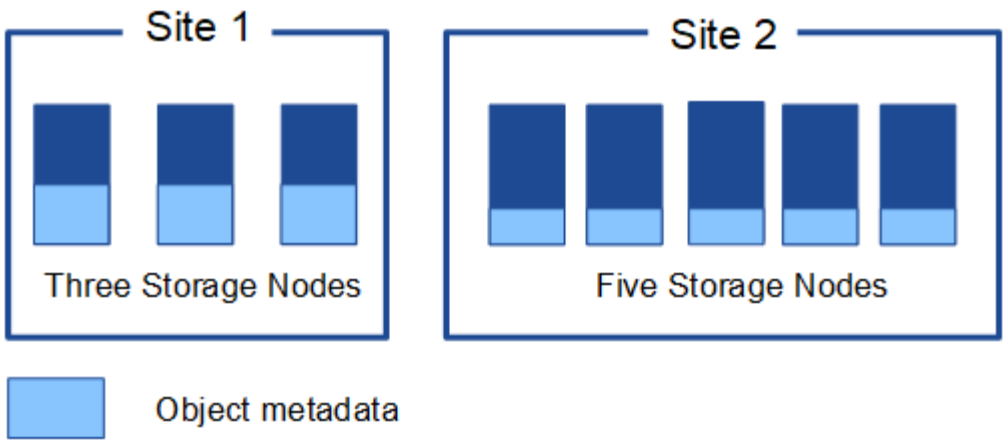
Für ein Objekt in StorageGRID enthalten die Objektmetadaten die folgenden Informationstypen:

- Systemmetadaten, einschließlich einer eindeutigen ID für jedes Objekt (UUID), dem Objektnamen, dem Namen des S3-Buckets oder Swift-Containers, dem Mandanten-Kontonamen oder -ID, der logischen Größe des Objekts, dem Datum und der Uhrzeit der ersten Erstellung des Objekts Und Datum und Uhrzeit der letzten Änderung des Objekts.
- Alle mit dem Objekt verknüpften Schlüssel-Wert-Paare für benutzerdefinierte Benutzer-Metadaten.
- Bei S3-Objekten sind alle dem Objekt zugeordneten Objekt-Tag-Schlüsselwert-Paare enthalten.
- Der aktuelle Storage-Standort jeder Kopie für replizierte Objektkopien
- Für Objektkopien mit Erasure-Coding-Verfahren wird der aktuelle Speicherort der einzelnen Fragmente gespeichert.
- Bei Objektkopien in einem Cloud Storage Pool befindet sich der Speicherort des Objekts, einschließlich des Namens des externen Buckets und der eindeutigen Kennung des Objekts.
- Für segmentierte Objekte und mehrteilige Objekte, Segment-IDs und Datengrößen.

Wie werden Objekt-Metadaten gespeichert?

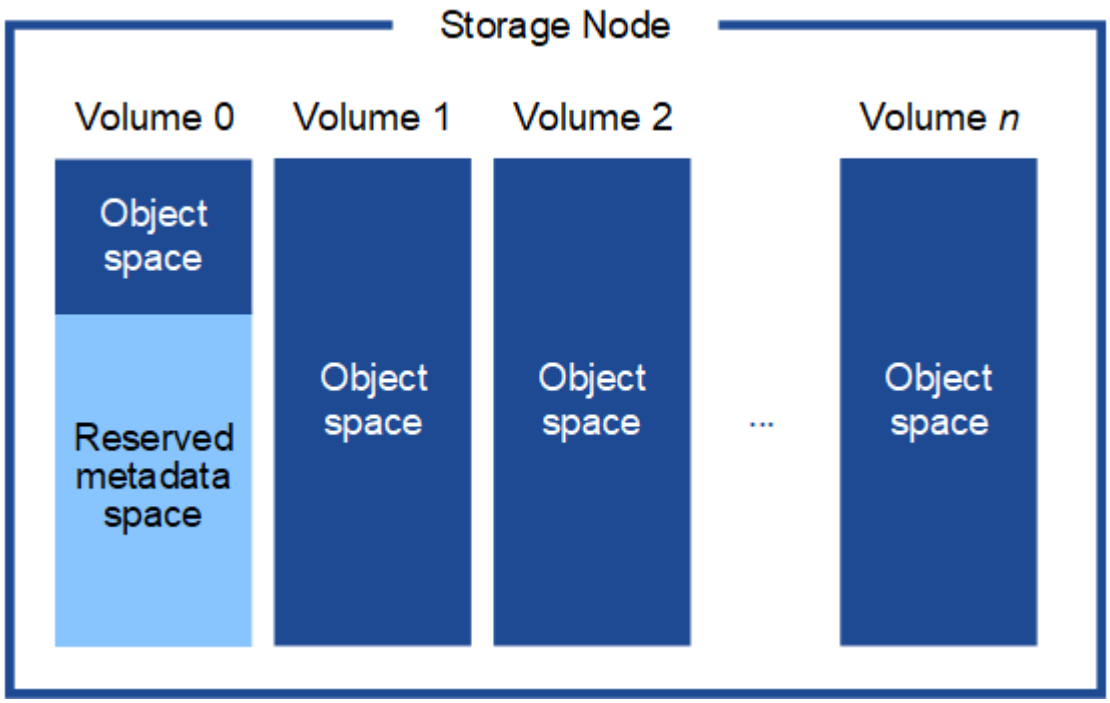
StorageGRID speichert Objektmetadaten in einer Cassandra-Datenbank, die unabhängig von Objektdaten gespeichert werden. Um Redundanz zu gewährleisten und Objekt-Metadaten vor Verlust zu schützen, speichert StorageGRID drei Kopien der Metadaten für alle Objekte im System an jedem Standort.

Diese Abbildung zeigt die Speicherknoten an zwei Standorten. Jeder Standort verfügt über die gleiche Menge an Objektmetadaten. Die Metadaten jedes Standorts werden unter alle Storage-Nodes an diesem Standort unterteilt.



Wo werden Objekt-Metadaten gespeichert?

Diese Abbildung zeigt die Storage Volumes für einen einzelnen Storage-Node.



Wie in der Abbildung dargestellt, reserviert StorageGRID Speicherplatz für Objekt-Metadaten auf dem Storage Volume 0 jedes Storage-Nodes. Sie verwendet den reservierten Speicherplatz zum Speichern von Objektmetadaten und zum Ausführen wichtiger Datenbankvorgänge. Alle übrigen Speicherplatz auf dem Storage Volume 0 und allen anderen Storage Volumes im Storage Node werden ausschließlich für Objektdaten (replizierte Kopien und nach Datenkonsistenz) verwendet.

Der Speicherplatz, der für Objektmetadaten auf einem bestimmten Storage Node reserviert ist, hängt von mehreren Faktoren ab, die im Folgenden beschrieben werden.

Einstellung für reservierten Speicherplatz für Metadaten

Die Einstellung *Metadaten Reserved Space* stellt die Menge an Speicherplatz dar, die für Metadaten auf Volume 0 jedes Storage-Node reserviert wird. Wie in der Tabelle gezeigt, basiert der Standardwert dieser Einstellung auf:

- Die Softwareversion, die Sie bei der Erstinstallation von StorageGRID verwendet haben.
- Die RAM-Menge auf jedem Storage-Node.

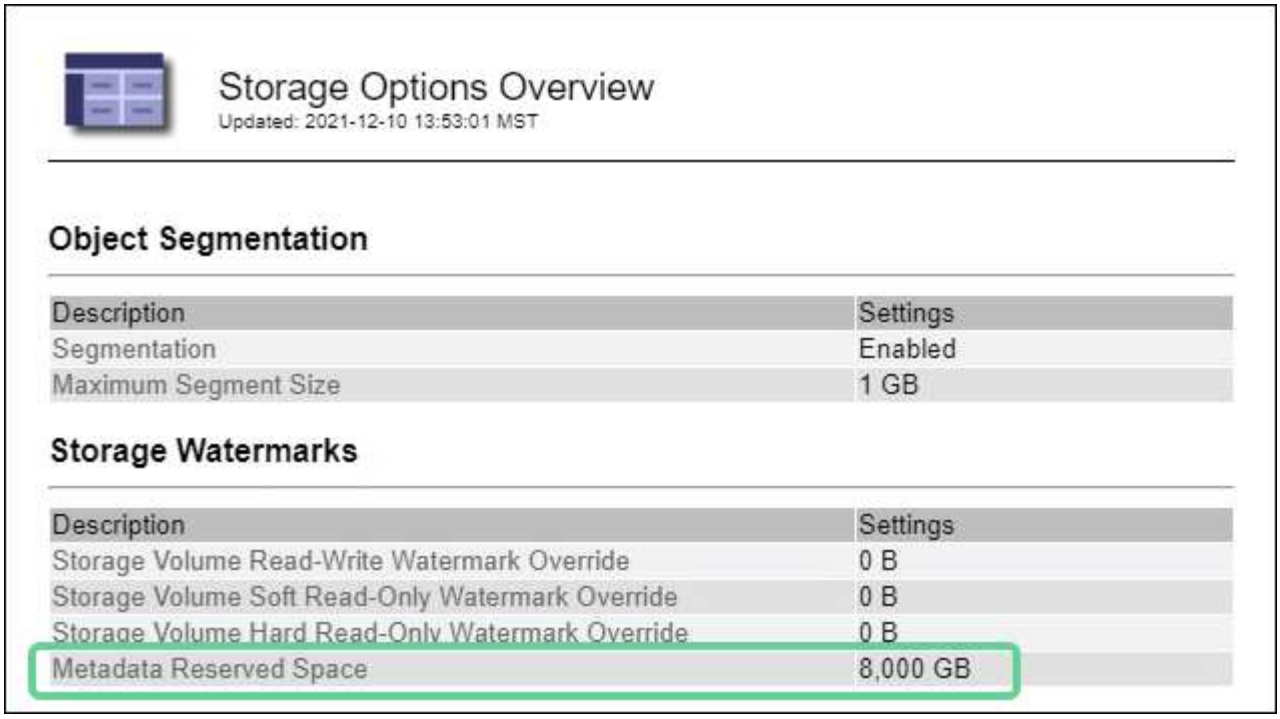
Für die Erstinstallation von StorageGRID verwendete Version	RAM-Größe auf Speicherknoten	Standardeinstellung für reservierten Speicherplatz für Metadaten
11.5 bis 11.7	128 GB oder mehr auf jedem Storage-Node im Grid	8 TB (8,000 GB)
	Weniger als 128 GB auf jedem Storage-Node im Grid	3 TB (3,000 GB)
11.1 bis 11.4	128 GB oder mehr auf jedem Speicherknoten an einem beliebigen Standort	4 TB (4,000 GB)
	Weniger als 128 GB auf jedem Speicherknoten an jedem Standort	3 TB (3,000 GB)
11.0 oder früher	Beliebiger Betrag	2 TB (2,000 GB)

Einstellung für reservierten Speicherplatz für Metadaten anzeigen

Befolgen Sie diese Schritte, um die Einstellung für reservierten Speicherplatz für Metadaten für Ihr StorageGRID-System anzuzeigen.

Schritte

1. Wählen Sie **KONFIGURATION** > **System** > **Speicheroptionen**.
2. Suchen Sie in der Tabelle Speicherwasserzeichen **Metadatenreservierter Speicherplatz**.



Im Screenshot beträgt der Wert **Metadaten reservierter Speicherplatz** 8,000 GB (8 TB). Dies ist die Standardeinstellung für eine neue StorageGRID 11.6 oder höher-Installation, bei der jeder Speicherknoten mindestens 128 GB RAM hat.

Tatsächlich reservierter Speicherplatz für Metadaten

Im Gegensatz zur Einstellung „systemweiter reservierter Speicherplatz für Metadaten“ wird für jeden Storage-Node der_tatsächlich reservierte Speicherplatz_ für Objektmetadaten ermittelt. Für jeden bestimmten Storage-Node hängt der tatsächlich reservierte Speicherplatz für Metadaten von der Größe des Volumes 0 für den Node und der systemweiten Einstellung **Metadaten reservierter Speicherplatz** ab.

Größe von Volume 0 für den Node	Tatsächlich reservierter Speicherplatz für Metadaten
Weniger als 500 GB (nicht in der Produktion)	10% des Volumens 0
500 GB oder mehr	Die kleineren Werte: • Lautstärke 0 • Einstellung für reservierten Speicherplatz für Metadaten

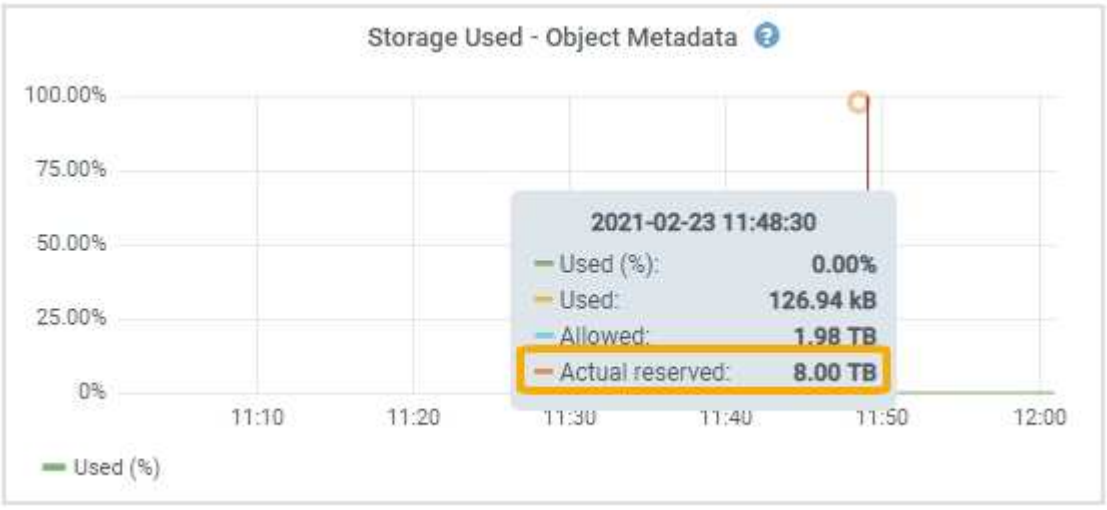
Zeigen Sie den tatsächlich reservierten Speicherplatz für Metadaten an

Führen Sie die folgenden Schritte aus, um den tatsächlich reservierten Speicherplatz für Metadaten auf einem bestimmten Storage-Node anzuzeigen.

Schritte

1. Wählen Sie im Grid Manager **NODES** > ***Storage Node*** aus.
2. Wählen Sie die Registerkarte **Storage** aus.

3. Setzen Sie den Cursor auf das Diagramm Speicher verwendet - Objekt Metadaten und suchen Sie den Wert **tatsächlich reserviert**.



Im Screenshot beträgt der **tatsächliche reservierte** Wert 8 TB. Dieser Screenshot ist für einen großen Speicherknoten in einer neuen StorageGRID 11.6 Installation. Da die Einstellung für den systemweiten reservierten Speicherplatz für Metadaten kleiner als das Volume 0 für diesen Storage-Node ist, entspricht der tatsächlich reservierte Speicherplatz für diesen Node der Einstellung für den reservierten Speicherplatz.

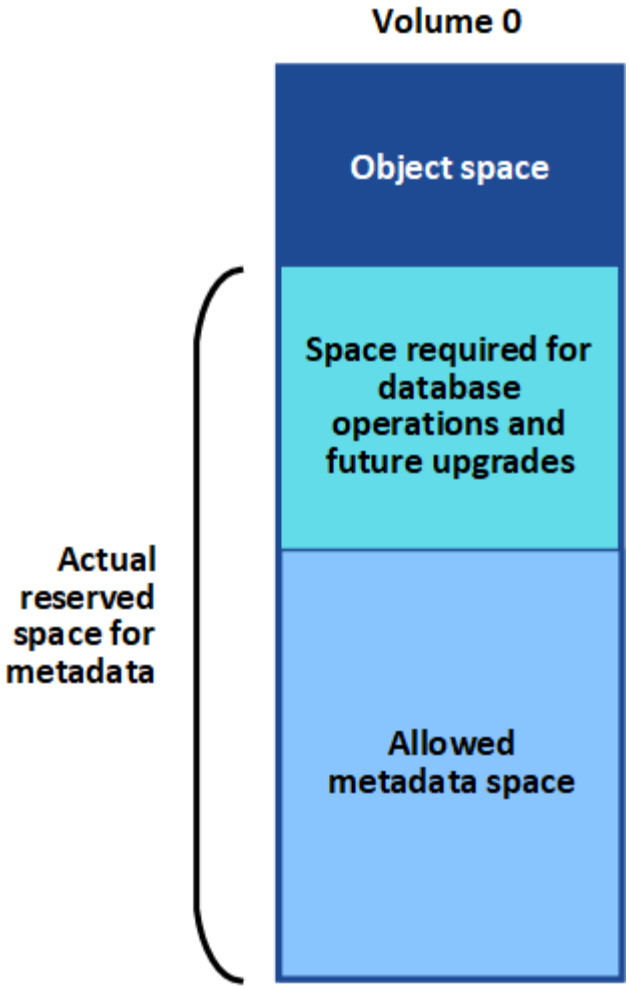
Beispiel für den tatsächlich reservierten Metadatenspeicherplatz

Angenommen, Sie installieren ein neues StorageGRID-System mit Version 11.7. Nehmen Sie in diesem Beispiel an, dass jeder Speicherknoten mehr als 128 GB RAM und dieses Volume 0 von Speicherknoten 1 (SN1) 6 TB hat. Basierend auf diesen Werten:

- Der systemweite **Metadaten reservierter Platz** ist auf 8 TB eingestellt. (Dies ist der Standardwert für eine neue StorageGRID 11.6-Installation oder höher, wenn jeder Speicherknoten mehr als 128 GB RAM hat.)
- Der tatsächlich reservierte Speicherplatz für Metadaten von SN1 beträgt 6 TB. (Das gesamte Volume ist reserviert, da Volume 0 kleiner ist als die Einstellung **Metadaten reservierter Speicherplatz**.)

Zulässiger Metadatenspeicherplatz

Der tatsächlich reservierte Speicherplatz jedes Storage-Node für Metadaten wird in den Speicherplatz für Objekt-Metadaten (den „ *zulässigen Metadatenspeicherplatz*“) und den Platzbedarf für wichtige Datenbankvorgänge (wie Data-Compaction und Reparatur) sowie zukünftige Hardware- und Software-Upgrades unterteilt. Der zulässige Metadatenspeicherplatz bestimmt die gesamte Objektkapazität.



Die folgende Tabelle zeigt, wie StorageGRID den **zulässigen Metadatenspeicherplatz** für verschiedene Storage-Nodes berechnet, basierend auf der Speichermenge für den Node und dem tatsächlich reservierten Speicherplatz für Metadaten.

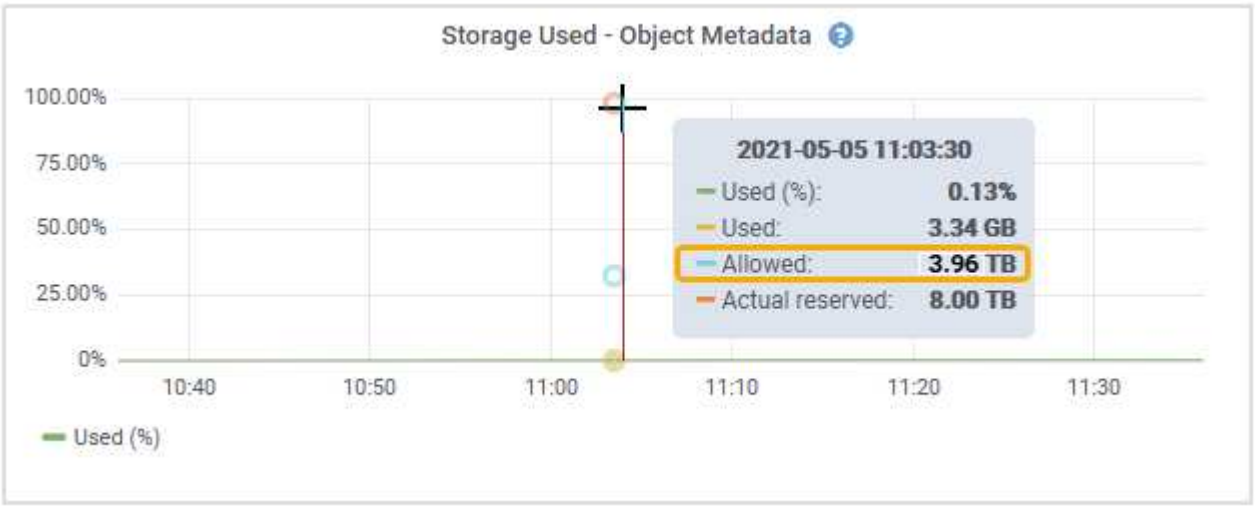
		Speichermenge auf Speicherknoten	
	≪ 128 GB	>= 128 GB	**Tatsächlich reservierter Platz für Metadaten**
≪= 4 TB	60 % des tatsächlich reservierten Speicherplatzes für Metadaten maximal 1.32 TB	60 % des tatsächlich reservierten Speicherplatzes für Metadaten maximal 1.98 TB	4 TB

Zeigen Sie den zulässigen Metadatenbereich an

Führen Sie die folgenden Schritte aus, um den zulässigen Metadatenspeicher für einen Storage-Node anzuzeigen.

Schritte

1. Wählen Sie im Grid Manager die Option **NODES** aus.
2. Wählen Sie den Speicherknoten aus.
3. Wählen Sie die Registerkarte **Storage** aus.
4. Setzen Sie den Cursor auf das Diagramm Speicher verwendet - Objekt Metadaten und suchen Sie den Wert **erlaubt**.



Im Screenshot beträgt der **zulässige**-Wert 3.96 TB, was der maximale Wert für einen Storage Node ist, dessen tatsächlicher reservierter Speicherplatz für Metadaten mehr als 4 TB beträgt.

Der **zulässige**-Wert entspricht dieser Prometheus-Metrik:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Beispiel für zulässigen Metadatenspeicherplatz

Angenommen, Sie installieren ein StorageGRID System mit Version 11.6. Nehmen Sie in diesem Beispiel an, dass jeder Speicherknoten mehr als 128 GB RAM und dieses Volume 0 von Speicherknoten 1 (SN1) 6 TB hat. Basierend auf diesen Werten:

- Der systemweite **Metadaten reservierter Platz** ist auf 8 TB eingestellt. (Dies ist der Standardwert für StorageGRID 11.6 oder höher, wenn jeder Speicher-Node mehr als 128 GB RAM hat.)
- Der tatsächlich reservierte Speicherplatz für Metadaten von SN1 beträgt 6 TB. (Das gesamte Volume ist reserviert, da Volume 0 kleiner ist als die Einstellung **Metadaten reservierter Speicherplatz**.)
- Der zulässige Speicherplatz für Metadaten auf SN1 beträgt 3 TB, basierend auf der im angegebenen Berechnung Tabelle für zulässigem Speicherplatz für Metadaten: (Tatsächlich reservierter Platz für Metadaten − 1 TB) × 60%, bis zu einem Maximum von 3.96 TB.

Storage-Nodes unterschiedlicher Größen beeinflussen die Objektkapazität

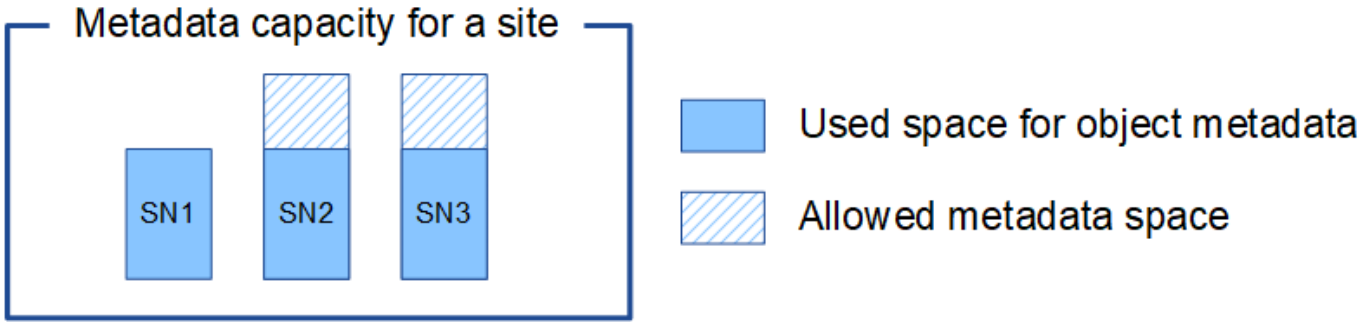
Wie oben beschrieben, verteilt StorageGRID Objektmetadaten gleichmäßig über Storage-Nodes an jedem Standort. Wenn ein Standort Storage-Nodes unterschiedlicher Größen enthält, bestimmt der kleinste Node am Standort die Metadaten-Kapazität des Standorts.

Beispiel:

- Sie haben ein Raster mit drei Storage Nodes unterschiedlicher Größe an einem einzigen Standort.
- Die Einstellung **Metadaten reservierter Platz** beträgt 4 TB.
- Die Storage-Nodes haben die folgenden Werte für den tatsächlich reservierten Metadatenspeicherplatz und den zulässigen Metadatenspeicherplatz.

Storage-Node	Größe von Volumen 0	Tatsächlich reservierter Metadatenspeicherplatz	Zulässiger Metadatenspeicherplatz
SN1	2.2 TB	2.2 TB	1.32 TB
SN2	5 TB	4 TB	1.98 TB
SN3	6 TB	4 TB	1.98 TB

Da Objektmetadaten gleichmäßig auf die Storage-Nodes an einem Standort verteilt werden, kann jeder Node in diesem Beispiel nur 1.32 TB Metadaten enthalten. Die zusätzlichen 0.66 TB an erlaubten Metadaten für SN2 und SN3 können nicht verwendet werden.



Da StorageGRID alle Objektmetadaten für ein StorageGRID System an jedem Standort speichert, wird die Gesamtkapazität der Metadaten eines StorageGRID Systems durch die Objektmetadaten des kleinsten Standorts bestimmt.

Und da die Objektmetadaten die maximale Objektanzahl steuern, wenn einem Node die Metadatenkapazität ausgeht, ist das Grid effektiv voll.

Verwandte Informationen

- Informationen zum Überwachen der Objektmetadatenkapazität für jeden Storage-Node finden Sie in den Anweisungen für "Monitoring von StorageGRID".
- Um die Objekt-Metadaten-Kapazität Ihres Systems zu erhöhen, "Erweitern Sie Ihr Raster" Durch Hinzufügen neuer Storage-Nodes.

Einstellung für reservierten Metadatenspeicher erhöhen

Sie können die Systemeinstellung „Reservierter Speicherplatz für Metadaten“ möglicherweise erhöhen, wenn Ihre Speicherknoten bestimmte Anforderungen an RAM und verfügbaren Speicherplatz erfüllen.

Was du brauchst

- Sie sind mit einem Konto beim Grid Manager angemeldet. "Unterstützter Webbrowser"Die

- Du hast die "Root-Zugriffsberechtigung oder Berechtigungen für die Konfiguration der Grid-Topologieseite und andere Grid-Konfigurationen"Die

Über diese Aufgabe

Möglicherweise können Sie die systemweite Einstellung für den reservierten Metadatenspeicher manuell auf bis zu 8 TB erhöhen.

Sie können den Wert der systemweiten Einstellung „Reservierter Speicherplatz für Metadaten“ nur erhöhen, wenn beide dieser Aussagen zutreffen:

- Die Speicherknoten an jedem Standort in Ihrem System verfügen jeweils über 128 GB oder mehr RAM.
- Die Speicherknoten an jedem Standort in Ihrem System verfügen jeweils über ausreichend verfügbaren Speicherplatz auf Speichervolume 0.

Beachten Sie, dass Sie durch Erhöhen dieser Einstellung gleichzeitig den für die Objektspeicherung verfügbaren Speicherplatz auf Speichervolume 0 aller Speicherknoten reduzieren. Aus diesem Grund möchten Sie den reservierten Speicherplatz für Metadaten möglicherweise lieber auf einen Wert kleiner als 8 TB festlegen, basierend auf den erwarteten Anforderungen an die Objektmetadaten.

> Im Allgemeinen ist es besser, einen höheren Wert als einen niedrigeren Wert zu verwenden. Wenn die Einstellung „Reservierter Speicherplatz für Metadaten“ zu groß ist, können Sie sie später verringern. Wenn Sie den Wert hingegen später erhöhen, muss das System möglicherweise Objektdaten verschieben, um Speicherplatz freizugeben.

Eine detaillierte Erklärung, wie sich die Einstellung „Reservierter Metadatenspeicherplatz“ auf den für die Speicherung von Objektmetadaten auf einem bestimmten Speicherknoten verfügbaren Speicherplatz auswirkt, finden Sie unter "Management von Objekt-Metadaten-Storage"Die

Schritte

1. Ermitteln Sie die aktuelle Einstellung für den reservierten Speicherplatz für Metadaten.
   a. Wählen Sie **KONFIGURATION** > **System** > **Speicheroptionen**.
   b. Beachten Sie im Abschnitt „Speicher-Wasserzeichen“ den Wert von **Reservierter Metadaten-Speicherplatz**.
2. Stellen Sie sicher, dass auf dem Speichervolume 0 jedes Speicherknotens genügend Speicherplatz verfügbar ist, um diesen Wert zu erhöhen.
   a. Wählen Sie **KNOTEN**.
   b. Wählen Sie den ersten Speicherknoten im Raster aus.
   c. Wählen Sie die Registerkarte Speicher.
   d. Suchen Sie im Abschnitt „Volumes“ den Eintrag **/var/local/rangedb/0**.
   e. Vergewissern Sie sich, dass der verfügbare Wert gleich oder größer als die Differenz zwischen dem neuen Wert ist, den Sie verwenden möchten, und dem aktuellen Wert für den reservierten Metadatenspeicher.

      Wenn beispielsweise die Einstellung „Reservierter Speicherplatz für Metadaten“ derzeit 4 TB beträgt und Sie diese auf 6 TB erhöhen möchten, muss der verfügbare Wert 2 TB oder höher sein.

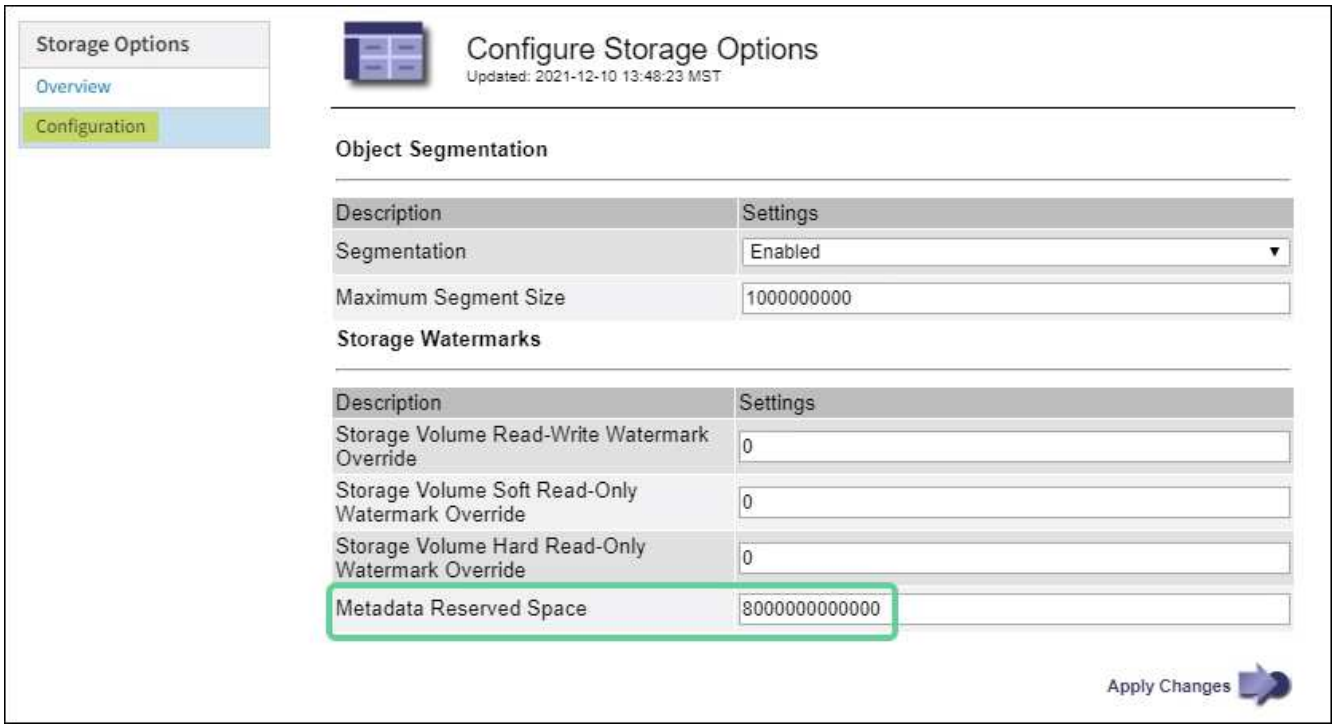
   f. Wiederholen Sie diese Schritte für alle Speicherknoten.
      - Wenn auf einem oder mehreren Speicherknoten nicht genügend Speicherplatz verfügbar ist, kann der Wert für den reservierten Speicherplatz für Metadaten nicht erhöht werden. Fahren Sie mit

diesem Vorgang nicht fort.

- Wenn auf jedem Speicherknoten genügend Speicherplatz auf Volume 0 verfügbar ist, fahren Sie mit dem nächsten Schritt fort.

3. Stellen Sie sicher, dass auf jedem Speicherknoten mindestens 128 GB RAM vorhanden sind.
   a. Wählen Sie **KNOTEN**.
   b. Wählen Sie den ersten Speicherknoten im Raster aus.
   c. Wählen Sie die Registerkarte **Hardware** aus.
   d. Bewegen Sie den Cursor über das Diagramm zur Speichernutzung. Stellen Sie sicher, dass der **Gesamtspeicher** mindestens 128 GB beträgt.
   e. Wiederholen Sie diese Schritte für alle Speicherknoten.
      - Wenn ein oder mehrere Speicherknoten nicht über genügend verfügbaren Gesamtspeicher verfügen, kann der Wert für den reservierten Metadatenspeicher nicht erhöht werden. Fahren Sie mit diesem Vorgang nicht fort.
      - Wenn jeder Speicherknoten über mindestens 128 GB Gesamtspeicher verfügt, fahren Sie mit dem nächsten Schritt fort.
4. Aktualisieren Sie die Einstellung „Reservierter Speicherplatz für Metadaten“.
   a. Wählen Sie **KONFIGURATION** > **System** > **Speicheroptionen**.
   b. Wählen Sie die Registerkarte „Konfiguration“ aus.
   c. Im Abschnitt „Speicherwasserzeichen“ wählen Sie **Reservierter Metadatenspeicherplatz** aus.
   d. Geben Sie den neuen Wert ein.

      Um beispielsweise 8 TB einzugeben, was der maximal unterstützte Wert ist, geben Sie **8000000000000** ein (8, gefolgt von 12 Nullen).



   a. Wählen Sie **Änderungen Anwenden**.

Gespeicherte Objekte komprimieren

Sie können die Objektkomprimierung aktivieren, um die Größe der in StorageGRID gespeicherten Objekte zu reduzieren und so weniger Storage zu belegen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Standardmäßig ist die Objektkomprimierung deaktiviert. Wenn Sie die Komprimierung aktivieren, versucht StorageGRID beim Speichern jedes Objekts mithilfe einer verlustfreien Komprimierung zu komprimieren.

> Wenn Sie diese Einstellung ändern, dauert es etwa eine Minute, bis die neue Einstellung angewendet wird. Der konfigurierte Wert wird für Performance und Skalierung zwischengespeichert.

Bevor Sie die Objektkomprimierung aktivieren, beachten Sie Folgendes:

- Sie sollten nicht **komprimieren gespeicherte Objekte** auswählen, es sei denn, Sie wissen, dass die gespeicherten Daten komprimierbar sind.
- Applikationen, die Objekte in StorageGRID speichern, komprimieren möglicherweise Objekte, bevor sie gespeichert werden. Wenn eine Client-Anwendung ein Objekt bereits komprimiert hat, bevor es in StorageGRID gespeichert wird, verringert die Auswahl dieser Option die Größe eines Objekts nicht weiter.
- Wählen Sie nicht **gespeicherte Objekte komprimieren** wenn Sie NetApp FabricPool mit StorageGRID verwenden.
- Wenn **compress Stored Objects** ausgewählt ist, sollten S3- und Swift-Client-Anwendungen die Ausführung VON GET Object-Operationen vermeiden, die einen Bereich von Bytes angeben, der zurückgegeben werden soll. Diese Vorgänge „`range Read`“ sind ineffizient, da StorageGRID die Objekte effektiv dekomprimieren muss, um auf die angeforderten Bytes zugreifen zu können. VORGÄNGE ZUM ABRUFEN von Objekten, die einen kleinen Byte-Bereich von einem sehr großen Objekt anfordern, sind besonders ineffizient, beispielsweise ist es ineffizient, einen Bereich von 10 MB von einem komprimierten 50-GB-Objekt zu lesen.

  Wenn Bereiche von komprimierten Objekten gelesen werden, können Client-Anforderungen eine Zeitdauer haben.

  > Wenn Sie Objekte komprimieren müssen und Ihre Client-Applikation Bereichslesevorgänge verwenden muss, erhöhen Sie die Zeitüberschreitung beim Lesen der Anwendung.

Schritte

1. Wählen Sie **CONFIGURATION** > **System** > **Objektkomprimierung**.
2. Aktivieren Sie das Kontrollkästchen **gespeicherte Objekte komprimieren**.
3. Wählen Sie **Speichern**.

Konfigurationseinstellungen für Storage-Nodes

Jeder Speicher-Node verwendet mehrere Konfigurationseinstellungen und Zähler. Möglicherweise müssen Sie die aktuellen Einstellungen anzeigen oder Zähler

zurücksetzen, um Alarme zu löschen (Legacy-System).

> Mit Ausnahme der in der Dokumentation ausdrücklich enthaltenen Anweisungen sollten Sie sich mit dem technischen Support in Verbindung setzen, bevor Sie die Konfigurationseinstellungen für den Storage-Node ändern. Nach Bedarf können Sie Ereigniszähler zurücksetzen, um ältere Alarme zu löschen.

Führen Sie die folgenden Schritte aus, um auf die Konfigurationseinstellungen und -Zähler eines Storage Node zuzugreifen.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***site*** > ***Storage Node*** aus.
3. Erweitern Sie den Speicherknoten, und wählen Sie den Dienst oder die Komponente aus.
4. Wählen Sie die Registerkarte **Konfiguration**.

In den folgenden Tabellen sind die Konfigurationseinstellungen für Storage Node zusammengefasst.

LDR

Attributname	Codieren	Beschreibung
HTTP-Status	HSTE	Der aktuelle Status von HTTP für S3, Swift und anderen internen StorageGRID-Datenverkehr: • Offline: Es sind keine Vorgänge zulässig. Jede Client-Anwendung, die versucht, eine HTTP-Sitzung für den LDR-Dienst zu öffnen, erhält eine Fehlermeldung. Aktive Sitzungen werden ordnungsgemäß geschlossen. • Online: Der Vorgang wird normal fortgesetzt
Automatisches Starten von HTTP	HTAS	• Wenn diese Option ausgewählt ist, hängt der Zustand des Systems beim Neustart vom Status der Komponente **LDR** > **Storage** ab. Wenn die Komponente **LDR** > **Storage** beim Neustart schreibgeschützt ist, ist auch die HTTP-Schnittstelle schreibgeschützt. Wenn die Komponente **LDR** > **Speicherung** Online ist, ist HTTP auch Online. Andernfalls bleibt die HTTP-Schnittstelle im Status Offline. • Wenn diese Option nicht aktiviert ist, bleibt die HTTP-Schnittstelle offline, bis sie explizit aktiviert ist.

LDR > Datenspeicher

Attributname	Codieren	Beschreibung
Anzahl Verlorener Objekte Zurücksetzen	RCOR	Setzen Sie den Zähler für die Anzahl der verlorenen Objekte dieses Dienstes zurück.

LDR > Storage

Attributname	Codieren	Beschreibung
Storage-Zustand - Gewünscht	SSDS	Eine vom Benutzer konfigurierbare Einstellung für den gewünschten Status der Speicherkomponente. Der LDR-Dienst liest diesen Wert und versucht, den durch dieses Attribut angegebenen Status zu entsprechen. Der Wert wird bei Neustarts dauerhaft verwendet. Mit dieser Einstellung können Sie beispielsweise dazu zwingen, dass Speicher schreibgeschützt wird, selbst wenn genügend Speicherplatz vorhanden ist. Dies kann bei der Fehlerbehebung hilfreich sein. Das Attribut kann einen der folgenden Werte annehmen: • Offline: Wenn der gewünschte Status Offline ist, schaltet der LDR-Dienst die **LDR** > **Storage** -Komponente offline. • Schreibgeschützt: Wenn der gewünschte Status schreibgeschützt ist, verschiebt der LDR-Service den Speicherstatus auf schreibgeschützt und hört auf, neue Inhalte zu akzeptieren. Beachten Sie, dass Inhalte möglicherweise noch für kurze Zeit im Speicherknoten gespeichert werden, bis offene Sitzungen geschlossen sind. • Online: Den Wert bei Online während des normalen Systembetriebs belassen. Der Speicherstatus – der aktuelle Status der Speicherkomponente wird durch den Service dynamisch festgelegt, basierend auf dem Zustand des LDR-Service, z. B. der Menge des verfügbaren Objektspeicherspeichers. Wenn der Speicherplatz knapp ist, ist die Komponente schreibgeschützt.
Zeitüberschreitung Bei Der Integritätsprüfung	SHCT	Die Zeitgrenze in Sekunden, innerhalb derer ein Integritätstest abgeschlossen werden muss, damit ein Speichervolumen als ordnungsgemäß angesehen wird. Ändern Sie diesen Wert nur, wenn Sie dazu vom Support aufgefordert werden.

LDR > Verifizierung

Attributname	Codieren	Beschreibung
Fehlende Objekte Zurücksetzen Anzahl	VCMI	Setzt die Anzahl der erkannten fehlenden Objekte zurück (OMIS). Nur nach Abschluss der Objektprüfung verwenden. Fehlende replizierte Objektdaten werden vom StorageGRID System automatisch wiederhergestellt.
Verifizierungsrate	VPRI	Legen Sie die Geschwindigkeit fest, mit der die Hintergrundüberprüfung durchgeführt wird. Weitere Informationen zur Konfiguration der Hintergrundüberprüfung finden Sie unter.
Anzahl Der Beschädigten Objekte Zurücksetzen	VCCR	Setzen Sie den Zähler für beschädigte, replizierte Objektdaten zurück, die während der Hintergrundüberprüfung gefunden wurden. Mit dieser Option können Sie den Alarmzustand der beschädigten Objekte löschen, die erkannt wurden (OCOR).
Objekte In Quarantäne Löschen	OQRT	Löschen Sie beschädigte Objekte aus dem Quarantäneverzeichnis, setzen Sie die Anzahl der isolierten Objekte auf Null zurück und löschen Sie den Alarm „Quarantäne Objekte erkannt“ (OQRT). Diese Option wird verwendet, nachdem beschädigte Objekte vom StorageGRID-System automatisch wiederhergestellt wurden. Wenn ein Alarm „Lost Objects“ ausgelöst wird, kann der technische Support auf die isolierten Objekte zugreifen. In manchen Fällen können isolierte Objekte für die Datenwiederherstellung oder das Debuggen der zugrunde liegenden Probleme, die die beschädigten Objektkopien verursacht haben, nützlich sein.

LDR > Erasure Coding

Attributname	Codieren	Beschreibung
Zurücksetzen Der Fehleranzahl Für Schreibvorgänge	RWF.	Setzen Sie den Zähler auf Schreibfehler von Objektdaten mit Erasure-Coding-Verfahren auf den Storage-Node zurück.
Anzahl Der Fehlgeschlagene Lesevorgänge Zurücksetzen	RSRF	Setzen Sie den Zähler für Leseausfälle von Objektdaten mit Erasure-Coding-Verfahren vom Storage-Node zurück.

Attributname	Codieren	Beschreibung
Zurücksetzen Löschen Fehleranzahl	RSDF	Setzen Sie den Zähler für Löschfehler von Objektdaten mit Erasure-Coding-Verfahren vom Storage-Node zurück.
Beschädigte Kopien Erkannte Anzahl Zurücksetzen	RSCC	Setzen Sie den Zähler für die Anzahl beschädigter Kopien von Objektdaten, die nach dem Erasure-Coding-Verfahren codiert wurden, auf dem Storage-Node zurück.
Beschädigte Fragmente Erkannte Anzahl Zurücksetzen	RCD	Setzen Sie den Zähler auf beschädigte Fragmente von Objektdaten mit Erasure-Coding-Verfahren auf dem Storage-Node zurück.
Fehlende Fragmente Erkannt Anzahl Zurücksetzen	RSMD	Setzen Sie den Zähler auf fehlende Fragmente von Objektdaten mit Erasure-Coding-Verfahren auf dem Storage Node zurück. Nur nach Abschluss der Objektprüfung verwenden.

LDR > Replikation

Attributname	Codieren	Beschreibung
Fehleranzahl Inbound Replication Zurücksetzen	RICR	Setzen Sie den Zähler auf Fehler bei eingehender Replikation zurück. Dies kann verwendet werden, um den RIRF-Alarm (Inbound Replication — failed) zu löschen.
Fehleranzahl Für Ausgehende Replikation Zurücksetzen	ROCR	Setzen Sie den Zähler auf Fehler bei ausgehenden Replikationen zurück. Dies kann verwendet werden, um den RORF-Alarm (ausgehende Replikationen — fehlgeschlagen) zu löschen.
Deaktivieren Sie Inbound Replication	DSIR	Wählen Sie diese Option aus, um die eingehende Replikation im Rahmen eines Wartungs- oder Testverfahrens zu deaktivieren. Während des normalen Betriebs nicht aktiviert lassen. Wenn die eingehende Replikation deaktiviert ist, können Objekte vom Speicherknoten abgerufen werden, um sie an andere Speicherorte im StorageGRID-System zu kopieren. Objekte können jedoch nicht von anderen Speicherorten auf diesen Speicherknoten kopiert werden: Der LDR-Dienst ist schreibgeschützt.

Attributname	Codieren	Beschreibung
Deaktivieren Sie Ausgehende Replikation	DSOR	Wählen Sie diese Option aus, um die ausgehende Replikation (einschließlich Inhaltsanforderungen für HTTP-Abrufvorgänge) im Rahmen eines Wartungs- oder Testverfahrens zu deaktivieren. Während des normalen Betriebs nicht aktiviert lassen. Wenn die ausgehende Replikation deaktiviert ist, können Objekte auf diesen Speicherknoten kopiert werden. Objekte können jedoch nicht vom Speicherknoten abgerufen werden, um sie an andere Speicherorte im StorageGRID-System zu kopieren. Der LDR-Service ist schreibgeschützt.

Management vollständiger Storage-Nodes

Wenn Storage-Nodes die Kapazität erreichen, müssen Sie das StorageGRID System durch Hinzufügen eines neuen Storage erweitern. Es sind drei Optionen verfügbar: Das Hinzufügen von Storage Volumes, das Hinzufügen von Shelfs zur Storage-Erweiterung und das Hinzufügen von Storage-Nodes.

Hinzufügen von Storage-Volumes

Jeder Storage-Node unterstützt eine maximale Anzahl an Storage-Volumes. Der definierte Höchstwert variiert je nach Plattform. Wenn ein Storage-Node weniger als die maximale Anzahl an Storage-Volumes enthält, können Sie Volumes hinzufügen, um seine Kapazität zu erhöhen. Siehe Anweisungen für "Erweitern eines StorageGRID Systems".

Hinzufügen von Shelfs zur Storage-Erweiterung

Einige Storage-Nodes von StorageGRID Appliances, z. B. SG6060, können zusätzliche Storage-Shelfs unterstützen. Bei StorageGRID Appliances mit Erweiterungsfunktionen, die nicht bereits auf die maximale Kapazität erweitert wurden, können Sie Storage-Shelfs zur Steigerung der Kapazität hinzufügen. Siehe Anweisungen für "Erweitern eines StorageGRID Systems".

Storage-Nodes Hinzufügen

Sie können die Storage-Kapazität durch Hinzufügen von Storage-Nodes erhöhen. Beim Hinzufügen von Storage müssen die aktuell aktiven ILM-Regeln und Kapazitätsanforderungen sorgfältig berücksichtigt werden. Siehe Anweisungen für "Erweitern eines StorageGRID Systems".

Managen Sie Admin-Nodes

Was ist ein Admin-Node?

Admin Nodes stellen Managementservices wie Systemkonfiguration, Monitoring und Protokollierung bereit. Jedes Grid muss einen primären Admin-Node haben und kann eine beliebige Anzahl nicht primärer Admin-Nodes für Redundanz aufweisen.

Wenn Sie sich beim Grid Manager oder dem Tenant Manager anmelden, stellen Sie eine Verbindung zu einem Admin-Node her. Sie können eine Verbindung zu einem beliebigen Admin-Knoten herstellen, und jeder Admin-

Knoten zeigt eine ähnliche Ansicht des StorageGRID-Systems an. Wartungsverfahren müssen jedoch mit dem primären Admin-Node durchgeführt werden.

Admin-Nodes können auch verwendet werden, um den S3- und Swift-Client-Datenverkehr auszugleichen.

Was ist der bevorzugte Absender

Wenn Ihre StorageGRID-Bereitstellung mehrere Administratorknoten umfasst, ist der primäre Administratorknoten der bevorzugte Absender für Warnmeldungen, AutoSupport-Nachrichten, SNMP-Traps und -Benachrichtigungen sowie ältere Alarmmeldungen.

Im normalen Systembetrieb sendet nur der bevorzugte Sender Benachrichtigungen. Alle anderen Admin-Knoten überwachen jedoch den bevorzugten Sender. Wenn ein Problem erkannt wird, fungieren andere Admin-Nodes als *Standby-Sender*.

In den folgenden Fällen können mehrere Benachrichtigungen gesendet werden:

- Wenn Admin-Knoten voneinander „islanded“ werden, versuchen sowohl der bevorzugte Sender als auch der Standby-Sender, Benachrichtigungen zu senden, und es können mehrere Kopien von Benachrichtigungen empfangen werden.
- Wenn der Standby-Sender Probleme mit dem bevorzugten Sender erkennt und mit dem Senden von Benachrichtigungen beginnt, kann der bevorzugte Sender möglicherweise wieder Benachrichtigungen senden. In diesem Fall können doppelte Benachrichtigungen gesendet werden. Der Standby-Sender hört auf, Benachrichtigungen zu senden, wenn Fehler auf dem bevorzugten Sender nicht mehr erkannt werden.

> ⓘ Wenn Sie AutoSupport-Meldungen testen, senden alle Administratorknoten die Test-E-Mail. Wenn Sie die Warnbenachrichtigungen testen, müssen Sie sich bei jedem Admin-Knoten anmelden, um die Verbindung zu überprüfen.

Primäre Dienste für Admin-Nodes

Die folgende Tabelle zeigt die primären Dienste für Admin-Nodes. Diese Tabelle enthält jedoch nicht alle Node-Services.

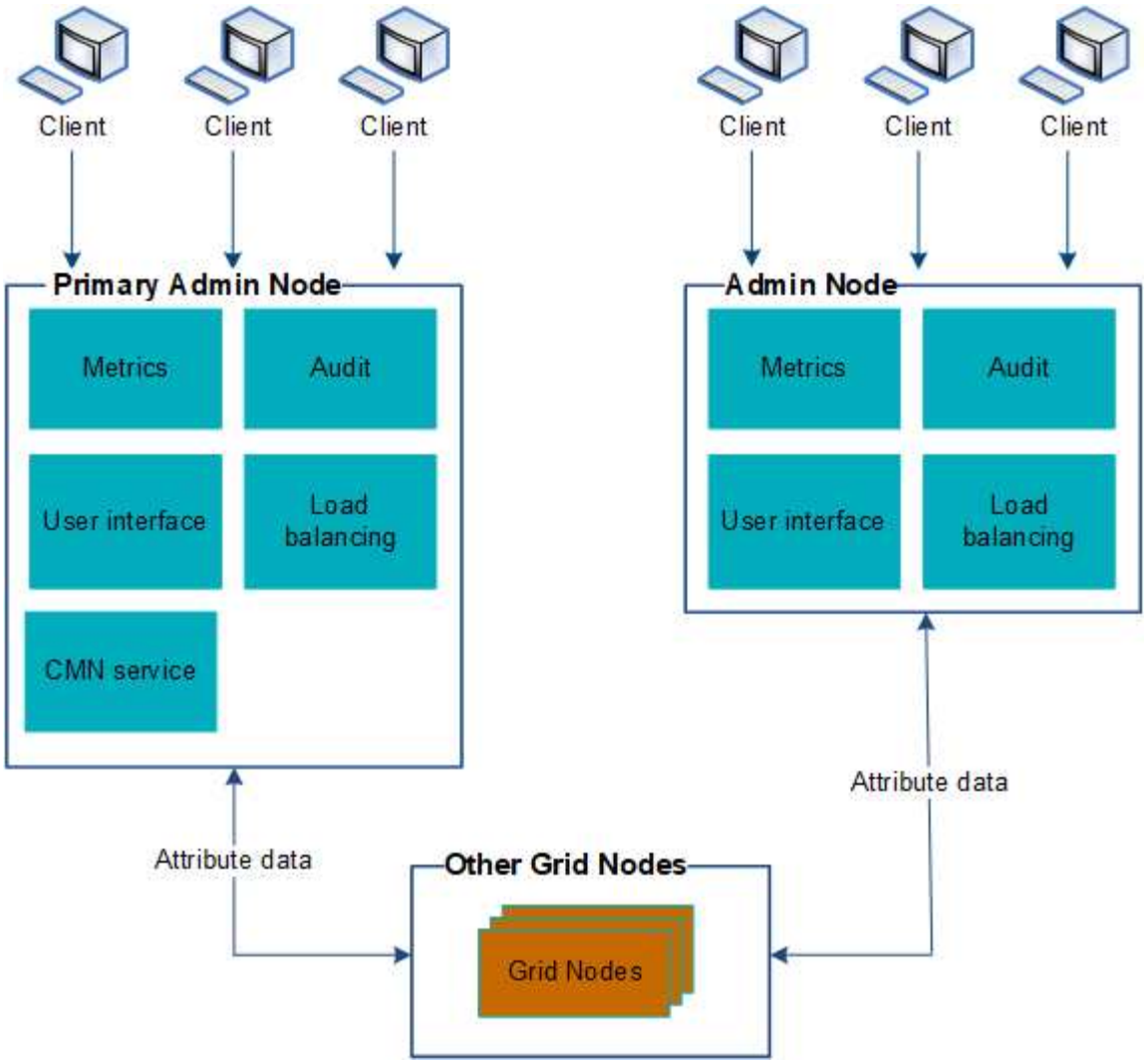
Service	Tastenfunktion
Audit Management System (AMS)	Verfolgt Systemaktivitäten und -Ereignisse.
Configuration Management Node (CMN)	Verwaltet die systemweite Konfiguration. Nur primärer Admin-Node.
Management-Applikations-Programmierschnittstelle (Management-API)	Verarbeitet Anforderungen aus der Grid-Management-API und der Mandantenmanagement-API.
Hochverfügbarkeit	Verwaltet hochverfügbare virtuelle IP-Adressen für Gruppen von Admin-Nodes und Gateway-Nodes. **Hinweis:** dieser Service befindet sich auch auf Gateway Nodes.

Service	Tastenfunktion
Lastausgleich	Sorgt für einen Lastenausgleich des S3- und Swift-Datenverkehrs von Clients zu Storage Nodes. **Hinweis:** dieser Service befindet sich auch auf Gateway Nodes.
Netzwerk-Management-System (NMS)	Bietet Funktionen für den Grid Manager.
Prometheus	Sammelt und speichert Zeitreihenmetriken von den Services auf allen Knoten.
Server Status Monitor (SSM)	Überwachung des Betriebssystems und der zugrunde liegenden Hardware

Verwenden Sie mehrere Admin-Nodes

Ein StorageGRID-System kann mehrere Admin-Knoten enthalten, damit Sie Ihr StorageGRID-System kontinuierlich überwachen und konfigurieren können, auch wenn ein Admin-Knoten ausfällt.

Wenn ein Admin-Knoten nicht mehr verfügbar ist, wird die Attributverarbeitung fortgesetzt, Alarme und Alarme (Legacy-System) werden immer noch ausgelöst und E-Mail-Benachrichtigungen und AutoSupport-Meldungen werden weiterhin gesendet. Das Vorhandensein mehrerer Admin-Nodes bietet jedoch keinen Failover-Schutz außer Benachrichtigungen und AutoSupport-Meldungen. Insbesondere werden Alarmbestätigungen von einem Admin-Knoten nicht in andere Admin-Knoten kopiert.



Es gibt zwei Optionen, um das StorageGRID-System weiterhin anzuzeigen und zu konfigurieren, wenn ein Admin-Knoten ausfällt:

- Webclients können sich mit jedem anderen verfügbaren Admin-Node verbinden.
- Wenn ein Systemadministrator eine Hochverfügbarkeitsgruppe von Admin-Nodes konfiguriert hat, können Webclients unter Verwendung der virtuellen IP-Adresse der HA-Gruppe weiterhin auf den Grid Manager oder den Mandanten Manager zugreifen. Siehe "Management von Hochverfügbarkeitsgruppen".

> Bei Verwendung einer HA-Gruppe wird der Zugriff unterbrochen, wenn der aktive Admin-Node ausfällt. Benutzer müssen sich erneut anmelden, nachdem die virtuelle IP-Adresse der HA-Gruppe auf einen anderen Admin-Node in der Gruppe Failover erfolgt.

Einige Wartungsarbeiten können nur mit dem primären Admin-Node ausgeführt werden. Wenn der primäre Admin-Node ausfällt, muss er wiederhergestellt werden, bevor das StorageGRID System wieder voll funktionsfähig ist.

Identifizieren Sie den primären Admin-Node

Der primäre Admin-Node hostet den CMN-Service. Einige Wartungsarbeiten können nur mit dem primären Admin-Node durchgeführt werden.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***Site*** > **Admin-Node**, und wählen Sie dann aus ➕ So erweitern Sie die Topologiestruktur und zeigen die auf diesem Admin-Node gehosteten Services an.

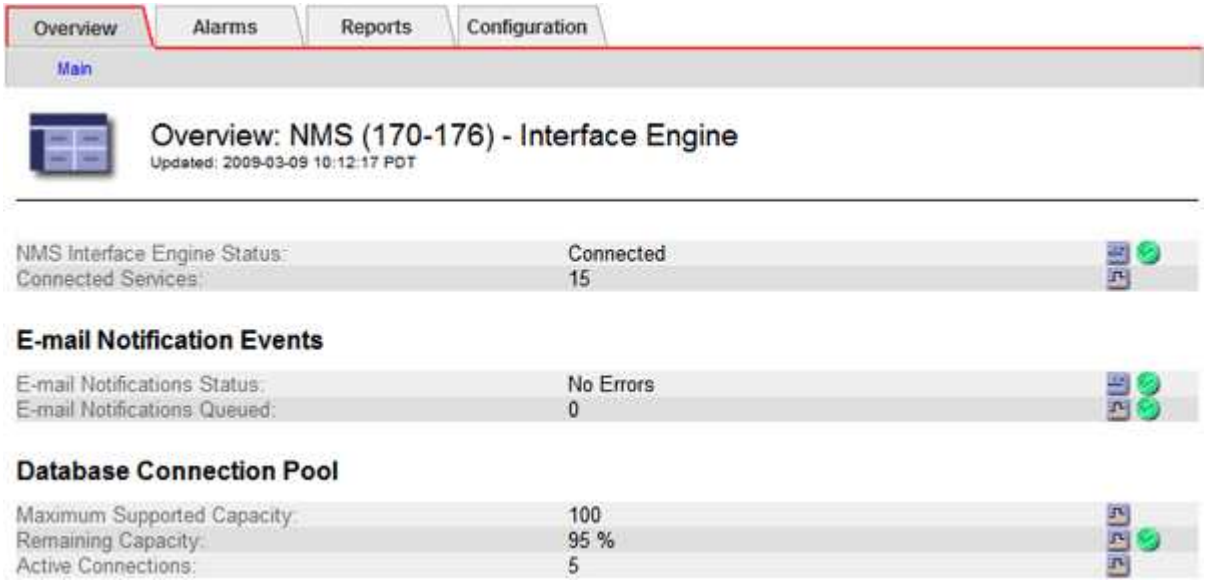
   Der primäre Admin-Node hostet den CMN-Service.

3. Wenn dieser Admin-Node den CMN-Dienst nicht hostet, prüfen Sie die anderen Admin-Nodes.

Benachrichtigungsstatus und -Warteschlangen anzeigen

Der NMS-Dienst (Network Management System) auf Admin Nodes sendet Benachrichtigungen an den Mail-Server. Sie können den aktuellen Status des NMS-Dienstes und die Größe der Benachrichtigungswarteschlange auf der Seite Interface Engine anzeigen.

Um auf die Seite Interface Engine zuzugreifen, wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie**. Wählen Sie schließlich ***site*** > ***Admin Node*** > **NMS** > **Interface Engine** aus.



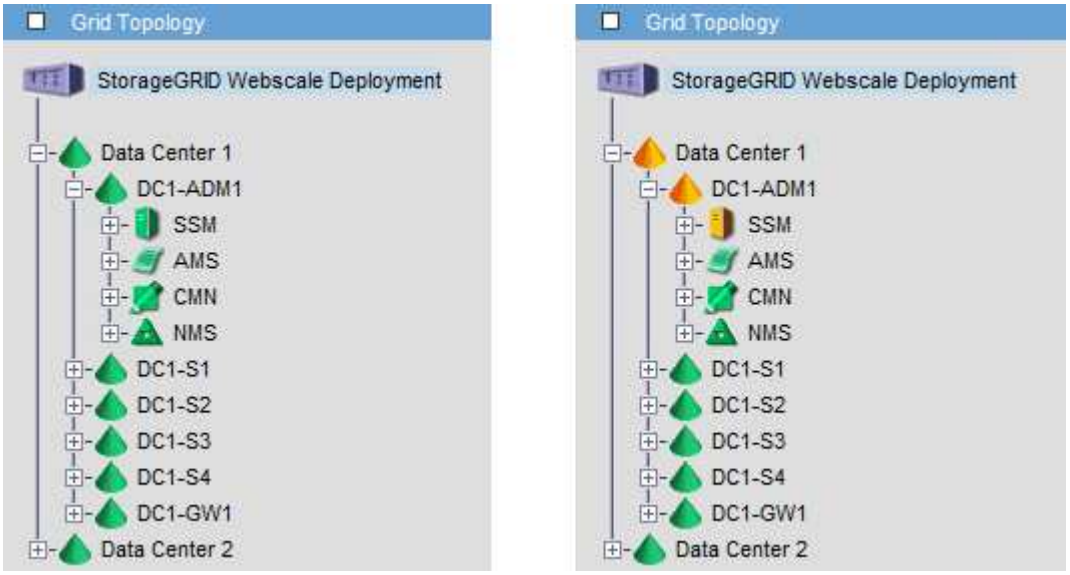
Benachrichtigungen werden über die E-Mail-Benachrichtigungswarteschlange verarbeitet und an den Mail-Server gesendet, einer nach dem anderen in der Reihenfolge, in der sie ausgelöst werden. Wenn ein Problem auftritt (z. B. ein Netzwerkverbindungsfehler) und der Mail-Server nicht verfügbar ist, wenn versucht wird, die Benachrichtigung zu senden, wird der Versuch unternommen, die Benachrichtigung an den Mailserver erneut zu senden, 60 Sekunden lang fortgesetzt. Wenn die Benachrichtigung nach 60 Sekunden nicht an den Mailserver gesendet wird, wird die Benachrichtigung aus der Benachrichtigungswarteschlange gelöscht und es wird versucht, die nächste Benachrichtigung in der Warteschlange zu senden.

Da Benachrichtigungen aus der Benachrichtigungswarteschlange gelöscht werden können, ohne gesendet zu werden, ist es möglich, dass ein Alarm ausgelöst werden kann, ohne dass eine Benachrichtigung gesendet wird. Wenn eine Benachrichtigung aus der Warteschlange gelöscht wird, ohne gesendet zu werden, wird der geringfügige ALARM MIN (E-Mail-Benachrichtigungsstatus) ausgelöst.

So zeigen Admin-Knoten bestätigte Alarme an (Legacy-System)

Wenn Sie einen Alarm an einem Admin-Knoten bestätigen, wird der bestätigte Alarm nicht auf einen anderen Admin-Knoten kopiert. Da Bestätigungen nicht in andere Admin-Knoten kopiert werden, sieht die Struktur der Grid-Topologie für jeden Admin-Knoten möglicherweise nicht gleich aus.

Dieser Unterschied kann nützlich sein, wenn Web-Clients verbunden werden. Web-Clients können je nach Administratoranforderungen unterschiedliche Ansichten des StorageGRID-Systems haben.



Beachten Sie, dass Benachrichtigungen vom Admin-Knoten gesendet werden, wo die Bestätigung erfolgt.

Konfigurieren des Zugriffs auf Audit-Clients

Konfigurieren Sie den Client-Zugriff für die Prüfung für NFS

Der Admin-Knoten protokolliert über den Service Audit Management System (AMS) alle überprüften Systemereignisse in eine Protokolldatei, die über die Revisionsfreigabe verfügbar ist und die zu jedem Admin-Knoten bei der Installation hinzugefügt wird. Die Revisionsfreigabe wird automatisch als schreibgeschützte Freigabe aktiviert.

Für den Zugriff auf Audit-Protokolle können Sie den Clientzugriff auf Audit-Freigaben für NFS konfigurieren. Sie können es auch "Verwenden Sie einen externen Syslog-Server".

Das StorageGRID System verwendet eine positive Bestätigung, um den Verlust von Audit-Meldungen zu verhindern, bevor sie in die Protokolldatei geschrieben werden. Eine Meldung bleibt an einem Dienst in der Warteschlange, bis der AMS-Dienst oder ein Zwischenaudit-Relaisdienst die Kontrolle über ihn bestätigt hat. Weitere Informationen finden Sie unter "Prüfung von Audit-Protokollen".

Bevor Sie beginnen

- Sie haben die `Passwords.txt` Datei mit dem Root-/Admin-Passwort.
- Sie haben die `Configuration.txt` Datei (verfügbar im Wiederherstellungspaket).
- Der Audit-Client verwendet die NFS-Version 3 (NFSv3).

Über diese Aufgabe

Führen Sie dieses Verfahren für jeden Admin-Knoten in einer StorageGRID-Bereitstellung durch, von der aus Sie Audit-Nachrichten abrufen möchten.

Schritte

1. Melden Sie sich beim primären Admin-Node an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

      Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Vergewissern Sie sich, dass alle Dienste den Status „ausgeführt“ oder „verifiziert“ aufweisen. Geben Sie Ein: `storagegrid-status`

   Wenn Services nicht als „aktiv“ oder „geprüft“ aufgeführt sind, beheben Sie Probleme, bevor Sie fortfahren.

3. Zurück zur Kommandozeile. Drücken Sie **Strg+C**.
4. Starten Sie das NFS-Konfigurationsprogramm. Geben Sie Ein: `config_nfs.rb`

```
----------------------------------------------------------------------
| Shares                | Clients              | Config           |
----------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config  |
| enable-disable-share  | remove-ip-from-share | refresh-config   |
|                       |                      | help             |
|                       |                      | exit             |
----------------------------------------------------------------------
```

5. Fügen Sie den Audit-Client hinzu: `add-audit-share`
   a. Geben Sie bei entsprechender Aufforderung die IP-Adresse oder den IP-Adressbereich des Audit-Clients für die Revisionsfreigabe ein: `client_IP_address`
   b. Drücken Sie auf der entsprechenden Aufforderung **Enter**.
6. Wenn mehr als ein Audit-Client auf die Revisionsfreigabe zugreifen darf, fügen Sie die IP-Adresse des zusätzlichen Benutzers hinzu: `add-ip-to-share`
   a. Geben Sie die Nummer der Revisionsfreigabe ein: *`audit_share_number`*
   b. Geben Sie bei entsprechender Aufforderung die IP-Adresse oder den IP-Adressbereich des Audit-Clients für die Revisionsfreigabe ein: *`client_IP_address`*
   c. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

      Das NFS-Konfigurationsprogramm wird angezeigt.

   d. Wiederholen Sie diese Teilschritte für jeden zusätzlichen Audit-Client, der Zugriff auf die Revisionsfreigabe hat.

7. Überprüfen Sie optional Ihre Konfiguration.
   a. Geben Sie Folgendes ein: `validate-config`

      Die Dienste werden überprüft und angezeigt.

   b. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

      Das NFS-Konfigurationsprogramm wird angezeigt.

   c. Schließen Sie das NFS-Konfigurationsdienstprogramm: `exit`
8. Legen Sie fest, ob die Revisionsfreigaben an anderen Standorten aktiviert werden müssen.
   - Wenn es sich bei der StorageGRID-Implementierung um einen einzelnen Standort handelt, mit dem nächsten Schritt fortfahren.
   - Wenn die StorageGRID-Bereitstellung Admin-Nodes an anderen Standorten umfasst, aktivieren Sie die folgenden Audit-Freigaben nach Bedarf:
     i. Remote-Anmeldung beim Admin-Node des Standorts:
        A. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
        B. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
        C. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
        D. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
     ii. Wiederholen Sie diese Schritte, um die Revisionsfreigaben für jeden zusätzlichen Admin-Node zu konfigurieren.
     iii. Schließen Sie die sichere Remote-Shell-Anmeldung am Remote-Admin-Node. Geben Sie Ein: `exit`
9. Melden Sie sich aus der Befehlsshell ab: `exit`

NFS-Audit-Clients erhalten auf Basis ihrer IP-Adresse Zugriff auf eine Revisionsfreigabe. Gewähren Sie einem neuen NFS-Audit-Client Zugriff auf die Revisionsfreigabe, indem Sie der Freigabe ihre IP-Adresse hinzufügen oder einen vorhandenen Audit-Client entfernen, indem Sie seine IP-Adresse entfernen.

Fügen Sie einem Audit-Share einen NFS-Audit-Client hinzu

NFS-Audit-Clients erhalten auf Basis ihrer IP-Adresse Zugriff auf eine Revisionsfreigabe. Gewähren Sie einem neuen NFS-Audit-Client Zugriff auf die Revisionsfreigabe, indem Sie dessen IP-Adresse zur Revisionsfreigabe hinzufügen.

Bevor Sie beginnen

- Sie haben die `Passwords.txt` Datei mit dem Passwort für das Root-/Administratorkonto.
- Sie haben die `Configuration.txt` Datei (verfügbar im Wiederherstellungspaket).
- Der Audit-Client verwendet die NFS-Version 3 (NFSv3).

Schritte

1. Melden Sie sich beim primären Admin-Node an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`

b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Starten Sie das NFS-Konfigurationsprogramm: `config_nfs.rb`

```
----------------------------------------------------------------
| Shares                | Clients              | Config          |
----------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
----------------------------------------------------------------
```

3. Geben Sie Ein: `add-ip-to-share`

Es wird eine Liste der auf dem Admin-Knoten aktivierten NFS-Audit-Freigaben angezeigt. Die Revisionsfreigabe ist wie folgt aufgelistet: `/var/local/audit/export`

4. Geben Sie die Nummer der Revisionsfreigabe ein: *`audit_share_number`*
5. Geben Sie bei entsprechender Aufforderung die IP-Adresse oder den IP-Adressbereich des Audit-Clients für die Revisionsfreigabe ein: *`client_IP_address`*

Der Audit-Client wird der Revisionsfreigabe hinzugefügt.

6. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das NFS-Konfigurationsprogramm wird angezeigt.

7. Wiederholen Sie die Schritte für jeden Audit-Client, der zur Revisionsfreigabe hinzugefügt werden soll.
8. Überprüfen Sie optional die Konfiguration: `validate-config`

Die Dienste werden überprüft und angezeigt.

a. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

Das NFS-Konfigurationsprogramm wird angezeigt.

9. Schließen Sie das NFS-Konfigurationsdienstprogramm: `exit`
10. Wenn es sich bei der StorageGRID-Implementierung um einen einzelnen Standort handelt, mit dem nächsten Schritt fortfahren.

Wenn die StorageGRID-Bereitstellung Admin-Nodes an anderen Standorten umfasst, aktivieren Sie andernfalls optional diese Audit-Shares nach Bedarf:

a. Remote-Anmeldung beim Admin-Node eines Standorts:
   i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`
   ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
   iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
b. Wiederholen Sie diese Schritte, um die Revisionsfreigaben für jeden Admin-Knoten zu konfigurieren.
c. Schließen Sie die sichere Remote-Shell-Anmeldung am Remote-Admin-Node: `exit`

11. Melden Sie sich aus der Befehlsshell ab: `exit`

Prüfung der NFS-Audit-Integration

Nachdem Sie eine Audit-Freigabe konfiguriert und einen NFS-Audit-Client hinzugefügt haben, können Sie die Audit-Client-Freigabe mounten und überprüfen, ob die Dateien über die Audit-Freigabe verfügbar sind.

Schritte

1. Überprüfen Sie die Konnektivität (oder Variante für das Clientsystem) mithilfe der clientseitigen IP-Adresse des Admin-Knotens, der den AMS-Dienst hostet. Geben Sie Ein: `ping IP_address`

   Stellen Sie sicher, dass der Server antwortet, und geben Sie die Konnektivität an.

2. Mounten Sie die schreibgeschützte Revisionsfreigabe mit einem dem Client-Betriebssystem entsprechenden Befehl. Ein Beispiel für Linux lautet (geben Sie in einer Zeile ein):

   `mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/audit/export myAudit`

   Verwenden Sie die IP-Adresse des Admin-Knotens, der den AMS-Dienst hostet, und den vordefinierten Freigabennamen für das Audit-System. Der Mount-Punkt kann ein beliebiger Name sein, der vom Client ausgewählt wurde (z. B. *myAudit* Im vorherigen Befehl).

3. Stellen Sie sicher, dass die Dateien über die Revisionsfreigabe verfügbar sind. Geben Sie Ein: `ls myAudit /*`

   Wo *myAudit* Ist der Bereitstellungspunkt der Revisionsfreigabe. Es sollte mindestens eine Protokolldatei aufgeführt sein.

Entfernen Sie einen NFS-Audit-Client aus der Revisionsfreigabe

NFS-Audit-Clients erhalten auf Basis ihrer IP-Adresse Zugriff auf eine Revisionsfreigabe. Sie können einen vorhandenen Audit-Client entfernen, indem Sie seine IP-Adresse entfernen.

Bevor Sie beginnen

- Sie haben die `Passwords.txt` Datei mit dem Passwort für das Root-/Administratorkonto.
- Sie haben die `Configuration.txt` Datei (verfügbar im Wiederherstellungspaket).

Über diese Aufgabe

Sie können die letzte IP-Adresse, die für den Zugriff auf die Überwachungsfreigabe zulässig ist, nicht entfernen.

Schritte

1. Melden Sie sich beim primären Admin-Node an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

      Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Starten Sie das NFS-Konfigurationsprogramm: `config_nfs.rb`

```
----------------------------------------------------------------------
| Shares                | Clients              | Config           |
----------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config  |
| enable-disable-share  | remove-ip-from-share | refresh-config   |
|                       |                      | help             |
|                       |                      | exit             |
----------------------------------------------------------------------
```

3. Entfernen Sie die IP-Adresse aus der Revisionsfreigabe: `remove-ip-from-share`

   Eine nummerierte Liste der auf dem Server konfigurierten Audit-Freigaben wird angezeigt. Die Revisionsfreigabe ist wie folgt aufgelistet: `/var/local/audit/export`

4. Geben Sie die Nummer für die Revisionsfreigabe ein: *`audit_share_number`*

   Eine nummerierte Liste mit IP-Adressen, die Zugriff auf die Revisionsfreigabe ermöglichen, wird angezeigt.

5. Geben Sie die Nummer für die IP-Adresse ein, die Sie entfernen möchten.

   Die Revisionsfreigabe wird aktualisiert, und der Zugriff ist von keinem Audit-Client mit dieser IP-Adresse mehr gestattet.

6. Drücken Sie auf der entsprechenden Aufforderung **Enter**.

   Das NFS-Konfigurationsprogramm wird angezeigt.

7. Schließen Sie das NFS-Konfigurationsdienstprogramm: `exit`
8. Wenn es sich bei Ihrer StorageGRID-Bereitstellung um mehrere Datacenter-Standortimplementierungen mit zusätzlichen Admin-Nodes an anderen Standorten handelt, deaktivieren Sie diese Revisionsfreigaben nach Bedarf:
   a. Remote-Anmeldung bei jedem Standort Admin-Node:

i. Geben Sie den folgenden Befehl ein: `ssh admin@grid_node_IP`

ii. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

iii. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`

iv. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

b. Wiederholen Sie diese Schritte, um die Revisionsfreigaben für jeden zusätzlichen Admin-Node zu konfigurieren.

c. Schließen Sie die sichere Remote-Shell-Anmeldung am Remote-Admin-Node: `exit`

9. Melden Sie sich aus der Befehlsshell ab: `exit`

Ändern der IP-Adresse eines NFS-Audit-Clients

Führen Sie diese Schritte aus, wenn Sie die IP-Adresse eines NFS-Audit-Clients ändern müssen.

Schritte

1. Fügen Sie einer vorhandenen NFS-Revisionsfreigabe eine neue IP-Adresse hinzu.
2. Entfernen Sie die ursprüngliche IP-Adresse.

Verwandte Informationen

- "Fügen Sie einem Audit-Share einen NFS-Audit-Client hinzu"
- "Entfernen Sie einen NFS-Audit-Client aus der Revisionsfreigabe"

Archiv-Nodes Managen

Was ist ein Archivknoten?

Optional kann jeder StorageGRID Datacenter-Standort mit einem Archiv-Node implementiert werden, sodass eine Verbindung zu einem externen Archiv-Storage-System wie Tivoli Storage Manager (TSM) hergestellt werden kann.

> Die Unterstützung für Archive Nodes (für die Archivierung in der Cloud mit der S3-API und die Archivierung auf Band mit TSM-Middleware) ist veraltet und wird in einer zukünftigen Version entfernt. Das Verschieben von Objekten von einem Archive Node in ein externes Archiv-Storage-System wurde durch ILM Cloud Storage Pools ersetzt, die mehr Funktionen bieten.
>
> Siehe:
>
> - "Migrieren von Objekten in einen Cloud-Storage-Pool"
> - "Verwendung Von Cloud Storage Pools"
>
> Darüber hinaus sollten Sie Archivknoten aus der aktiven ILM-Richtlinie in StorageGRID 11.7 oder früher entfernen. Das Entfernen von Objektdaten, die auf Archive Nodes gespeichert sind, vereinfacht zukünftige Upgrades. Siehe "Arbeiten mit ILM-Regeln und ILM-Richtlinien".

Der Archive Node bietet eine Schnittstelle, über die Sie ein externes Archiv-Storage-System zur langfristigen Speicherung von Objektdaten gezielt einsetzen können. Der Archivknoten überwacht darüber hinaus diese Verbindung und die Übertragung von Objektdaten zwischen dem StorageGRID System und dem angestrebten

externen Archiv-Storage-System.

Nachdem Sie Verbindungen zum externen Ziel konfiguriert haben, können Sie den Archiv-Node so konfigurieren, dass die TSM-Performance optimiert wird, einen Archiv-Node offline schalten, wenn sich ein TSM-Server der Kapazität nähert oder nicht mehr verfügbar ist, und Einstellungen für Replikation und Abruf konfigurieren. Sie können auch benutzerdefinierte Alarme für den Knoten Archiv einstellen.

Objektdaten, auf die nicht gelöscht werden können, aber nicht regelmäßig zugegriffen wird, können jederzeit von den rotierenden Festplatten eines Storage-Nodes auf externen Archiv-Storage wie die Cloud oder auf Tapes verschoben werden. Diese Archivierung von Objektdaten erfolgt durch die Konfiguration des Archiv-Nodes eines Datacenter-Standorts und anschließend die Konfiguration von ILM-Regeln, bei denen dieser Archivknoten als „Ziel“ für Anweisungen zur Content-Platzierung ausgewählt wird. Der Archivknoten verwaltet die archivierten Objektdaten nicht selbst; dies wird durch das externe Archivgerät erreicht.

Objektmetadaten werden nicht archiviert, bleiben aber auf Storage-Nodes erhalten.

Was der ARC-Service ist

Der ARC-Dienst (Archive Nodes) stellt die Managementoberfläche bereit, über die Sie Verbindungen zu externen Archivspeichern konfigurieren können, z. B. Bandmedien über TSM Middleware.

Der ARC-Service interagiert mit einem externen Archivspeichersystem, sendet Objektdaten für Nearline-Speicherung und führt Abrufvorgänge durch, wenn eine Client-Anwendung ein archiviertes Objekt anfordert. Wenn eine Client-Anwendung ein archiviertes Objekt anfordert, fordert ein Storage Node die Objektdaten vom ARC-Service an. Der ARC-Dienst stellt eine Anfrage an das externe Archiv-Speichersystem, das die angeforderten Objektdaten abruft und diese an den ARC-Dienst sendet. Der ARC-Dienst überprüft die Objektdaten und leitet sie an den Speicherknoten weiter, der wiederum das Objekt an die anfordernde Client-Anwendung zurückgibt.

Anfragen nach über TSM Middleware auf Tape archivierten Objektdaten werden für eine effiziente Abrufvorgänge verwaltet. Anfragen können so bestellt werden, dass Objekte, die nacheinander auf Band gespeichert sind, in derselben sequenziellen Reihenfolge angefordert werden. Anforderungen werden dann in die Warteschlange gestellt, um sie an das Speichergerät zu übertragen. Je nach Archivgerät können mehrere Anfragen für Objekte auf verschiedenen Volumes gleichzeitig verarbeitet werden.

Archivierung in der Cloud über die S3-API

Ein Archivierungs-Node kann so konfiguriert werden, dass er eine direkte Verbindung zu Amazon Web Services (AWS) oder einem anderen System herstellt, das über die S3-API mit dem StorageGRID-System verbunden werden kann.

Die Unterstützung für Archive Nodes (für die Archivierung in der Cloud mit der S3-API und die Archivierung auf Band mit TSM-Middleware) ist veraltet und wird in einer zukünftigen Version entfernt. Das Verschieben von Objekten von einem Archive Node in ein externes Archiv-Storage-System wurde durch ILM Cloud Storage Pools ersetzt, die mehr Funktionen bieten.

Siehe "Verwendung Von Cloud Storage Pools".

Konfigurieren Sie die Verbindungseinstellungen für die S3-API

Wenn Sie über die S3-Schnittstelle eine Verbindung zu einem Archiv-Node herstellen, müssen Sie die Verbindungseinstellungen für die S3-API konfigurieren. Bis diese Einstellungen konfiguriert sind, bleibt der ARC-Dienst in einem wichtigen Alarmzustand,

da er nicht mit dem externen Archivspeichersystem kommunizieren kann.

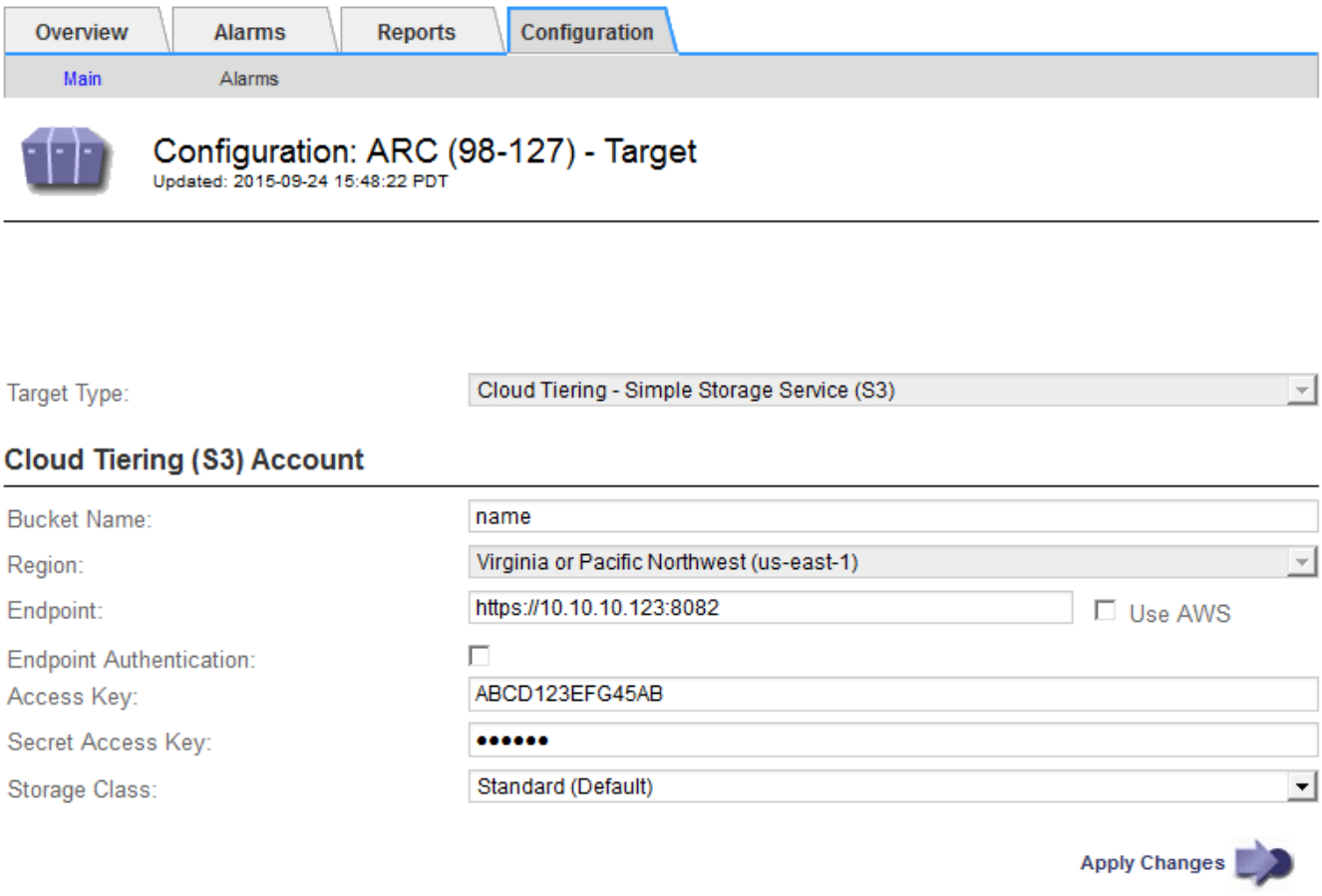
> Die Unterstützung für Archive Nodes (für die Archivierung in der Cloud mit der S3-API und die Archivierung auf Band mit TSM-Middleware) ist veraltet und wird in einer zukünftigen Version entfernt. Das Verschieben von Objekten von einem Archive Node in ein externes Archiv-Storage-System wurde durch ILM Cloud Storage Pools ersetzt, die mehr Funktionen bieten.
>
> Siehe "Verwendung Von Cloud Storage Pools".

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben auf dem Ziel-Archiv-Storage-System einen Bucket erstellt:
  - Der Bucket ist einem einzelnen Archiv-Node zugewiesen. Sie kann nicht von anderen Archivierungs-Knoten oder anderen Anwendungen verwendet werden.
  - Der Bucket hat die für Ihren Standort ausgewählte Region.
  - Der Bucket sollte mit der Versionierung als ausgesetzt konfiguriert werden.
- Objektsegmentierung ist aktiviert, und die maximale Segmentgröße beträgt weniger als oder gleich 4.5 gib (4,831,838,208 Byte). S3-API-Anfragen, die diesen Wert überschreiten, schlagen fehl, wenn S3 als externes Archiv-Storage-System verwendet wird.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie **Archivknoten** > **ARC** > **Ziel**.
3. Wählen Sie **Konfiguration** > **Main**.



4. Wählen Sie in der Dropdown-Liste Zieltyp * Cloud Tiering - Simple Storage Service (S3)* aus.

   Konfigurationseinstellungen sind erst verfügbar, wenn Sie einen Zieltyp auswählen.

5. Konfigurieren Sie das Cloud-Tiering-Konto (S3), über das der Archive-Node eine Verbindung zum externen S3-fähigen Archiv-Storage-System herstellen soll.

   Die meisten Felder auf dieser Seite sind selbsterklärend. Im folgenden werden die Felder beschrieben, für die Sie möglicherweise Hinweise benötigen.

   - **Region**: Nur verfügbar, wenn **AWS verwenden** ausgewählt ist. Die ausgewählte Region muss mit der Region des Buckets übereinstimmen.
   - **Endpunkt** und **AWS verwenden**: Für Amazon Web Services (AWS) wählen Sie **AWS verwenden**. **Endpunkt** wird dann automatisch mit einer Endpunkt-URL auf der Grundlage der Attribute Bucket-Name und Region ausgefüllt. Beispiel:

     ```
     https://bucket.region.amazonaws.com
     ```

     Geben Sie bei einem nicht von AWS stammenden Ziel die URL des Systems ein, das den Bucket hostet, einschließlich der Portnummer. Beispiel:

```
https://system.com:1080
```

   - **Endpunktauthentifizierung**: Standardmäßig aktiviert. Wenn das Netzwerk zum externen Archivspeichersystem vertrauenswürdig ist, können Sie das Kontrollkästchen deaktivieren, um die Überprüfung von SSL-Zertifikaten und Hostnamen für das Zielspeichersystem für die externe Archivierung zu deaktivieren. Wenn eine andere Instanz eines StorageGRID-Systems das Archiv-

Zielspeichergerät ist und das System mit öffentlich signierten Zertifikaten konfiguriert ist, können Sie das Kontrollkästchen aktivieren.

- **Speicherklasse**: Wählen Sie **Standard (Standard)** für die normale Lagerung. Wählen Sie **reduzierte Redundanz** nur für Objekte, die einfach neu erstellt werden können. **Reduzierte Redundanz** bietet kostengünstige Speicherung mit weniger Zuverlässigkeit. Wenn das zielgerichtete Archivspeichersystem eine weitere Instanz des StorageGRID-Systems ist, steuert **Speicherklasse**, wie viele Zwischenkopien des Objekts bei der Aufnahme auf das Zielsystem erstellt werden, wenn bei Aufnahme von Objekten Dual Commit verwendet wird.

6. Wählen Sie **Änderungen Anwenden**.

   Die angegebenen Konfigurationseinstellungen werden validiert und auf Ihr StorageGRID System angewendet. Nach der Konfiguration kann das Ziel nicht mehr geändert werden.

Ändern der Verbindungseinstellungen für die S3-API

Nachdem der Archivknoten über die S3 API für die Verbindung zu einem externen Archiv-Storage-System konfiguriert wurde, können Sie einige Einstellungen ändern, wenn sich die Verbindung ändert.

Bevor Sie beginnen

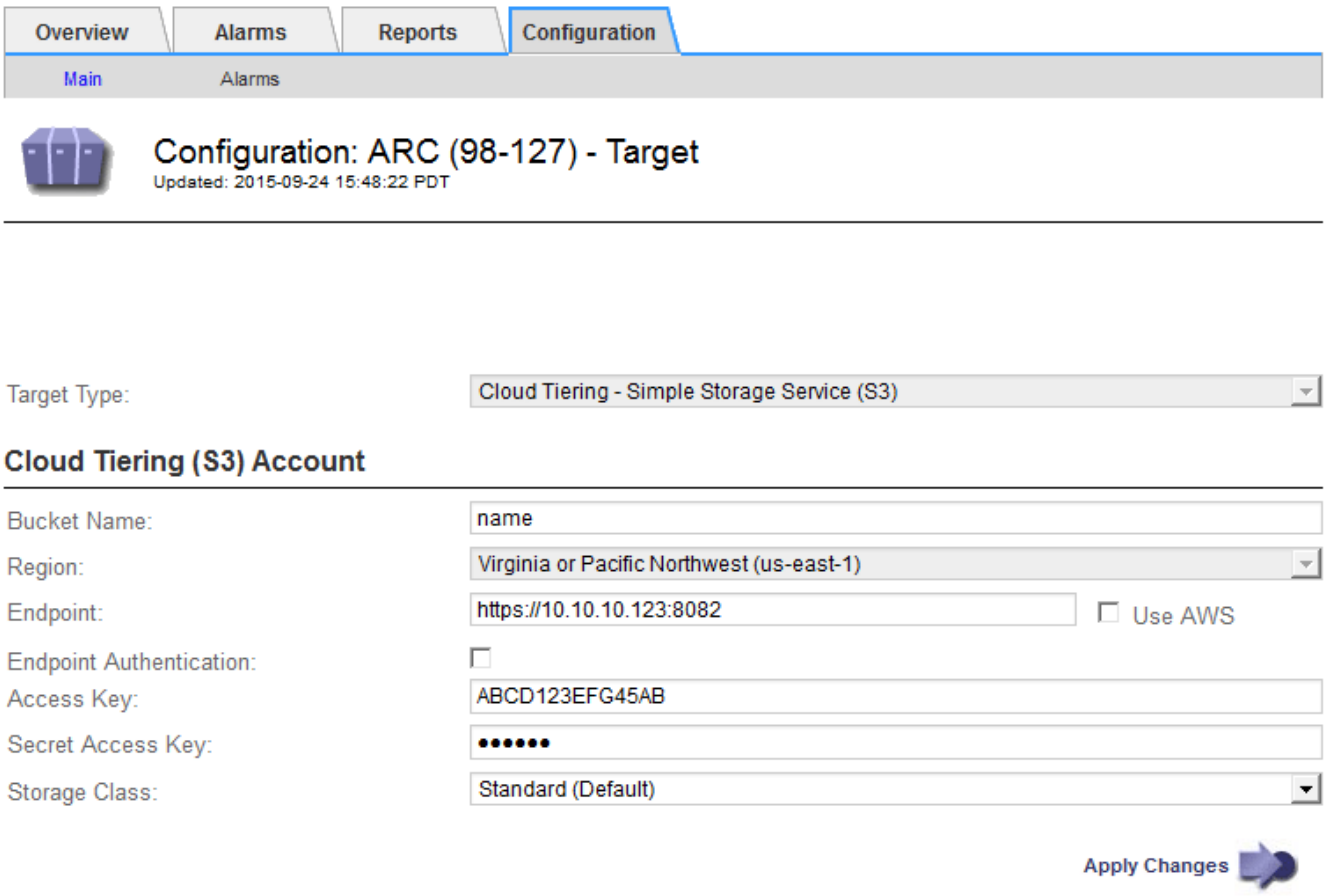
- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Wenn Sie das Cloud Tiering (S3) Konto ändern, müssen Sie sicherstellen, dass die Anmeldedaten für Benutzerzugriff auch auf den Bucket Lese-/Schreibzugriff haben, einschließlich aller Objekte, die zuvor vom Archiv-Node in den Bucket aufgenommen wurden.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***Archivknoten*** > **ARC** > **Ziel** aus.
3. Wählen Sie **Konfiguration** > **Main**.



4. Ändern Sie ggf. die Kontoinformationen.

   Wenn Sie die Storage-Klasse ändern, werden neue Objektdaten mit der neuen Storage-Klasse gespeichert. Vorhandene Objekte werden bei der Aufnahme weiterhin unter dem Storage-Klassensatz gespeichert.

   Bucket-Name, Region und Endpunkt: Verwenden Sie AWS-Werte und können nicht geändert werden.

5. Wählen Sie **Änderungen Anwenden**.

Ändern Sie den Status des Cloud Tiering Service

Sie können die Lese- und Schreibvorgänge des Archiv-Nodes auf das externe Archiv-Storage-System steuern, das über die S3 API verbunden ist, indem Sie den Status des Cloud Tiering Service ändern.

Bevor Sie beginnen

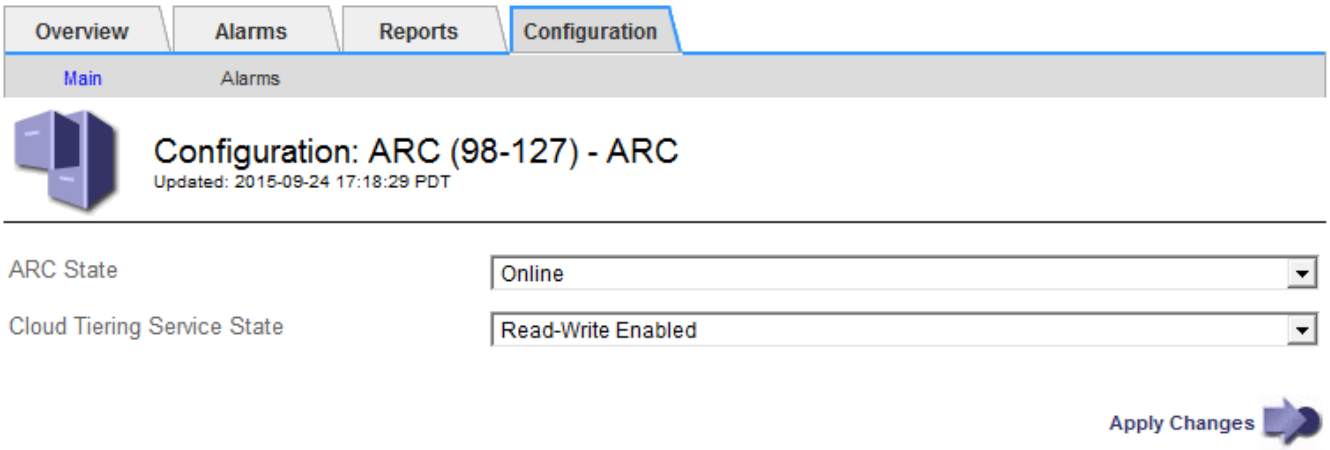
- Sie müssen mit einem beim Grid Manager angemeldet sein "Unterstützter Webbrowser".
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Der Archivknoten muss konfiguriert sein.

Über diese Aufgabe

Sie können den Archiv-Knoten effektiv offline setzen, indem Sie den Cloud-Tiering-Servicenstatus in **Lesen-Schreiben deaktiviert** ändern.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***Archivknoten*** > **ARC** aus.
3. Wählen Sie **Konfiguration** > **Main**.



4. Wählen Sie einen **Cloud Tiering Service-Status** aus.
5. Wählen Sie **Änderungen Anwenden**.

Zurücksetzen der Speicherfehler-Anzahl für S3-API-Verbindung

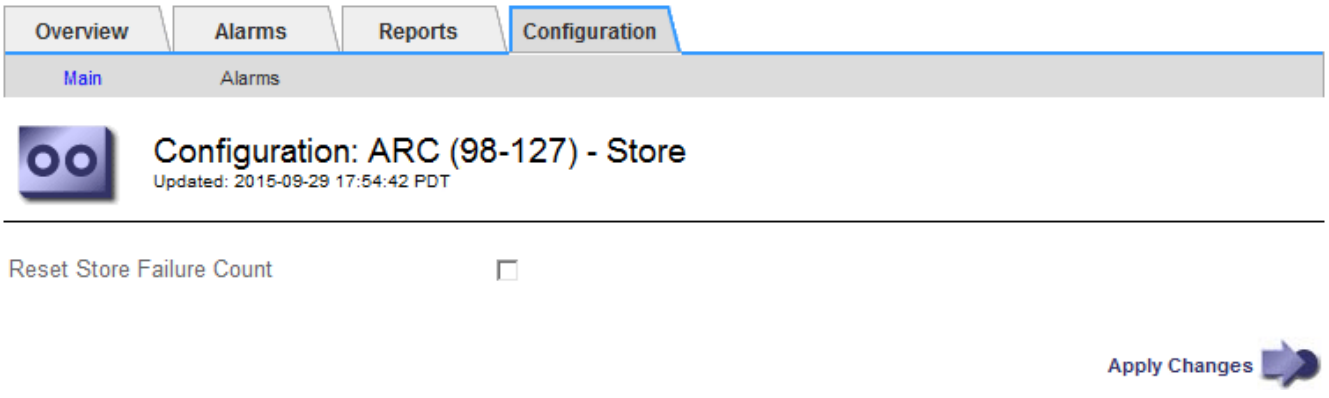
Wenn Ihr Archiv-Node über die S3-API eine Verbindung zu einem Archivspeichersystem herstellt, können Sie die Anzahl der Speicherfehler zurücksetzen, die zum Löschen des ARVF-Alarms (Store Failures) verwendet werden kann.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***Archivknoten*** > **ARC** > **Store** aus.
3. Wählen Sie **Konfiguration** > **Main**.



4. Wählen Sie **Anzahl Der Fehler Im Store Zurücksetzen** Aus.

5. Wählen Sie **Änderungen Anwenden**.

   Das Attribut Fehler speichern wird auf Null zurückgesetzt.

Migrieren Sie Objekte von Cloud Tiering – S3 zu einem Cloud-Storage-Pool

Wenn Sie derzeit die Funktion **Cloud Tiering - Simple Storage Service (S3)** verwenden, um Objektdaten in einen S3-Bucket zu verschieben, sollten Sie stattdessen Ihre Objekte in einen Cloud-Storage-Pool migrieren. Cloud Storage Pools bieten einen skalierbaren Ansatz, der alle Storage-Nodes in Ihrem StorageGRID System nutzt.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben bereits Objekte im S3-Bucket gespeichert, der für Cloud Tiering konfiguriert ist.

> Vor der Migration von Objektdaten sollten Sie den NetApp Ansprechpartner kontaktieren, um die damit verbundenen Kosten zu verstehen und zu managen.

Über diese Aufgabe

Aus einer ILM-Perspektive ähnelt ein Cloud-Storage-Pool einem Storage-Pool. Während Storage-Pools jedoch aus Storage-Nodes oder Archiv-Nodes innerhalb des StorageGRID Systems bestehen, besteht ein Cloud Storage-Pool aus einem externen S3-Bucket.

Vor der Migration von Objekten aus Cloud Tiering – S3 zu einem Cloud-Storage-Pool müssen Sie zuerst einen S3-Bucket erstellen und dann den Cloud-Storage-Pool in StorageGRID erstellen. Dann können Sie eine neue ILM-Richtlinie erstellen und die ILM-Regel ersetzen, die zum Speichern von Objekten im Cloud Tiering Bucket verwendet wird, durch eine geklonte ILM-Regel, die dieselben Objekte im Cloud-Storage-Pool speichert.

> Wenn Objekte in einem Cloud-Storage-Pool gespeichert sind, können Kopien dieser Objekte nicht auch in StorageGRID gespeichert werden. Wenn die ILM-Regel, die Sie derzeit für Cloud Tiering verwenden, so konfiguriert ist, um Objekte an mehreren Standorten gleichzeitig zu speichern, sollten Sie bedenken, ob Sie diese optionale Migration dennoch durchführen möchten, da diese Funktion verloren geht. Wenn Sie mit dieser Migration fortfahren, müssen Sie neue Regeln erstellen, anstatt die vorhandenen zu klonen.

Schritte

1. Erstellen Sie einen Cloud-Storage-Pool.

   Verwenden Sie einen neuen S3-Bucket für den Cloud-Storage-Pool, um sicherzustellen, dass er nur die Daten enthält, die vom Cloud-Storage-Pool gemanagt werden.

2. Suchen Sie alle ILM-Regeln der aktiven ILM-Richtlinie, die dazu führen, dass Objekte im Cloud Tiering Bucket gespeichert werden.
3. Jede dieser Regeln klonen.
4. Ändern Sie in den geklonten Regeln den Speicherort in den neuen Cloud-Storage-Pool.
5. Speichern Sie die geklonten Regeln.
6. Erstellen Sie eine neue Richtlinie, die die neuen Regeln verwendet.

7. Simulieren und aktivieren Sie die neue Richtlinie.

   Wenn die neue Richtlinie aktiviert ist und eine ILM-Bewertung erfolgt, werden die Objekte vom für Cloud Tiering konfigurierten S3-Bucket in den für den Cloud-Storage-Pool konfigurierten S3-Bucket verschoben. Der nutzbare Speicherplatz im Raster ist nicht betroffen. Nachdem die Objekte in den Cloud Storage Pool verschoben wurden, werden sie aus dem Cloud Tiering Bucket entfernt.

Verwandte Informationen

"Objektmanagement mit ILM"

Archivierung auf Band über TSM Middleware

Sie können einen Archiv-Node so konfigurieren, dass er als Ziel für einen Tivoli Storage Manager (TSM)-Server dient, der eine logische Schnittstelle zum Speichern und Abrufen von Objektdaten an Random- oder Sequential-Access-Speichergeräten, einschließlich Tape Libraries, bereitstellt.

Der ARC-Service des Archivknotens fungiert als Client zum TSM-Server und verwendet Tivoli Storage Manager als Middleware zur Kommunikation mit dem Archivspeichersystem.

> Die Unterstützung für Archive Nodes (für die Archivierung in der Cloud mit der S3-API und die Archivierung auf Band mit TSM-Middleware) ist veraltet und wird in einer zukünftigen Version entfernt. Das Verschieben von Objekten von einem Archive Node in ein externes Archiv-Storage-System wurde durch ILM Cloud Storage Pools ersetzt, die mehr Funktionen bieten.
>
> Siehe "Verwendung Von Cloud Storage Pools".

TSM Management-Klassen

Durch die TSM Middleware definierte Managementklassen beschreiben, wie die TSM's Backup- und Archivierungsvorgänge funktionieren und können verwendet werden, um Regeln für Inhalte festzulegen, die vom TSM-Server angewendet werden. Diese Regeln laufen unabhängig von der ILM-Richtlinie des StorageGRID Systems und müssen im Einklang mit der Anforderung des StorageGRID Systems stehen, dass Objekte dauerhaft gespeichert und für den Abruf durch den Archivierungs-Node immer verfügbar sind. Nachdem die Objektdaten vom Archiv-Node an einen TSM-Server gesendet wurden, werden die Regeln für den TSM Lebenszyklus und die Aufbewahrung angewendet, während die Objektdaten auf dem vom TSM-Server verwalteten Band gespeichert werden.

Die TSM-Managementklasse wird vom TSM-Server verwendet, um Regeln für den Datenspeicherort oder die Aufbewahrung anzuwenden, nachdem Objekte vom Archiv-Node an den TSM-Server gesendet wurden. So können beispielsweise als Datenbank-Backups identifizierte Objekte (temporärer Content, der mit neueren Daten überschrieben werden kann) anders behandelt werden als Applikationsdaten (unveränderlicher Inhalt, der unendlich lange aufbewahrt werden muss).

Konfigurieren Sie Verbindungen zur TSM Middleware

Bevor der Archive Node mit der Tivoli Storage Manager (TSM) Middleware kommunizieren kann, müssen Sie mehrere Einstellungen konfigurieren.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".

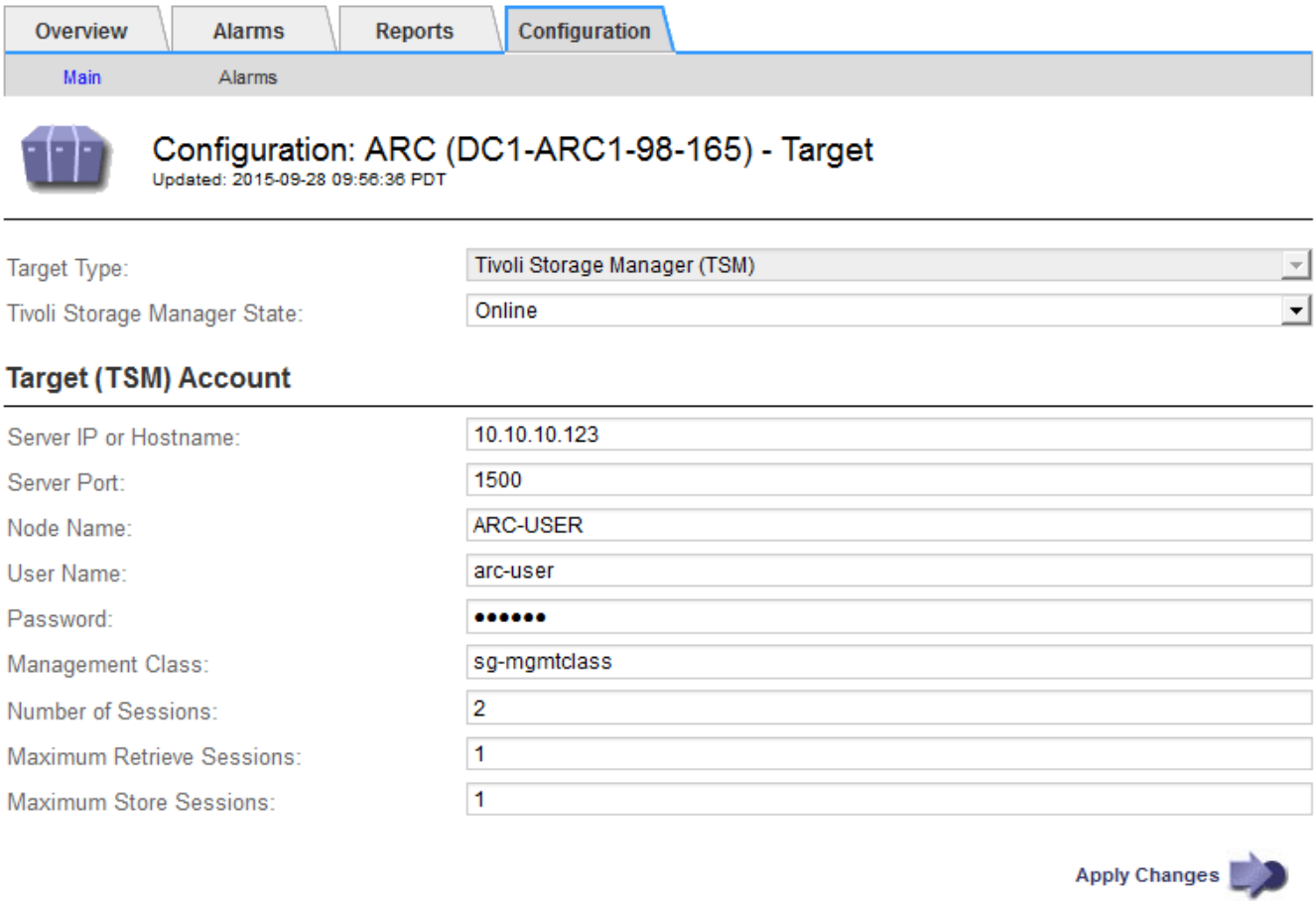
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Bis diese Einstellungen konfiguriert sind, bleibt der ARC-Dienst in einem wichtigen Alarmzustand, da er nicht mit dem Tivoli Storage Manager kommunizieren kann.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***Archivknoten*** > **ARC** > **Ziel** aus.
3. Wählen Sie **Konfiguration** > **Main**.



4. Wählen Sie aus der Dropdown-Liste **Zieltyp** die Option **Tivoli Storage Manager (TSM)** aus.
5. Wählen Sie für den **Tivoli Storage Manager State Offline** aus, um Rückrufe vom TSM Middleware-Server zu verhindern.

   Standardmäßig ist der Status von Tivoli Storage Manager auf Online eingestellt, was bedeutet, dass der Archive Node Objektdaten vom TSM Middleware-Server abrufen kann.

6. Geben Sie die folgenden Informationen an:

   - **Server IP oder Hostname**: Geben Sie die IP-Adresse oder den vollqualifizierten Domänennamen des TSM Middleware-Servers an, der vom ARC-Dienst verwendet wird. Die Standard-IP-Adresse ist 127.0.0.1.
   - **Server-Port**: Geben Sie die Portnummer auf dem TSM Middleware-Server an, mit dem der ARC-Dienst eine Verbindung herstellen wird. Der Standardwert ist 1500.

- **Knotenname**: Geben Sie den Namen des Archiv-Knotens an. Sie müssen den Namen (Arc-user) eingeben, den Sie auf dem TSM Middleware-Server registriert haben.
- **Benutzername**: Geben Sie den Benutzernamen an, den der ARC-Dienst zur Anmeldung am TSM-Server verwendet. Geben Sie den Standardbenutzernamen (Arc-user) oder den administrativen Benutzer ein, den Sie für den Archiv-Node angegeben haben.
- **Passwort**: Geben Sie das Passwort an, das der ARC-Dienst zur Anmeldung am TSM-Server verwendet.
- **Managementklasse**: Geben Sie die Standardverwaltungsklasse an, die verwendet werden soll, wenn beim Speichern des Objekts auf dem StorageGRID-System keine Managementklasse angegeben ist oder die angegebene Managementklasse nicht auf dem TSM Middleware-Server definiert ist.
- **Anzahl der Sitzungen**: Geben Sie die Anzahl der Bandlaufwerke auf dem TSM Middleware-Server an, die dem Archiv-Knoten gewidmet sind. Der Archivknoten erstellt gleichzeitig maximal eine Sitzung pro Bereitstellungspunkt plus eine kleine Anzahl zusätzlicher Sitzungen (weniger als fünf).

  Sie müssen diesen Wert ändern, um den für MAXNUMMP festgelegten Wert (maximale Anzahl von Mount-Punkten) zu erhalten, wenn der Archivknoten registriert oder aktualisiert wurde. (Im Register-Befehl ist der Standardwert von MAXNUMMP verwendet 1, wenn kein Wert festgelegt ist.)

Außerdem müssen Sie den Wert von MAXSESSIONS für den TSM-Server auf eine Zahl ändern, die mindestens so groß ist wie die Anzahl der Sitzungen, die für den ARC-Dienst festgelegt wurden. Der Standardwert von MAXSESSIONS auf dem TSM-Server ist 25.

- **Maximum Retrieve Sessions**: Geben Sie die maximale Anzahl von Sitzungen an, die der ARC-Dienst für den TSM Middleware-Server für Abrufvorgänge öffnen kann. In den meisten Fällen ist der entsprechende Wert die Anzahl der Sitzungen abzüglich der maximalen Speichersitzungen. Wenn Sie ein Bandlaufwerk für die Speicherung und den Abruf freigeben möchten, geben Sie einen Wert an, der der Anzahl der Sitzungen entspricht.
- **Maximum Store Sessions**: Geben Sie die maximale Anzahl gleichzeitiger Sitzungen an, die der ARC-Dienst für den TSM Middleware-Server für Archivierungsvorgänge öffnen kann.

  Dieser Wert sollte auf eins gesetzt werden, außer wenn das gezielte Archivspeichersystem voll ist und nur Abrufvorgänge durchgeführt werden können. Setzen Sie diesen Wert auf Null, um alle Sitzungen für Abrufvorgänge zu verwenden.

7. Wählen Sie **Änderungen Anwenden**.

Optimieren Sie einen Archiv-Node für TSM Middleware-Sitzungen

Sie können die Performance eines Archivierungs-Knotens, der sich mit Tivoli Server Manager (TSM) verbindet, optimieren, indem Sie die Sitzungen des Archivierungs-Nodes konfigurieren.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.

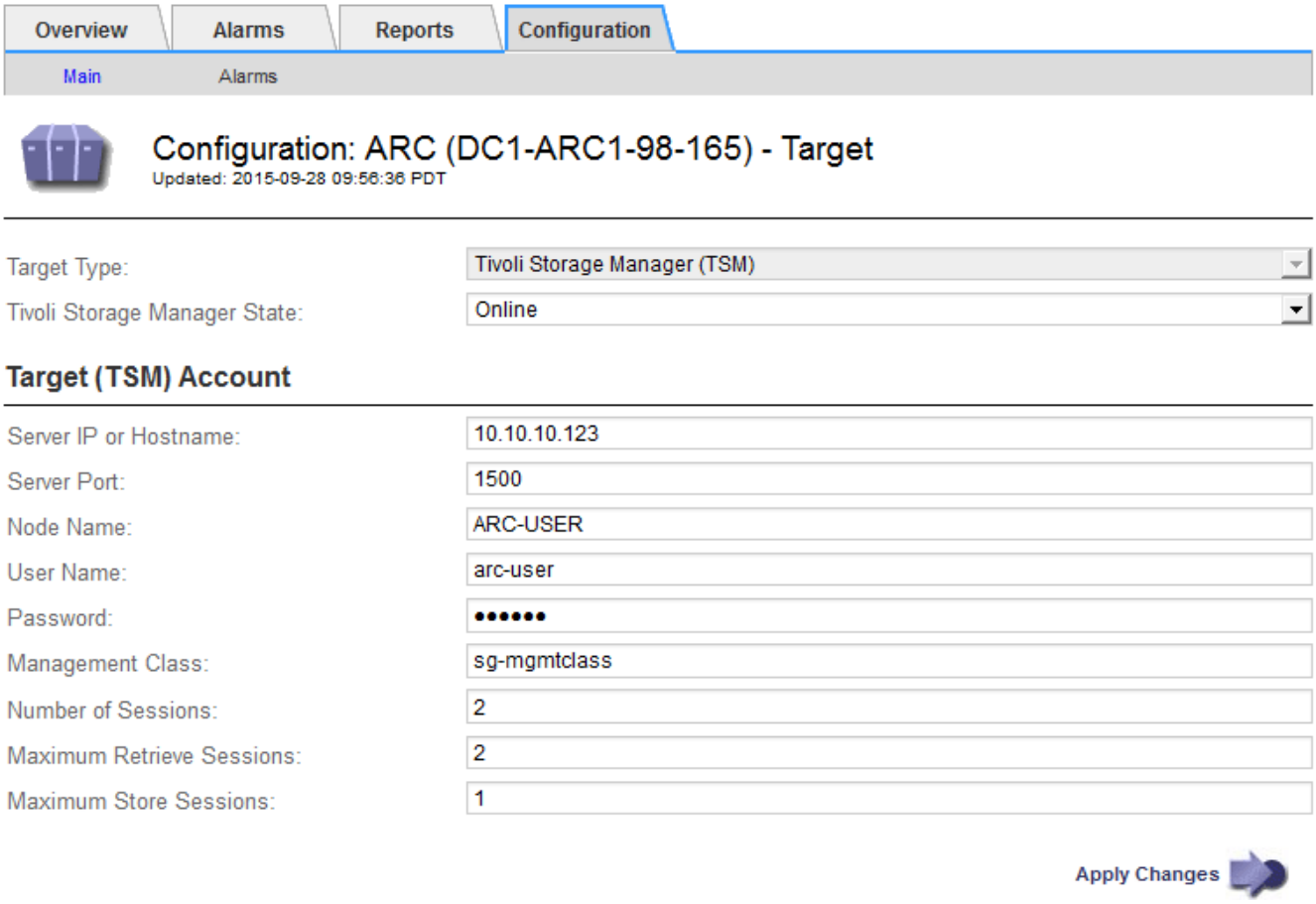
Über diese Aufgabe

In der Regel ist die Anzahl der gleichzeitigen Sitzungen, die der Archivknoten für den TSM Middleware-Server offen hat, auf die Anzahl der Bandlaufwerke eingestellt, die der TSM-Server dem Archiv-Node zugewiesen hat. Ein Bandlaufwerk wird für den Speicher zugewiesen, während der Rest für den Abruf zugewiesen wird. Wenn jedoch ein Speicherknoten aus Archive Node Kopien neu aufgebaut wird oder der Archivknoten im

schreibgeschützten Modus arbeitet, können Sie die TSM-Serverleistung optimieren, indem Sie die maximale Anzahl der Abrufsitzungen so einstellen, dass sie mit der Anzahl der gleichzeitigen Sitzungen identisch sind. Das Ergebnis ist, dass alle Laufwerke gleichzeitig für den Abruf genutzt werden können. Höchstens kann eines dieser Laufwerke zur Lagerung verwendet werden.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***Archivknoten*** > **ARC** > **Ziel** aus.
3. Wählen Sie **Konfiguration** > **Main**.
4. Ändern Sie **Maximum Retrieve Sessions** als **Anzahl der Sitzungen**.



5. Wählen Sie **Änderungen Anwenden**.

Konfigurieren Sie den Archivierungsstatus und die Zähler für TSM

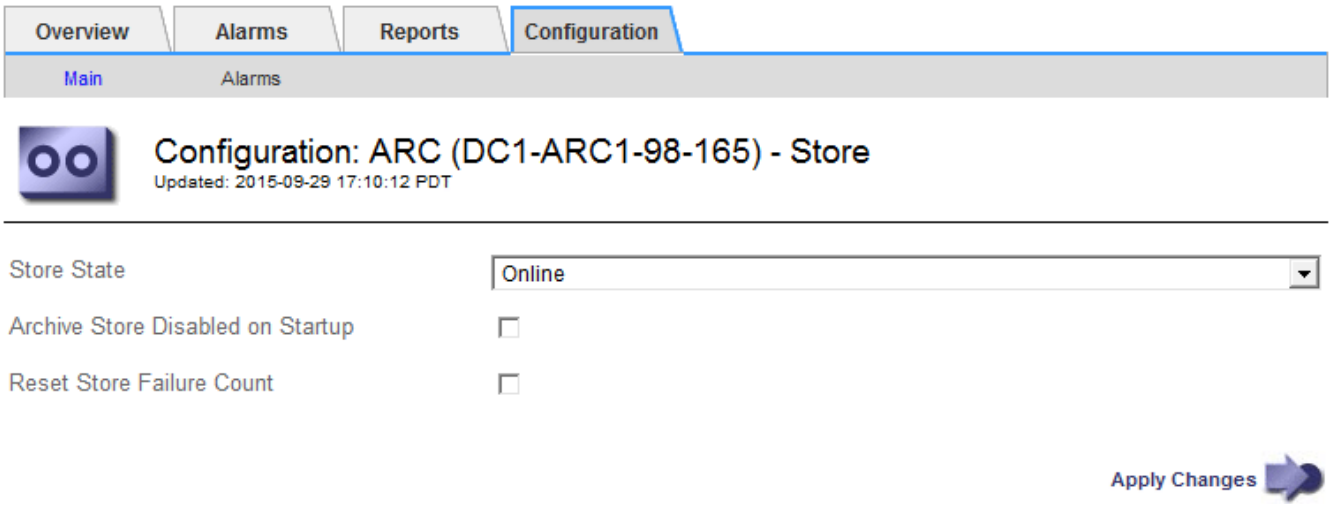
Wenn der Archivknoten eine Verbindung zu einem TSM Middleware-Server herstellt, können Sie den Status des Archivspeichers eines Archiv-Knotens in Online oder Offline konfigurieren. Sie können den Archivspeicher auch deaktivieren, wenn der Archivknoten zum ersten Mal gestartet wird, oder die Fehleranzahl, die für den zugehörigen Alarm nachverfolgt wird, zurücksetzen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***Archivknoten*** > **ARC** > **Store** aus.
3. Wählen Sie **Konfiguration** > **Main**.



4. Ändern Sie bei Bedarf die folgenden Einstellungen:
   - Speicherstatus: Legen Sie den Komponentenstatus auf entweder:
     - Online: Der Archiv-Node ist zur Verarbeitung von Objektdaten zum Speichern im Archiv-Storage-System verfügbar.
     - Offline: Der Archiv-Node ist nicht verfügbar, um Objektdaten zum Speichern im Archiv-Storage-System zu verarbeiten.
   - Archivspeicher beim Start deaktiviert: Wenn diese Option ausgewählt ist, bleibt die Komponente Archivspeicher beim Neustart im schreibgeschützten Zustand. Wird verwendet, um Speicher dauerhaft für das Zielspeichersystem zu deaktivieren. Nützlich, wenn das ausgewählte Archivspeichersystem keine Inhalte akzeptieren kann.
   - Reset Store Failure Count: Setzt den Zähler für Store Failures zurück. Dies kann verwendet werden, um den ARVF-Alarm (Stores Failure) zu löschen.
5. Wählen Sie **Änderungen Anwenden**.

Verwandte Informationen

"Verwalten Sie einen Archiv-Node, wenn der TSM-Server die Kapazität erreicht"

Verwalten Sie einen Archiv-Node, wenn der TSM-Server die Kapazität erreicht

Der TSM-Server hat keine Möglichkeit, den Archiv-Node zu benachrichtigen, wenn sich die Kapazität der TSM-Datenbank oder des vom TSM-Server verwalteten Archivmedienspeichers befindet. Dies kann durch proaktive Überwachung des TSM-Servers vermieden werden.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Der Archivknoten akzeptiert weiterhin Objektdaten für die Übertragung an den TSM-Server, nachdem der TSM-Server keine neuen Inhalte mehr akzeptiert. Dieser Inhalt kann nicht auf Medien geschrieben werden, die vom TSM-Server verwaltet werden. In diesem Fall wird ein Alarm ausgelöst.

Verhindern, dass der ARC-Dienst Inhalte an den TSM-Server sendet

Um zu verhindern, dass der ARC-Service weitere Inhalte an den TSM-Server sendet, können Sie den Archiv-Node offline schalten, indem Sie die **ARC** > **Store**-Komponente offline schalten. Dieses Verfahren kann auch nützlich sein, um Alarme zu vermeiden, wenn der TSM-Server nicht zur Wartung verfügbar ist.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***Archivknoten*** > **ARC** > **Store** aus.
3. Wählen Sie **Konfiguration** > **Main**.

4. Ändern Sie **Store State** in `Offline`.
5. Wählen Sie * Archivspeicher beim Start deaktiviert* aus.
6. Wählen Sie **Änderungen Anwenden**.

Stellen Sie Archive Node auf „Read-Only“ ein, wenn die TSM Middleware die Kapazität erreicht

Wenn der angestrebte TSM Middleware-Server seine Kapazität erreicht, kann der Archivknoten optimiert werden, um nur die Abrufvorgänge durchzuführen.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***Archivknoten*** > **ARC** > **Ziel** aus.
3. Wählen Sie **Konfiguration** > **Main**.
4. Ändern Sie die maximale Anzahl der Abruf-Sitzungen auf dieselbe Weise wie die Anzahl der gleichzeitigen Sitzungen, die in der Anzahl der Sitzungen aufgeführt sind.
5. Ändern Sie die maximale Anzahl von Sitzungen im Store auf 0.

> Das Ändern der maximalen Speichersitzungen auf 0 ist nicht erforderlich, wenn der Archivknoten schreibgeschützt ist. Speichersitzungen werden nicht erstellt.

6. Wählen Sie **Änderungen Anwenden**.

Konfigurieren Sie die Einstellungen für den Abruf von Archivknoten

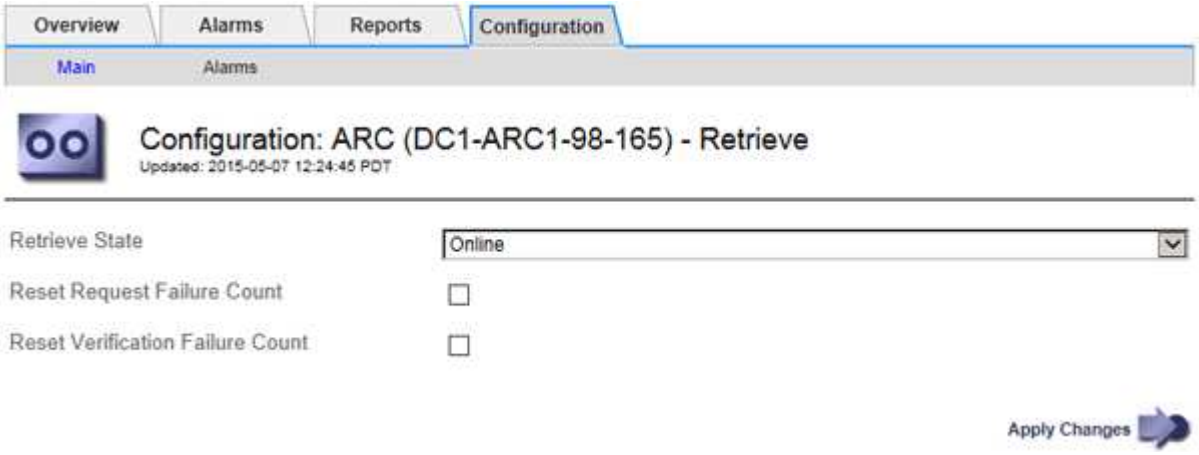
Sie können die Einstellungen für den Abruf eines Archiv-Knotens so konfigurieren, dass der Status auf Online oder Offline gesetzt wird, oder die Fehleranzahl, die für die zugehörigen Alarme nachverfolgt wird, zurücksetzen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie **Archivknoten** > **ARC** > **Abruf**.
3. Wählen Sie **Konfiguration** > **Main**.



4. Ändern Sie bei Bedarf die folgenden Einstellungen:
   - **Retrieve Status**: Den Komponentenzustand auf entweder einstellen:
     - Online: Der Grid-Node ist verfügbar, um Objektdaten vom Archivierungsmedium abzurufen.
     - Offline: Der Grid-Node ist zum Abrufen von Objektdaten nicht verfügbar.
   - Anzahl der fehlgeschlagenen Anfragen zurücksetzen: Aktivieren Sie das Kontrollkästchen, um den Zähler für Anforderungsfehler zurückzusetzen. Dieser kann verwendet werden, um den ARRF-Alarm (Request Failures) zu löschen.
   - Anzahl der fehlgeschlagenen Verifizierungen zurücksetzen: Aktivieren Sie das Kontrollkästchen, um den Zähler für Überprüfungsfehler bei abgerufenen Objektdaten zurückzusetzen. Dies kann verwendet werden, um den ARRV-Alarm (Verifizierungsfehler) zu löschen.
5. Wählen Sie **Änderungen Anwenden**.

Konfigurieren Sie die Replikation des Archivierungs-Knotens

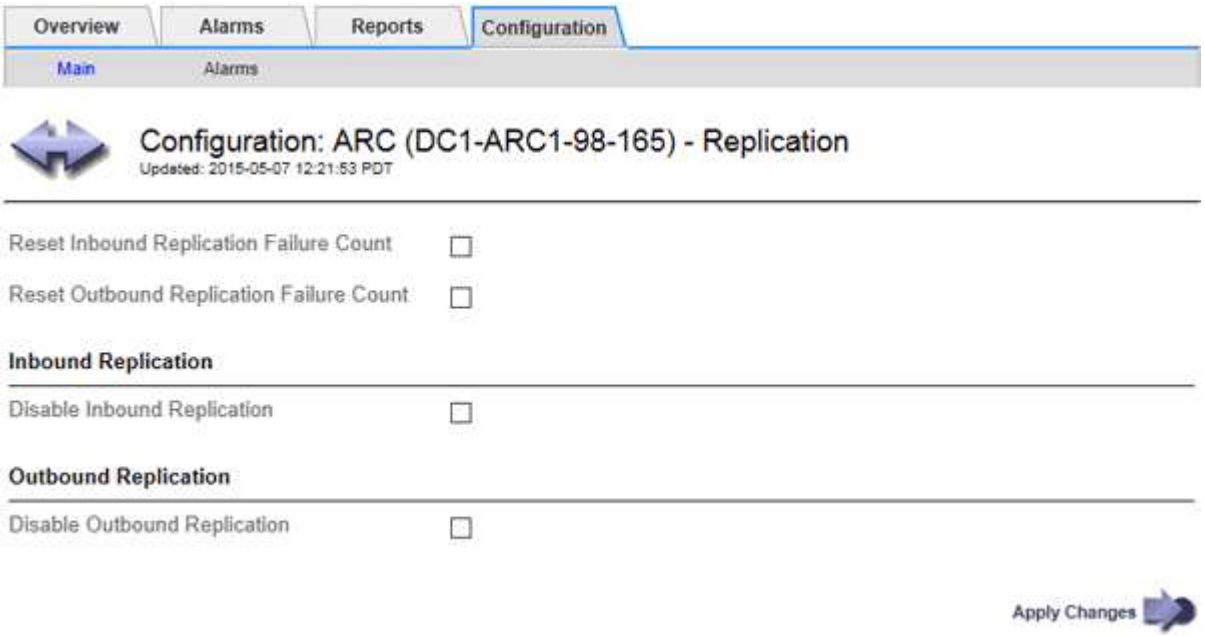
Sie können die Replikationseinstellungen für einen Archivknoten konfigurieren und die ein- und ausgehende Replikation deaktivieren oder die für die zugehörigen Alarme zu protokollierenden Fehlerzählungen zurücksetzen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus.
2. Wählen Sie ***Archivknoten*** > **ARC** > **Replikation** aus.
3. Wählen Sie **Konfiguration** > **Main**.



4. Ändern Sie bei Bedarf die folgenden Einstellungen:
   - **Fehleranzahl Inbound Replication zurücksetzen**: Wählen Sie, um den Zähler für eingehende Replikationsfehler zurückzusetzen. Dies kann verwendet werden, um den RIRF-Alarm (eingehende Replikationen — fehlgeschlagen) zu löschen.
   - **Fehleranzahl bei ausgehenden Replikationsfehlern zurücksetzen**: Wählen Sie, um den Zähler für ausgehende Replikationsfehler zurückzusetzen. Dies kann verwendet werden, um den RORF-Alarm (ausgehende Replikationen — fehlgeschlagen) zu löschen.
   - **Inbound Replication** deaktivieren: Wählen Sie aus, um die eingehende Replikation im Rahmen eines Wartungs- oder Testverfahrens zu deaktivieren. Während des normalen Betriebs löschen lassen.

     Wenn die eingehende Replikation deaktiviert ist, können Objektdaten vom ARC-Dienst zur Replikation an andere Standorte im StorageGRID-System abgerufen werden. Objekte können jedoch nicht von anderen Systemstandorten auf diesen ARC-Dienst repliziert werden. Der ARC-Dienst wird-only gelesen.

   - **Ausgehende Replikation deaktivieren**: Aktivieren Sie das Kontrollkästchen, um die ausgehende Replikation (einschließlich Inhaltsanforderungen für HTTP-Abfragen) im Rahmen eines Wartungs- oder Testverfahrens zu deaktivieren. Während des normalen Betriebs nicht aktiviert lassen.

     Wenn die ausgehende Replikation deaktiviert ist, können Objektdaten zu diesem ARC-Dienst kopiert werden, um ILM-Regeln zu erfüllen. Objektdaten können jedoch nicht vom ARC-Dienst abgerufen werden, um an andere Orte im StorageGRID-System kopiert zu werden. Der ARC-Dienst ist nur schreiben-.

5. Wählen Sie **Änderungen Anwenden**.

Legen Sie benutzerdefinierte Alarme für den Knoten Archiv fest

Sie sollten benutzerdefinierte Alarme für die ARQL- und ARRL-Attribute einrichten, die zur Überwachung der Geschwindigkeit und Effizienz des Datenabrufs von Objektdaten vom Archivspeichersystem durch den Knoten Archiv verwendet werden.

- ARQL: Durchschnittliche Warteschlangenlänge. Die durchschnittliche Zeit in Mikrosekunden dieser Objektdaten wird zum Abruf aus dem Archivspeichersystem in die Warteschlange verschoben.
- ARRL: Durchschnittliche Anfragelatenz. Die durchschnittliche Zeit in Mikrosekunden, die der Archive-Node benötigt, um Objektdaten aus dem Archiv-Storage-System abzurufen.

Die akzeptablen Werte dieser Attribute hängen davon ab, wie das Archivspeichersystem konfiguriert und verwendet wird. (Gehen Sie zu **ARC** > **Abrufen** > **Übersicht** > **Haupt**.) Die Werte, die für die Timeouts von Anfragen festgelegt sind, und die Anzahl der Sitzungen, die für Abrufanfragen zur Verfügung gestellt werden, haben einen besonderen Einfluss.

Nach Abschluss der Integration überwachen Sie die Abfrage der Objektdaten des Archivknoten, um Werte für die normalen Abrufzeiten und Warteschlangenlänge zu ermitteln. Erstellen Sie dann benutzerdefinierte Alarme für ARQL und ARRL, die ausgelöst werden, wenn eine anormale Betriebsbedingung auftritt. Siehe Anweisungen für "Verwalten von Alarmen (Altsystem)".

Integration Von Tivoli Storage Manager

Konfiguration und Betrieb des Archivierungs-Node

Ihr StorageGRID-System managt den Archiv-Node als Speicherort, an dem Objekte unendlich gespeichert werden und stets zugänglich sind.

Bei der Aufnahme eines Objekts werden auf Basis der für das StorageGRID System definierten Regeln für das Information Lifecycle Management Kopien an allen erforderlichen Speicherorten, einschließlich Archiv-Nodes, erstellt. Der Archivknoten fungiert als Client auf einem TSM-Server, und die TSM-Clientbibliotheken sind auf dem Archiv-Knoten durch den Installationsvorgang der StorageGRID-Software installiert. Objektdaten, die zum Archiv-Node für Speicher geleitet werden, werden beim Empfang direkt auf dem TSM-Server gespeichert. Der Archivknoten stellt keine Objektdaten vor dem Speichern auf dem TSM-Server dar und führt auch keine Objektaggregation durch. Der Archivknoten kann jedoch in einer einzigen Transaktion mehrere Kopien an den TSM-Server senden, wenn die Datenraten dies erfordern.

Nachdem der Archivknoten Objektdaten auf dem TSM-Server speichert, werden die Objektdaten unter Anwendung der Lifecycle-/Aufbewahrungsrichtlinien vom TSM-Server gemanagt. Diese Aufbewahrungsrichtlinien müssen definiert werden, damit sie mit dem Vorgang des Archivierungs-Nodes kompatibel sind. Das bedeutet, dass vom Archiv-Node gespeicherte Objektdaten unbegrenzt gespeichert werden müssen und vom Archiv-Node immer darauf zugegriffen werden muss, es sei denn, sie werden vom Archiv-Node gelöscht.

Es besteht keine Verbindung zwischen den ILM-Regeln des StorageGRID Systems und den Lifecycle-/Aufbewahrungsrichtlinien des TSM Servers. Jeder arbeitet unabhängig voneinander. Wenn jedoch jedes Objekt in das StorageGRID System aufgenommen wird, kann ihm eine TSM Management-Klasse zugewiesen werden. Diese Managementklasse wird gemeinsam mit Objektdaten an den TSM Server übergeben. Durch das Zuweisen verschiedener Managementklassen zu unterschiedlichen Objekttypen können Sie den TSM-Server so konfigurieren, dass Objektdaten in verschiedenen Storage-Pools gespeichert werden, oder unterschiedliche Migrations- oder Aufbewahrungsrichtlinien anwenden. Beispielsweise können als Datenbank-

Backups identifizierte Objekte (temporärer Content als mit neueren Daten überschrieben werden kann) anders als Applikationsdaten behandelt werden (unveränderlicher Inhalt, der für unbegrenzte Zeit aufbewahrt werden muss).

Der Archivknoten kann in einen neuen oder vorhandenen TSM-Server integriert werden; es ist kein dedizierter TSM-Server erforderlich. TSM-Server können mit anderen Clients gemeinsam genutzt werden, vorausgesetzt, der TSM-Server ist für die erwartete maximale Last angemessen dimensioniert. TSM muss auf einem vom Archiv-Node getrennten Server oder einer virtuellen Maschine installiert sein.

Es ist möglich, mehr als einen Archivknoten zu konfigurieren, um auf denselben TSM-Server zu schreiben; diese Konfiguration wird jedoch nur empfohlen, wenn die Archiv-Knoten unterschiedliche Datensätze auf den TSM-Server schreiben. Die Konfiguration von mehr als einem Archiv-Node zum Schreiben auf denselben TSM-Server wird nicht empfohlen, wenn jeder Archiv-Node Kopien derselben Objektdaten in das Archiv schreibt. Bei einem letzteren Szenario unterliegen beide Kopien einem Single Point of Failure (dem TSM-Server), da sie unabhängige, redundante Kopien von Objektdaten sind.

Archive Nodes verwenden die hierarchische Speicherverwaltung (HSM)-Komponente von TSM nicht.

Best Practices für die Konfiguration

Wenn Sie den TSM-Server dimensionieren und konfigurieren, gibt es Best Practices, die Sie anwenden sollten, um ihn für die Arbeit mit dem Archiv-Knoten zu optimieren.

Bei der Dimensionierung und Konfiguration des TSM-Servers sollten folgende Faktoren berücksichtigt werden:

- Da der Archivknoten keine Objekte aggregiert, bevor sie auf dem TSM-Server gespeichert werden, muss die TSM-Datenbank so dimensioniert sein, dass sie Verweise auf alle Objekte enthält, die auf den Archiv-Node geschrieben werden.
- Archive Node-Software kann die Latenz beim Schreiben von Objekten direkt auf Band oder andere Wechselmedien nicht tolerieren. Daher muss der TSM-Server mit einem Festplatten-Speicherpool für den ursprünglichen Speicher der Daten konfiguriert werden, die vom Archiv-Node gespeichert werden, wenn Wechseldatenträger verwendet werden.
- Sie müssen TSM-Aufbewahrungsrichtlinien konfigurieren, um die ereignisbasierte Aufbewahrung zu verwenden-. Der Archivierungs-Node unterstützt keine auf der Erstellung basierenden TSM-Aufbewahrungsrichtlinien. Verwenden Sie in der Aufbewahrungsrichtlinie die folgenden empfohlenen Einstellungen von remin=0 und rever=0 (dies bedeutet, dass die Aufbewahrung beginnt, wenn der Archivknoten ein Archivierungsereignis auslöst und danach 0 Tage lang aufbewahrt wird). Diese Werte für Remin und Rever sind jedoch optional.

Der Laufwerk-Pool muss so konfiguriert sein, dass Daten in den Bandpool migriert werden (das heißt, der Bandpool muss NXTSTGPOOL des Laufwerk-Pools sein). Der Bandpool darf nicht als Kopierpool des Laufwerkspools konfiguriert werden, der gleichzeitig in beide Pools schreibt (d. h. der Bandpool kann kein COPYSTGPOOL für den Laufwerkspool sein). Um Offline-Kopien der Bänder zu erstellen, die Daten von Archivierungs-Nodes enthalten, konfigurieren Sie den TSM-Server mit einem zweiten Bandpool, der ein Kopie-Pool des für Archiv-Node-Daten verwendeten Bandpools ist.

Schließen Sie die Konfiguration des Archivierungs-Knotens ab

Der Archivknoten funktioniert nicht, nachdem Sie den Installationsprozess abgeschlossen haben. Bevor das StorageGRID-System Objekte auf dem TSM-Archivknoten speichern kann, müssen Sie die Installation und Konfiguration des TSM-Servers abschließen und den Archivknoten für die Kommunikation mit dem TSM-Server konfigurieren.

Beachten Sie bei Bedarf die folgende IBM-Dokumentation, wenn Sie Ihren TSM-Server für die Integration mit dem Archiv-Node in einem StorageGRID-System vorbereiten:

- "IBM Bandgerätetreiber – Installations- und Benutzerhandbuch"
- "Programmierreferenz für IBM Bandgerätetreiber"

Installieren Sie einen neuen TSM-Server

Sie können den Archiv-Knoten entweder mit einem neuen oder einem vorhandenen TSM-Server integrieren. Wenn Sie einen neuen TSM-Server installieren, befolgen Sie die Anweisungen in der TSM-Dokumentation, um die Installation abzuschließen.

Ein Archive Node kann nicht mit einem TSM-Server gemeinsam gehostet werden.

Konfigurieren Sie den TSM-Server

Dieser Abschnitt enthält Beispielanweisungen zur Vorbereitung eines TSM-Servers gemäß den Best Practices von TSM.

Die folgenden Anweisungen führen Sie durch den Prozess von:

- Definieren eines Festplatten-Speicherpools und eines Bandspeicherpools (falls erforderlich) auf dem TSM-Server
- Definieren einer Domänenrichtlinie, die die TSM-Managementklasse für die Daten verwendet, die im Knoten Archiv gespeichert sind, und Registrieren eines Knotens für diese Domänenrichtlinie

Diese Anweisungen dienen nur zu Ihrer Orientierung; sie sind nicht als Ersatz für die TSM-Dokumentation gedacht oder als vollständige und umfassende Anweisungen, die für alle Konfigurationen geeignet sind. Eine Anleitung zur Implementierung sollte von einem TSM-Administrator bereitgestellt werden, der sowohl mit Ihren detaillierten Anforderungen als auch mit dem vollständigen Satz der TSM-Server-Dokumentation vertraut ist.

Definieren Sie TSM Tape- und Festplatten-Storage-Pools

Der Archivknoten schreibt in einen Festplatten-Speicherpool. Um Inhalte auf Band zu archivieren, müssen Sie den Festplatten-Speicherpool konfigurieren, um Inhalte in einen Bandspeicher-Pool zu verschieben.

Über diese Aufgabe

Bei einem TSM-Server müssen Sie einen Bandspeicher-Pool und einen Festplatten-Speicherpool in Tivoli Storage Manager definieren. Erstellen Sie nach Definition des Laufwerk-Pools ein Laufwerk-Volume und weisen Sie es dem Laufwerk-Pool zu. Ein Bandpool-nicht erforderlich, wenn Ihr TSM-Server nur Festplatten-Storage verwendet.

Sie müssen mehrere Schritte auf dem TSM-Server durchführen, bevor Sie einen Bandspeicherpool erstellen können. (Erstellen Sie eine Bandbibliothek und mindestens ein Laufwerk in der Bandbibliothek. Definieren Sie einen Pfad vom Server zur Bibliothek und vom Server zu den Laufwerken und definieren Sie dann eine Geräteklasse für die Laufwerke.) Die Details dieser Schritte können je nach Hardwarekonfiguration und Storage-Anforderungen des Standorts variieren. Weitere Informationen finden Sie in der TSM-Dokumentation.

Die folgenden Anweisungen veranschaulichen den Prozess. Sie sollten beachten, dass die Anforderungen an Ihren Standort je nach Bereitstellungsanforderungen unterschiedlich sein können. Weitere Informationen zur

Konfiguration und zu Anweisungen finden Sie in der TSM-Dokumentation.

Sie müssen sich beim Server mit Administratorrechten anmelden und das dsmadmc-Tool verwenden, um die folgenden Befehle auszuführen.

Schritte

1. Erstellen einer Tape Library

   `define library tapelibrary libtype=scsi`

   Wo `tapelibrary` Ist ein willkürlicher Name, der für die Bandbibliothek und den Wert von ausgewählt wurde `libtype` Je nach Art der Tape Library kann es variieren.

2. Definieren Sie einen Pfad vom Server zur Bandbibliothek.

   `define path servername tapelibrary srctype=server desttype=library device=lib-devicename`

   - `servername` Ist der Name des TSM-Servers
   - `tapelibrary` Ist der von Ihnen definierte Bandbibliothek
   - `lib-devicename` Ist der Gerätename für die Bandbibliothek

3. Legen Sie ein Laufwerk für die Bibliothek fest.

   `define drive tapelibrary drivename`

   - `drivename` Ist der Name, den Sie für das Laufwerk angeben möchten
   - `tapelibrary` Ist der von Ihnen definierte Bandbibliothek

     Je nach Hardwarekonfiguration möchten Sie möglicherweise ein zusätzliches Laufwerk oder weitere Laufwerke konfigurieren. (Wenn beispielsweise der TSM-Server mit einem Fibre Channel-Switch verbunden ist, der über zwei Eingaben aus einer Bandbibliothek verfügt, sollten Sie für jede Eingabe möglicherweise ein Laufwerk definieren.)

4. Definieren Sie einen Pfad vom Server zum Laufwerk, das Sie definiert haben.

   `define path servername drivename srctype=server desttype=drive library=tapelibrary device=drive-dname`

   - `drive-dname` Ist der Gerätename für das Laufwerk
   - `tapelibrary` Ist der von Ihnen definierte Bandbibliothek

     Wiederholen Sie diesen Vorgang für jedes Laufwerk, das Sie für die Bandbibliothek definiert haben, mit einem separaten Laufwerk `drivename` Und `drive-dname` Für jedes Laufwerk.

5. Definieren Sie eine Geräteklasse für die Laufwerke.

   `define devclass DeviceClassName devtype=lto library=tapelibrary format=tapetype`

   - `DeviceClassName` Ist der Name der Geräteklasse

- `lto` Ist der Laufwerkstyp, der mit dem Server verbunden ist
- `tapelibrary` Ist der von Ihnen definierte Bandbibliothek
- `tapetype` Ist der Tape-Typ, z. B. ultrium3

6. Fügen Sie dem Bestand der Bibliothek Bandvolumen hinzu.

   ```
   checkin libvolume tapelibrary
   ```

   `tapelibrary` Ist der von Ihnen definierte Bandbibliothek.

7. Erstellen Sie den primären Bandspeicherpool.

   ```
   define stgpool SGWSTapePool DeviceClassName description=description
   collocate=filespace maxscratch=XX
   ```

   - `SGWSTapePool` Ist der Name des Bandspeicherpools des Archiv-Nodes. Sie können einen beliebigen Namen für den Bandspeicher-Pool auswählen (sofern der Name die vom TSM-Server erwarteten Syntaxkonventionen verwendet).
   - `DeviceClassName` Ist der Name des Klassennamens für die Bandbibliothek.
   - `description` Ist eine Beschreibung des Speicherpools, der mithilfe des auf dem TSM-Server angezeigt werden kann `query stgpool` Befehl. Beispiel: „`Bandspeicher-Pool für den Archiv-Node`“
   - `collocate=filespace` Gibt an, dass der TSM-Server Objekte aus demselben Dateispeicher auf ein einzelnes Band schreiben soll.
   - `XX` Ist eine der folgenden Optionen:
     - Die Anzahl der leeren Bänder in der Bandbibliothek (falls der Archivknoten die einzige Anwendung ist, die die Bibliothek verwendet).
     - Die Anzahl der vom StorageGRID System zugewiesenen Tapes (in Fällen, in denen die Tape-Bibliothek gemeinsam genutzt wird).

8. Erstellen Sie auf einem TSM-Server einen Festplatten-Speicherpool. Geben Sie an der Administrationskonsole des TSM-Servers ein

   ```
   define stgpool SGWSDiskPool disk description=description
   maxsize=maximum_file_size nextstgpool=SGWSTapePool highmig=percent_high
   lowmig=percent_low
   ```

   - `SGWSDiskPool` Ist der Name des Festplatten-Pools des Archiv-Nodes. Sie können einen beliebigen Namen für den Festplatten-Speicherpool auswählen (sofern der Name die vom TSM erwarteten Syntaxkonventionen verwendet).
   - `description` Ist eine Beschreibung des Speicherpools, der mithilfe des auf dem TSM-Server angezeigt werden kann `query stgpool` Befehl. Beispiel: „`DFestplatten-Storage-Pool für den Archiv-Node`“
   - `maximum_file_size` Zwingt das Schreiben von Objekten, die größer sind als diese Größe, direkt auf Tape, statt im Festplatten-Pool gespeichert zu werden. Es wird empfohlen, die Einstellung festzulegen `maximum_file_size` Bis 10 GB.
   - `nextstgpool=SGWSTapePool` Bezeichnet den Festplatten-Speicherpool auf den für den Archiv-Node definierten Bandspeicher-Pool.

- *percent_high* Legt den Wert fest, mit dem der Laufwerk-Pool seine Inhalte in den Bandpool migriert. Es wird empfohlen, die Einstellung festzulegen *percent_high* Zu 0, sodass sofort die Datenmigration beginnt
- *percent_low* Legt den Wert fest, mit dem die Migration zum Bandpool angehalten wird. Es wird empfohlen, die Einstellung festzulegen *percent_low* Zu 0, um den Laufwerk-Pool zu löschen.

9. Erstellen Sie auf einem TSM-Server ein Festplatten-Volume (oder Volumes) und weisen Sie es dem Festplatten-Pool zu.

   `define volume SGWSDiskPool volume_name formatsize=size`

   - *SGWSDiskPool* Ist der Name des Disk-Pools.
   - *volume_name* Ist der vollständige Pfad zum Speicherort des Volumes (z. B. `/var/local/arc/stage6.dsm`) Auf dem TSM-Server, wo er den Inhalt des Laufwerk-Pools in Vorbereitung für die Übertragung auf Band schreibt.
   - *size* Ist die Größe des Datenträgers in MB.

     Wenn Sie beispielsweise ein einzelnes Laufwerk-Volume so erstellen möchten, dass der Inhalt eines Festplattenpools ein einzelnes Band enthält, setzen Sie den Wert der Größe auf 200000, wenn das Bandvolumen 200 GB hat.

     Es könnte jedoch wünschenswert sein, mehrere Festplatten-Volumes einer kleineren Größe zu erstellen, da der TSM-Server auf jedes Volume im Festplatten-Pool schreiben kann. Wenn die Bandgröße beispielsweise 250 GB beträgt, erstellen Sie 25 Festplatten-Volumes mit jeweils 10 GB (10000).

   Der TSM-Server weist im Verzeichnis für das Festplatten-Volume vorab Speicherplatz zu. Dies kann einige Zeit in Anspruch nehmen (mehr als drei Stunden für ein 200-GB-Laufwerk).

Definieren Sie eine Domänenrichtlinie und registrieren Sie einen Knoten

Sie müssen eine Domänenrichtlinie definieren, die die TSM-Managementklasse für die Daten verwendet, die vom Archiv-Node gespeichert wurden, und dann einen Knoten registrieren, um diese Domänenrichtlinie zu verwenden.

> Archive Node-Prozesse können Speicher auslaufen, wenn das Clientpasswort für den Archive Node im Tivoli Storage Manager (TSM) abläuft. Stellen Sie sicher, dass der TSM-Server so konfiguriert ist, dass der Client-Benutzername/das Passwort für den Archiv-Node nie abläuft.

Wenn Sie einen Knoten auf dem TSM-Server für die Verwendung des Archiv-Knotens registrieren (oder einen vorhandenen Knoten aktualisieren), müssen Sie die Anzahl der Mount-Punkte angeben, die der Knoten für Schreibvorgänge verwenden kann, indem Sie den MAXNUMMP-Parameter für den BEFEHL REGISTER NODE angeben. Die Anzahl der Bereitstellungspunkte entspricht in der Regel der Anzahl der Bandlaufwerksköpfe, die dem Archiv-Node zugewiesen sind. Die für MAXNUMMP auf dem TSM-Server angegebene Zahl muss mindestens so groß sein wie der für den **ARC** > **Ziel** > **Konfiguration** > **Haupt** > **maximale Store Sessions** für den Archive Node festgelegte Wert, Der auf den Wert 0 oder 1 gesetzt ist, da gleichzeitige Speichersitzungen vom Archive Node nicht unterstützt werden.

Der Wert des MAXSESSIONS-Satzes für den TSM-Server steuert die maximale Anzahl von Sitzungen, die für den TSM-Server von allen Client-Anwendungen geöffnet werden können. Der auf dem TSM angegebene MAXSESSIONS-Wert muss mindestens so groß sein wie der für **ARC** > **Ziel** > **Konfiguration** > **Main** >

Anzahl Sitzungen im Grid Manager für den Archiv-Node angegebene Wert. Der Archivknoten erstellt gleichzeitig höchstens eine Sitzung pro Bereitstellungspunkt plus eine kleine Zahl (< 5) zusätzlicher Sitzungen.

Der dem Archiv-Node zugewiesene TSM-Node verwendet eine benutzerdefinierte Domänenrichtlinie `tsm-domain`. Der `tsm-domain` Die Domänenrichtlinie ist eine geänderte Version der Domänenrichtlinie „`standard`“, die auf Band geschrieben und als Speicherpool des StorageGRID Systems das Archivziel festgelegt wurde (*`SGWSDiskPool`*).

> Sie müssen sich am TSM-Server mit Administratorrechten anmelden und das dsmadmc-Tool verwenden, um die Domänenrichtlinie zu erstellen und zu aktivieren.

Erstellen und aktivieren Sie die Domänenrichtlinie

Sie müssen eine Domänenrichtlinie erstellen und diese dann aktivieren, um den TSM-Server so zu konfigurieren, dass die vom Archiv-Node gesendeten Daten gespeichert werden.

Schritte

1. Eine Domänenrichtlinie erstellen.

   ```
   copy domain standard tsm-domain
   ```

2. Wenn Sie keine vorhandene Management-Klasse verwenden, geben Sie eine der folgenden Optionen ein:

   ```
   define policyset tsm-domain standard
   ```

   ```
   define mgmtclass tsm-domain standard default
   ```

   `default` Ist die Standard-Managementklasse für die Bereitstellung.

3. Erstellen Sie eine Copygroup in den entsprechenden Speicherpool. Geben Sie (in einer Zeile) ein:

   ```
   define copygroup tsm-domain standard default type=archive
   destination=SGWSDiskPool retinit=event retmin=0 retver=0
   ```

   `default` Ist die Standard-Managementklasse für den Archivknoten. Die Werte von `retinit`, `retmin`, und `retver` Wurden ausgewählt, um das Aufbewahrungsverhalten wiederzugeben, das derzeit vom Archiv-Knoten verwendet wird

   > Nicht einstellen `retinit` Bis `retinit=create`. Einstellung `retinit=create` Blockiert das Löschen von Inhalten durch den Archivknoten, da Aufbewahrungsereignisse zum Entfernen von Inhalten vom TSM-Server verwendet werden.

4. Weisen Sie die Managementklasse als Standard zu.

   ```
   assign defmgmtclass tsm-domain standard default
   ```

5. Legen Sie den neuen Richtliniensatz als aktiv fest.

   ```
   activate policyset tsm-domain standard
   ```

   Ignorieren Sie die Warnung „`no Backup copy Group`“, die beim Eingeben des Befehls activate

angezeigt wird.

6. Registrieren Sie einen Knoten, um den neuen Richtliniensatz auf dem TSM-Server zu verwenden. Geben Sie auf dem TSM-Server (in einer Zeile) Folgendes ein:

   ```
   register node arc-user arc-password passexp=0 domain=tsm-domain
   MAXNUMMP=number-of-sessions
   ```

   Arc-user und Arc-password sind der Name und das Kennwort des Client-Knotens, den Sie auf dem Archiv-Node definieren, und der Wert von MAXNUMMP ist auf die Anzahl der Bandlaufwerke festgelegt, die für Archive Node Store-Sessions reserviert sind.

   Durch die Registrierung eines Knotens wird standardmäßig eine Administrator-Benutzer-ID mit der Berechtigung des Clienteigentümers erstellt, wobei das für den Knoten definierte Passwort angegeben ist.

Datenmigration zu StorageGRID

Sie können große Datenmengen bei gleichzeitigem Einsatz des StorageGRID Systems auf das StorageGRID System migrieren.

Verwenden Sie diesen Leitfaden, wenn Sie eine Migration großer Datenmengen in das StorageGRID System planen. Sie ist kein allgemeiner Leitfaden für die Datenmigration und enthält keine detaillierten Schritte zur Durchführung einer Migration. Befolgen Sie die Richtlinien und Anweisungen in diesem Abschnitt, um sicherzustellen, dass Daten effizient in das StorageGRID System migriert werden, ohne den täglichen Betrieb zu beeinträchtigen und dass die migrierten Daten vom StorageGRID System entsprechend gehandhabt werden.

Bestätigen Sie die Kapazität des StorageGRID Systems

Bevor Sie große Datenmengen in das StorageGRID System migrieren, vergewissern Sie sich, dass das StorageGRID System über die Festplattenkapazität verfügt, um das erwartete Volume zu verwalten.

Wenn das StorageGRID-System einen Archivknoten enthält und eine Kopie der migrierten Objekte im Nearline-Speicher (z. B. Band) gespeichert wurde, stellen Sie sicher, dass der Speicher des Archivknotens über genügend Kapazität für das erwartete Volumen der migrierten Daten verfügt.

Sehen Sie sich als Teil der Kapazitätsbewertung das Datenprofil der zu migrierenden Objekte an und berechnen Sie die erforderliche Festplattenkapazität. Weitere Informationen zum Monitoring der Festplattenkapazität Ihres StorageGRID Systems finden Sie unter "Managen Sie Storage-Nodes" Und die Anweisungen für "Monitoring von StorageGRID".

ILM-Richtlinie für migrierte Daten bestimmen

Die ILM-Richtlinie von StorageGRID bestimmt, wie viele Kopien erstellt werden, an welchen Standorten Kopien gespeichert werden und wie lange diese Kopien aufbewahrt werden. Eine ILM-Richtlinie besteht aus mehreren ILM-Regeln, die die Filterung von Objekten und das Managen von Objektdaten über einen längeren Zeitraum beschreiben.

Je nachdem, wie migrierte Daten verwendet werden und Ihre Anforderungen für migrierte Daten erfüllt werden, können Sie eindeutige ILM-Regeln für migrierte Daten definieren, die sich von den ILM-Regeln unterscheiden, die für tägliche Betriebsabläufe verwendet werden. Wenn z. B. für das tägliche Datenmanagement unterschiedliche gesetzliche Anforderungen gelten als für die in der Migration enthaltenen Daten, möchten Sie

möglicherweise eine andere Anzahl von Kopien der zu migrierenden Daten in einer anderen Storage-Klasse nutzen.

Sie können Regeln konfigurieren, die ausschließlich für migrierte Daten gelten, wenn es möglich ist, zwischen migrierten Daten und Objektdaten, die von den täglichen Abläufen gespeichert werden, eindeutig zu unterscheiden.

Wenn Sie mit einem der Metadatenkriterien zuverlässig zwischen den Datentypen unterscheiden können, können Sie anhand dieser Kriterien eine ILM-Regel definieren, die nur für migrierte Daten gilt.

Bevor Sie mit der Datenmigration beginnen, sollten Sie sich mit der ILM-Richtlinie des StorageGRID Systems und der Anwendung auf die migrierten Daten vertraut machen und alle Änderungen an der ILM-Richtlinie vorgenommen und getestet haben. Siehe "Objektmanagement mit ILM".

> Eine falsch angegebene ILM-Richtlinie kann zu nicht wiederherstellbaren Datenverlusten führen. Überprüfen Sie alle Änderungen an einer ILM-Richtlinie sorgfältig, bevor Sie sie aktivieren, um sicherzustellen, dass die Richtlinie wie vorgesehen funktioniert.

Bewerten der Auswirkung der Migration auf den Betrieb

Ein StorageGRID System wurde entwickelt, um einen effizienten Objekt-Storage- und -Abruf-Service zu ermöglichen. Durch die nahtlose Erstellung redundanter Kopien von Objektdaten und Metadaten ist ein hervorragender Schutz vor Datenverlust gewährleistet.

Die Datenmigration muss jedoch gemäß den Anweisungen in diesem Leitfaden sorgfältig durchgeführt werden, um Auswirkungen auf den täglichen Systembetrieb oder, in Extremfällen, die Gefahr eines Datenverlusts bei einem Ausfall im StorageGRID-System zu vermeiden.

Die Migration großer Datenmengen belastet das System zusätzlich. Bei starker Beladung des StorageGRID Systems reagiert das System langsamer auf Anfragen zum Speichern und Abrufen von Objekten. Dies beeinträchtigt das Speichern und Abrufen von Anfragen, die von wesentlicher Bedeutung für die täglichen Betriebsabläufe sind. Die Migration kann auch andere betriebliche Probleme verursachen. Wenn sich beispielsweise ein Storage-Node der Kapazität nähert, kann die hohe intermittierende Last aufgrund der Batch-Aufnahme dazu führen, dass der Storage Node zwischen Lese- und Schreibvorgängen wechseln und Meldungen generieren kann.

Bei hoher Auslastung können sich Warteschlangen für verschiedene Vorgänge entwickeln, die das StorageGRID System durchführen muss, um vollständige Redundanz von Objektdaten und -Metadaten sicherzustellen.

Die Datenmigration muss entsprechend den Richtlinien in diesem Dokument sorgfältig gemanagt werden, um einen sicheren und effizienten Betrieb des StorageGRID Systems während der Migration sicherzustellen. Nehmen Sie bei der Datenmigration Objekte in Batches auf oder drosseln Sie kontinuierlich die Aufnahme. Überwachen Sie dann kontinuierlich das StorageGRID-System, um sicherzustellen, dass verschiedene Attributwerte nicht überschritten werden.

Planung und Überwachung der Datenmigration

Die Datenmigration muss bei Bedarf geplant und überwacht werden, um sicherzustellen, dass die Daten gemäß der ILM-Richtlinie innerhalb der erforderlichen Frist abgelegt werden.

Planen Sie die Datenmigration

Vermeiden Sie die Datenmigration während der wichtigsten Geschäftszeiten. Begrenzen Sie die Datenmigration auf Abende, Wochenenden und andere Zeiten, in denen die Systemauslastung knapp ist.

Planen Sie nach Möglichkeit keine Datenmigration in Phasen mit hoher Aktivität ein. Wenn es jedoch nicht sinnvoll ist, den hohen Aktivitätszeitraum vollständig zu vermeiden, ist es sicher, so lange vorzugehen, wie Sie die relevanten Attribute genau überwachen und Maßnahmen ergreifen, wenn sie akzeptable Werte überschreiten.

Monitoring der Datenmigration

In dieser Tabelle sind die Attribute aufgeführt, die während der Datenmigration überwacht werden müssen, und die jeweiligen Probleme aufgeführt.

Wenn Sie Traffic-Klassifizierungsrichtlinien mit Geschwindigkeitsbegrenzungen zur Drosselung verwenden, können Sie die beobachtete Rate in Verbindung mit den in der folgenden Tabelle beschriebenen Statistiken überwachen und die Grenzwerte bei Bedarf reduzieren.

Überwachen	Beschreibung
Anzahl an Objekten, die auf die ILM-Bewertung warten	1. Wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie** aus. 2. Wählen Sie ***Deployment*** > **Übersicht** > **Main**. 3. Überwachen Sie im Abschnitt ILM-Aktivität die Anzahl der für die folgenden Attribute angezeigten Objekte: ◦ **Ausstehend - alles (XQUZ)**: Die Gesamtzahl der Objekte, die auf die ILM-Bewertung warten. ◦ **Ausstehend - Client (XCQZ)**: Die Gesamtzahl der Objekte, die auf eine ILM-Bewertung aus Client-Operationen warten (zum Beispiel Aufnahme). 4. Wenn die Anzahl der für eines dieser Attribute angezeigten Objekte 100,000 überschreitet, drosseln Sie die Aufnahmegeschwindigkeit von Objekten, um die Last auf dem StorageGRID-System zu verringern.
Storage-Kapazität eines Targeted Archivsystems	Wenn durch die ILM-Richtlinie eine Kopie der migrierten Daten auf ein zielgerichtetes Storage-System (Band oder Cloud) gespeichert wird, überwachen Sie die Kapazität des Zielspeichersystems, um sicherzustellen, dass genügend Kapazität für die migrierten Daten vorhanden ist.
Archiv-Knoten > **ARC** > **Store**	Wenn ein Alarm für das Attribut **Store Failures (ARVF)** ausgelöst wird, hat das zielgerichtete Archivspeichersystem möglicherweise die Kapazität erreicht. Überprüfen Sie das ausgewählte Archivspeichersystem, und beheben Sie alle Probleme, die einen Alarm ausgelöst haben.

Objektmanagement mit ILM

Objekte mit ILM managen: Übersicht

Sie managen die Objekte in einem StorageGRID System, indem Sie eine ILM-Richtlinie (Information Lifecycle Management) konfigurieren, die aus einer oder mehreren ILM-Regeln besteht. Die ILM-Regeln erklären StorageGRID, wie Kopien von Objektdaten

erstellt und verteilt werden und wie diese Kopien über einen längeren Zeitraum gemanagt werden.

Informationen zu diesen Anweisungen

Für die Entwicklung und Implementierung von ILM-Regeln und der ILM-Richtlinie ist eine sorgfältige Planung erforderlich. Betriebliche Anforderungen, die Topologie des StorageGRID Systems, die Anforderungen an die Objektsicherung und die verfügbaren Storage-Typen sind unbedingt bekannt. Anschließend müssen Sie festlegen, wie unterschiedliche Objekttypen kopiert, verteilt und gespeichert werden sollen.

Mithilfe dieser Anweisungen können Sie:

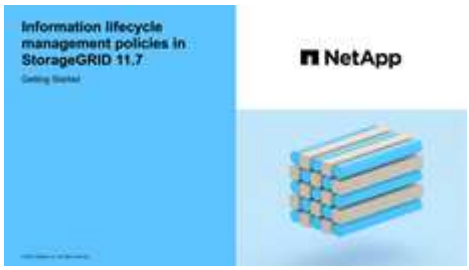
- Erfahren Sie mehr über StorageGRID ILM, einschließlich "Wie ILM im gesamten Leben eines Objekts funktioniert".
- Erfahren Sie mehr über die Konfiguration "Storage-Pools", "Cloud-Storage-Pools", und "ILM-Regeln".
- Erfahren Sie, wie Sie "Erstellen, Simulieren und Aktivieren einer ILM-Richtlinie" Auf diese Weise werden Objektdaten an einem oder mehreren Standorten gesichert.
- Erfahren Sie, wie Sie "Managen von Objekten mit S3 Object Lock", Wodurch sichergestellt wird, dass Objekte in bestimmten S3 Buckets nicht für einen bestimmten Zeitraum gelöscht oder überschrieben werden.

Weitere Informationen .

Sehen Sie sich die folgenden Videos an, um mehr zu erfahren:

- "Video: Information Lifecycle Management Regeln in StorageGRID 11.7".

- "Video: Information Lifecycle Management Policies in StorageGRID 11.7"



ILM und Objekt-Lebenszyklus

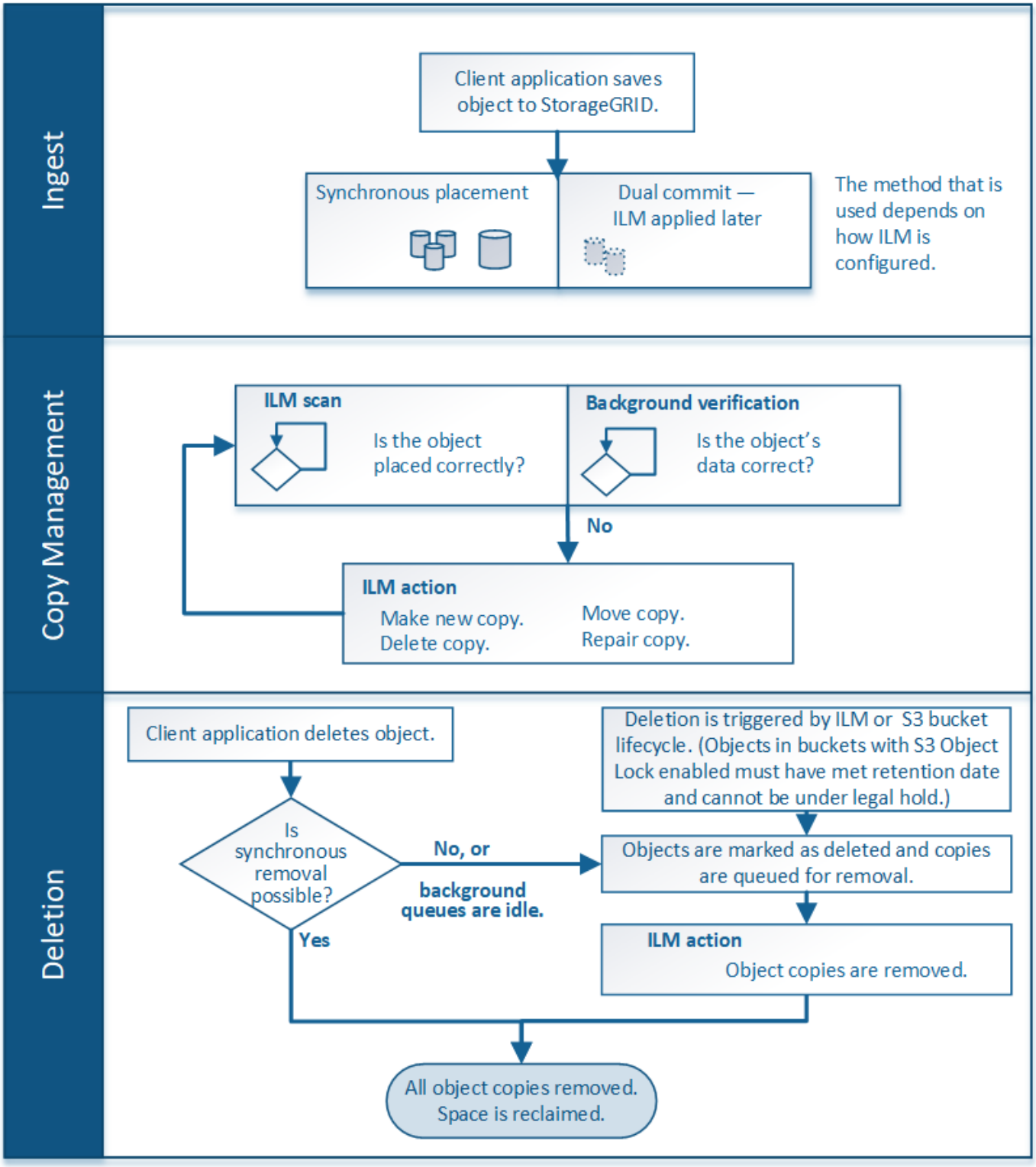
Wie ILM im gesamten Leben eines Objekts funktioniert

Wenn Sie verstehen, wie StorageGRID ILM für das Management von Objekten in jeder Lebensphase verwendet, können Sie eine effektivere Richtlinie entwickeln.

- **Aufnahme**: Aufnahme beginnt, wenn eine S3- oder Swift-Client-Anwendung eine Verbindung zum Speichern eines Objekts in das StorageGRID-System herstellt und abgeschlossen ist, wenn StorageGRID eine „`Aufnahme erfolgreich`“-Nachricht an den Client zurückgibt. Objektdaten werden bei der Aufnahme entweder durch sofortiges Anwenden von ILM-Anweisungen (synchrone Platzierung) oder durch Erstellen von zwischenzeitlichen Kopien und spätere Anwendung von ILM (Dual Commit) gesichert, je nachdem, wie die ILM-Anforderungen angegeben wurden.
- **Kopierverwaltung**: Nach dem Erstellen der Anzahl und des Typs der Objektkopien, die in den Anweisungen zur Platzierung des ILM angegeben sind, verwaltet StorageGRID Objektorte und schützt Objekte vor Verlust.
  - ILM-Scan und -Bewertung: StorageGRID scannt kontinuierlich die Liste der im Grid gespeicherten Objekte und überprüft, ob die aktuellen Kopien den ILM-Anforderungen entsprechen. Wenn unterschiedliche Typen, Ziffern oder Standorte von Objektkopien erforderlich sind, erstellt, löscht oder verschiebt StorageGRID Kopien nach Bedarf.
  - Hintergrundüberprüfung: StorageGRID führt kontinuierlich Hintergrundüberprüfung durch, um die Integrität von Objektdaten zu überprüfen. Wenn ein Problem gefunden wird, erstellt StorageGRID automatisch eine neue Objektkopie oder ein durch Löschung codiertes Objektfragment für den Austausch, das die aktuellen ILM-Anforderungen erfüllt. Siehe "Überprüfen Sie die Objektintegrität".
- **Objektlöschung**: Verwaltung eines Objekts endet, wenn alle Kopien aus dem StorageGRID-System entfernt werden. Objekte können als Ergebnis einer Löschanforderung durch einen Client oder als Ergebnis eines Löschvorgangs durch ILM oder Löschung aufgrund des Ablaufs eines S3-Bucket-Lebenszyklus entfernt werden.

> Objekte in einem Bucket, für den die S3-Objektsperrung aktiviert ist, können nicht gelöscht werden, wenn sie sich unter einer Legal Hold befinden oder wenn ein Aufbewahrungsdatum angegeben, aber noch nicht erfüllt wurde.

Das Diagramm fasst die Funktionsweise von ILM im gesamten Lebenszyklus eines Objekts zusammen.



Aufnahme von Objekten

Aufnahmeoptionen

Wenn Sie eine ILM-Regel erstellen, geben Sie eine von drei Optionen zum Schutz der Objekte bei der Aufnahme an: Doppelter Commit, strenger oder ausgeglichener Storage.

Je nach Ihrer Wahl erstellt StorageGRID später vorläufige Kopien und Warteschlangen für die ILM-Bewertung.

Alternativ nutzt es die synchrone Platzierung und erstellt sofort Kopien zur Erfüllung der ILM-Anforderungen.

Flussdiagramm der Aufnahmeoptionen

Das Flussdiagramm zeigt, was passiert, wenn Objekte mit einer ILM-Regel abgeglichen werden, die jede der drei Aufnahmeoptionen nutzt.

Doppelte Provisionierung

Wenn Sie die Option Dual Commit auswählen, erstellt StorageGRID sofort interim-Objektkopien auf zwei verschiedenen Storage-Nodes und gibt dem Client eine „`Ingest Successful`“-Nachricht zurück. Das Objekt wird zur ILM-Evaluierung in eine Warteschlange gestellt und Kopien, die den Anweisungen zur Platzierung der Regel entsprechen, werden später erstellt.

Wann sollten Sie die Option Dual Commit verwenden

Verwenden Sie in einem der folgenden Fälle die Dual-Commit-Option:

- Die wichtigsten Überlegungen dabei sind die Verwendung von ILM-Regeln für mehrere Standorte und die Client-Erfassungs-Latenz. Wenn Sie Dual Commit verwenden, müssen Sie sicherstellen, dass Ihr Grid die zusätzliche Arbeit beim Erstellen und Entfernen der Dual-Commit-Kopien ausführen kann, wenn sie ILM nicht erfüllen. Im Detail:
  - Die Last am Grid muss so gering sein, dass kein ILM-Rückstand mehr vorhanden ist.
  - Das Grid muss über überschüssige Hardware-Ressourcen verfügen (IOPS, CPU, Arbeitsspeicher, Netzwerkbandbreite usw.).
- Sie verwenden ILM-Regeln für mehrere Standorte und die WAN-Verbindung zwischen den Standorten weist normalerweise eine hohe Latenz oder eine begrenzte Bandbreite auf. In diesem Szenario kann die Verwendung der Dual-Commit-Option dazu beitragen, Client-Timeouts zu verhindern. Bevor Sie sich für die Dual Commit-Option entscheiden, sollten Sie die Client-Applikation mit realistischen Workloads testen.

Streng

Wenn Sie die strenge Option auswählen, verwendet StorageGRID bei der Aufnahme eine synchrone Platzierung und erstellt sofort alle Objektkopien, die in der Plazierung der Regel angegeben sind. Die Aufnahme schlägt fehl, wenn StorageGRID nicht alle Kopien erstellen kann, z. B. weil ein erforderlicher Speicherort vorübergehend nicht verfügbar ist. Der Client muss den Vorgang wiederholen.

Wann die strenge Option verwendet werden soll

Verwenden Sie die Option streng, wenn Sie eine betriebliche oder gesetzliche Anforderung haben, Objekte sofort nur an den in der ILM-Regel aufgeführten Standorten zu speichern. Um beispielsweise eine gesetzliche Vorgabe zu erfüllen, müssen Sie möglicherweise die Option „Strict“ und einen erweiterten Filter „Speicherortbeschränkung“ verwenden, um sicherzustellen, dass Objekte niemals in bestimmten Rechenzentren gespeichert werden.

Siehe "Beispiel 5: ILM-Regeln und Richtlinie für striktes Ingest-Verhalten".

Ausgeglichen (Standard)

Wenn Sie die Option „Ausgleich“ auswählen, verwendet StorageGRID bei der Aufnahme auch die synchrone Platzierung und erstellt sofort alle Kopien, die in den Anweisungen zur Platzierung der Regel angegeben sind. Wenn StorageGRID nicht sofort alle Kopien erstellen kann, verwendet man im Gegensatz zur strengen Option

„Dual Commit“.

Wann sollte die Option „Balance“ verwendet werden

Die ausgewogene Option erzielt die beste Kombination aus Datensicherung, Grid-Performance und Aufnahme-Erfolg. Ausgeglichen ist die Standardoption im Assistenten zum Erstellen von ILM-Regeln.

Vorteile, Nachteile und Einschränkungen der Aufnahmsoptionen

Wenn Sie die vor- und Nachteile der drei Optionen zum Schutz von Daten bei der Aufnahme (ausgewogen, streng oder Dual-Commit) kennen, können Sie leichter entscheiden, welche für eine ILM-Regel ausgewählt werden soll.

Eine Übersicht über die Aufnahmeoptionen finden Sie unter "Aufnahmeoptionen".

Vorteile der ausgewogenen und strengen Optionen

Im Vergleich zu Dual-Commit, das während der Aufnahme zwischenzeitliche Kopien erstellt, bieten die zwei Optionen zur synchronen Platzierung folgende Vorteile:

- **Bessere Datensicherheit**: Objektdaten werden sofort gemäß den Anweisungen zur Platzierung der ILM-Regel geschützt, die so konfiguriert werden können, dass sie vor einer Vielzahl von Ausfallszenarien, einschließlich des Ausfalls von mehr als einem Speicherort, geschützt werden. Bei zwei Daten kann nur der Schutz vor dem Verlust einer einzelnen lokalen Kopie geschützt werden.
- **Effizienterer Netzbetrieb**: Jedes Objekt wird nur einmal verarbeitet, wie es aufgenommen wird. Da das StorageGRID System die Interimskopien nicht nachverfolgen oder löschen muss, sinkt der Verarbeitungsbedarf und der Datenbankspeicherplatz wird verringert.
- **(ausgewogen) Empfohlen**: Die ausgewogene Option bietet optimale ILM-Effizienz. Die Verwendung der Balanced-Option wird empfohlen, es sei denn, es ist ein striktes Aufnahmeverhalten erforderlich oder das Grid erfüllt alle Kriterien für die Verwendung von Dual Commit.
- **(striktes) Gewissheit über Objektstandorte**: Die strenge Option garantiert, dass Objekte sofort nach den Platzierungsanweisungen in der ILM-Regel gespeichert werden.

Nachteile der ausgewogenen und strengen Optionen

Im Vergleich zu Dual Commit haben die ausgewogenen und strengen Optionen einige Nachteile:

- **Längere Client-Ingest**: Client-Ingest-Latenzen können länger sein. Wenn Sie die Optionen „ausgeglichen“ oder „streng“ verwenden, wird die Meldung „`Ingest successful`“ erst an den Client zurückgegeben, wenn alle Fragmente, die nach der Löschung codiert wurden, oder replizierte Kopien erstellt und gespeichert werden. Objektdaten werden allerdings sehr wahrscheinlich die endgültige Platzierung viel schneller erreichen.
- **(streng) höhere Aufnahmeraten**: Bei der strengen Option schlägt die Aufnahme fehl, wenn StorageGRID nicht sofort alle in der ILM-Regel angegebenen Kopien erstellen kann. Falls ein benötigter Speicherplatz vorübergehend offline ist oder Netzwerkprobleme auftreten, die zu Verzögerungen beim Kopieren von Objekten zwischen Standorten führen, ist unter Umständen ein hoher Aufnahmefehler zu beobachten.
- **(strict) S3-Multipart-Upload-Platzierungen sind unter Umständen nicht wie erwartet**: Bei strikter Prüfung erwarten Sie, dass Objekte entweder wie in der ILM-Regel beschrieben platziert werden oder dass die Aufnahme fehlschlägt. Bei einem S3-Multipart-Upload wird ILM für jeden aufgenommenen Teil des Objekts und für das gesamte Objekt evaluiert, wenn der mehrteilige Upload abgeschlossen ist. Unter den folgenden Umständen kann dies zu Platzierungen führen, die sich von Ihnen unterscheiden:

    - **Wenn sich ILM ändert, während ein S3-Multipart-Upload im Gange ist**: Da jedes Teil gemäß der Regel platziert wird, die bei der Aufnahme des Teils aktiv ist, entsprechen einige Teile des Objekts möglicherweise nicht den aktuellen ILM-Anforderungen, wenn der mehrteilige Upload abgeschlossen ist. In diesen Fällen schlägt die Aufnahme des Objekts nicht fehl. Stattdessen wird jedes Teil, das nicht korrekt platziert wird, in die Warteschlange für eine erneute ILM-Bewertung eingereiht und später an den richtigen Speicherort verschoben.
    - **Wenn ILM-Regeln Filter auf Größe**: Bei der Bewertung von ILM für ein Teil filtert StorageGRID die Größe des Teils, nicht die Größe des Objekts. Das bedeutet, dass Teile eines Objekts an Orten gespeichert werden können, die die ILM-Anforderungen für das gesamte Objekt nicht erfüllen. Wenn z. B. eine Regel angibt, dass alle Objekte ab 10 GB auf DC1 gespeichert werden, während alle kleineren Objekte an DC2 gespeichert sind, wird bei Aufnahme jeder 1 GB-Teil eines 10-teiligen mehrteiligen Uploads auf DC2 gespeichert. Wenn ILM für das Objekt bewertet wird, werden alle Teile des Objekts auf DC1 verschoben.
- **(strict) Aufnahme scheitert nicht, wenn Objekt-Tags oder Metadaten aktualisiert werden und neu erforderliche Platzierungen nicht gemacht werden können**: Mit strikter, erwarten Sie, dass Objekte entweder wie in der ILM-Regel beschrieben platziert werden oder dass die Aufnahme fehlschlägt. Wenn Sie jedoch Metadaten oder Tags für ein Objekt aktualisieren, das bereits im Raster gespeichert ist, wird das Objekt nicht erneut aufgenommen. Das bedeutet, dass Änderungen an der Objektplatzierung, die durch die Aktualisierung ausgelöst werden, nicht sofort vorgenommen werden. Änderungen an der Platzierung werden vorgenommen, wenn ILM durch normale ILM-Prozesse im Hintergrund neu bewertet wird. Wenn erforderliche Platzierungsänderungen nicht vorgenommen werden können (z. B. weil ein neu erforderlicher Standort nicht verfügbar ist), behält das aktualisierte Objekt seine aktuelle Platzierung bei, bis die Platzierungsänderungen möglich sind.

Einschränkungen bei Objektplatzierungen mit den ausgewogenen und strengen Optionen

Die ausgewogenen oder strikten Optionen können nicht für ILM-Regeln verwendet werden, die über eine der folgenden Platzierungsanweisungen verfügen:

- Platzierung in einem Cloud-Storage-Pool am Tag 0
- Platzierung in einem Archiv-Knoten an Tag 0.
- Platzierungen in einem Cloud-Speicherpool oder einem Archiv-Node, wenn die Regel eine benutzerdefinierte Erstellungszeit als Referenzzeit hat.

Diese Einschränkungen bestehen, da StorageGRID nicht synchron Kopien auf einen Cloud-Speicherpool oder Archivknoten erstellen kann und eine benutzerdefinierte Erstellungszeit auf die Gegenwart aufgelöst werden kann.

Auswirkungen von ILM-Regeln und Konsistenzkontrollen auf die Datensicherung

Sowohl Ihre ILM-Regel als auch Ihre Wahl der Konsistenzkontrolle beeinflussen den Schutz von Objekten. Diese Einstellungen können interagieren.

Das für eine ILM-Regel ausgewählte Aufnahmeverhalten wirkt sich beispielsweise auf die anfängliche Platzierung von Objektkopien aus, während sich die beim Speichern eines Objekts verwendete Konsistenzkontrolle auf die anfängliche Platzierung von Objekt-Metadaten auswirkt. StorageGRID benötigt zur Erfüllung von Clientanforderungen sowohl Zugriff auf die Daten eines Objekts als auch auf die Metadaten. Durch die Auswahl der passenden Schutzstufen für die Konsistenzstufe und das Aufnahmeverhalten können die Daten anfangs besser gesichert und Systemantworten vorhersehbarer.

Hier finden Sie eine kurze Zusammenfassung der in StorageGRID verfügbaren Konsistenzkontrollen:

- **Alle**: Alle Knoten erhalten sofort Objektmetadaten oder die Anfrage schlägt fehl.

- **Stark-global**: Objektmetadaten werden sofort auf alle Seiten verteilt. Garantierte Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen an allen Standorten.
- **Strong-site**: Objektmetadaten werden sofort auf andere Knoten am Standort verteilt. Garantiert Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen innerhalb eines Standorts.
- **Read-after-New-write**: Sorgt für die Konsistenz von Read-after-write für neue Objekte und eventuelle Konsistenz von Objekt-Updates. Hochverfügbarkeit und garantierte Datensicherung Empfohlen für die meisten Fälle.
- **Verfügbar**: Bietet eventuelle Konsistenz für neue Objekte und Objekt-Updates. Verwenden Sie für S3-Buckets nur nach Bedarf (z. B. für einen Bucket mit Protokollwerten, die nur selten gelesen werden, oder für HEAD- oder GET-Vorgänge für nicht vorhandene Schlüssel). Nicht unterstützt für S3 FabricPool-Buckets.

> Lesen Sie vor Auswahl einer Konsistenzstufe die vollständige Beschreibung der Consistency Controls in den Anweisungen für "S3-REST-API VERWENDEN". Vor dem Ändern des Standardwerts sollten Sie die Vorteile und Einschränkungen kennen.

Beispiel für die Interaktion zwischen Konsistenzkontrolle und ILM-Regel

Angenommen, Sie haben ein Grid mit zwei Standorten mit der folgenden ILM-Regel und der folgenden Einstellung für die Konsistenzstufe:

- **ILM-Regel**: Erstellen Sie zwei Objektkopien, eine am lokalen Standort und eine an einem entfernten Standort. Das strikte Aufnahmeverhalten wird ausgewählt.
- **Konsistenzstufe**: “strong-global” (Objektmetadaten werden sofort auf alle Standorte verteilt.)

Wenn ein Client ein Objekt im Grid speichert, erstellt StorageGRID sowohl Objektkopien als auch verteilt Metadaten an beiden Standorten, bevor der Kunde zum Erfolg zurückkehrt.

Das Objekt ist zum Zeitpunkt der Aufnahme der Nachricht vollständig gegen Verlust geschützt. Wenn beispielsweise der lokale Standort kurz nach der Aufnahme verloren geht, befinden sich Kopien der Objektdaten und der Objektmetadaten am Remote-Standort weiterhin. Das Objekt kann vollständig abgerufen werden.

Falls Sie stattdessen dieselbe ILM-Regel und die Konsistenzstufe „`strong-Site`“ verwendet haben, erhält der Client möglicherweise eine Erfolgsmeldung, nachdem die Objektdaten an den Remote Standort repliziert wurden, aber bevor die Objektmetadaten dort verteilt werden. In diesem Fall entspricht die Sicherung von Objektmetadaten nicht dem Schutzniveau für Objektdaten. Falls der lokale Standort kurz nach der Aufnahme verloren geht, gehen Objektmetadaten verloren. Das Objekt kann nicht abgerufen werden.

Die Wechselbeziehung zwischen Konsistenzstufen und ILM-Regeln kann komplex sein. Wenden Sie sich an NetApp, wenn Sie Hilfe benötigen.

Verwandte Informationen

- "Beispiel 5: ILM-Regeln und Richtlinie für striktes Ingest-Verhalten"

Speicherung von Objekten (Replizierung oder Erasure Coding)

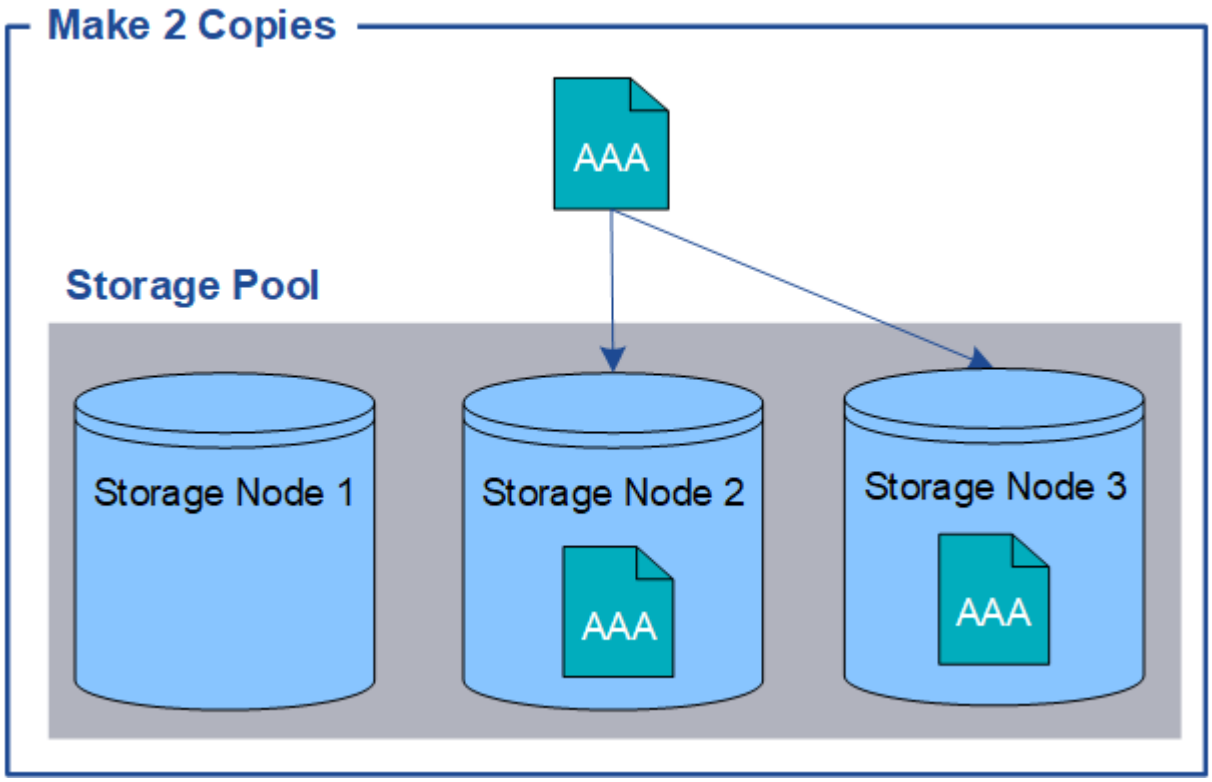
Was ist Replikation?

Die Replizierung ist eine von zwei Methoden, die von StorageGRID zum Speichern von Objektdaten verwendet werden. Wenn Objekte mit einer ILM-Regel übereinstimmen, die

Replizierung verwendet, erstellt das System exakte Kopien von Objektdaten und speichert die Kopien auf Storage-Nodes oder Archiv-Nodes.

Wenn Sie eine ILM-Regel zum Erstellen replizierter Kopien konfigurieren, geben Sie an, wie viele Kopien erstellt werden sollen, wo diese Kopien erstellt werden sollen und wie lange die Kopien an jedem Standort gespeichert werden sollen.

Im folgenden Beispiel gibt die ILM-Regel an, dass zwei replizierte Kopien jedes Objekts in einem Storage-Pool mit drei Storage-Nodes platziert werden.



Wenn StorageGRID Objekte mit dieser Regel übereinstimmt, werden zwei Kopien des Objekts erstellt, wobei jede Kopie auf einem anderen Storage-Node im Storage-Pool platziert wird. Die beiden Kopien können auf zwei der drei verfügbaren Storage-Nodes platziert werden. In diesem Fall wurden in der Regel Objektkopien auf Speicherknoten 2 und 3 platziert. Da es zwei Kopien gibt, kann das Objekt abgerufen werden, wenn einer der Nodes im Speicherpool ausfällt.

> StorageGRID kann nur eine replizierte Kopie eines Objekts auf einem beliebigen Storage Node speichern. Wenn Ihr Grid drei Storage-Nodes enthält und Sie eine ILM-Regel mit 4 Kopien erstellen, werden nur drei Kopien erstellt: Eine Kopie für jeden Storage-Node. Die Warnung **ILM-Platzierung unerreichbar** wird ausgelöst, um anzuzeigen, dass die ILM-Regel nicht vollständig angewendet werden konnte.

Verwandte Informationen

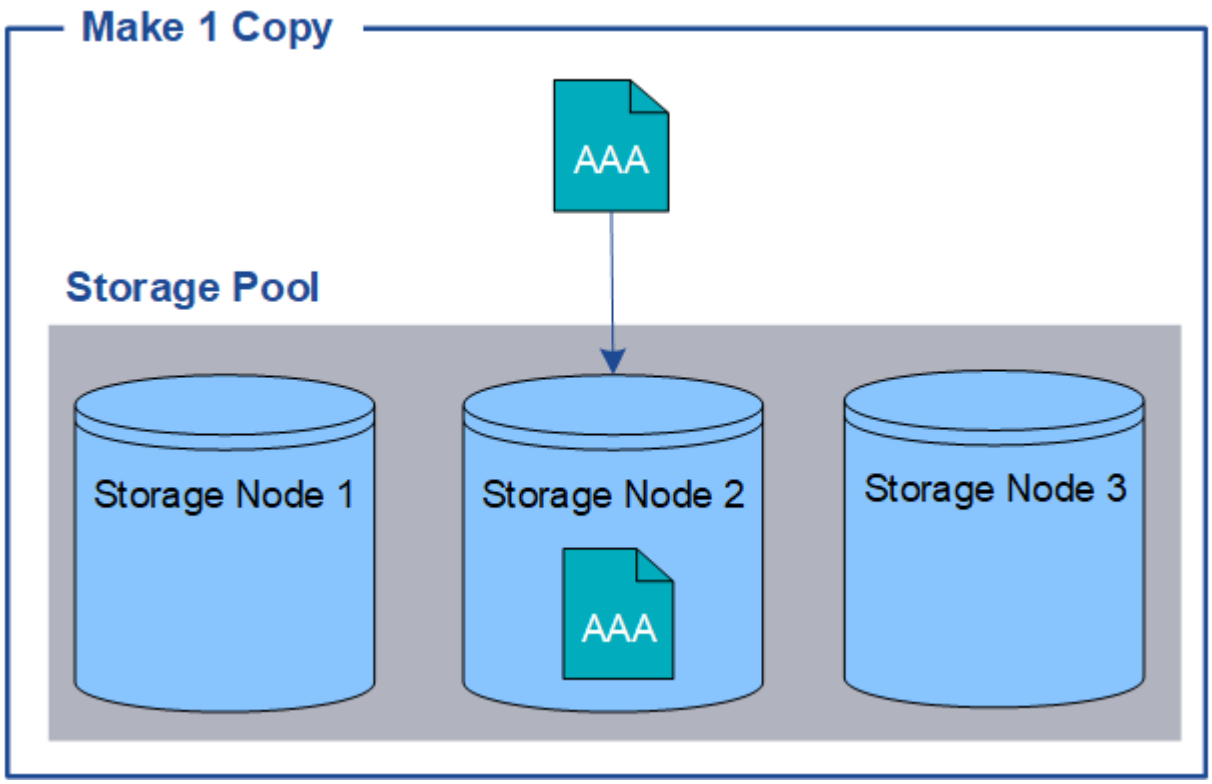
- "Was ist Erasure Coding?"
- "Was ist ein Speicherpool?"
- "Schutz vor Standortausfällen durch Replizierung und Erasure Coding"

Warum sollten Sie keine Replizierung mit nur einer Kopie verwenden

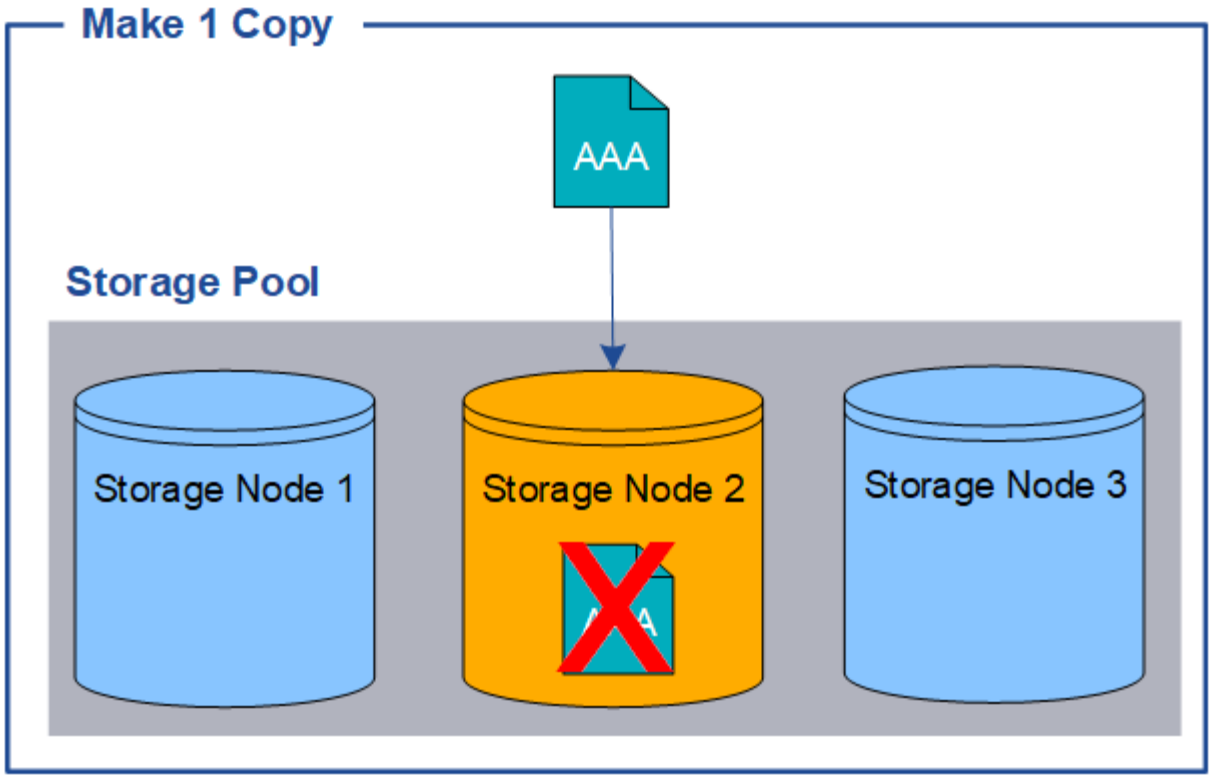
Beim Erstellen einer ILM-Regel zum Erstellen replizierter Kopien sollten Sie immer mindestens zwei Kopien für einen beliebigen Zeitraum in den Anweisungen zur Platzierung angeben.

> Verwenden Sie keine ILM-Regel, die nur eine replizierte Kopie für einen beliebigen Zeitraum erstellt. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen beträchtlichen Fehler hat. Während Wartungsarbeiten wie Upgrades verlieren Sie auch vorübergehend den Zugriff auf das Objekt.

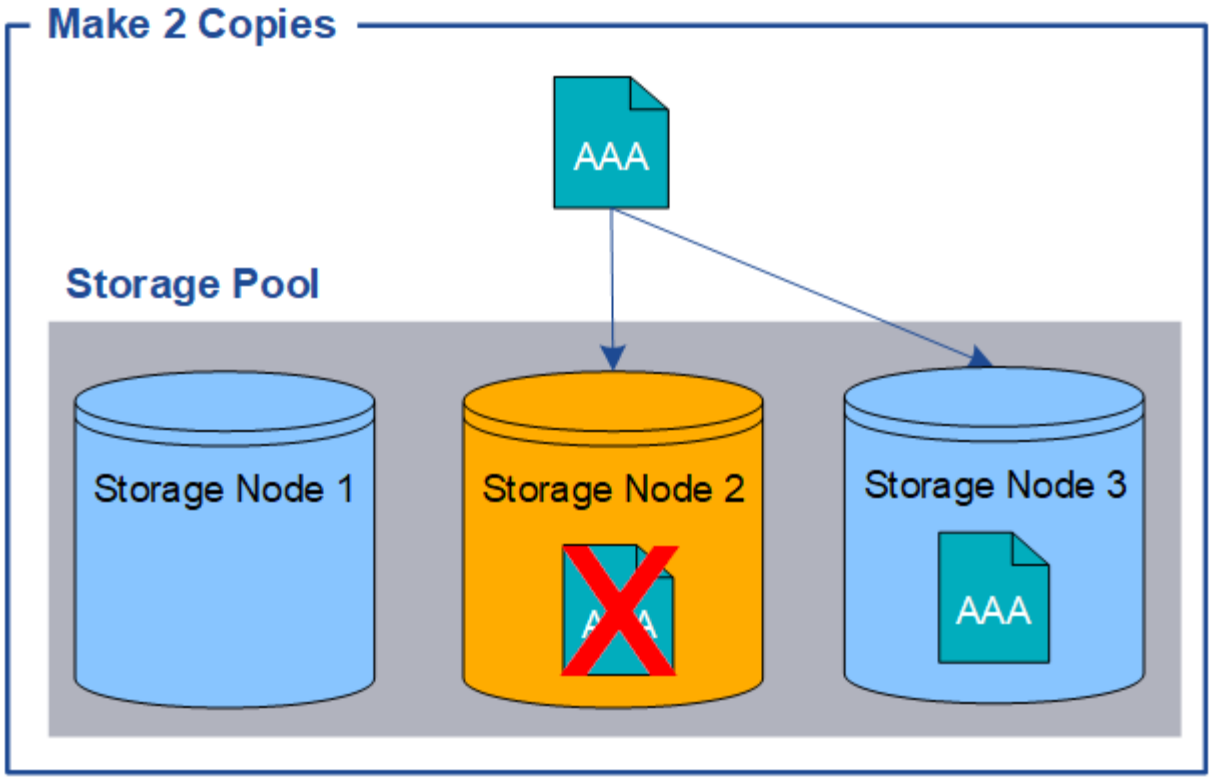
Im folgenden Beispiel gibt die ILM-Regel „1 Kopie erstellen“ an, dass eine replizierte Kopie eines Objekts in einem Speicherpool platziert wird, der drei Storage-Nodes enthält. Wenn ein Objekt aufgenommen wird, das dieser Regel entspricht, platziert StorageGRID eine einzelne Kopie auf nur einem Storage-Node.



Wenn eine ILM-Regel nur eine replizierte Kopie eines Objekts erstellt, ist der Zugriff auf das Objekt möglich, wenn der Storage-Node nicht verfügbar ist. In diesem Beispiel verlieren Sie vorübergehend den Zugriff auf das Objekt AAA, wenn Storage Node 2 offline ist, z. B. während eines Upgrades oder eines anderen Wartungsverfahrens. Sie verlieren das Objekt AAA vollständig, wenn Storage Node 2 ausfällt.



Um den Verlust von Objektdaten zu vermeiden, sollten immer mindestens zwei Kopien aller Objekte erstellt werden, die durch die Replizierung gesichert werden sollen. Wenn zwei oder mehr Kopien vorhanden sind, können Sie weiterhin auf das Objekt zugreifen, wenn ein Storage-Node ausfällt oder offline geht.



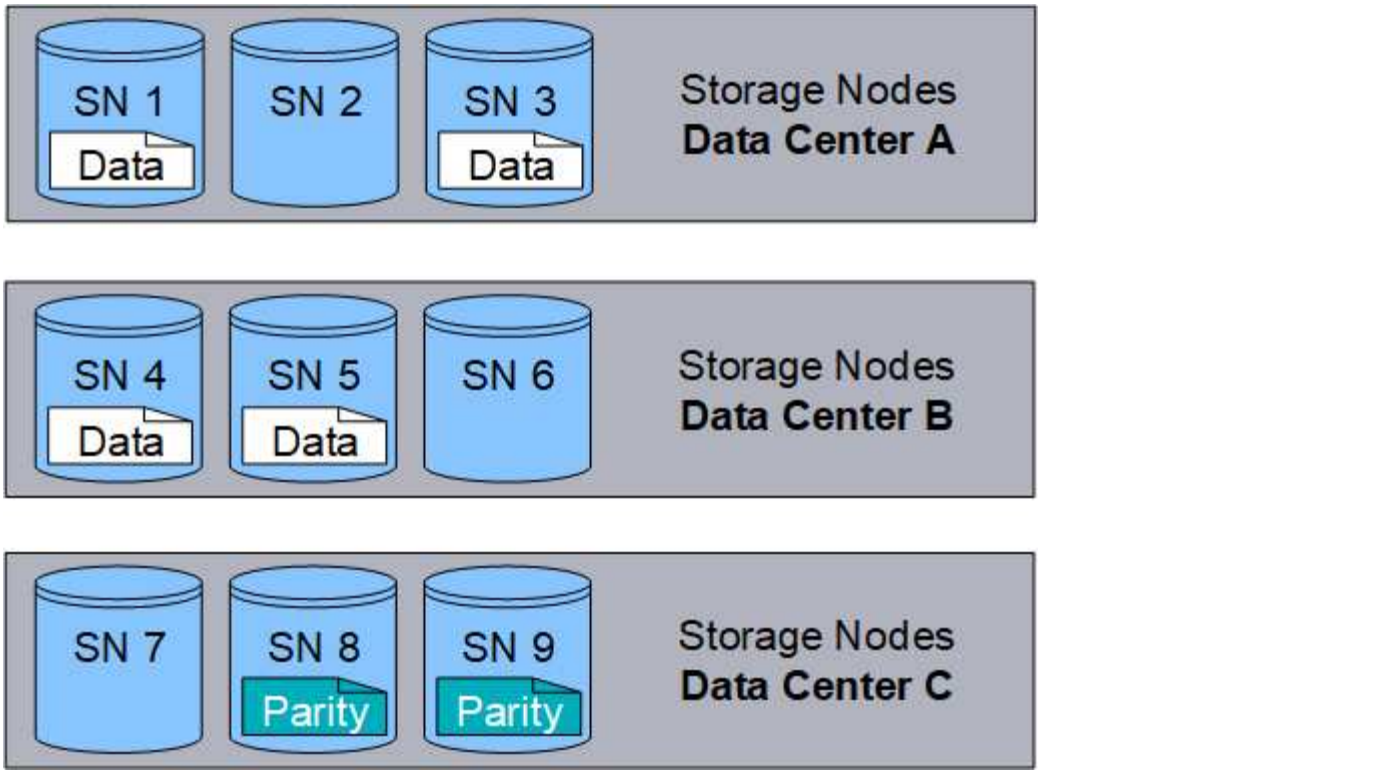
Was ist Erasure Coding?

Erasure Coding ist eine von zwei Methoden, die StorageGRID zum Speichern von Objektdaten verwendet. Wenn Objekte mit einer ILM-Regel übereinstimmen, die Erasure Coding verwendet, werden diese Objekte in Datenfragmente geteilt, weitere Paritätsfragmente werden berechnet und jedes Fragment wird auf einem anderen Storage Node gespeichert.

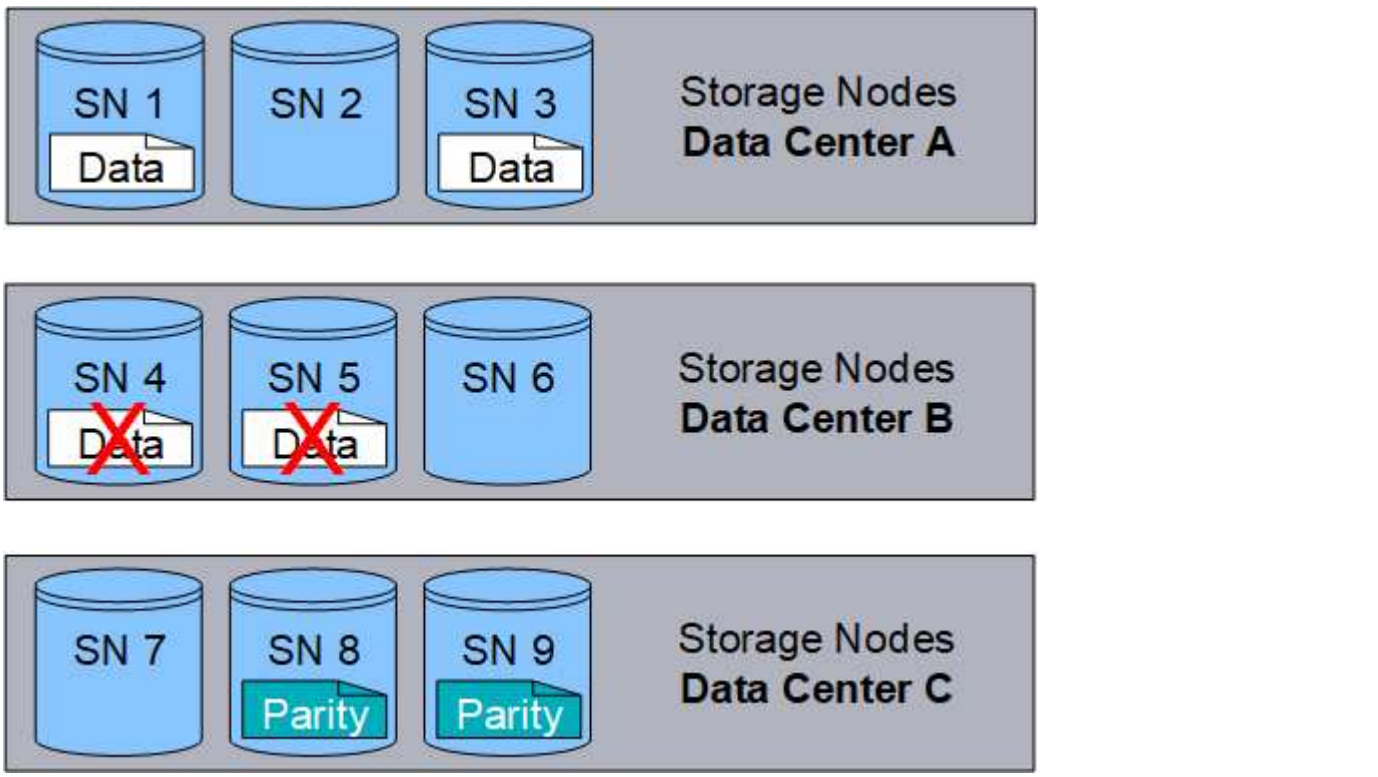
Wenn auf ein Objekt zugegriffen wird, wird es anhand der gespeicherten Fragmente neu zusammengesetzt. Wenn ein Daten oder ein Paritätsfragment beschädigt wird oder verloren geht, kann der Algorithmus zur Fehlerkorrektur dieses Fragment mit einer Teilmenge der verbleibenden Daten und Paritätsfragmente neu erstellen.

Beim Erstellen von ILM-Regeln erstellt StorageGRID Profile, die Erasure Coding unterstützen. Sie können eine Liste der Profile zum Erasure Coding anzeigen, "Umbenennen eines Profils für die Erasure Coding", Oder "Deaktivieren Sie ein Erasure Coding-Profil, wenn es derzeit nicht in ILM-Regeln verwendet wird".

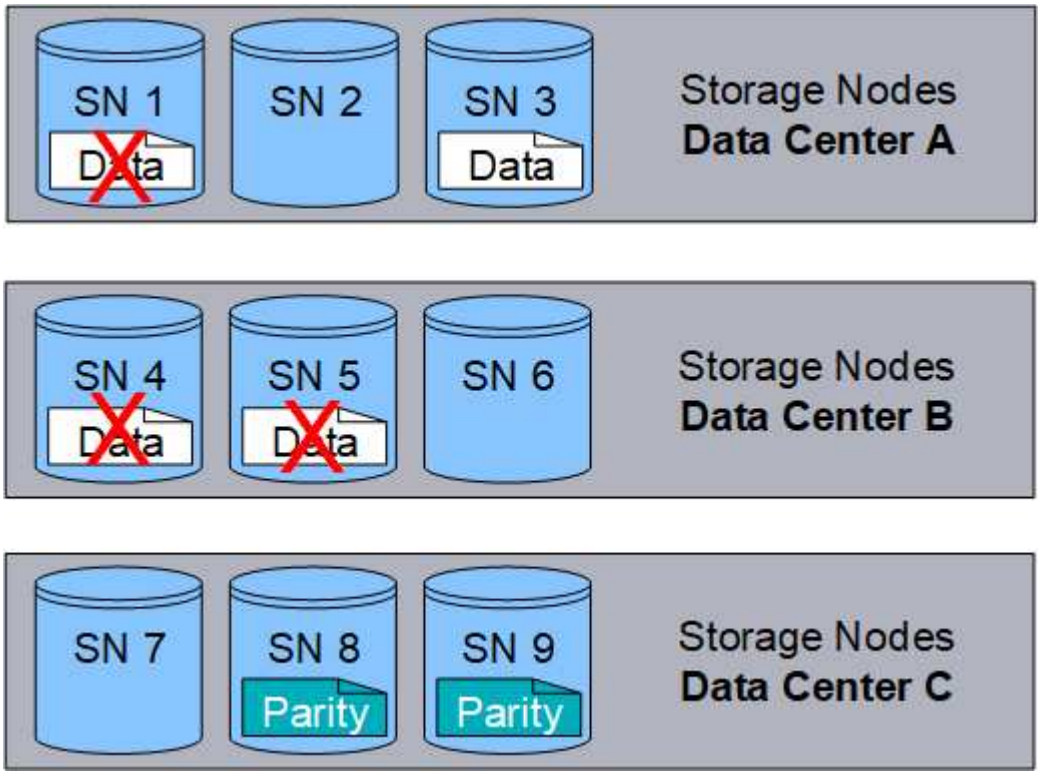
Im folgenden Beispiel wird der Algorithmus zur Einhaltung von Datenkonsistenz (Erasure Coding) für Objektdaten dargestellt. In diesem Beispiel verwendet die ILM-Regel ein 4+2-Schema zur Einhaltung von Datenkonsistenz. Jedes Objekt wird in vier gleiche Datenfragmente geteilt und aus den Objektdaten werden zwei Paritätsfragmente berechnet. Jedes der sechs Fragmente wird auf einem anderen Node über drei Datacenter-Standorte gespeichert, um Daten bei Node-Ausfällen oder Standortausfällen zu sichern.



Das 4+2 Erasure Coding-Schema kann auf verschiedene Weise konfiguriert werden. Sie können beispielsweise einen Speicherpool mit einem Standort konfigurieren, der sechs Storage-Nodes enthält. Für "Schutz vor Standortausfällen", Sie können einen Speicherpool verwenden, der drei Standorte mit drei Storage Nodes an jedem Standort enthält. Ein Objekt kann abgerufen werden, solange vier der sechs Fragmente (Daten oder Parität) verfügbar sind. Bis zu zwei Fragmente können ohne Verlust der Objektdaten verloren gehen. Wenn ein ganzer Standort verloren geht, kann das Objekt dennoch abgerufen oder repariert werden, solange alle anderen Fragmente zugänglich bleiben.



Wenn mehr als zwei Speicherknoten verloren gehen, kann das Objekt nicht abgerufen werden.



Verwandte Informationen

- "Was ist Replikation?"
- "Was ist ein Speicherpool?"
- "Was sind Erasure Coding-Systeme?"
- "Umbenennen eines Profils für die Erasure Coding"
- "Deaktivieren Sie ein Erasure Coding-Profil"

Was sind Erasure Coding-Systeme?

Erasure Coding steuert die Anzahl von Datenfragmenten und die Anzahl der Parity-Fragmente für jedes Objekt.

Wenn Sie das Profil zur Einhaltung von Datenkonsistenz für eine ILM-Regel konfigurieren, wählen Sie ein verfügbares Erasure-Coding-Schema basierend auf der Anzahl der Storage-Nodes und -Standorte des Storage-Pools aus, den Sie verwenden möchten.

Das StorageGRID-System verwendet den Reed-Solomon-Erasure-Coding-Algorithmus. Der Algorithmus teilt ein Objekt in ein `k` Datenfragmente und -Berechnung `m` Paritätsfragmente. Der `k + m = n` Fragmente werden verteilt `n` Storage-Nodes für die Datensicherung. Ein Objekt kann bis zu erhalten `m` Verlorene oder beschädigte Fragmente. Um ein Objekt abzurufen oder zu reparieren, `k` Fragmente werden benötigt.

Verwenden Sie bei der Auswahl des Speicherpools für eine Regel, die eine Kopie mit Verfahren zur Fehlerkorrektur erstellt, die folgenden Richtlinien für Speicherpools:

- Der Speicherpool muss drei oder mehr Standorte oder exakt einen Standort umfassen.

Sie können kein Erasure Coding verwenden, wenn der Storage-Pool zwei Standorte umfasst.

  - Verfahren zur Einhaltung von Datenkonsistenz für Storage-Pools mit drei oder mehr Standorten
  - Verfahren zur Einhaltung von Datenkonsistenz für Storage-Pools an einem Standort

- Verwenden Sie keinen Speicherpool, der den Standardstandort „Alle Standorte“ enthält.
- Der Speicherpool sollte mindestens enthalten *k+m* +1 Storage-Nodes:

  Die Mindestanzahl der erforderlichen Storage-Nodes ist k+m. Durch mindestens einen zusätzlichen Storage-Node können jedoch Ingest- oder ILM-Backlogs verhindert werden, wenn ein erforderlicher Storage-Node vorübergehend nicht verfügbar ist.

Der Storage-Overhead eines Erasure-Coding-Schemas wird durch Division der Anzahl der Paritätsfragmente berechnet (m) Durch die Anzahl der Datenfragmente (k). Der Storage Overhead lässt sich ermitteln, wie viel Festplattenspeicher jedes mit Erasure-Coding-Objekt benötigt:

*disk space = object size + (object size * storage overhead)*

Wenn Sie beispielsweise ein Objekt mit 10 MB unter Verwendung des Schemas von 4+2 speichern (mit einem Mehraufwand von 50 %), verbraucht das Objekt 15 MB Grid Storage. Wenn Sie dasselbe 10 MB große Objekt mit dem Schema 6+2 speichern (mit einem Mehraufwand von 33 %), verbraucht das Objekt etwa 13.3 MB.

Wählen Sie das Erasure-Coding-Schema mit dem niedrigsten Gesamtwert von aus k+m Das entspricht Ihren Bedürfnissen. Erasure-Coding-Schemata mit einer geringeren Anzahl von Fragmenten sind insgesamt recheneffizienter, da weniger Fragmente erstellt und verteilt (oder abgerufen) werden, aufgrund der größeren Fragmentgröße eine bessere Performance aufweisen und bei einer Erweiterung weniger Nodes hinzugefügt werden müssen, wenn mehr Storage benötigt wird. (Informationen zur Planung einer Speichererweiterung finden Sie im "Anweisungen zur Erweiterung von StorageGRID".)

Verfahren zur Einhaltung von Datenkonsistenz für Storage-Pools mit drei oder mehr Standorten

Die folgende Tabelle beschreibt die von StorageGRID derzeit unterstützten Erasure Coding-Schemata für Storage-Pools, die drei oder mehr Standorte umfassen. Alle diese Maßnahmen bieten einen Standortausfallschutz. Ein Standort kann verloren gehen, und das Objekt ist weiterhin verfügbar.

Für Erasure Coding-Schemata, die Schutz vor Standortausfällen bieten, ist die empfohlene Anzahl von Storage-Nodes im Speicherpool größer *k+m* +1 Da jeder Standort mindestens drei Storage-Nodes erfordert.

Schema zur Einhaltung von Datenkonsistenz (Erasure Coding) (*k+m*)	Mindestanzahl der bereitgestellten Standorte	Empfohlene Anzahl von Storage-Nodes an jedem Standort	Insgesamt empfohlene Anzahl von Storage-Nodes	Schutz vor Standortausfällen?	Storage Overhead
4 + 2	3	3	9	Ja.	50 % erzielt
6 + 2	4	3	12	Ja.	33 % erzielt
8 + 2	5	3	15	Ja.	25 % erzielt

Schema zur Einhaltung von Datenkonsistenz (Erasure Coding) (*k+m*)	Mindestanzahl der bereitgestellten Standorte	Empfohlene Anzahl von Storage-Nodes an jedem Standort	Insgesamt empfohlene Anzahl von Storage-Nodes	Schutz vor Standortausfällen?	Storage Overhead
6 + 3	3	4	12	Ja.	50 % erzielt
9 + 3	4	4	16	Ja.	33 % erzielt
2+1	3	3	9	Ja.	50 % erzielt
4+1	5	3	15	Ja.	25 % erzielt
6+1	7	3	21	Ja.	17 % erzielt
7 + 5	3	5	15	Ja.	71 % erzielt

StorageGRID erfordert mindestens drei Storage-Nodes pro Standort. Für die Verwendung des Schemas 7+5 benötigt jeder Standort mindestens vier Speicherknoten. Es wird empfohlen, fünf Storage-Nodes pro Standort zu verwenden.

Bei der Auswahl eines Löschungsschemas, das Standortschutz bietet, sollte die relative Bedeutung der folgenden Faktoren in Einklang gestellt werden:

- **Anzahl der Fragmente**: Leistung und Expansionsflexibilität sind im Allgemeinen besser, wenn die Gesamtzahl der Fragmente geringer ist.
- **Fehlertoleranz**: Die Fehlertoleranz wird erhöht, indem mehr Paritätssegmente vorhanden sind (das heißt, wann `m` Hat einen höheren Wert.)
- **Netzwerkverkehr**: Bei der Wiederherstellung nach Ausfällen, mit einem Schema mit mehr Fragmenten (das heißt, eine höhere Summe für `k+m`) Erzeugt mehr Netzwerkverkehr.
- **Storage Overhead**: Bei Systemen mit höherem Overhead wird mehr Speicherplatz pro Objekt benötigt.

Wenn Sie beispielsweise zwischen einem Schema 4+2 und dem Schema 6+3 (mit jeweils 50 % Storage Overhead) entscheiden, wählen Sie das Schema 6+3 aus, wenn eine zusätzliche Fehlertoleranz erforderlich ist. Wählen Sie das Schema 4+2 aus, wenn die Netzwerkressourcen begrenzt sind. Wenn alle anderen Faktoren gleich sind, wählen Sie 4+2 aus, da die Gesamtzahl der Fragmente geringer ist.

Wenn Sie sich nicht sicher sind, welches Schema Sie verwenden möchten, wählen Sie 4+2 oder 6+3 aus, oder wenden Sie sich an den technischen Support.

Verfahren zur Einhaltung von Datenkonsistenz für Storage-Pools an einem Standort

Ein Storage-Pool an einem Standort unterstützt alle Erasure Coding-Schemata, die für drei oder mehr Standorte definiert sind, sofern der Standort über ausreichend Storage-Nodes verfügt.

Die Mindestanzahl der erforderlichen Storage-Nodes ist `k+m`, Aber ein Speicherpool mit `k+m +1` Storage-Nodes werden empfohlen. Zum Beispiel erfordert das Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) 2+1 einen Speicherpool mit mindestens drei Storage-Nodes, es werden jedoch vier Storage-Nodes

empfohlen.

Schema zur Einhaltung von Datenkonsistenz (Erasure Coding) (*k+m*)	Mindestanzahl Storage-Nodes	Empfohlene Anzahl von Storage-Nodes	Storage Overhead
4 + 2	6	7	50 % erzielt
6 + 2	8	9	33 % erzielt
8 + 2	10	11	25 % erzielt
6 + 3	9	10	50 % erzielt
9 + 3	12	13	33 % erzielt
2+1	3	4	50 % erzielt
4+1	5	6	25 % erzielt
6+1	7	8	17 % erzielt
7 + 5	12	13	71 % erzielt

Vor- und Nachteile sowie Anforderungen für Erasure Coding

Bevor Sie sich entscheiden, ob Sie zum Schutz von Objektdaten mithilfe von Replizierungs- oder Erasure Coding vor Verlust schützen möchten, sollten Sie die Vorteile und Nachteile sowie die Anforderungen für Verfahren zur Einhaltung von Datenkonsistenz kennen.

Vorteile von Erasure Coding

Im Vergleich zur Replizierung bietet das Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) verbesserte Zuverlässigkeit, Verfügbarkeit und Storage-Effizienz.

- **Zuverlässigkeit**: Die Zuverlässigkeit wird in Bezug auf Fehlertoleranz gemessen - das ist die Anzahl der gleichzeitigen Ausfälle, die ohne Datenverlust aufrechterhalten werden können. Mithilfe der Replizierung werden mehrere identische Kopien auf unterschiedlichen Nodes und über mehrere Standorte hinweg gespeichert. Bei der Einhaltung von Datenkonsistenz wird ein Objekt in Daten- und Paritätsfragmente codiert und über viele Nodes und Standorte verteilt. Diese Verteilung bietet Schutz vor Standort- und Node-Ausfällen. Im Vergleich zur Replizierung bietet Erasure Coding eine höhere Zuverlässigkeit bei vergleichbaren Storage-Kosten.
- **Verfügbarkeit**: Verfügbarkeit kann definiert werden als die Möglichkeit, Objekte abzurufen, wenn Speicherknoten ausfallen oder unzugänglich werden. Im Vergleich zur Replizierung bietet Erasure Coding eine höhere Verfügbarkeit bei vergleichbaren Storage-Kosten.
- **Storage-Effizienz**: Für ein ähnliches Maß an Verfügbarkeit und Zuverlässigkeit benötigen die durch das Erasure Coding geschützten Objekte weniger Speicherplatz als die gleichen Objekte, wenn sie durch Replikation geschützt sind. Ein Objekt mit 10 MB, das an zwei Standorten repliziert wird, benötigt

beispielsweise 20 MB Festplattenspeicher (zwei Kopien), während ein Objekt, das über drei Standorte mit einem Erasure Coding-Schema mit 6+3 codiert wird, nur 15 MB Festplattenspeicher in Anspruch nimmt.

> Der Festplattenspeicher für Objekte, die mit Erasure-Coding-Verfahren codiert wurden, wird als Objektgröße und als Storage Overhead berechnet. Der prozentuale Storage Overhead entspricht der Anzahl der Paritätsfragmente, geteilt durch die Anzahl an Datenfragmenten.

Nachteile des Erasure Coding

Im Vergleich zur Replizierung hat das Verfahren zur Einhaltung von Datenkonsistenz folgende Nachteile:

- Je nach Erasure Coding-Schema wird eine erhöhte Anzahl von Storage-Nodes und -Standorten empfohlen. Wenn Sie hingegen Objektdaten replizieren, benötigen Sie pro Kopie nur einen Storage Node. Siehe "Erasure Coding für Storage-Pools mit drei oder mehr Standorten" Und "Erasure Coding für Storage-Pools an einem Standort".
- Höhere Kosten und Komplexität der Storage-Erweiterungen. Um eine Implementierung zu erweitern, bei der Replizierung verwendet wird, fügen Sie an jedem Ort, an dem Objektkopien erstellt werden, Storage-Kapazitäten hinzu. Um eine Implementierung zu erweitern, bei der Erasure Coding zum Einsatz kommt, müssen Sie sowohl das verwendete Verfahren zur Einhaltung von Datenkonsistenz als auch die Kapazität vorhandener Storage-Nodes in Betracht ziehen. Wenn Sie beispielsweise warten, bis die vorhandenen Nodes zu 100 % voll sind, müssen Sie mindestens hinzufügen `k+m` Storage-Nodes: Wenn Sie jedoch erweitern, wenn vorhandene Nodes zu 70 % ausgelastet sind, können Sie zwei Nodes pro Standort hinzufügen und gleichzeitig die nutzbare Storage-Kapazität maximieren. Weitere Informationen finden Sie unter "Erweitern Sie Storage-Kapazität für Objekte, die nach dem Erasure-Coding-Verfahren codiert wurden".
- Wenn Erasure Coding über geografisch verteilte Standorte hinweg verwendet wird, erhöht sich die Latenzzeiten beim Abruf. Die Objektfragmente für ein Objekt, das mit Erasure-Coding und Verteilung auf Remote-Standorte codiert und über WAN-Verbindungen verteilt ist, dauern länger, bis es über ein Objekt abgerufen wird, das repliziert und lokal verfügbar ist (derselbe Standort, an dem der Client eine Verbindung herstellt).
- Bei Verwendung von Erasure Coding für geografisch verteilte Standorte kommt ein höherer WAN-Netzwerkverkehr für Abrufvorgänge und Reparaturen zum Einsatz, insbesondere bei häufig abgerufenen Objekten oder bei Objektreparaturen über WAN-Netzwerkverbindungen.
- Wenn Sie standortübergreifend Erasure Coding verwenden, nimmt der maximale Objektdurchsatz ab, da die Netzwerklatenz zwischen Standorten zunimmt. Diese Abnahme ist auf die entsprechende Abnahme des TCP-Netzwerkdurchsatzes zurückzuführen, was sich darauf auswirkt, wie schnell das StorageGRID-System Objektfragmente speichern und abrufen kann.
- Höhere Auslastung von Computing-Ressourcen:

Wann sollte das Erasure Coding verwendet werden

Das Verfahren zur Einhaltung von Datenkonsistenz eignet sich am besten für folgende Anforderungen:

- Objekte größer als 1 MB.

> Das Verfahren zur Einhaltung von Datenkonsistenz eignet sich am besten für Objekte mit einer Größe von mehr als 1 MB. Verwenden Sie kein Erasure Coding für Objekte, die kleiner als 200 KB sind, um zu vermeiden, dass man sehr kleine Fragmente, die zur Fehlerkorrektur codiert wurden, managen muss.

- Langfristige oder kalte Storage-Lösung für selten abgerufene Inhalte

- Hohe Datenverfügbarkeit und -Zuverlässigkeit
- Schutz vor vollständigem Standort- und Node-Ausfall.
- Storage-Effizienz:
- Implementierungen an einem einzigen Standort, die eine effiziente Datensicherung benötigen und nur eine einzige Kopie mit Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) als mehrere replizierte Kopien benötigen
- Implementierungen an mehreren Standorten, bei denen die Latenz zwischen den Standorten weniger als 100 ms beträgt

Wie die Aufbewahrung von Objekten bestimmt wird

StorageGRID bietet sowohl Grid-Administratoren als auch einzelnen Mandantenbenutzer Optionen, um die Speicherdauer von Objekten festzulegen. Im Allgemeinen haben alle von einem Mandantenbenutzer bereitgestellten Aufbewahrungsanweisungen Vorrang vor den Aufbewahrungsanweisungen, die vom Grid-Administrator bereitgestellt werden.

Wie Mandantenbenutzer die Aufbewahrung von Objekten steuern

Mandantenbenutzer haben drei primäre Möglichkeiten, um zu steuern, wie lange ihre Objekte in StorageGRID gespeichert sind:

- Wenn die globale S3-Objektsperreneinstellung für das Grid aktiviert ist, können Nutzer von S3-Mandanten Buckets erstellen, deren S3-Objektsperre aktiviert ist. Anschließend können sie über die S3-REST-API Aufbewahrungseinstellungen für jede zu diesem Bucket hinzugefügte Objektversion festlegen.
  - Eine Objektversion, die sich unter einem Legal Hold befindet, kann mit keiner Methode gelöscht werden.
  - Bevor das Aufbewahrungsdatum einer Objektversion erreicht ist, kann diese Version nicht mit einer Methode gelöscht werden.
  - Objekte in Buckets mit aktivierter S3-Objektsperre werden durch ILM „`Forever`“ beibehalten. Nachdem jedoch eine Aufbewahrungsfrist erreicht ist, kann eine Objektversion durch eine Client-Anfrage oder den Ablauf des Bucket-Lebenszyklus gelöscht werden. Siehe "Objekte managen mit S3 Object Lock".
- Benutzer von S3-Mandanten können ihren Buckets eine Lifecycle-Konfiguration hinzufügen, für die eine Ablaufaktion festgelegt ist. Wenn ein Bucket-Lebenszyklus vorhanden ist, speichert StorageGRID ein Objekt, bis das Datum oder die Anzahl der Tage, die im Verfallsvorgang angegeben sind, erreicht ist, es sei denn, der Client löscht das Objekt zuerst. Siehe "S3-Lebenszykluskonfiguration erstellen".
- Ein S3- oder Swift-Client kann eine delete-Objektanforderung ausgeben. StorageGRID priorisiert Löschanfragen von Clients immer über den S3-Bucket-Lebenszyklus oder ILM, wenn sie bestimmen, ob ein Objekt gelöscht oder aufbewahrt werden soll.

Grid-Administratoren steuern die Objektaufbewahrung

Grid-Administratoren steuern mithilfe von ILM-Speicheranweisungen, wie lange Objekte gespeichert werden. Wenn Objekte mit einer ILM-Regel abgeglichen werden, speichert StorageGRID diese Objekte bis zum letzten Zeitraum der ILM-Regel verstrichen ist. Objekte werden unbefristet aufbewahrt, wenn „`forever`“ für die Platzierungsanweisungen angegeben ist.

Unabhängig davon, wer die Aufbewahrung von Objekten steuert, steuern ILM-Einstellungen, welche Arten von Objektkopien (repliziert oder Erasure Coding) gespeichert werden und wo sich die Kopien befinden (Storage-

Nodes, Cloud Storage Pools oder Archiv-Nodes).

Interaktion von S3-Bucket-Lebenszyklus und ILM

Die Aktion „Ablaufdatum“ in einem S3-Bucket-Lebenszyklus überschreibt immer die ILM-Einstellungen. Aus diesem Grund kann ein Objekt auch dann im Grid verbleiben, wenn ILM-Anweisungen zum Auflegen des Objekts verfallen sind.

Beispiele für die Aufbewahrung von Objekten

Die folgenden Beispiele sollten zur besseren Übersicht über die Interaktionen zwischen S3 Objektsperre, Bucket-Lebenszykluseinstellungen, Clientlöschanforderungen und ILM verwendet werden.

Beispiel 1: S3-Bucket-Lebenszyklus hält Objekte länger als ILM

ILM

Speichern von zwei Kopien für 1 Jahr (365 Tage)

Bucket-Lebenszyklus

Verfalle Objekte in 2 Jahren (730 Tage)

Ergebnis

StorageGRID speichert das Objekt 730 Tage lang. StorageGRID verwendet die Bucket-Lifecycle-Einstellungen, um zu bestimmen, ob ein Objekt gelöscht oder aufbewahrt werden soll.

> Wenn im Bucket-Lebenszyklus angegeben wird, dass Objekte länger aufbewahrt werden sollen als durch ILM angegeben, verwendet StorageGRID beim Bestimmen der Anzahl und des Typs der zu speichernden Kopien weiterhin die Anweisungen zur ILM-Platzierung. In diesem Beispiel werden zwei Kopien des Objekts von 366 bis 730 Tagen im StorageGRID gespeichert.

Beispiel 2: S3-Bucket-Lebenszyklus läuft Objekte vor ILM ab

ILM

Speichern von zwei Kopien für 2 Jahre (730 Tage)

Bucket-Lebenszyklus

Verfalle Objekte in 1 Jahr (365 Tage)

Ergebnis

StorageGRID löscht beide Kopien des Objekts nach Tag 365.

Beispiel 3: Beim Löschen von Clients wird der Bucket-Lebenszyklus und ILM überschrieben

ILM

Speichern von zwei Kopien auf Storage-Nodes „`Forever`“

Bucket-Lebenszyklus

Verfalle Objekte in 2 Jahren (730 Tage)

Anforderung zum Löschen des Clients

Ausgestellt am 400. Tag

Ergebnis

StorageGRID löscht beide Kopien des Objekts am Tag 400 als Antwort auf die Anforderung zum Löschen des Clients.

Beispiel 4: S3 Object Lock überschreibt die Anforderung zum Löschen des Clients

S3-Objektsperre

Aufbewahrung bis zum Datum für eine Objektversion ist 2026-03-31. Eine gesetzliche Aufbewahrungspflichten sind nicht in Kraft.

Kompatible ILM-Regel

Speichern Sie zwei Kopien auf Storage-Nodes „`Forever.`“

Anforderung zum Löschen des Clients

Ausgestellt am 2024-03-31.

Ergebnis

StorageGRID wird die Objektversion nicht löschen, da die Aufbewahrung bis zum Datum noch zwei Jahre entfernt ist.

So werden Objekte gelöscht

StorageGRID kann Objekte entweder als direkte Antwort auf eine Client-Anfrage oder automatisch aufgrund des Ablaufs eines S3-Bucket-Lebenszyklus oder der Anforderungen der ILM-Richtlinie löschen. Wenn Sie verstehen, auf welche Weise Objekte gelöscht werden können und wie StorageGRID Löschanfragen verarbeitet, können Sie Objekte effizienter managen.

StorageGRID kann Objekte auf eine von zwei Methoden löschen:

- Synchrones Löschen: Erhält StorageGRID eine Client-Löschanforderung, werden alle Objektkopien sofort entfernt. Der Client wird informiert, dass das Löschen nach dem Entfernen der Kopien erfolgreich war.
- Objekte werden zum Löschen in die Warteschlange eingereiht: Wenn StorageGRID eine Löschanforderung empfängt, wird das Objekt zum Löschen in die Warteschlange verschoben. Der Client wird umgehend darüber informiert, dass das Löschen erfolgreich war. Objektkopien werden später durch ILM-Verarbeitung im Hintergrund entfernt.

Beim Löschen von Objekten verwendet StorageGRID die Methode, die das Löschen der Performance optimiert, mögliche Rückprotokolle für das Löschen minimiert und Speicherplatz am schnellsten freigegeben wird.

Die Tabelle fasst zusammen, wann StorageGRID die einzelnen Methoden verwendet.

Löschmethode	Wenn verwendet
Objekte werden zum Löschen in eine Warteschlange eingereiht	Wenn **eine** der folgenden Bedingungen zutrifft: • Das automatische Löschen von Objekten wurde von einem der folgenden Ereignisse ausgelöst: ◦ Das Ablaufdatum oder die Anzahl der Tage in der Lebenszykluskonfiguration für einen S3-Bucket erreicht ist. ◦ Der letzte in einer ILM-Regel angegebene Zeitraum ist abgelaufen. **Hinweis:** Objekte in einem Bucket, für den S3 Object Lock aktiviert ist, können nicht gelöscht werden, wenn sie sich unter einem Legal Hold befinden oder wenn ein Aufbewahrungsdatum angegeben, aber noch nicht erfüllt wurde. • Ein S3- oder Swift-Client fordert eine Löschung an. Eine oder mehrere der folgenden Bedingungen gilt: ◦ Kopien können nicht innerhalb von 30 Sekunden gelöscht werden, da z. B. ein Objektspeicherort vorübergehend nicht verfügbar ist. ◦ Löschwarteschlangen im Hintergrund sind inaktiv.
Objekte werden sofort entfernt (synchrones Löschen)	Wenn ein S3- oder Swift-Client eine Löschanfrage erstellt und **alle** der folgenden Bedingungen erfüllt sind: • Alle Kopien können innerhalb von 30 Sekunden entfernt werden. • Warteschlangen zum Löschen im Hintergrund enthalten Objekte, die verarbeitet werden sollen.

Wenn S3- oder Swift-Clients Löschanforderungen durchführen, beginnt StorageGRID, indem Objekte der Löschwarteschlange hinzugefügt werden. Anschließend wechselt er zur Durchführung des synchronen Löschvorgangs. Wenn sichergestellt wird, dass in der Warteschlange zum Löschen im Hintergrund Objekte verarbeitet werden, kann StorageGRID das Löschen von Löschungen effizienter verarbeiten, insbesondere bei Clients mit geringer Parallelität. Gleichzeitig wird verhindert, dass die Backlogs von Clients gelöscht werden.

Erforderliche Zeit zum Löschen von Objekten

Die Art und Weise, wie StorageGRID Objekte löscht, kann sich auf die Ausführung des Systems auswirken:

- Wenn StorageGRID das synchrone Löschen durchführt, kann StorageGRID bis zu 30 Sekunden dauern, bis ein Ergebnis an den Client zurückgegeben wird. Das heißt, das Löschen kann scheinbar langsamer erfolgen, auch wenn Kopien tatsächlich schneller entfernt werden als wenn StorageGRID Objekte zum Löschen Warteschlangen.
- Falls Sie die Löschleistung während eines Massenlöschs genau überwachen, kann es vorkommen, dass sich die Löschrate nach dem Löschen einer bestimmten Anzahl von Objekten verlangsamt. Diese Änderung tritt auf, wenn StorageGRID von Objekten aus der Warteschlange zum Löschen auf das synchrone Löschen verschiebt. Die offensichtliche Reduzierung der Löschrate bedeutet nicht, dass Objektkopien langsamer entfernt werden. Im Gegenteil: Er zeigt an, dass durchschnittlich Speicherplatz schneller freigegeben wird.

Wenn Sie eine große Anzahl von Objekten löschen und Ihre Priorität darin besteht, Speicherplatz schnell freizugeben, ziehen Sie in Betracht, Objekte mithilfe einer Client-Anfrage zu löschen, anstatt sie mit ILM oder anderen Methoden zu löschen. Im Allgemeinen wird Speicherplatz schneller freigegeben, wenn das Löschen durch Clients durchgeführt wird, da StorageGRID das synchrone Löschen verwenden kann.

Die Zeit, die erforderlich ist, um nach dem Löschen eines Objekts Speicherplatz freizugeben, hängt von mehreren Faktoren ab:

- Gibt an, ob Objektkopien synchron entfernt werden oder später zur Entfernung in die Warteschlange verschoben werden (für Client-Löschanfragen).
- Weitere Faktoren wie die Anzahl der Objekte im Grid oder die Verfügbarkeit von Grid-Ressourcen, wenn Objektkopien zur Entfernung in eine Warteschlange verschoben werden (für Clientlöschungen und andere Methoden).

Löschen von S3-versionierten Objekten

Wenn die Versionierung für einen S3-Bucket aktiviert ist, befolgt StorageGRID das Verhalten von Amazon S3, wenn es auf Löschanfragen reagiert, unabhängig davon, ob diese Anfragen von einem S3-Client, dem Ablauf eines S3-Bucket-Lebenszyklus oder den Anforderungen der ILM-Richtlinie stammen.

Wenn Objekte versioniert sind, löschen Objekt-Löschanforderungen nicht die aktuelle Version des Objekts und geben keinen Speicherplatz frei. Stattdessen erzeugt eine Anfrage zum Löschen eines Objekts eine Löschmarkierung als aktuelle Version des Objekts, wodurch die vorherige Version des Objekts „`noncurrent`“ wird.

Auch wenn das Objekt nicht entfernt wurde, verhält sich StorageGRID so, als ob die aktuelle Version des Objekts nicht mehr verfügbar ist. Anfragen an dieses Objekt geben 404 nicht gefunden zurück. Da jedoch nicht aktuelle Objektdaten nicht entfernt wurden, können Anforderungen, die eine nicht aktuelle Version des Objekts angeben, erfolgreich ausgeführt werden.

Um beim Löschen versionierter Objekte Speicherplatz freizugeben, verwenden Sie eine der folgenden Optionen:

- **S3 Client Request**: Geben Sie die Objektversion-ID in der S3 DELETE Object Anfrage an (`DELETE /object?versionId=ID`). Beachten Sie, dass diese Anforderung nur Objektkopien für die angegebene Version entfernt (die anderen Versionen belegen noch Speicherplatz).
- **Bucket-Lebenszyklus**: Verwenden Sie das `NoncurrentVersionExpiration` Aktionen in der Bucket-Lifecycle-Konfiguration Wenn die angegebene Anzahl von nicht-currentDays erreicht ist, entfernt StorageGRID dauerhaft alle Kopien nicht aktueller Objektversionen. Diese Objektversionen können nicht wiederhergestellt werden.

  Der `NewerNoncurrentVersions` Durch die Aktion in der Bucket-Lebenszykluskonfiguration wird die Anzahl der nicht-aktuellen Versionen angegeben, die in einem versionierten S3-Bucket aufbewahrt wurden. Wenn mehr nicht aktuelle Versionen als vorhanden sind `NewerNoncurrentVersions` Gibt an, dass StorageGRID die älteren Versionen entfernt, sobald der Wert „nicht-currentDays“ abgelaufen ist. Der `NewerNoncurrentVersions` Schwellenwert überschreibt Lebenszyklusregeln, die von ILM bereitgestellt werden. Das bedeutet, dass ein nicht aktuelles Objekt mit einer Version im vorliegt `NewerNoncurrentVersions` Der Schwellenwert wird beibehalten, wenn ILM die Löschung anfordert.

- **ILM**: "Klont die aktive Richtlinie" Und fügen Sie der neuen vorgeschlagenen Richtlinie zwei ILM-Regeln hinzu:
  - Erste Regel: Verwenden Sie “nicht aktuelle Zeit” als Referenzzeit, um mit den nicht aktuellen Versionen des Objekts zu übereinstimmen. In "Schritt 1 (Details eingeben) des Assistenten zum Erstellen einer

ILM-Regel", Wählen Sie **Ja** für die Frage “Diese Regel nur auf ältere Objektversionen anwenden (in S3 Buckets mit aktivierter Versionierung)?”

- Zweite Regel: Verwenden Sie **Ingest time**, um die aktuelle Version anzupassen. Die Regel „`Noncurrent time`“ muss in der Richtlinie über der Regel **Ingest Time** angezeigt werden.

Löschen von S3-Löschmarkierungen

Wenn ein versioniertes Objekt gelöscht wird, erstellt StorageGRID als aktuelle Version des Objekts eine Löschmarkierung. Um die Null-Byte-Löschmarkierung aus dem Bucket zu entfernen, muss der S3-Client die Objektversion explizit löschen. Löschmarkierungen werden nicht durch ILM, Bucket-Lebenszyklusregeln oder Objekte in Bucket-Operationen gelöscht.

Verwandte Informationen

- "S3-REST-API VERWENDEN"
- "Beispiel 4: ILM-Regeln und -Richtlinie für versionierte Objekte mit S3"

Speicherklassen erstellen und zuweisen

Speicherklassen identifizieren den Speichertyp, der von einem Speicherknoten verwendet wird. Sie können Storage-Klassen erstellen, wenn ILM-Regeln bestimmte Objekte auf bestimmten Storage-Nodes platzieren sollen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Wenn Sie StorageGRID zum ersten Mal installieren, wird die Speicherklasse **Default** automatisch jedem Speicherknoten in Ihrem System zugewiesen. Nach Bedarf können Sie optional benutzerdefinierte Storage-Klassen definieren und sie verschiedenen Storage-Nodes zuweisen.

Mit benutzerdefinierten Speicherqualitäten können Sie ILM-Speicherpools erstellen, die nur einen bestimmten Typ von Speicher-Node enthalten. Möglicherweise möchten Sie beispielsweise bestimmte Objekte auf Ihren schnellsten Storage-Nodes wie z. B. StorageGRID All-Flash Storage Appliances speichern.

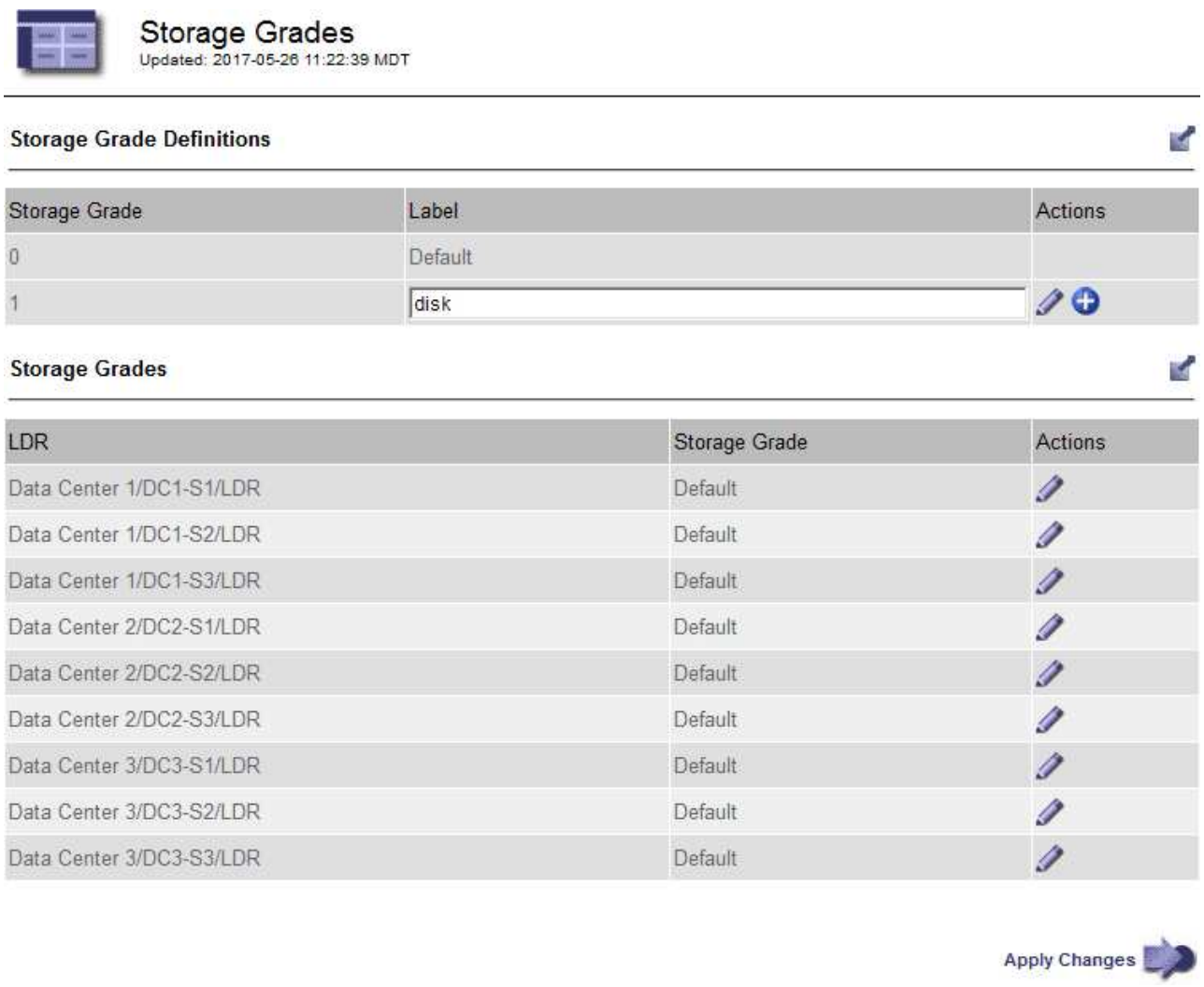
Wenn es nicht um die Speichergüte geht (zum Beispiel sind alle Speicher-Nodes identisch), können Sie dieses Verfahren überspringen und die Auswahl **includes all Storage Grade** für die Speicherklasse verwenden, wenn Sie "Erstellen von Speicherpools". Mit dieser Auswahl wird sichergestellt, dass der Speicherpool jeden Storage Node am Standort umfasst, unabhängig von seiner Speicherklasse.

> Erstellen Sie nicht mehr Storage-Klassen als erforderlich. Erstellen Sie beispielsweise keine Storage-Klasse für jeden Storage-Node. Weisen Sie jede Storage-Klasse zwei oder mehr Nodes zu. Storage-Klassen, die nur einem Node zugewiesen sind, können ILM-Backlogs verursachen, wenn der Node nicht mehr verfügbar ist.

Schritte

1. Wählen Sie **ILM** > **Speicherklassen**.
2. Benutzerdefinierte Storage-Klassen definieren:
   a. Wählen Sie für jede benutzerdefinierte Speicherklasse, die Sie hinzufügen möchten, **Einfügen** aus Um eine Zeile hinzuzufügen.

b. Geben Sie eine beschreibende Bezeichnung ein.



c. Wählen Sie **Änderungen Anwenden**.

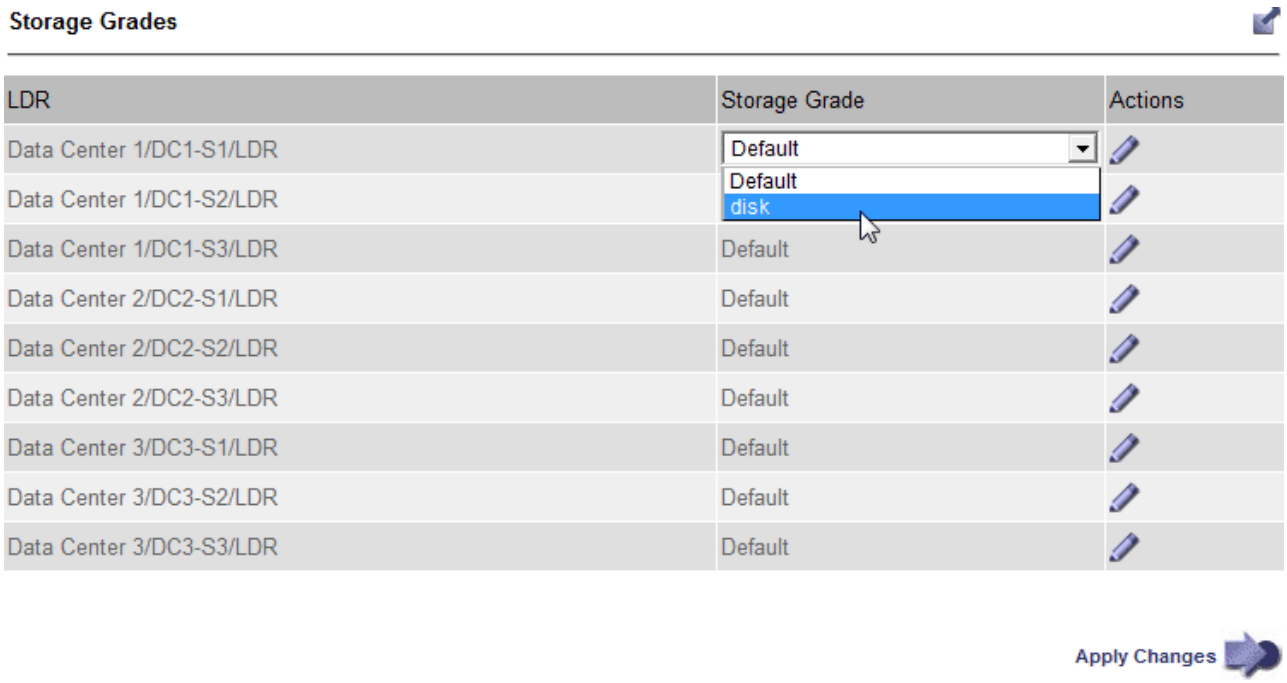
d. Wenn Sie ein gespeichertes Label ändern möchten, wählen Sie optional **Bearbeiten** Und wählen Sie **Änderungen übernehmen**.

Speicherqualitäten können nicht gelöscht werden.

3. Storage-Nodes neue Storage-Klassen zuweisen:

a. Suchen Sie den Storage Node in der LDR-Liste, und wählen Sie dessen Symbol * Bearbeiten* aus .

b. Wählen Sie den entsprechenden Speichergrad aus der Liste aus.



> Weisen Sie einem bestimmten Speicherknoten nur einmal eine Speicherklasse zu. Bei einem nach einem Ausfall wiederhergestellten Storage-Node wird die zuvor zugewiesene Storage-Klasse erhalten. Ändern Sie diese Zuweisung nicht, nachdem die ILM-Richtlinie aktiviert wurde. Wenn die Zuweisung geändert wird, werden die Daten auf Basis der neuen Speicherklasse gespeichert.

a. Wählen Sie **Änderungen Anwenden**.

Nutzung von Speicherpools

Was ist ein Speicherpool?

Ein Speicherpool ist eine logische Gruppierung von Storage-Nodes oder Archiv-Nodes.

Bei der Installation von StorageGRID wird automatisch ein Speicherpool pro Standort erstellt. Sie können zusätzliche Speicherpools je nach Bedarf konfigurieren.

> Die Unterstützung für Archive Nodes (für die Archivierung in der Cloud mit der S3-API und die Archivierung auf Band mit TSM-Middleware) ist veraltet und wird in einer zukünftigen Version entfernt. Das Verschieben von Objekten von einem Archive Node in ein externes Archiv-Storage-System wurde durch ILM Cloud Storage Pools ersetzt, die mehr Funktionen bieten.
>
> Siehe "Verwendung Von Cloud Storage Pools".

Storage-Pools haben zwei Attribute:

- **Speicherklasse**: Für Storage-Nodes, die relative Performance beim Sichern von Speicher.
- **Standort**: Das Rechenzentrum, in dem Objekte gespeichert werden.

Storage-Pools werden in ILM-Regeln verwendet, um zu bestimmen, wo Objektdaten gespeichert werden und welcher Storage-Typ verwendet wird. Wenn Sie ILM-Regeln für die Replikation konfigurieren, wählen Sie einen oder mehrere Storage-Pools aus, die entweder Storage-Nodes oder Archiv-Nodes enthalten. Wenn Sie Profile

für das Erasure Coding erstellen, wählen Sie einen Storage-Pool aus, der Storage-Nodes umfasst.

Richtlinien zur Erstellung von Speicherpools

Konfiguration und Verwendung von Speicherpools zur Absicherung gegen Datenverluste durch Verteilung von Daten über mehrere Standorte hinweg Für replizierte Kopien und Kopien, die zur Fehlerkorrektur codiert wurden, sind unterschiedliche Konfigurationen von Storage-Pools erforderlich.

Siehe "Beispiele für den Schutz vor Standortausfällen durch Replikation und Erasure Coding".

Richtlinien für alle Speicherpools

- Halten Sie Storage-Pool-Konfigurationen so einfach wie möglich. Erstellen Sie nicht mehr Speicherpools als nötig.
- Erstellung von Storage-Pools mit so vielen Nodes wie möglich Jeder Storage-Pool sollte zwei oder mehr Nodes enthalten. Ein Storage-Pool mit unzureichenden Nodes kann ILM-Backlogs verursachen, wenn ein Node nicht mehr verfügbar ist.
- Vermeiden Sie es, Storage-Pools zu erstellen oder zu verwenden, die sich überlappen (einen oder mehrere derselben Nodes enthalten). Bei Überschneidungen von Storage-Pools kann es sein, dass mehrere Kopien von Objektdaten auf demselben Node gespeichert werden.
- Verwenden Sie im Allgemeinen nicht den Speicherpool Alle Speicherknoten (StorageGRID 11.6 und früher) oder den Standort Alle Standorte. Diese Elemente werden automatisch aktualisiert, um alle neuen Sites, die Sie einer Erweiterung hinzufügen, aufzunehmen, was möglicherweise nicht das gewünschte Verhalten ist.

Richtlinien für Storage-Pools, die für replizierte Kopien verwendet werden

- Zum Schutz vor Standortausfällen mit "Replizierung", Geben Sie einen oder mehrere standortspezifische Speicherpools im an "Anweisungen zur Platzierung der einzelnen ILM-Regeln".

  Während der StorageGRID-Installation wird für jeden Standort automatisch ein Storage-Pool erstellt.

  Durch die Verwendung eines Storage Pools für jeden Standort wird sichergestellt, dass replizierte Objektkopien genau an den erwarteten Ort platziert werden (z. B. eine Kopie jedes Objekts an jedem Standort zum Site-Loss-Schutz).

- Wenn Sie einer Erweiterung einen Standort hinzufügen, erstellen Sie einen neuen Speicherpool, der nur den neuen Standort enthält. Dann, "Aktualisieren Sie die ILM-Regeln" Um zu steuern, welche Objekte auf der neuen Site gespeichert werden.
- Wenn die Anzahl der Kopien geringer ist als die Anzahl der Speicherpools, verteilt das System die Kopien, um die Festplattennutzung zwischen den Pools auszugleichen.
- Wenn sich die Speicherpools überschneiden (die gleichen Storage-Nodes enthalten), werden möglicherweise alle Kopien des Objekts an nur einem Standort gespeichert. Sie müssen sicherstellen, dass die ausgewählten Speicherpools nicht dieselben Speicher-Nodes enthalten.

Richtlinien für Storage-Pools, die für Kopien mit Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) verwendet werden

- Zum Schutz vor Standortausfällen mit "Erasure Coding"Erstellen Sie Speicherpools, die aus mindestens drei Standorten bestehen. Wenn ein Storage-Pool nur zwei Standorte umfasst, kann dieser Storage-Pool nicht für Erasure Coding verwendet werden. Für einen Speicherpool mit zwei Standorten stehen keine

Erasure Coding-Schemata zur Verfügung.

- Die Anzahl der im Speicherpool enthaltenen Storage-Nodes und -Standorte bestimmt, welche "Erasure Coding-Schemata" Verfügbar sind.
- Wenn möglich, sollte ein Speicherpool mehr als die Mindestanzahl an Speicherknoten enthalten, die für das ausgewählte Erasure-Coding-Schema erforderlich ist. Wenn Sie beispielsweise ein 6+3-Schema zur Codierung von Löschverfahren verwenden, müssen Sie mindestens neun Storage-Nodes haben. Es wird jedoch empfohlen, mindestens einen zusätzlichen Storage-Node pro Standort zu haben.
- Verteilen Sie Storage Nodes so gleichmäßig wie möglich auf Standorte. Um beispielsweise ein 6+3 Erasure Coding-Schema zu unterstützen, konfigurieren Sie einen Storage-Pool, der mindestens drei Storage-Nodes an drei Standorten enthält.
- Wenn Sie hohe Durchsatzanforderungen haben, wird die Verwendung eines Speicherpools mit mehreren Standorten nicht empfohlen, wenn die Netzwerklatenz zwischen Standorten mehr als 100 ms beträgt. Mit steigender Latenz sinkt auch die Rate, mit der StorageGRID Objektfragmente erstellen, platzieren und abrufen kann, aufgrund des geringeren TCP-Netzwerkdurchsatzes erheblich.

  Der Rückgang des Durchsatzes wirkt sich auf die maximal erreichbaren Raten bei der Aufnahme und dem Abruf von Objekten aus (wenn Balance oder Strict als Aufnahmeverhalten ausgewählt werden) oder kann zu ILM-Warteschlangen-Backlogs führen (wenn Dual Commit als Aufnahmeverhalten ausgewählt wird). Siehe "ILM-Regel Aufnahme-Verhalten".

> ⓘ Wenn Ihr Grid nur einen Standort umfasst, können Sie den Speicherpool Alle Storage-Nodes (StorageGRID 11.6 und früher) oder den Standardstandort aller Standorte in einem Erasure Coding-Profil nicht verwenden. Dieses Verhalten verhindert, dass das Profil ungültig wird, wenn ein zweiter Standort hinzugefügt wird.

- Archivierungs-Nodes können nicht für Daten verwendet werden, die nach der Datenlöschung codiert wurden.

Richtlinien für Speicherpools, die für archivierte Kopien verwendet werden

> ⚠ Die Unterstützung für Archive Nodes (für die Archivierung in der Cloud mit der S3-API und die Archivierung auf Band mit TSM-Middleware) ist veraltet und wird in einer zukünftigen Version entfernt. Das Verschieben von Objekten von einem Archive Node in ein externes Archiv-Storage-System wurde durch ILM Cloud Storage Pools ersetzt, die mehr Funktionen bieten.
>
> Siehe "Migrieren von Objekten in einen Cloud-Storage-Pool".
>
> Darüber hinaus sollten Sie Archivknoten aus der aktiven ILM-Richtlinie in StorageGRID 11.7 oder früher entfernen. Das Entfernen von Objektdaten, die auf Archive Nodes gespeichert sind, vereinfacht zukünftige Upgrades. Siehe "Arbeiten mit ILM-Regeln und ILM-Richtlinien".

- Sie können keinen Speicherpool erstellen, der sowohl Storage-Nodes als auch Archive Nodes umfasst. Für archivierte Kopien ist ein Storage-Pool erforderlich, der nur Archiv-Nodes enthält.
- Wenn Sie einen Speicherpool verwenden, der Archivierungs-Nodes enthält, sollten Sie außerdem mindestens eine replizierte oder mit Erasure Coding versehende Kopie in einem Speicherpool mit Storage-Nodes verwalten.
- Wenn die globale S3-Objektsperrung aktiviert ist und Sie eine konforme ILM-Regel erstellen, können Sie keinen Speicherpool verwenden, der Archive Nodes umfasst. Anweisungen zum Verwalten von Objekten mit S3 Object Lock finden Sie in den Anleitungen.
- Wenn der Zieltyp eines Archiv-Node Cloud Tiering - Simple Storage Service (S3) lautet, muss sich der Archiv-Node im eigenen Storage-Pool befinden.

Schutz vor Standortausfällen

Wenn die Implementierung von StorageGRID mehrere Standorte umfasst, können Sie für den Schutz vor Standortausfällen Replizierung und Erasure Coding mit entsprechend konfigurierten Storage-Pools verwenden.

Für Replizierung und Erasure Coding sind unterschiedliche Storage-Pool-Konfigurationen erforderlich:

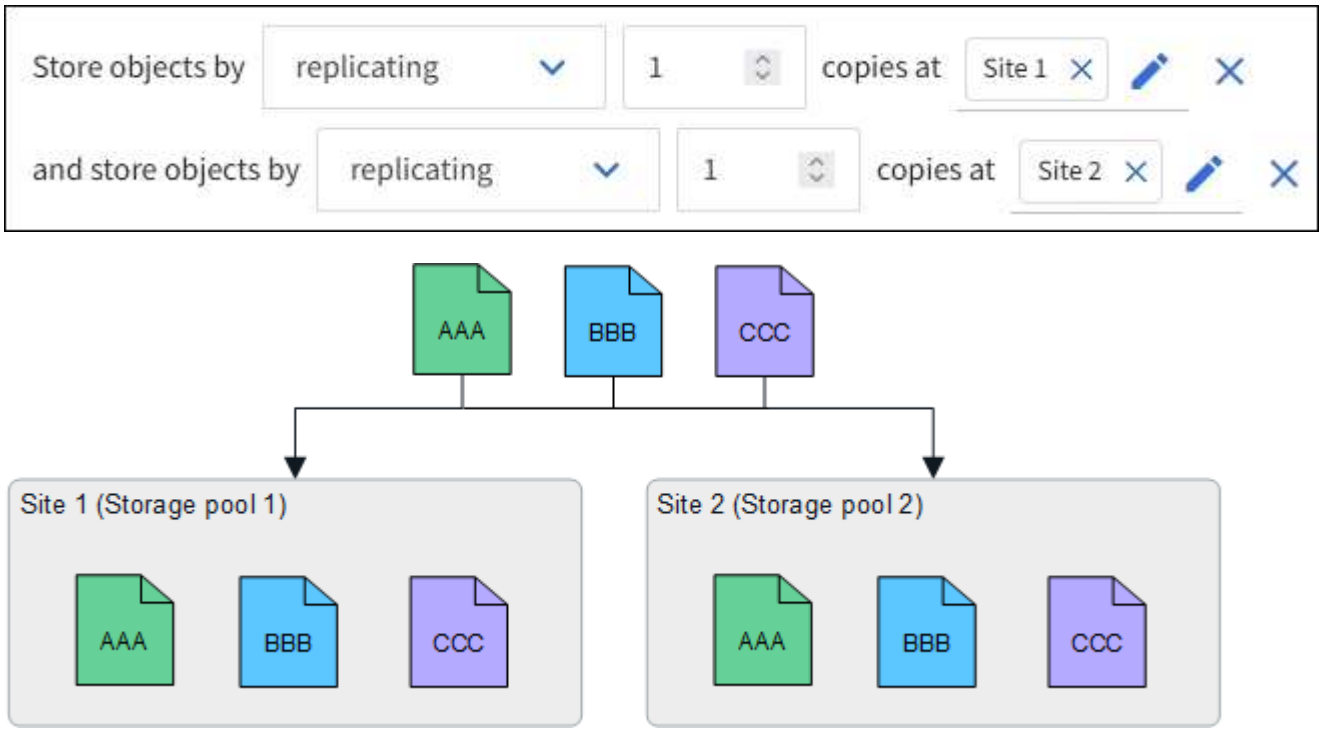
- Um die Replikation zum Schutz vor Standortausfällen zu verwenden, verwenden Sie die standortspezifischen Speicherpools, die bei der StorageGRID-Installation automatisch erstellt werden. Erstellen Sie dann ILM-Regeln mit "Anweisungen zur Platzierung" Die mehrere Speicherpools angeben, sodass eine Kopie jedes Objekts an jedem Standort platziert wird.
- Um Erasure Coding für Site-Loss-Schutz zu verwenden, "Erstellen Sie Speicherpools, die aus mehreren Standorten bestehen". Erstellen Sie dann ILM-Regeln, die einen Storage-Pool verwenden, der aus mehreren Standorten und einem beliebigen verfügbaren Erasure-Coding-Schema besteht.

Beispiel für die Replikation

Standardmäßig wird während der StorageGRID-Installation ein Speicherpool für jeden Standort erstellt. Wenn Speicherpools nur aus einem Standort bestehen, können Sie ILM-Regeln konfigurieren, die die Replikation für den Schutz vor Standortausfällen verwenden. In diesem Beispiel:

- Speicherpool 1 enthält Standort 1
- Speicherpool 2 enthält Standort 2
- Die ILM-Regel enthält zwei Platzierungen:
  - Speichern Sie Objekte, indem Sie 1 Kopie an Standort 1 replizieren
  - Speichern Sie Objekte, indem Sie 1 Kopie an Standort 2 replizieren

ILM-Regelplatzierungen:



Wenn ein Standort verloren geht, sind Kopien der Objekte am anderen Standort verfügbar.

Beispiel für Erasure Coding

Wenn Storage-Pools aus mehr als einem Standort pro Storage-Pool bestehen, können Sie ILM-Regeln konfigurieren, die Erasure Coding für Site-Loss-Schutz verwenden. In diesem Beispiel:

- Speicherpool 1 enthält die Standorte 1 bis 3
- Die ILM-Regel enthält eine Platzierung: Speichern Sie Objekte mithilfe eines Erasure Coding mithilfe eines 4+2 EC-Schemas in Storage Pool 1, das drei Standorte enthält

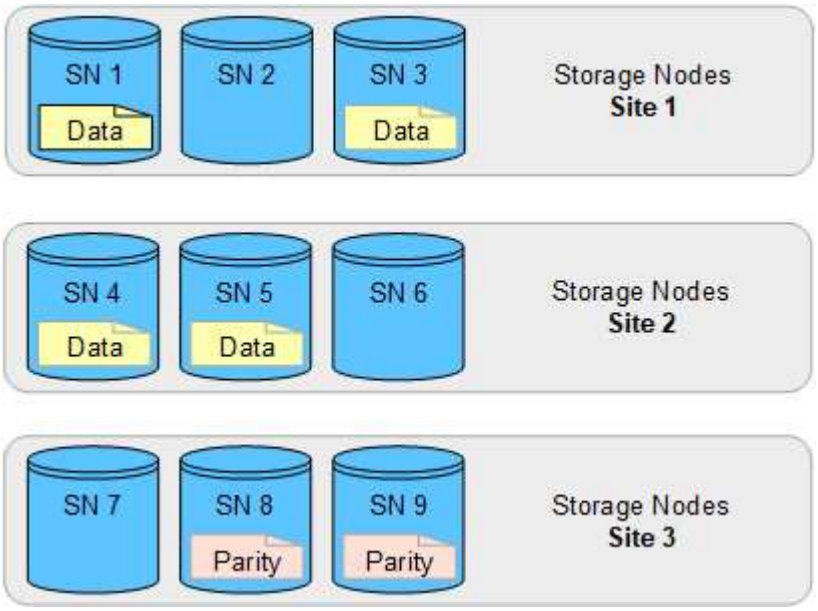
ILM-Regelplatzierungen:

In diesem Beispiel:

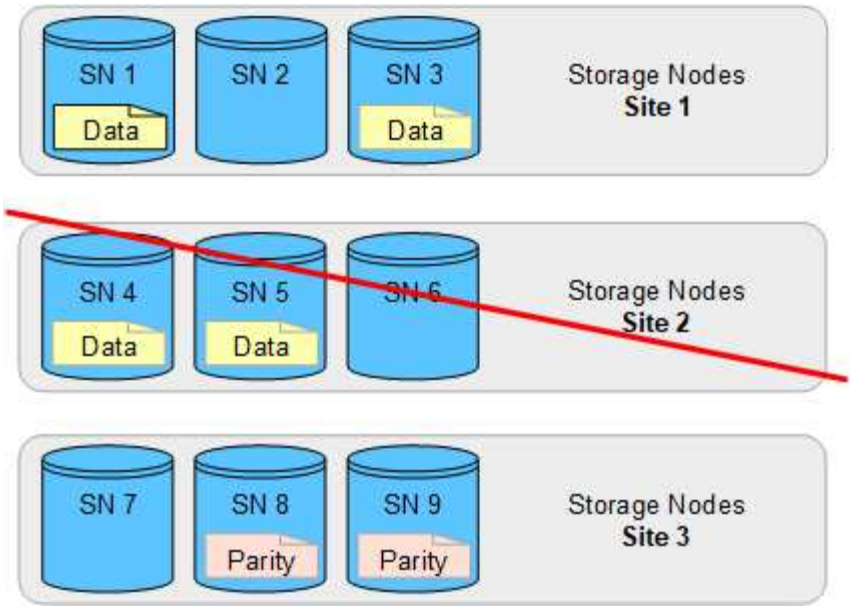
- Die ILM-Regel verwendet ein 4+2 Erasure Coding-Schema.
- Jedes Objekt wird in vier gleiche Datenfragmente geteilt und aus den Objektdaten werden zwei Paritätsfragmente berechnet.
- Jedes der sechs Fragmente wird auf einem anderen Node über drei Datacenter-Standorte gespeichert, um Daten bei Node-Ausfällen oder Standortausfällen zu sichern.

> Erasure Coding ist in Speicherpools erlaubt, die eine beliebige Anzahl von Standorten mit Ausnahme von zwei Standorten enthalten.

ILM-Regel gemäß 4+2 Erasure-Coding-Schema:



Wenn ein Standort verloren geht, können die Daten immer noch wiederhergestellt werden:



Erstellen Sie einen Speicherpool

Sie erstellen Storage-Pools, um zu bestimmen, wo das StorageGRID-System Objektdaten und den verwendeten Storage-Typ speichert. Jeder Speicherpool umfasst einen oder mehrere Standorte und eine oder mehrere Speicherklassen.

> Bei der Installation von StorageGRID 11.7 in einem neuen Grid werden automatisch Storage-Pools für jeden Standort erstellt, um die Anzahl der zum Erstellen neuer ILM-Regeln erforderlichen Schritte zu verringern. Bei der Aktualisierung auf StorageGRID 11.7 werden jedoch keine Speicherpools für jeden Standort erstellt.

Wenn Sie Cloud-Speicherpools erstellen möchten, um Objektdaten außerhalb Ihres StorageGRID-Systems zu speichern, finden Sie Informationen im "Informationen zur Verwendung von Cloud Storage Pools".

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben die Richtlinien zum Erstellen von Speicherpools überprüft.

Über diese Aufgabe

Storage Pools legen fest, wo Objektdaten gespeichert sind. Die Anzahl der erforderlichen Storage-Pools hängt von der Anzahl der Standorte in Ihrem Grid und den gewünschten Kopien ab: Repliziert oder Erasure Coding.

- Für Replizierung und Erasure Coding für einen Standort erstellen Sie für jeden Standort einen Storage-Pool. Wenn Sie beispielsweise replizierte Objektkopien an drei Standorten speichern möchten, erstellen Sie drei Storage Pools.
- Erstellen Sie für das Erasure Coding an drei oder mehr Standorten einen Storage-Pool mit einem Eintrag für jeden Standort. Wenn Sie beispielsweise Objekte aus drei Standorten löschen möchten, erstellen Sie einen Speicherpool.

Schließen Sie den Standort Alle Standorte nicht in einen Speicherpool ein, der in einem Erasure Coding-Profil verwendet wird. Fügen Sie stattdessen für jeden Standort, der Daten mit dem Erasure Coding speichert, einen separaten Eintrag in den Storage-Pool ein. Siehe Diesem Schritt Beispiel:

- Wenn Sie mehr als eine Storage-Klasse verwenden, sollten Sie an einem einzelnen Standort keinen Storage-Pool erstellen, der verschiedene Storage-Klassen umfasst. Siehe "Richtlinien zur Erstellung von Speicherpools".

Schritte

1. Wählen Sie **ILM** > **Storage Pools** aus.

   Auf der Registerkarte Speicherpools werden alle definierten Speicherpools aufgeführt.

   Bei Neuinstallationen von StorageGRID 11.6 oder früher wird der Speicherpool Alle Speicherknoten automatisch aktualisiert, sobald Sie neue Rechenzentrumsstandorte hinzufügen. Verwenden Sie diesen Pool nicht in ILM-Regeln.

2. Um einen neuen Speicherpool zu erstellen, wählen Sie **Erstellen**.
3. Geben Sie einen eindeutigen Namen für den Speicherpool ein. Verwenden Sie einen Namen, der sich leicht identifizieren lässt, wenn Sie Profile für das Erasure Coding und ILM-Regeln konfigurieren.
4. Wählen Sie aus der Dropdown-Liste **Standort** einen Standort für diesen Speicherpool aus.

   Wenn Sie einen Standort auswählen, wird die Anzahl der Speicherknoten und Archivknoten in der Tabelle automatisch aktualisiert.

   Im Allgemeinen sollten Sie den Standort „Alle Standorte“ nicht in einem Speicherpool verwenden. ILM-Regeln, die einen Storage-Pool an allen Standorten verwenden, platzieren Objekte an jedem beliebigen verfügbaren Standort, wodurch Sie weniger Kontrolle über die Objektplatzierung haben. Außerdem verwendet ein Speicherpool für alle Standorte sofort die Speicherknoten an einem neuen Standort, was möglicherweise nicht das erwartete Verhalten ist.

5. Wählen Sie aus der Dropdown-Liste **Speichergrad** den Speichertyp aus, der verwendet werden soll, wenn eine ILM-Regel diesen Speicherpool verwendet.

   Die Speicherklasse umfasst alle Storage-Klassen und umfasst alle Storage-Nodes am ausgewählten Standort. Die Standard-Speicherklasse Archiv-Knoten umfasst alle Archiv-Knoten am ausgewählten Standort. Wenn Sie zusätzliche Speicherklassen für die Speicherknoten in Ihrem Raster erstellt haben, werden diese im Dropdown-Menü aufgelistet.

6. Wenn Sie den Speicherpool in einem Profil für die Kennzeichnung von Löschvorgängen mit mehreren Standorten verwenden möchten, wählen Sie **Weitere Knoten hinzufügen**, um dem Speicherpool einen Eintrag für jeden Standort hinzuzufügen.

   Sie können keine doppelten Einträge erstellen oder einen Speicherpool erstellen, der sowohl die Speicherklasse Archive Nodes als auch jede Speicherklasse mit Speicherknoten umfasst.

   Sie werden gewarnt, wenn Sie mehr als einen Eintrag mit unterschiedlichen Speicherqualitäten für einen Standort hinzufügen.

   Um einen Eintrag zu entfernen, wählen Sie das Löschsymbol ✕.

7. Wenn Sie mit Ihrer Auswahl zufrieden sind, wählen Sie **Speichern**.

   Der neue Speicherpool wird der Liste hinzugefügt.

Zeigen Sie Details zum Speicherpool an

Sie können die Details eines Speicherpools anzeigen, um zu bestimmen, wo der Speicherpool verwendet wird, und um zu sehen, welche Nodes und Speicherklassen enthalten sind.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.

Schritte

1. Wählen Sie **ILM** > **Storage Pools** aus.

   Die Tabelle Speicherpools enthält die folgenden Informationen für jeden Speicherpool, der Speicher-Nodes umfasst:

   - **Name**: Der eindeutige Anzeigename des Speicherpools.
   - **Knotenanzahl**: Die Anzahl der Knoten im Speicherpool.
   - **Speichernutzung**: Der Prozentsatz des gesamten nutzbaren Speicherplatzes, der für Objektdaten auf diesem Knoten verwendet wurde. Dieser Wert enthält keine Objektmetadaten.
   - **Gesamtkapazität**: Die Größe des Speicherpools, die der Gesamtmenge des nutzbaren Speicherplatzes für Objektdaten für alle Knoten im Speicherpool entspricht.
   - **ILM-Nutzung**: Wie der Speicherpool derzeit genutzt wird. Ein Storage-Pool wird möglicherweise nicht verwendet oder kann in einem oder mehreren ILM-Regeln, Erasure-Coding-Profilen oder beiden verwendet werden.

     Ein Speicherpool kann nicht entfernt werden, wenn er verwendet wird.

2. Um Details zu einem bestimmten Speicherpool anzuzeigen, wählen Sie dessen Namen aus.

   Die Detailseite für den Speicherpool wird angezeigt.

3. Sehen Sie sich die Registerkarte **Nodes** an, um mehr über die im Speicherpool enthaltenen Speicher-Nodes oder Archiv-Nodes zu erfahren.

   Die Tabelle enthält die folgenden Informationen für jeden Node:

   - Node-Name
   - Standortname
   - Storage-Klasse
   - Speichernutzung (%): Der Prozentsatz des gesamten nutzbaren Speicherplatzes für Objektdaten, der für den Speicher-Node verwendet wurde. Dieses Feld ist für Archive Node Pools nicht sichtbar.

Der gleiche Wert für die Speichernutzung (%) wird auch im Diagramm Speicher verwendet - Objektdaten für jeden Speicherknoten angezeigt (wählen Sie **NODES** > ***Storage Node*** > **Storage**).

4. Wählen Sie die Registerkarte **ILM-Nutzung** aus, um zu ermitteln, ob der Speicherpool derzeit in ILM-Regeln oder Erasure Coding-Profilen verwendet wird.
5. Optional können Sie auf der Seite **ILM-Regeln** weitere Informationen zu den Regeln erhalten, die den Speicherpool verwenden.

   Siehe "Anweisungen zum Arbeiten mit ILM-Regeln".

Speicherpool bearbeiten

Sie können einen Speicherpool bearbeiten, um seinen Namen zu ändern oder Standorte und Speicherklassen zu aktualisieren.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben die geprüft "Richtlinien für die Erstellung von Speicherpools".
- Wenn Sie einen Speicherpool bearbeiten möchten, der von einer Regel in der aktiven ILM-Richtlinie verwendet wird, haben Sie überlegt, wie sich Ihre Änderungen auf die Platzierung von Objektdaten auswirken.

Über diese Aufgabe

Wenn Sie einen neuen Standort oder eine Speicherklasse zu einem Speicherpool hinzufügen, der in der aktiven ILM-Richtlinie verwendet wird, beachten Sie, dass die Speicherknoten am neuen Standort oder der Speicherklasse nicht automatisch verwendet werden. Um StorageGRID zu zwingen, einen neuen Standort oder eine neue Speicherklasse zu verwenden, müssen Sie eine neue ILM-Richtlinie aktivieren, nachdem Sie den bearbeiteten Speicherpool gespeichert haben.

Schritte

1. Wählen Sie **ILM** > **Storage Pools** aus.
2. Aktivieren Sie das Kontrollkästchen für den Speicherpool, den Sie bearbeiten möchten.

   Der Speicherpool „Alle Speicherknoten“ (StorageGRID 11.6 und früher) kann nicht bearbeitet werden.

3. Wählen Sie **Bearbeiten**.
4. Ändern Sie bei Bedarf den Namen des Speicherpools.
5. Wählen Sie bei Bedarf andere Standorte und Lagersorten aus.

Sie können den Standort oder die Storage-Klasse nicht ändern, wenn der Speicherpool in einem Erasure Coding-Profil verwendet wird und die Änderung dazu führen würde, dass das Erasure Coding-Schema ungültig wird. Wenn beispielsweise ein Storage-Pool in einem Profil für Erasure Coding derzeit eine Storage-Klasse mit nur einem Standort umfasst, können Sie eine Storage-Klasse mit zwei Standorten nicht verwenden, da die Änderung das Erasure Coding-Schema ungültig machen würde.

6. Wählen Sie **Speichern**.

Nachdem Sie fertig sind

Wenn Sie einem Speicherpool, der in der aktiven ILM-Richtlinie verwendet wird, einen neuen Standort oder eine neue Storage-Klasse hinzugefügt haben, aktivieren Sie eine neue ILM-Richtlinie, um StorageGRID zu zwingen, den neuen Standort oder die neue Storage-Klasse zu verwenden. Klonen Sie beispielsweise Ihre vorhandene ILM-Richtlinie und aktivieren Sie dann den Klon. Siehe "Arbeiten Sie mit ILM-Regeln und ILM-Richtlinien".

Entfernen Sie einen Speicherpool

Sie können einen Speicherpool entfernen, der nicht verwendet wird.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Erforderliche Zugriffsberechtigungen".

Schritte

1. Wählen Sie **ILM** > **Storage Pools** aus.
2. Überprüfen Sie in der Spalte ILM-Nutzung in der Tabelle, ob Sie den Speicherpool entfernen können.

   Sie können einen Storage-Pool nicht entfernen, wenn er in einer ILM-Regel oder in einem Erasure Coding-Profil verwendet wird. Wählen Sie bei Bedarf ***Storage Pool Name*** > **ILM usage**, um zu bestimmen, wo der Speicherpool verwendet wird.

3. Wenn der Speicherpool, den Sie entfernen möchten, nicht verwendet wird, aktivieren Sie das Kontrollkästchen.
4. Wählen Sie **Entfernen**.
5. Wählen Sie **OK**.

Verwendung Von Cloud Storage Pools

Was ist ein Cloud-Storage-Pool?

In einem Cloud Storage Pool können Sie ILM verwenden, um Objektdaten aus Ihrem StorageGRID System zu verschieben. Beispielsweise können Sie selten genutzte Objekte auf kostengünstigeren Cloud-Storage verschieben, wie z. B. Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud oder die Archiv-Zugriffs-Tier in Microsoft Azure Blob Storage. Alternativ möchten Sie auch ein Cloud-Backup von StorageGRID Objekten beibehalten, um die Disaster Recovery zu verbessern.

Aus einer ILM-Perspektive ähnelt ein Cloud-Storage-Pool einem Storage-Pool. Um Objekte an beiden Standorten zu speichern, wählen Sie den Pool aus, wenn Sie die Anweisungen zur Platzierung einer ILM-Regel erstellen. Während Storage-Pools jedoch aus Storage-Nodes oder Archiv-Nodes innerhalb des StorageGRID-Systems bestehen, besteht ein Cloud Storage Pool aus einem externen Bucket (S3) oder Container (Azure Blob-Storage).

Das Verschieben von Objekten von einem Archive Node über die S3-API in ein externes Archiv-Storage-System ist veraltet und wurde durch ILM Cloud Storage Pools ersetzt, die mehr Funktionen bieten. Wenn Sie derzeit einen Archive Node mit der Option Cloud Tiering – Simple Storage Service (S3) verwenden, "Migrieren Sie Ihre Objekte in einen Cloud-Storage-Pool" Stattdessen.

Die Tabelle vergleicht Speicherpools mit Cloud-Speicherpools und zeigt die grundlegenden Ähnlichkeiten und Unterschiede.

	Storage-Pool	**Cloud-Storage-Pool**
Wie wird sie erstellt?	Verwenden der Option **ILM** > **Storage Pools** im Grid Manager.	Verwenden der Option **ILM** > **Speicherpools** > **Cloud-Speicherpools** im Grid Manager. Sie müssen den externen Bucket oder Container einrichten, bevor Sie den Cloud Storage-Pool erstellen können.
Wie viele Pools können Sie erstellen?	Unbegrenzt.	Bis zu 10.
Wo werden Objekte gespeichert ?	Auf einem oder mehreren Speicherknoten oder Archivknoten innerhalb von StorageGRID.	In Amazon S3 Bucket, Azure Blob Storage-Container oder Google Cloud, die außerhalb des StorageGRID-Systems sind Wenn der Cloud Storage Pool ein Amazon S3-Bucket ist: • Optional kann ein Bucket-Lebenszyklus konfiguriert werden, um Objekte auf kostengünstigen Langzeit-Storage wie Amazon S3 Glacier oder S3 Glacier Deep Archive zu verschieben. Das externe Storage-System muss die Glacier Storage-Klasse und die S3 POST Object Restore API unterstützen. • Sie können Cloud-Storage-Pools zur Verwendung mit AWS Commercial Cloud Services (C2S) erstellen, die die AWS Secret Region unterstützen. Wenn der Cloud-Storage-Pool ein Azure Blob-Storage-Container ist, überträgt StorageGRID das Objekt auf die Archiv-Tier. **Hinweis:** im Allgemeinen sollten Sie Azure Blob Storage-Lifecycle-Management nicht für den Container konfigurieren, der für einen Cloud-Speicherpool verwendet wird. Die Wiederherstellung VON OBJEKTEN NACH DER Objekt-WIEDERHERSTELLUNG im Cloud-Storage-Pool kann vom konfigurierten Lebenszyklus betroffen sein.
Welche Kontrollen steuern die Objektplatzierung?	Eine ILM-Regel in der aktiven ILM-Richtlinie.	Eine ILM-Regel in der aktiven ILM-Richtlinie.

	Storage-Pool	Cloud-Storage-Pool
Welche Datenschutzmethode wird verwendet?	Replizierung oder Erasure Coding:	Replizierung:
Wie viele Kopien jedes Objekts sind erlaubt?	Mehrere:	Eine Kopie im Cloud-Storage-Pool und optional eine oder mehrere Kopien in StorageGRID. **Hinweis:** ein Objekt kann zu keinem Zeitpunkt in mehr als einem Cloud-Speicherpool gespeichert werden.
Worin liegen die Vorteile?	Objekte sind jederzeit schnell abrufbar.	Kostengünstiger Storage:
		Hinweis: FabricPool-Daten können nicht in Cloud-Speicherpools verschoben werden. Objekte mit aktivierter S3-Objektsperre können nicht in Cloud-Storage-Pools platziert werden.

Lebenszyklus eines Cloud-Storage-Pool-Objekts

Überprüfen Sie vor der Implementierung von Cloud-Storage-Pools den Lebenszyklus der Objekte, die in jedem Typ von Cloud-Storage-Pool gespeichert sind.

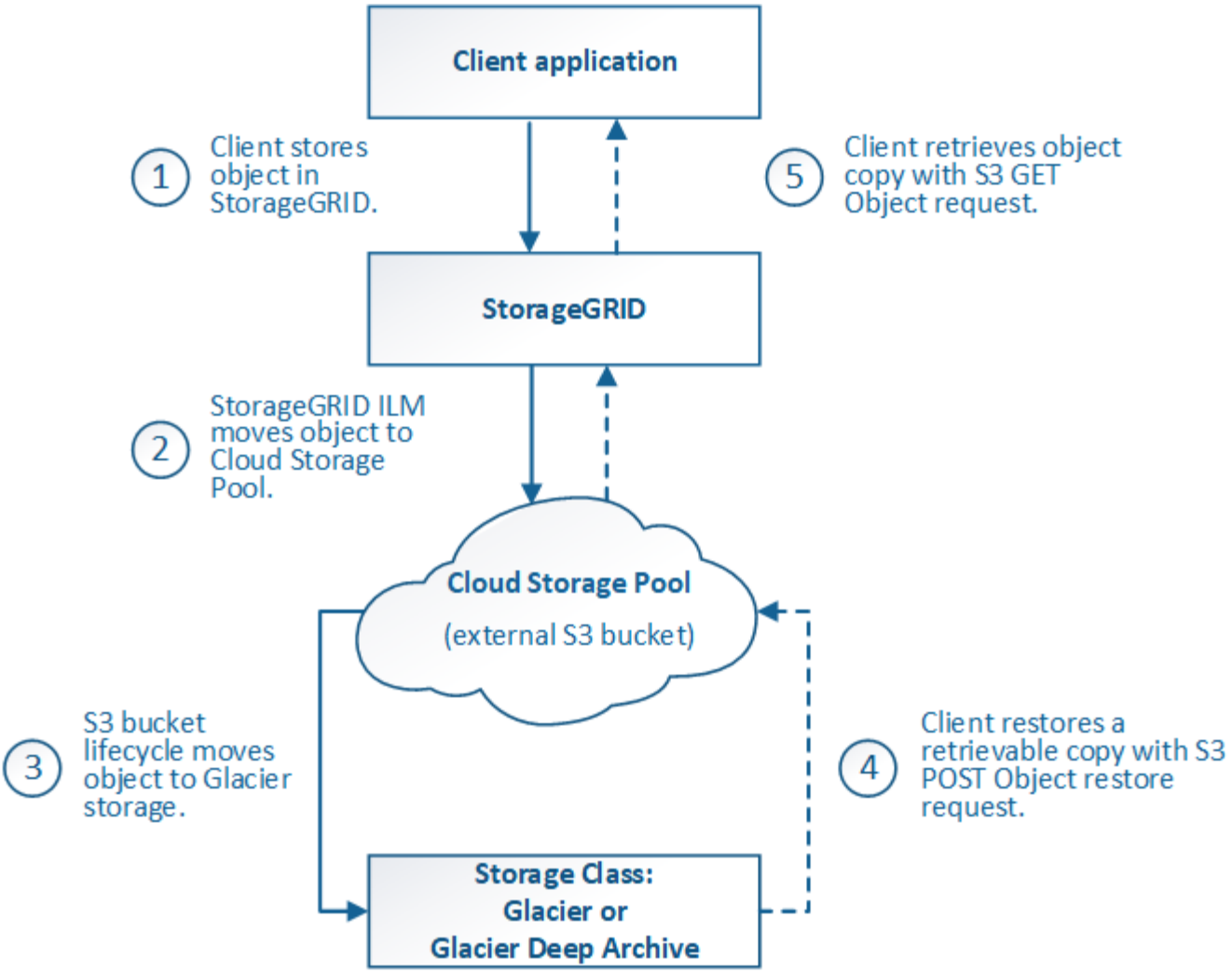
- S3: Lebenszyklus eines Cloud-Storage-Pool-Objekts
- Azure: Lebenszyklus eines Cloud-Storage-Pool-Objekts

S3: Lebenszyklus eines Cloud-Storage-Pool-Objekts

Die Abbildung zeigt die Lebenszyklusphasen eines Objekts, das in einem S3 Cloud-Storage-Pool gespeichert ist.

In der Abbildung und den Erläuterungen bezieht sich „`Glacier`“ sowohl auf die Glacier Storage-Klasse als auch auf die Glacier Deep Archive Storage-Klasse. Eine Ausnahme bilden die Glacier Deep Archive Storage-Klasse, die Expedited Restore Tier nicht unterstützt. Nur Bulk- oder Standard-Abruf wird unterstützt.

Die Google Cloud Platform (GCP) unterstützt den Abruf von Objekten aus langfristigem Storage ohne EINE WIEDERHERSTELLUNG NACH DER WIEDERHERSTELLUNG.



1. **Objekt gespeichert in StorageGRID**

   Zum Starten des Lebenszyklus speichert eine Client-Applikation ein Objekt in StorageGRID.

2. **Objekt in S3 Cloud Storage Pool verschoben**
   - Wenn das Objekt mit einer ILM-Regel übereinstimmt, die einen S3 Cloud-Storage-Pool als Speicherort verwendet, verschiebt StorageGRID das Objekt in den vom Cloud-Storage-Pool angegebenen externen S3-Bucket.
   - Sobald das Objekt in den S3-Cloud-Storage-Pool verschoben wurde, kann die Client-Applikation es mithilfe einer S3-GET-Objektanforderung von StorageGRID abrufen, es sei denn, das Objekt wurde auf Glacier Storage migriert.
3. **Objekt ist auf Glacier umgestiegen (nicht-Retrieable-Zustand)**
   - Optional kann das Objekt auf Glacier Storage verschoben werden. Der externe S3-Bucket verwendet beispielsweise möglicherweise Lifecycle-Konfigurationen, um ein Objekt sofort oder nach einigen Tagen in Glacier Storage zu verschieben.

> Wenn Sie Objekte verschieben möchten, müssen Sie eine Lebenszykluskonfiguration für den externen S3-Bucket erstellen. Außerdem ist eine Storage-Lösung erforderlich, die die Glacier Storage-Klasse implementiert und die S3-API FÜR DIE WIEDERHERSTELLUNG NACH Objekten unterstützt.

> Verwenden Sie Cloud-Storage-Pools nicht für Objekte, die von Swift-Clients aufgenommen wurden. Swift unterstützt keine Wiederherstellungsanforderungen NACH dem Objekt, daher kann StorageGRID keine Swift Objekte abrufen, die auf S3 Glacier Storage verschoben wurden. Die Ausgabe einer Swift GET Objektanforderung zum Abrufen dieser Objekte schlägt fehl (403 Verbotene).

  - Während des Übergangs kann die Client-Applikation mithilfe einer S3 HEAD Object-Anfrage den Status des Objekts überwachen.

4. **Objekt vom Glacier-Speicher wiederhergestellt**

   Wenn ein Objekt in den Glacier Storage verschoben wurde, kann die Client-Applikation eine S3-POST-Object-Wiederherstellungsanforderung ausgeben, um eine abrufbare Kopie in den S3 Cloud Storage Pool wiederherzustellen. Die Anfrage gibt an, wie viele Tage die Kopie im Cloud Storage Pool und auf die Datenzugriffsebene für den Wiederherstellungsvorgang (Expedited, Standard oder Bulk) verfügbar sein soll. Wenn das Ablaufdatum der abrufbaren Kopie erreicht ist, wird die Kopie automatisch in einen nicht aufrufbaren Zustand zurückgeführt.

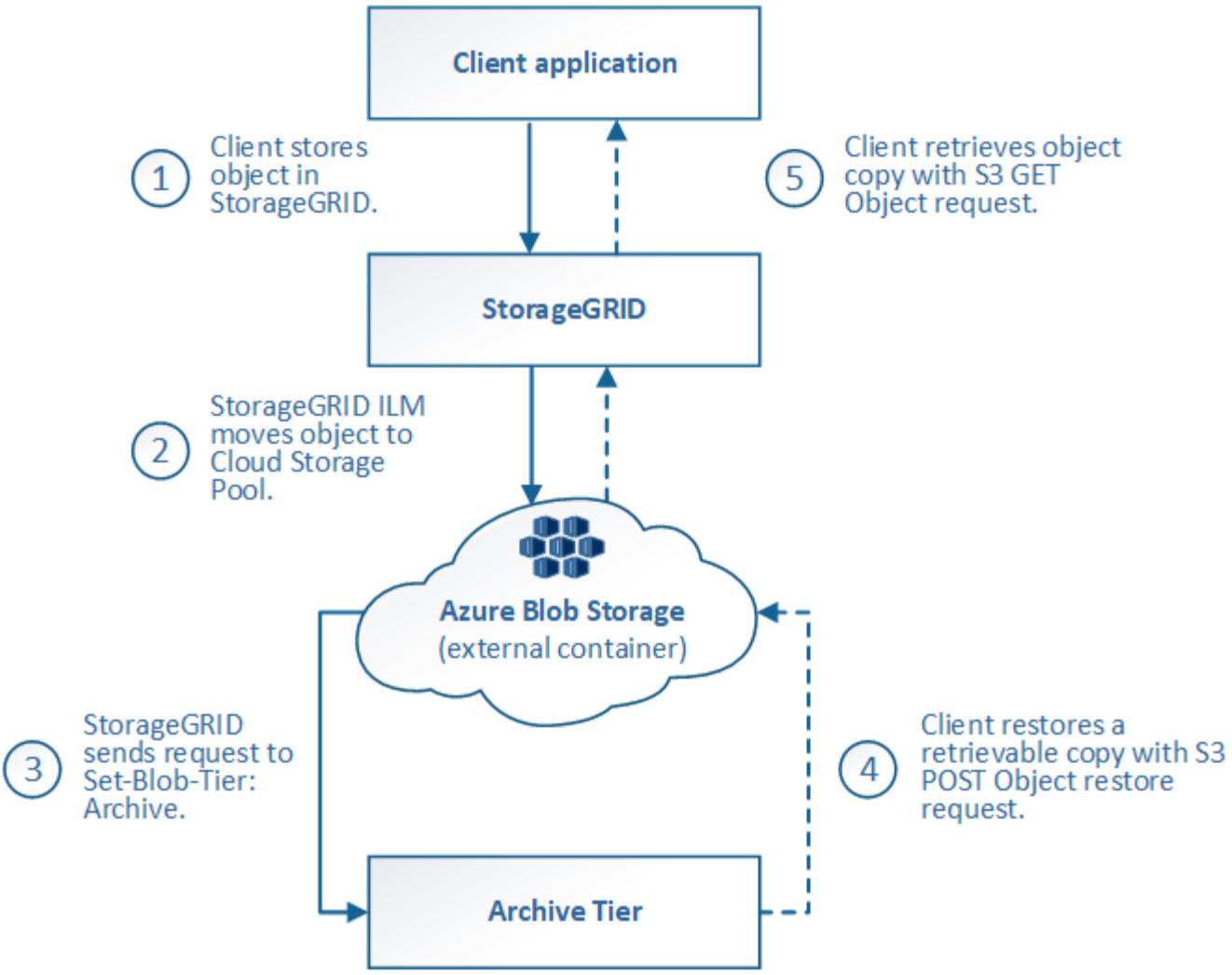
   > Wenn eine oder mehrere Kopien des Objekts auch auf Speicherknoten innerhalb von StorageGRID vorhanden sind, muss das Objekt nicht von Glacier wiederhergestellt werden, indem eine Anforderung zur Wiederherstellung NACH dem Objekt gestellt wird. Stattdessen kann die lokale Kopie direkt mit Hilfe einer GET Object-Anforderung abgerufen werden.

5. **Objekt abgerufen**

   Sobald ein Objekt wiederhergestellt ist, kann die Client-Applikation eine GET Object-Anforderung ausgeben, um das wiederhergestellte Objekt abzurufen.

Azure: Lebenszyklus eines Cloud-Storage-Pool-Objekts

Die Abbildung zeigt die Lebenszyklusphasen eines Objekts, das in einem Azure Cloud-Storage-Pool gespeichert ist.



1. **Objekt gespeichert in StorageGRID**

   Zum Starten des Lebenszyklus speichert eine Client-Applikation ein Objekt in StorageGRID.

2. **Objekt in Azure Cloud Storage Pool verschoben**

   Wird das Objekt mit einer ILM-Regel abgeglichen, die einen Azure Cloud Storage Pool als Speicherort verwendet, verschiebt StorageGRID das Objekt in den externen Azure Blob-Storage-Container, der vom Cloud-Storage-Pool festgelegt wurde

   > Verwenden Sie Cloud-Storage-Pools nicht für Objekte, die von Swift-Clients aufgenommen wurden. Swift unterstützt keine Anfragen zur WIEDERHERSTELLUNG NACH einem Objekt, daher kann StorageGRID keine Swift Objekte abrufen, die auf die Azure Blob Storage-Archivebene übertragen wurden. Die Ausgabe einer Swift GET Objektanforderung zum Abrufen dieser Objekte schlägt fehl (403 Verbotene).

3. **Objekt in Archivebene (nicht-Retrieable-Status)** umgestiegen

   Unmittelbar nach dem Verschieben des Objekts in den Azure Cloud Storage Pool überträgt StorageGRID das Objekt automatisch auf die Azure Blob Storage-Archivebene.

4. **Objekt vom Archiv Tier** wiederhergestellt

Wenn ein Objekt in die Archivebene migriert wurde, kann die Client-Applikation eine S3-RÜCKSTELLUNGSANFRAGE aus DEM NACHBEARBEITUNGSOBJEKT senden, um eine abrufbare Kopie in den Azure Cloud Storage Pool wiederherzustellen.

Wenn StorageGRID die POST-Objekt-Wiederherstellung empfängt, wird das Objekt vorübergehend in den Azure Blob-Storage Cool-Tier verlagert. Sobald das Ablaufdatum in der Wiederherstellungsanforderung FÜR NACHOBJEKTE erreicht ist, überträgt StorageGRID das Objekt zurück in die Archivebene.

> ⓘ Wenn eine oder mehrere Kopien des Objekts auch auf Storage-Nodes innerhalb von StorageGRID vorhanden sind, muss das Objekt durch Ausgabe einer Anforderung zur WIEDERHERSTELLUNG NACH DEM Objekt nicht aus der Zugriffsebene für Archive wiederhergestellt werden. Stattdessen kann die lokale Kopie direkt mit Hilfe einer GET Object-Anforderung abgerufen werden.

5. **Objekt abgerufen**

   Sobald ein Objekt im Azure Cloud Storage Pool wiederhergestellt ist, kann die Client-Applikation EINE GET Object-Anfrage stellen, um das wiederhergestellte Objekt abzurufen.

Verwandte Informationen

"S3-REST-API VERWENDEN"

Wann sollten Sie Cloud Storage Pools nutzen

Mit Cloud Storage Pools können Sie Daten an einem externen Ort sichern oder per Tiering übertragen. Darüber hinaus können Daten in mehreren Clouds gesichert oder per Tiering verschoben werden.

Backup von StorageGRID Daten an einem externen Speicherort

Sie können einen Cloud-Speicherpool verwenden, um StorageGRID Objekte an einem externen Ort zu sichern.

Wenn der Zugriff auf die Kopien in StorageGRID nicht möglich ist, können die Objektdaten im Cloud-Storage-Pool für Client-Anforderungen verwendet werden. Möglicherweise müssen Sie jedoch eine Anforderung zur Wiederherstellung VON S3-OBJEKTEN NACH DEM Wiederherstellen ausgeben, um auf die Backup-Objektkopie im Cloud-Storage-Pool zuzugreifen.

Die Objektdaten in einem Cloud Storage Pool können auch verwendet werden, um bei einem Ausfall eines Storage-Volumes oder eines Storage-Nodes verlorene Daten von StorageGRID wiederherzustellen. Wenn sich die einzige verbleibende Kopie eines Objekts in einem Cloud-Storage-Pool befindet, stellt StorageGRID das Objekt vorübergehend wieder her und erstellt eine neue Kopie auf dem wiederhergestellten Storage-Node.

So implementieren Sie eine Backup-Lösung:

1. Erstellen Sie einen einzelnen Cloud-Storage-Pool.
2. Konfiguration einer ILM-Regel, die Objektkopien gleichzeitig auf Storage Nodes (als replizierte oder Erasure-codierte Kopien) und einer einzelnen Objektkopie im Cloud Storage Pool speichert
3. Fügen Sie die Regel zur ILM-Richtlinie hinzu. Anschließend simulieren und aktivieren Sie die Richtlinie.

Daten-Tiering von StorageGRID auf externen Standort

Sie können einen Cloud-Speicherpool verwenden, um Objekte außerhalb des StorageGRID Systems zu speichern. Angenommen, Sie haben eine große Anzahl von Objekten, die Sie aufbewahren müssen, aber Sie erwarten, dass Sie auf diese Objekte selten zugreifen, wenn überhaupt. Mit einem Cloud-Storage-Pool können Sie die Objekte auf kostengünstigeren Storage verschieben und Speicherplatz in StorageGRID freigeben.

So implementieren Sie eine Tiering-Lösung:

1. Erstellen Sie einen einzelnen Cloud-Storage-Pool.
2. Konfiguration einer ILM-Regel, die selten genutzte Objekte von Storage-Nodes in den Cloud Storage-Pool verschiebt
3. Fügen Sie die Regel zur ILM-Richtlinie hinzu. Anschließend simulieren und aktivieren Sie die Richtlinie.

Diverse Cloud-Endpunkte beibehalten

Sie können diverse Cloud-Storage-Pool-Endpunkte konfigurieren, wenn Objektdaten in mehr als einer Cloud verschoben oder gesichert werden sollen. Mit den Filtern Ihrer ILM-Regeln können Sie festlegen, welche Objekte in den einzelnen Cloud Storage-Pools gespeichert werden. Beispielsweise können Sie Objekte von einigen Mandanten oder Buckets in Amazon S3 Glacier und Objekte von anderen Mandanten oder Buckets im Azure Blob Storage speichern. Alternativ können Sie Daten zwischen Amazon S3 Glacier und Azure Blob Storage verschieben.

> Bei der Nutzung mehrerer Cloud-Storage-Pool-Endpunkte sollte berücksichtigt werden, dass ein Objekt nur in einem Cloud-Storage-Pool gleichzeitig gespeichert werden kann.

So implementieren Sie diverse Cloud-Endpunkte:

1. Erstellung von bis zu 10 Cloud-Storage-Pools
2. Konfiguration von ILM-Regeln, um die entsprechenden Objektdaten zur entsprechenden Zeit in jedem Cloud-Storage-Pool zu speichern Speichern Sie beispielsweise Objekte aus Bucket A in Cloud Storage Pool A und speichern Sie Objekte aus Bucket B in Cloud Storage Pool B. Oder speichern Sie Objekte für eine gewisse Zeit im Cloud Storage Pool A und verschieben Sie sie dann in Cloud Storage Pool B.
3. Fügen Sie Regeln zu Ihrer ILM-Richtlinie hinzu. Anschließend simulieren und aktivieren Sie die Richtlinie.

Überlegungen zu Cloud-Storage-Pools

Wenn Sie einen Cloud Storage Pool zum Verschieben von Objekten aus dem StorageGRID System verwenden möchten, müssen Sie die Überlegungen für die Konfiguration und Verwendung von Cloud Storage Pools prüfen.

Allgemeine Überlegungen

- Im Allgemeinen ist Cloud-Archiv-Storage, wie Amazon S3 Glacier oder Azure Blob Storage, ein kostengünstiger Ort für die Speicherung von Objektdaten. Die Kosten für den Abruf von Daten aus dem Cloud-Archiv-Storage sind jedoch relativ hoch. Um die niedrigsten Gesamtkosten zu erreichen, müssen Sie berücksichtigen, wann und wie oft Sie auf die Objekte im Cloud Storage Pool zugreifen. Die Verwendung eines Cloud-Storage-Pools wird nur für Inhalte empfohlen, auf die Sie voraussichtlich nur selten zugreifen.
- Verwenden Sie Cloud-Storage-Pools nicht für Objekte, die von Swift-Clients aufgenommen wurden. Swift unterstützt keine Anforderungen für DIE WIEDERHERSTELLUNG NACH dem Objekt, sodass StorageGRID keine Swift Objekte abrufen kann, die auf S3 Glacier Storage oder in die Azure Blob

Storage-Archivebene verschoben wurden. Die Ausgabe einer Swift GET Objektanforderung zum Abrufen dieser Objekte schlägt fehl (403 Verbotene).

- Die Verwendung von Cloud Storage Pools mit FabricPool wird nicht unterstützt, weil die zusätzliche Latenz zum Abrufen eines Objekts aus dem Cloud-Storage-Pool-Ziel hinzugefügt wird.
- Objekte mit aktivierter S3-Objektsperre können nicht in Cloud-Storage-Pools platziert werden.
- Wenn für den Ziel-S3-Bucket für einen Cloud-Storage-Pool die S3-Objektsperre aktiviert ist, schlägt der Versuch, die Bucket-Replizierung (PutBucketReplication) zu konfigurieren, mit einem Fehler bei AccessDenied fehl.

Überlegungen zu den Ports, die für Cloud-Storage-Pools verwendet werden

Um sicherzustellen, dass die ILM-Regeln Objekte in den und aus dem angegebenen Cloud Storage-Pool verschieben können, müssen Sie das Netzwerk oder die Netzwerke konfigurieren, die Storage-Nodes Ihres Systems enthalten. Sie müssen sicherstellen, dass die folgenden Ports mit dem Cloud-Speicherpool kommunizieren können.

Standardmäßig verwenden Cloud-Speicherpools die folgenden Ports:

- **80**: Für Endpunkt-URIs, die mit http beginnen
- **443**: Für Endpunkt-URIs, die mit https beginnen

Sie können einen anderen Port angeben, wenn Sie einen Cloud-Speicherpool erstellen oder bearbeiten.

Wenn Sie einen nicht-transparenten Proxy-Server verwenden, müssen Sie auch "Konfigurieren Sie einen Speicher-Proxy" Damit Nachrichten an externe Endpunkte gesendet werden können, z. B. an einem Endpunkt im Internet.

Überlegungen zu Kosten

Der Zugriff auf den Storage in der Cloud mit einem Cloud Storage Pool erfordert Netzwerkkonnektivität zur Cloud. Dabei müssen die Kosten der Netzwerkinfrastruktur berücksichtigt werden, die für den Zugriff auf die Cloud und die entsprechende Bereitstellung gemäß der Datenmenge verwendet werden, die Sie voraussichtlich zwischen StorageGRID und der Cloud mithilfe des Cloud-Storage-Pools verschieben möchten.

Wenn sich StorageGRID mit dem Endpunkt eines externen Cloud-Storage-Pools verbinden, werden diverse Anfragen zur Überwachung der Konnektivität bearbeitet, um sicherzustellen, dass die IT die erforderlichen Operationen ausführen kann. Während mit diesen Anforderungen einige zusätzliche Kosten verbunden sind, dürfen die Kosten für die Überwachung eines Cloud Storage Pools nur einen kleinen Bruchteil der Gesamtkosten für das Speichern von Objekten in S3 oder Azure ausmachen.

Es können jedoch weitere erhebliche Kosten entstehen, wenn Sie Objekte von einem externen Endpunkt eines Cloud-Storage-Pools zurück auf StorageGRID verschieben müssen. Objekte können in einem der folgenden Fälle zurück auf StorageGRID verschoben werden:

- Die einzige Kopie des Objekts befindet sich in einem Cloud-Storage-Pool, und Sie entscheiden, das Objekt stattdessen in StorageGRID zu speichern. In diesem Fall konfigurieren Sie Ihre ILM-Regeln und -Richtlinien neu. Wenn eine ILM-Bewertung erfolgt, gibt StorageGRID mehrere Anforderungen aus, um das Objekt aus dem Cloud Storage Pool abzurufen. StorageGRID erstellt dann lokal die angegebene Anzahl von replizierten oder mit Erasure Coding verschlüsselten Kopien. Nachdem das Objekt zurück in den StorageGRID verschoben wurde, wird die Kopie im Cloud-Speicherpool gelöscht.
- Objekte sind aufgrund eines Ausfalls des Storage-Nodes verloren. Wenn sich die einzige verbleibende Kopie eines Objekts in einem Cloud-Storage-Pool befindet, stellt StorageGRID das Objekt vorübergehend wieder her und erstellt eine neue Kopie auf dem wiederhergestellten Storage-Node.

Wenn Objekte von einem Cloud-Storage-Pool aus zurück zu StorageGRID verschoben werden, gibt StorageGRID diverse Anfragen an den Cloud-Storage-Pool-Endpunkt für jedes Objekt aus. Bevor Sie eine große Anzahl von Objekten verschieben, wenden Sie sich an den technischen Support, um den Zeitrahmen und die damit verbundenen Kosten zu schätzen.

S3: Für den Cloud Storage Pool Bucket sind Berechtigungen erforderlich

Die Bucket-Richtlinie für den externen S3-Bucket, der für Cloud Storage Pool verwendet wird, muss StorageGRID-Berechtigung erteilen, ein Objekt in den Bucket zu verschieben, den Status eines Objekts zu erhalten, bei Bedarf ein Objekt aus dem Glacier Storage wiederherzustellen usw. Idealerweise sollte StorageGRID über vollständigen Kontrollzugriff auf den Bucket verfügen (`s3:*`Ist dies jedoch nicht möglich, muss die Bucket-Richtlinie StorageGRID die folgenden S3-Berechtigungen erteilen:

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`
- `s3:RestoreObject`

S3: Überlegungen für den Lebenszyklus externer Buckets

Das Verschieben von Objekten zwischen StorageGRID und dem im Cloud Storage Pool angegebenen externen S3-Bucket wird durch ILM-Regeln und die aktive ILM-Richtlinie in StorageGRID gesteuert. Im Gegensatz dazu wird die Transition von Objekten vom im Cloud Storage Pool angegebenen externen S3-Bucket auf Amazon S3 Glacier oder S3 Glacier Deep Archive (oder auf eine Storage-Lösung, die die Glacier Storage-Klasse implementiert) über die Lifecycle-Konfiguration dieses Buckets gesteuert.

Wenn Sie Objekte aus dem Cloud Storage Pool verschieben möchten, müssen Sie eine entsprechende Lebenszykluskonfiguration auf dem externen S3-Bucket erstellen. Außerdem muss eine Storage-Lösung verwendet werden, die die Glacier Storage-Klasse implementiert und die S3-API FÜR DIE WIEDERHERSTELLUNG NACH Objekten unterstützt.

Wenn Sie beispielsweise möchten, dass alle Objekte, die von StorageGRID in den Cloud-Storage-Pool verschoben werden, sofort in Amazon S3 Glacier Storage migriert werden. Sie würden eine Lebenszykluskonfiguration auf dem externen S3-Bucket erstellen, die eine einzelne Aktion (**Transition**) wie folgt festlegt:

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
       <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Diese Regel würde alle Bucket-Objekte an dem Tag der Erstellung auf Amazon S3 Glacier übertragen (d. h. an dem Tag, an dem sie von StorageGRID in den Cloud-Storage-Pool verschoben wurden).

> Wenn Sie den Lebenszyklus des externen Buckets konfigurieren, verwenden Sie niemals **Expiration**-Aktionen, um zu definieren, wann Objekte ablaufen. Durch Ablaufaktionen wird das Löschen abgelaufener Objekte im externen Speichersystem verursacht. Wenn Sie später versuchen, von StorageGRID auf ein abgelaufenes Objekt zuzugreifen, wird das gelöschte Objekt nicht gefunden.

Wenn Sie Objekte im Cloud Storage Pool zum S3 Glacier Deep Archive verschieben möchten (statt zu Amazon S3 Glacier), geben Sie an `<StorageClass>DEEP_ARCHIVE</StorageClass>` Im Bucket-Lebenszyklus: Beachten Sie jedoch, dass Sie die nicht verwenden können `Expedited` Tier zur Wiederherstellung von Objekten aus S3 Glacier Deep Archive.

Azure: Überlegungen für Zugriffsebene

Wenn Sie ein Azure-Speicherkonto konfigurieren, können Sie die Standard-Zugriffsebene auf „Hot“ oder „Cool“ festlegen. Wenn Sie ein Speicherkonto für die Verwendung mit einem Cloud-Speicherpool erstellen, sollten Sie den Hot-Tier als Standardebene verwenden. Auch wenn StorageGRID beim Verschieben von Objekten in den Cloud-Speicherpool sofort den Tier auf Archivierung setzt, stellt mit einer Standardeinstellung von Hot sicher, dass für Objekte, die vor dem 30-Tage-Minimum aus dem Cool Tier entfernt wurden, keine Gebühr für vorzeitiges Löschen berechnet wird.

Azure: Lifecycle-Management nicht unterstützt

Verwenden Sie das Azure Blob Storage-Lifecycle-Management nicht für den Container, der mit einem Cloud-Storage-Pool verwendet wird. Lifecycle-Operationen beeinträchtigen möglicherweise Cloud-Storage-Pool-Vorgänge.

Verwandte Informationen

- "Erstellen Sie einen Cloud-Storage-Pool"

Vergleich der Replizierung von Cloud-Storage-Pools und CloudMirror

Wenn Sie mit Cloud-Speicherpools beginnen, wäre es möglicherweise hilfreich, die

Ähnlichkeiten und Unterschiede zwischen Cloud-Speicherpools und dem Replizierungsservice für StorageGRID CloudMirror zu verstehen.

	Cloud-Storage-Pool	**CloudMirror Replikationsservice**
Was ist der primäre Zweck?	Fungiert als Archivziel. Die Objektkopie im Cloud-Storage-Pool kann die einzige Kopie des Objekts sein oder es kann eine zusätzliche Kopie sein. Das heißt, statt zwei Kopien vor Ort zu behalten, kann eine Kopie im StorageGRID behalten und eine Kopie an den Cloud-Storage-Pool senden.	Ermöglicht einem Mandanten, automatisch Objekte aus einem Bucket in StorageGRID (Quelle) in einen externen S3-Bucket (Ziel) zu replizieren Erstellt eine unabhängige Kopie eines Objekts in einer unabhängigen S3-Infrastruktur
Wie ist es eingerichtet?	Definiert auf dieselbe Weise wie Speicherpools, mit dem Grid Manager oder der Grid-Management-API. Kann als Speicherort in einer ILM-Regel ausgewählt werden. Während ein Storage-Pool aus einer Gruppe von Storage-Nodes besteht, wird ein Cloud-Storage-Pool mit einem Remote-S3- oder Azure-Endpunkt (IP-Adresse, Zugangsdaten usw.) definiert.	Ein Mandantenbenutzer "Konfiguration der CloudMirror-Replizierung" CloudMirror-Endpunkt (IP-Adresse, Anmeldeinformationen usw.) werden mithilfe des Tenant Manager oder der S3-API definiert. Nachdem der CloudMirror Endpunkt eingerichtet wurde, können alle Buckets dieses Mandantenkontos so konfiguriert werden, dass sie auf den CloudMirror Endpunkt verweisen.
Wer ist für die Einrichtung zuständig?	In der Regel ist ein Grid-Administrator erforderlich	In der Regel ein Mandantenbenutzer
Was ist das Ziel?	• Alle kompatiblen S3-Infrastrukturen (einschließlich Amazon S3) • Azure Blob Archivebene • Google Cloud Platform (GCP)	• Alle kompatiblen S3-Infrastrukturen (einschließlich Amazon S3) • Google Cloud Platform (GCP)
Was bewirkt, dass Objekte zum Ziel verschoben werden?	Ein oder mehrere ILM-Regeln in der aktiven ILM-Richtlinie Die ILM-Regeln legen fest, welche Objekte die StorageGRID in den Cloud-Storage-Pool verschoben und wann sie verschoben werden.	Aufnahme eines neuen Objekts in einen Quell-Bucket, der mit einem CloudMirror-Endpunkt konfiguriert wurde Objekte, die sich im Quell-Bucket befanden, bevor der Bucket mit dem CloudMirror-Endpunkt konfiguriert wurde, werden nur repliziert, wenn sie geändert wurden.

	Cloud-Storage-Pool	CloudMirror Replikationsservice
Wie werden Objekte abgerufen?	Applikationen müssen Anfragen an StorageGRID stellen, um Objekte abzurufen, die in einen Cloud-Speicherpool verschoben wurden. Wenn die einzige Kopie eines Objekts in den Archiv-Storage verschoben wurde, managt StorageGRID den Prozess der Wiederherstellung des Objekts, um es abgerufen werden zu können.	Da die gespiegelte Kopie im Ziel-Bucket eine unabhängige Kopie ist, können Applikationen das Objekt abrufen. Dazu müssen sie Anfragen entweder an StorageGRID oder an das S3-Ziel stellen. Angenommen, Sie verwenden CloudMirror Replizierung, um Objekte auf eine Partnerorganisation zu spiegeln. Der Partner kann mithilfe eigener Applikationen Objekte direkt vom S3-Ziel lesen oder aktualisieren. Die Verwendung von StorageGRID ist nicht erforderlich.
Können Sie direkt vom Ziel lesen?	Nein Objekte, die in einen Cloud-Storage-Pool verschoben werden, werden von StorageGRID gemanagt. Leseanforderungen müssen an StorageGRID gerichtet sein (und StorageGRID ist für den Abruf aus Cloud Storage Pool verantwortlich).	Ja, da die gespiegelte Kopie eine unabhängige Kopie ist.
Was geschieht, wenn ein Objekt aus der Quelle gelöscht wird?	Das Objekt wird auch aus dem Cloud-Speicher-Pool gelöscht.	Die Löschaktion wird nicht repliziert. Ein gelöschtes Objekt ist nicht mehr im StorageGRID-Bucket vorhanden, ist jedoch weiterhin im Ziel-Bucket vorhanden. Ebenso können Objekte im Ziel-Bucket gelöscht werden, ohne dass die Quelle beeinträchtigt wird.
Wie greifen Sie nach einem Ausfall auf Objekte zu (StorageGRID System nicht betriebsbereit)?	Fehlerhafte StorageGRID-Knoten müssen wiederhergestellt werden. Während dieses Prozesses können Kopien replizierter Objekte mithilfe der Kopien im Cloud Storage Pool wiederhergestellt werden.	Die Objektkopien im CloudMirror Zielsystem sind unabhängig von StorageGRID, sodass sie direkt vor dem Recovery der StorageGRID-Nodes zugänglich sind.

Erstellen Sie einen Cloud-Storage-Pool

Ein Cloud-Storage-Pool gibt einen einzelnen externen Amazon S3-Bucket oder einen anderen S3-kompatiblen Provider oder Azure Blob-Storage-Container an.

Wenn Sie einen Cloud-Storage-Pool erstellen, geben Sie den Namen und den Speicherort des externen Buckets oder Containers an, den StorageGRID zum Speichern von Objekten verwendet, den Cloud-Provider-Typ (Amazon S3/GCP oder Azure Blob Storage) und die Informationen, die StorageGRID für den Zugriff auf den externen Bucket oder Container benötigt.

StorageGRID validiert den Cloud-Storage-Pool, sobald Sie ihn speichern. Sie müssen also sicherstellen, dass der im Cloud-Speicherpool angegebene Bucket oder Container vorhanden ist und erreichbar ist.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Erforderliche Zugriffsberechtigungen".
- Sie haben die geprüft "Überlegungen zu Cloud-Storage-Pools".
- Der externe Bucket oder Container, auf den der Cloud-Storage-Pool verweist, ist bereits vorhanden, und Sie kennen seinen Namen und seinen Speicherort.
- Für den Zugriff auf den Bucket oder Container stehen Ihnen die folgenden Informationen für den von Ihnen gewählten Authentifizierungstyp zur Verfügung:

S3 Zugriffsschlüssel

Für den externen S3-Bucket

- Die Zugriffsschlüssel-ID für das Konto, dem der externe Bucket gehört.
- Der zugehörige geheime Zugriffsschlüssel.

Alternativ können Sie Anonymous für den Authentifizierungstyp angeben.

C2S-Zugangsportal

Für Commercial Cloud Services (C2S) S3 Service

Sie haben Folgendes:

- Vollständige URL, die StorageGRID verwendet, um temporäre Anmeldeinformationen vom C2S-Zugriffsportal (CAP)-Server zu erhalten, einschließlich aller erforderlichen und optionalen API-Parameter, die Ihrem C2S-Konto zugewiesen sind.
- Zertifikat der Server-Zertifizierungsstelle, ausgestellt von einer entsprechenden Zertifizierungsstelle (Government Certificate Authority, CA). StorageGRID verwendet dieses Zertifikat, um die Identität des CAP-Servers zu überprüfen. Das Server-CA-Zertifikat muss die PEM-Kodierung verwenden.
- Kundenzertifikat, ausgestellt von einer entsprechenden Zertifizierungsstelle (Government Certificate Authority, CA). StorageGRID verwendet dieses Zertifikat zur Identität des CAP-Servers. Das Clientzertifikat muss PEM-Kodierung verwenden und Zugriff auf Ihr C2S-Konto haben.
- PEM-codierter privater Schlüssel für das Clientzertifikat.
- Passphrase zur Entschlüsselung des privaten Schlüssels für das Clientzertifikat, sofern es verschlüsselt ist.

> Wenn das Clientzertifikat verschlüsselt wird, verwenden Sie das herkömmliche Format für die Verschlüsselung. Das verschlüsselte PKCS #8-Format wird nicht unterstützt.

Azure Blob Storage

Für den externen Container

- Uniform Resource Identifier (URI), der für den Zugriff auf den Blob-Speicher-Container verwendet wird.
- Name des Speicherkontos und des Kontoschlüssels. Im Azure-Portal finden Sie diese Werte.

Schritte

1. Wählen Sie **ILM** > **Speicherpools** > **Cloud-Speicherpools**.
2. Wählen Sie **Create**, und geben Sie die folgenden Informationen ein:

Feld	Beschreibung
Name des Cloud-Storage-Pools	Ein Name, der kurz den Cloud Storage Pool und dessen Zweck beschreibt. Verwenden Sie einen Namen, der leicht zu erkennen ist, wann Sie ILM-Regeln konfigurieren.
Anbietertyp	Welcher Cloud-Provider nutzen Sie für diesen Cloud-Storage-Pool? • **Amazon S3/GCP**: Wählen Sie diese Option für einen Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) oder einen anderen S3-kompatiblen Anbieter. • * Azure Blob Storage*
Eimer oder Container	Der Name des externen S3-Buckets oder Azure-Containers. Sie können diesen Wert nicht ändern, nachdem der Cloud-Speicherpool gespeichert wurde.

3. Geben Sie je nach Auswahl des Anbietertyps die Informationen zum Service-Endpunkt ein.

Amazon S3/GCP

a. Wählen Sie für das Protokoll entweder HTTPS oder HTTP aus.

> Verwenden Sie keine HTTP-Verbindungen für sensible Daten.

b. Geben Sie den Hostnamen ein. Beispiel:

`s3-aws-region.amazonaws.com`

c. URL-Stil auswählen:

Option	Beschreibung
Automatische Erkennung	Versuchen Sie, basierend auf den bereitgestellten Informationen automatisch zu erkennen, welchen URL-Stil verwendet werden soll. Wenn Sie beispielsweise eine IP-Adresse angeben, verwendet StorageGRID eine URL im Pfadstil. Wählen Sie diese Option nur aus, wenn Sie nicht wissen, welcher Stil verwendet werden soll.
Virtual-Hosted-Style	Verwenden Sie eine URL im virtuellen Hosted-Stil, um auf den Bucket zuzugreifen. Virtuelle gehostete URLs enthalten den Bucket-Namen als Teil des Domain-Namens. Beispiel: `https://bucket-name.s3.company.com/key-name`
Pfadstil	Verwenden Sie eine URL im Pfadstil, um auf den Bucket zuzugreifen. URLs im Pfadstil enthalten am Ende den Bucket-Namen Beispiel: `https://s3.company.com/bucket-name/key-name` **Hinweis:** die URL-Option im Pfadstil wird nicht empfohlen und wird in einer zukünftigen Version von StorageGRID veraltet sein.

d. Geben Sie optional die Portnummer ein, oder verwenden Sie den Standardport: 443 für HTTPS oder 80 für HTTP.

Azure Blob Storage

a. Geben Sie unter Verwendung eines der folgenden Formate den URI für den Service-Endpunkt ein.

- `https://host:port`
- `http://host:port`

Beispiel: `https://myaccount.blob.core.windows.net:443`

Wenn Sie keinen Port angeben, wird standardmäßig Port 443 für HTTPS und Port 80 für HTTP verwendet.

4. Wählen Sie **Weiter**. Wählen Sie dann den Authentifizierungstyp aus und geben Sie die erforderlichen Informationen für den Endpunkt des Cloud-Storage-Pools ein:

Zugriffsschlüssel

Nur für Amazon S3/GCP Provider type

a. Geben Sie für **Zugriffsschlüssel-ID** die Zugriffsschlüssel-ID für das Konto ein, dem der externe Bucket gehört.

b. Geben Sie für **Secret Access key** den geheimen Zugriffsschlüssel ein.

KAPPE (C2S-Zugangsportal)

Für Commercial Cloud Services (C2S) S3 Service

a. Geben Sie für die URL der temporären Anmeldeinformationen * die vollständige URL ein, die StorageGRID zum Abrufen temporärer Anmeldeinformationen vom CAP-Server verwendet, einschließlich aller erforderlichen und optionalen API-Parameter, die Ihrem C2S-Konto zugewiesen sind.

b. Wählen Sie für **Server-CA-Zertifikat Durchsuchen** aus, und laden Sie das PEM-kodierte CA-Zertifikat hoch, das StorageGRID zur Überprüfung des CAP-Servers verwendet.

c. Wählen Sie für **Clientzertifikat Durchsuchen** aus, und laden Sie das PEM-kodierte Zertifikat hoch, das StorageGRID verwendet, um sich auf dem CAP-Server zu identifizieren.

d. Wählen Sie für **Client private key Browse** aus, und laden Sie den PEM-kodierten privaten Schlüssel für das Clientzertifikat hoch.

e. Wenn der private Clientschlüssel verschlüsselt ist, geben Sie die Passphrase zum Entschlüsseln des privaten Clientschlüssels ein. Andernfalls lassen Sie das Feld **Client Private Key Passphrase** leer.

Azure Blob Storage

a. Geben Sie für **Kontoname** den Namen des Blob-Speicherkontos ein, dem der externe Service-Container gehört.

b. Geben Sie für **Account key** den geheimen Schlüssel für das Blob-Speicherkonto ein.

Anonym

Es sind keine zusätzlichen Informationen erforderlich.

5. Wählen Sie **Weiter**. Wählen Sie dann die Art der Serverüberprüfung aus, die Sie verwenden möchten:

Option	Beschreibung
Verwenden Sie Stammzertifizierungsstellen-Zertifikate in Storage Node OS	Verwenden Sie zum Sichern der Verbindungen die auf dem Betriebssystem installierten Grid CA-Zertifikate.
Benutzerdefiniertes CA-Zertifikat verwenden	Verwenden Sie ein benutzerdefiniertes CA-Zertifikat. Wählen Sie **Browse**, und laden Sie das PEM-kodierte Zertifikat hoch.
Verifizieren Sie das Zertifikat nicht	Das für die TLS-Verbindung verwendete Zertifikat wird nicht verifiziert.

6. Wählen Sie **Speichern**.

Beim Speichern eines Cloud-Speicherpools führt StorageGRID Folgendes aus:

- Überprüft, ob der Bucket oder Container und der Service-Endpunkt vorhanden sind und ob sie mit den von Ihnen angegebenen Anmeldedaten erreicht werden können.
- Schreibt eine Markierungsdatei in den Bucket oder Container, um sie als Cloud-Storage-Pool zu identifizieren. Entfernen Sie niemals diese Datei, die benannt ist `x-ntap-sgws-cloud-pool-uuid`.

  Wenn die Validierung des Cloud-Storage-Pools fehlschlägt, erhalten Sie eine Fehlermeldung, die erklärt, warum die Validierung fehlgeschlagen ist. Beispielsweise kann ein Fehler gemeldet werden, wenn ein Zertifikatfehler vorliegt oder der Bucket oder Container, den Sie angegeben haben, nicht bereits vorhanden ist.

7. Wenn ein Fehler auftritt, lesen Sie die "Anweisungen zur Fehlerbehebung bei Cloud Storage Pools"Beheben Sie alle Probleme, und versuchen Sie dann erneut, den Cloud-Speicherpool zu speichern.

Bearbeiten eines Cloud-Speicherpools

Sie können einen Cloud-Storage-Pool bearbeiten, um dessen Namen, Service-Endpunkt oder andere Details zu ändern. Sie können jedoch nicht den S3-Bucket oder Azure-Container für einen Cloud-Storage-Pool ändern.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben die geprüft "Überlegungen zu Cloud-Storage-Pools".

Schritte

1. Wählen Sie **ILM** > **Speicherpools** > **Cloud-Speicherpools**.

   In der Tabelle Cloud-Storage-Pools werden die vorhandenen Cloud-Storage-Pools aufgeführt.

2. Aktivieren Sie das Kontrollkästchen für den Cloud-Storage-Pool, den Sie bearbeiten möchten.
3. Wählen Sie **Actions** > **Edit**.
4. Ändern Sie bei Bedarf den Anzeigenamen, den Dienstendpunkt, die Authentifizierungsdaten oder die Methode zur Zertifikatvalidierung.

   > Sie können den Provider-Typ oder den S3-Bucket oder Azure-Container für einen Cloud-Storage-Pool nicht ändern.

   Wenn Sie zuvor ein Server- oder Client-Zertifikat hochgeladen haben, können Sie **Zertifikatdetails** auswählen, um das derzeit verwendete Zertifikat zu überprüfen.

5. Wählen Sie **Speichern**.

   Wenn Sie einen Cloud-Storage-Pool speichern, überprüft StorageGRID, ob der Bucket oder Container und der Service-Endpunkt vorhanden sind. Ob sie mit den von Ihnen angegebenen Zugangsdaten erreicht werden können.

   Wenn die Validierung des Cloud-Speicherpools fehlschlägt, wird eine Fehlermeldung angezeigt. Ein Fehler kann z. B. gemeldet werden, wenn ein Zertifikatfehler vorliegt.

   Siehe Anweisungen für "Fehlerbehebung bei Cloud Storage Pools", Beheben Sie das Problem, und versuchen Sie dann erneut, den Cloud-Speicher-Pool zu speichern.

Entfernen Sie einen Cloud-Speicherpool

Sie können einen Cloud-Speicherpool entfernen, wenn er nicht in einer ILM-Regel verwendet wird und keine Objektdaten enthält.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Erforderliche Zugriffsberechtigungen".

Verwenden Sie bei Bedarf ILM, um Objektdaten zu verschieben

Wenn der Cloud Storage Pool, den Sie entfernen möchten, Objektdaten enthält, müssen Sie ILM verwenden, um die Daten an einen anderen Speicherort zu verschieben. Sie können die Daten beispielsweise in Storage Nodes in Ihrem Grid oder in einen anderen Cloud-Storage-Pool verschieben.

Schritte

1. Wählen Sie **ILM** > **Speicherpools** > **Cloud-Speicherpools**.
2. Prüfen Sie in der Spalte „ILM-Nutzung“ der Tabelle, ob Sie den Cloud Storage-Pool entfernen können.

   Sie können einen Cloud Storage-Pool nicht entfernen, wenn er in einer ILM-Regel oder in einem Profil für Erasure Coding verwendet wird.

3. Wenn der Cloud Storage Pool verwendet wird, wählen Sie ***Cloud Storage Pool Name*** > **ILM usage** aus.
4. "Klonen jeder ILM-Regel" Damit werden Objekte im Cloud-Storage-Pool platziert, den Sie entfernen möchten.
5. Legen Sie fest, wo die vorhandenen Objekte, die von den einzelnen von Ihnen geklonten Regeln verwaltet werden, verschoben werden sollen.

   Sie können einen oder mehrere Speicherpools oder einen anderen Cloud-Speicherpool verwenden.

6. Bearbeiten Sie jede der von Ihnen geklonten Regeln.

   Wählen Sie für Schritt 2 des Assistenten zum Erstellen von ILM-Regeln den neuen Speicherort aus dem Feld **copies at** aus.

7. "Erstellen einer neuen vorgeschlagenen ILM-Richtlinie" Und ersetzen Sie jede der alten Regeln durch eine geklonte Regel.
8. Aktivieren Sie die neue Richtlinie.
9. Warten Sie, bis ILM Objekte aus dem Cloud Storage-Pool entfernt und an dem neuen Speicherort platziert hat.

Cloud Storage-Pool Löschen

Wenn der Cloud Storage Pool leer ist und in keiner ILM-Regel verwendet wird, können Sie ihn löschen.

Bevor Sie beginnen

- Sie haben alle ILM-Regeln entfernt, die den Pool möglicherweise verwendet haben.
- Sie haben bestätigt, dass der S3-Bucket oder der Azure-Container keine Objekte enthält.

  Ein Fehler tritt auf, wenn Sie versuchen, einen Cloud-Speicherpool zu entfernen, wenn er Objekte enthält. Siehe "Fehlerbehebung Bei Cloud Storage Pools".

Beim Erstellen eines Cloud Storage-Pools schreibt StorageGRID eine Markierungsdatei in den Bucket oder Container, um sie als Cloud-Storage-Pool zu identifizieren. Entfernen Sie diese Datei, die den Namen hat, nicht `x-ntap-sgws-cloud-pool-uuid`.

Schritte

1. Wählen Sie **ILM** > **Speicherpools** > **Cloud-Speicherpools**.
2. Wenn in der Spalte „ILM-Nutzung“ angezeigt wird, dass Cloud Storage Pool nicht verwendet wird, aktivieren Sie das Kontrollkästchen.
3. Wählen Sie **Aktionen** > **Entfernen**.
4. Wählen Sie **OK**.

Fehlerbehebung Bei Cloud Storage Pools

Verwenden Sie diese Fehlerbehebungsschritte, um Fehler zu beheben, die beim Erstellen, Bearbeiten oder Löschen eines Cloud-Speicherpools auftreten können.

Ermitteln Sie, ob ein Fehler aufgetreten ist

StorageGRID führt einmal pro Minute eine einfache Zustandsprüfung für jeden Cloud Storage Pool durch, um sicherzustellen, dass auf den Cloud Storage Pool zugegriffen werden kann und dass er ordnungsgemäß funktioniert. Wenn durch die Integritätsprüfung ein Problem erkannt wird, wird auf der Seite Speicherpools in der Spalte Letzter Fehler der Tabelle Cloud-Speicherpools eine Meldung angezeigt.

In der Tabelle ist der aktuellste Fehler aufgeführt, der bei den einzelnen Cloud-Storage-Pools erkannt wurde. Der Fehler ist vor langer Zeit aufgetreten.

Zusätzlich wird eine Meldung mit * Cloud Storage Pool Verbindungsfehler* ausgelöst, wenn die Systemprüfung feststellt, dass innerhalb der letzten 5 Minuten ein oder mehrere neue Cloud Storage Pool-Fehler aufgetreten sind. Wenn Sie eine E-Mail-Benachrichtigung für diese Warnung erhalten, gehen Sie zur Seite Speicherpools (wählen Sie **ILM** > **Speicherpools**), überprüfen Sie die Fehlermeldungen in der Spalte Letzter Fehler und lesen Sie die unten stehenden Richtlinien zur Fehlerbehebung.

Überprüfen Sie, ob ein Fehler behoben wurde

Nach der Behebung von Problemen können Sie feststellen, ob der Fehler behoben ist. Wählen Sie auf der Seite Cloud Storage Pool den Endpunkt aus, und wählen Sie **Fehler löschen** aus. Eine Bestätigungsmeldung gibt an, dass StorageGRID den Fehler für den Cloud-Speicherpool gelöscht hat.

Wenn das zugrunde liegende Problem behoben wurde, wird die Fehlermeldung nicht mehr angezeigt. Wenn das zugrunde liegende Problem jedoch nicht behoben wurde (oder ein anderer Fehler auftritt), wird die Fehlermeldung innerhalb weniger Minuten in der Spalte Letzter Fehler angezeigt.

Fehler: Dieser Cloud-Speicherpool enthält unerwartete Inhalte

Dieser Fehler wird möglicherweise auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu erstellen, zu bearbeiten oder zu löschen. Dieser Fehler tritt auf, wenn der Bucket oder Container den enthält `x-ntap-sgws-cloud-pool-uuid` Markierungsdatei, aber diese Datei verfügt nicht über die erwartete UUID.

In der Regel wird dieser Fehler nur angezeigt, wenn Sie einen neuen Cloud Storage-Pool erstellen, und eine andere Instanz von StorageGRID verwendet bereits den gleichen Cloud Storage-Pool.

Versuchen Sie mit diesen Schritten das Problem zu beheben:

- Vergewissern Sie sich, dass niemand in Ihrem Unternehmen diesen Cloud-Speicherpool verwendet.
- Löschen Sie die `x-ntap-sgws-cloud-pool-uuid` Datei und versuchen Sie erneut, den Cloud-Speicherpool zu konfigurieren.

Fehler: Cloud-Speicherpool konnte nicht erstellt oder aktualisiert werden. Fehler vom Endpunkt

Dieser Fehler wird möglicherweise auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu erstellen oder zu bearbeiten. Dieser Fehler zeigt an, dass eine Art von Verbindungs- oder Konfigurationsproblem darin besteht, dass StorageGRID das Schreiben in den Cloud Storage Pool verhindert.

Überprüfen Sie die Fehlermeldung vom Endpunkt, um das Problem zu beheben.

- Wenn die Fehlermeldung enthält `Get *url*: EOF`Überprüfen Sie, ob der für den Cloud-Speicher-Pool verwendete Service-Endpunkt HTTP nicht für einen Container oder Bucket verwendet, der HTTPS erfordert.
- Wenn die Fehlermeldung enthält `Get *url*: net/http: request canceled while waiting for connection`, Überprüfen Sie, ob die Netzwerkkonfiguration Storage-Knoten Zugriff auf den Service-Endpunkt erlaubt, der für den Cloud Storage Pool verwendet wird.
- Versuchen Sie bei allen anderen Fehlermeldungen am Endpunkt eine oder mehrere der folgenden Optionen:
  - Erstellen Sie einen externen Container oder Bucket mit demselben Namen, den Sie für den Cloud-Storage-Pool eingegeben haben, und versuchen Sie, den neuen Cloud-Storage-Pool erneut zu speichern.
  - Korrigieren Sie den für den Cloud Storage Pool angegebenen Container- oder Bucket-Namen und versuchen Sie, den neuen Cloud Storage-Pool erneut zu speichern.

Fehler: Fehler beim Parsen des CA-Zertifikats

Dieser Fehler wird möglicherweise auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu erstellen oder zu bearbeiten. Der Fehler tritt auf, wenn StorageGRID das bei der Konfiguration des Cloud-Speicherpools eingegebene Zertifikat nicht analysieren konnte.

Überprüfen Sie zum Beheben des Problems das von Ihnen bereitgestellte CA-Zertifikat auf Probleme.

Fehler: Ein Cloud-Speicherpool mit dieser ID wurde nicht gefunden

Dieser Fehler wird möglicherweise auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu bearbeiten oder zu löschen. Dieser Fehler tritt auf, wenn der Endpunkt eine 404-Antwort zurückgibt. Dies kann eine der folgenden Optionen bedeuten:

- Die für den Cloud-Storage-Pool verwendeten Anmeldeinformationen haben keine Leseberechtigung für den Bucket.
- Der für den Cloud-Storage-Pool verwendete Bucket enthält nicht den `x-ntap-sgws-cloud-pool-uuid` Markierungsdatei.

Versuchen Sie mindestens einen der folgenden Schritte, um das Problem zu beheben:

- Stellen Sie sicher, dass der dem konfigurierten Zugriffsschlüssel zugeordnete Benutzer über die erforderlichen Berechtigungen verfügt.
- Bearbeiten Sie den Cloud Storage Pool mit Zugangsdaten, die über die entsprechenden Berechtigungen verfügen.

- Wenn die Berechtigungen korrekt sind, wenden Sie sich an den Support.

Fehler: Der Inhalt des Cloud-Speicherpools konnte nicht überprüft werden. Fehler vom Endpunkt

Dieser Fehler wird möglicherweise auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu löschen. Dieser Fehler zeigt an, dass eine Art von Verbindungs- oder Konfigurationsproblem darin besteht, dass StorageGRID den Inhalt des Cloud Storage Pool Buckets liest.

Überprüfen Sie die Fehlermeldung vom Endpunkt, um das Problem zu beheben.

Fehler: Objekte wurden bereits in diesen Bucket platziert

Dieser Fehler wird möglicherweise auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu löschen. Sie können einen Cloud-Storage-Pool nicht löschen, wenn er Daten enthält, die durch ILM dorthin verschoben wurden, Daten, die sich vor dem Konfigurieren des Cloud-Storage-Pools im Bucket befinden, oder Daten, die nach der Erstellung des Cloud-Storage-Pools von einer anderen Quelle in den Bucket verschoben wurden.

Versuchen Sie mindestens einen der folgenden Schritte, um das Problem zu beheben:

- Folgen Sie den Anweisungen, um Objekte in „`Lifecycle eines Cloud-Storage-Pool-Objekts zurück in StorageGRID zu verschieben.`“
- Wenn Sie sicher sind, dass die verbleibenden Objekte nicht durch ILM im Cloud-Storage-Pool platziert wurden, löschen Sie die Objekte manuell aus dem Bucket.

> Löschen Sie nie Objekte manuell aus einem Cloud-Storage-Pool, der eventuell durch ILM gespeichert wurde. Wenn Sie später versuchen, auf ein manuell gelöschtes Objekt aus StorageGRID zuzugreifen, wird das gelöschte Objekt nicht gefunden.

Fehler: Beim Versuch, den Cloud-Speicherpool zu erreichen, ist ein externer Fehler aufgetreten

Dieser Fehler kann auftreten, wenn Sie zwischen Storage-Nodes einen nicht transparenten Storage Proxy und den externen S3-Endpunkt konfiguriert haben, der für den Cloud Storage-Pool verwendet wird. Dieser Fehler tritt auf, wenn der externe Proxyserver den Endpunkt des Cloud-Speicherpools nicht erreichen kann. Beispielsweise kann der DNS-Server den Hostnamen möglicherweise nicht lösen, oder es könnte ein externes Netzwerkproblem geben.

Versuchen Sie mindestens einen der folgenden Schritte, um das Problem zu beheben:

- Überprüfen Sie die Einstellungen für den Cloud Storage Pool (**ILM** > **Storage Pools**).
- Überprüfen Sie die Netzwerkkonfiguration des Storage Proxy-Servers.

Verwandte Informationen

"Lebenszyklus eines Cloud-Storage-Pool-Objekts"

Profile für das Erasure Coding managen

Sie können bei Bedarf ein Profil für die Erasure Coding umbenennen. Sie können ein Profil für Erasure Coding deaktivieren, wenn es derzeit nicht in ILM-Regeln verwendet wird.

Umbenennen eines Profils für die Erasure Coding

Möglicherweise möchten Sie ein Erasure Coding-Profil umbenennen, um es deutlicher zu machen, was das Profil tut.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Erforderliche Zugriffsberechtigungen".

Schritte

1. Wählen Sie **ILM** > **Erasure Coding** aus.
2. Wählen Sie das Profil aus, das Sie umbenennen möchten.
3. Wählen Sie **Umbenennen**.
4. Geben Sie einen eindeutigen Namen für das Erasure Coding-Profil ein.

   Der Name des Erasure Coding-Profils wird in der Platzierungsanweisung für eine ILM-Regel an den Namen des Speicherpools angehängt.

   > ⓘ Profilnamen für das Erasure Coding müssen eindeutig sein. Ein Validierungsfehler tritt auf, wenn Sie den Namen eines vorhandenen Profils verwenden, auch wenn dieses Profil deaktiviert wurde.

5. Wählen Sie **Speichern**.

Deaktivieren Sie ein Erasure Coding-Profil

Sie können ein Profil für Erasure Coding deaktivieren, wenn Sie es nicht mehr verwenden möchten und das Profil derzeit in keiner ILM-Regel verwendet wird.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Erforderliche Zugriffsberechtigungen".
- Sie haben bestätigt, dass derzeit keine Reparatur- oder Deaktivierung von Daten mithilfe von Erasure Coding ausgeführt wird. Wenn Sie versuchen, ein Erasure Coding-Profil zu deaktivieren, während eines dieser Vorgänge ausgeführt wird, wird eine Fehlermeldung ausgegeben.

Über diese Aufgabe

Wenn Sie ein Erasure Coding-Profil deaktivieren, wird das Profil weiterhin auf der Seite Erasure Coding Profiles angezeigt, sein Status ist jedoch **deactivated**.

Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
2+1 Data Center 1	Used In ILM Rule	Data Center 1	3	1	2+1	50	1	No
New profile	Deactivated	Data Center 1	3	1	2+1	50	1	No

Sie können kein deaktiviertes Erasure Coding-Profil mehr verwenden. Ein deaktiviertes Profil wird nicht angezeigt, wenn Sie die Platzierungsanweisungen für eine ILM-Regel erstellen. Ein deaktiviertes Profil kann nicht reaktiviert werden.

StorageGRID verhindert, dass Sie ein Erasure Coding-Profil deaktivieren, wenn eine der folgenden Optionen zutrifft:

- Das Erasure Coding-Profil wird derzeit in einer ILM-Regel verwendet.
- Das Erasure Coding-Profil wird in keiner ILM-Regel mehr verwendet, es existieren jedoch noch Objektdaten und Paritätsfragmente für das Profil.

Schritte

1. Wählen Sie **ILM** > **Erasure Coding** aus.
2. Überprüfen Sie die Spalte **Status**, um zu bestätigen, dass das Erasure Coding-Profil, das Sie deaktivieren möchten, in keiner ILM-Regel verwendet wird.

   Sie können ein Profil für Erasure Coding nicht deaktivieren, wenn es in einer ILM-Regel verwendet wird. Im Beispiel wird das Profil **2+1 Data Center 1** in mindestens einer ILM-Regel verwendet.

Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
2+1 Data Center 1	Used In ILM Rule	Data Center 1	3	1	2+1	50	1	No
New profile	Deactivated	Data Center 1	3	1	2+1	50	1	No

3. Wenn das Profil in einer ILM-Regel verwendet wird, führen Sie die folgenden Schritte aus:
   a. Wählen Sie **ILM** > **Regeln**.
   b. Wählen Sie jede Regel aus, und prüfen Sie das Aufbewahrungsdiagramm, um festzustellen, ob die Regel das zu deaktivierende Erasure Coding-Profil verwendet.
   c. Wenn die ILM-Regel das Profil für die Erasure Coding verwendet, das Sie deaktivieren möchten, bestimmen Sie, ob die Regel in der aktiven ILM-Richtlinie oder in einer vorgeschlagenen Richtlinie verwendet wird.
   d. Führen Sie die zusätzlichen Schritte in der Tabelle aus, je nachdem, wo das Erasure Coding-Profil verwendet wird.

Wo wurde das Profil verwendet?	**Weitere Schritte, die vor dem Deaktivieren des Profils ausgeführt werden müssen**	**Beachten Sie diese zusätzlichen Anweisungen**
Nie in einer ILM-Regel verwendet	Weitere Schritte sind nicht erforderlich. Fahren Sie mit diesem Verfahren fort.	*Keine*
In einer ILM-Regel, die noch nie in einer ILM-Richtlinie verwendet wurde	i. Alle betroffenen ILM-Regeln bearbeiten oder löschen. Wenn Sie die Regel bearbeiten, entfernen Sie alle Platzierungen, die das Erasure Coding-Profil verwenden. ii. Fahren Sie mit diesem Verfahren fort.	"Arbeiten Sie mit ILM-Regeln und ILM-Richtlinien"

Wo wurde das Profil verwendet?	Weitere Schritte, die vor dem Deaktivieren des Profils ausgeführt werden müssen	Beachten Sie diese zusätzlichen Anweisungen
In einer ILM-Regel, die sich derzeit in der aktiven ILM-Richtlinie befindet	i. Klonen der aktiven Richtlinie ii. Entfernen Sie die ILM-Regel, die das Profil für das Erasure Coding verwendet. iii. Fügen Sie mindestens eine neue ILM-Regel hinzu, um die Sicherheit von Objekten zu gewährleisten. iv. Speichern, simulieren und aktivieren Sie die neue Richtlinie. v. Warten Sie, bis die neue Richtlinie angewendet wird und vorhandene Objekte basierend auf den neuen Regeln, die Sie hinzugefügt haben, an neue Orte verschoben werden. **Hinweis:** abhängig von der Anzahl der Objekte und der Größe Ihres StorageGRID-Systems kann es Wochen oder sogar Monate dauern, bis ILM-Vorgänge die Objekte auf der Grundlage der neuen ILM-Regeln an neue Orte verschieben. Obwohl Sie sicher versuchen können, ein Erasure Coding-Profil zu deaktivieren, während es noch mit Daten verknüpft ist, schlägt die Deaktivierung fehl. Eine Fehlermeldung informiert Sie darüber, ob das Profil noch nicht deaktiviert werden kann. vi. Bearbeiten oder löschen Sie die Regel, die Sie aus der Richtlinie entfernt haben. Wenn Sie die Regel bearbeiten, entfernen Sie alle Platzierungen, die das Erasure Coding-Profil verwenden. vii. Fahren Sie mit diesem Verfahren fort.	"ILM-Richtlinie erstellen" "Arbeiten Sie mit ILM-Regeln und ILM-Richtlinien"
In einer ILM-Regel, die sich derzeit in einer vorgeschlagenen ILM-Richtlinie befindet	i. Bearbeiten Sie die vorgeschlagene Richtlinie. ii. Entfernen Sie die ILM-Regel, die das Profil für das Erasure Coding verwendet. iii. Fügen Sie ein oder mehrere neue ILM-Regeln hinzu, um sicherzustellen, dass alle Objekte geschützt sind. iv. Speichern Sie die vorgeschlagene Richtlinie. v. Bearbeiten oder löschen Sie die Regel, die Sie aus der Richtlinie entfernt haben. Wenn Sie die Regel bearbeiten, entfernen Sie alle Platzierungen, die das Erasure Coding-Profil verwenden. vi. Fahren Sie mit diesem Verfahren fort.	"ILM-Richtlinie erstellen" "Arbeiten Sie mit ILM-Regeln und ILM-Richtlinien"

Wo wurde das Profil verwendet?	Weitere Schritte, die vor dem Deaktivieren des Profils ausgeführt werden müssen	Beachten Sie diese zusätzlichen Anweisungen
In einer ILM-Regel, die sich in einer historischen ILM-Richtlinie befindet	i. Bearbeiten oder löschen Sie die Regel. Wenn Sie die Regel bearbeiten, entfernen Sie alle Platzierungen, die das Erasure Coding-Profil verwenden. (Die Regel wird nun als historische Regel in der historischen Richtlinie angezeigt.) ii. Fahren Sie mit diesem Verfahren fort.	"Arbeiten Sie mit ILM-Regeln und ILM-Richtlinien"

e. Aktualisieren Sie die Seite Erasure Coding Profiles, um sicherzustellen, dass das Profil nicht in einer ILM-Regel verwendet wird.

4. Wenn das Profil nicht in einer ILM-Regel verwendet wird, aktivieren Sie das Optionsfeld und wählen Sie **Deaktivieren**.

   Das Dialogfeld EC-Profil deaktivieren wird angezeigt.

5. Wenn Sie sicher sind, dass Sie das Profil deaktivieren möchten, wählen Sie **Deactivate**.
   - Wenn StorageGRID das Erasure Coding-Profil deaktivieren kann, ist sein Status **deactivated**. Sie können dieses Profil nicht mehr für eine ILM-Regel auswählen.
   - Wenn StorageGRID das Profil nicht deaktivieren kann, wird eine Fehlermeldung angezeigt. Wenn Objektdaten weiterhin mit diesem Profil verknüpft sind, wird beispielsweise eine Fehlermeldung angezeigt. Sie müssen möglicherweise mehrere Wochen warten, bevor Sie den Deaktivierungsprozess erneut versuchen.

Regionen konfigurieren (nur optional und S3)

ILM-Regeln können Objekte auf Basis der Bereiche filtern, in denen S3-Buckets erstellt werden, und so Objekte aus verschiedenen Regionen an unterschiedlichen Storage-Standorten speichern.

Wenn Sie einen S3-Bucket-Bereich als Filter in einer Regel verwenden möchten, müssen Sie zuerst die Regionen erstellen, die von den Buckets in Ihrem System verwendet werden können.

Sie können den Bereich für einen Bucket nicht ändern, nachdem der Bucket erstellt wurde.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Beim Erstellen eines S3-Buckets können Sie angeben, dass er in einer bestimmten Region erstellt wird. Wenn Sie eine Region angeben, kann der Bucket sich in geografischer Nähe zu seinen Benutzern befinden, um die Latenz zu optimieren, Kosten zu minimieren und gesetzliche Anforderungen zu erfüllen.

Wenn Sie eine ILM-Regel erstellen, möchten Sie die Region, die einem S3-Bucket zugeordnet ist, möglicherweise als erweiterten Filter verwenden. Sie können zum Beispiel eine Regel entwerfen, die sich nur

auf Objekte bezieht, die in den in uns-West-2 erstellten S3-Buckets gelten. Sie können dann angeben, die Kopien dieser Objekte an Storage-Nodes an einem Datacenter-Standort innerhalb dieser Region platziert werden, um die Latenz zu optimieren.

Befolgen Sie bei der Konfiguration von Regionen die folgenden Richtlinien:

- Standardmäßig gehören alle Buckets zu US-East-1-Region.
- Sie müssen die Regionen mit dem Grid Manager erstellen, bevor Sie beim Erstellen von Buckets mithilfe der Mandanten-Manager- oder Mandantenmanagement-API oder mit dem LocationConstraint-Anforderungselement für S3 PUT-Bucket-API-Anforderungen eine nicht standardmäßige Region angeben können. Ein Fehler tritt auf, wenn eine PUT-Bucket-Anforderung eine Region verwendet, die nicht in StorageGRID definiert wurde.
- Sie müssen beim Erstellen des S3-Buckets den genauen Regionalnamen verwenden. Bei Regionalnamen wird zwischen Groß- und Kleinschreibung unterschieden. Gültige Zeichen sind Zahlen, Buchstaben und Bindestriche.

  > Die EU gilt nicht als ein Alias für eu-West-1. Wenn Sie die Region EU oder eu-West-1 nutzen möchten, müssen Sie den genauen Namen verwenden.

- Sie können eine Region nicht löschen oder ändern, wenn sie derzeit innerhalb der aktiven ILM-Richtlinie oder der vorgeschlagenen ILM-Richtlinie verwendet wird.
- Wenn die Region, die als erweiterter Filter in einer ILM-Regel verwendet wird, ungültig ist, kann diese Regel noch zur vorgeschlagenen Richtlinie hinzugefügt werden. Es tritt jedoch ein Fehler auf, wenn Sie versuchen, die vorgeschlagene Richtlinie zu speichern oder zu aktivieren.

  Eine ungültige Region kann sich ergeben, wenn Sie eine Region als erweiterten Filter in einer ILM-Regel verwenden, diese Region jedoch später löschen oder wenn Sie die Grid-Management-API zum Erstellen einer Regel und zum Festlegen einer Region verwenden, die Sie nicht definiert haben.

- Wenn Sie eine Region löschen, nachdem Sie sie zum Erstellen eines S3-Buckets verwendet haben, müssen Sie die Region erneut hinzufügen, wenn Sie den erweiterten Filter Speicherungsbedingung verwenden möchten, um Objekte in diesem Bucket zu finden.

Schritte

1. Wählen Sie **ILM** > **Regionen**.

   Die Seite Regionen wird angezeigt, wobei die derzeit definierten Regionen aufgelistet sind. **Region 1** zeigt die Standardregion, `us-east-1`, Die nicht geändert oder entfernt werden können.

2. So fügen Sie eine Region hinzu:
   a. Wählen Sie das Einfügesymbol aus ➕ Rechts neben dem letzten Eintrag.
   b. Geben Sie den Namen einer Region ein, die Sie beim Erstellen von S3-Buckets verwenden möchten.

      Sie müssen diesen genauen Regionalnamen als LocationConstraint Request Element verwenden, wenn Sie den entsprechenden S3-Bucket erstellen.

3. Um eine nicht verwendete Region zu entfernen, wählen Sie das Löschsymbol aus ✕.

   Wenn Sie versuchen, eine Region zu entfernen, die derzeit in der aktiven Richtlinie oder der vorgeschlagenen Richtlinie verwendet wird, wird eine Fehlermeldung angezeigt.

4. Wenn Sie Änderungen vorgenommen haben, wählen Sie **Speichern**.

Sie können diese Bereiche nun im Abschnitt Erweiterte Filter in Schritt 1 des Assistenten zum Erstellen von ILM-Regeln auswählen. Siehe "Verwenden Sie erweiterte Filter in ILM-Regeln".

ILM-Regel erstellen

Erstellen Sie eine ILM-Regel: Überblick

Zum Managen von Objekten erstellen Sie eine Reihe von Regeln für das Information Lifecycle Management (ILM) und organisieren diese in eine ILM-Richtlinie.

Jedes im System aufgenommene Objekt wird anhand der aktiven Richtlinie ausgewertet. Wenn eine Regel in der Richtlinie mit den Metadaten eines Objekts übereinstimmt, bestimmen die Anweisungen in der Regel, welche Aktionen StorageGRID zum Kopieren und Speichern des Objekts ergreift.

> Objektmetadaten werden nicht durch ILM-Regeln gemanagt. Stattdessen werden Objekt-Metadaten in einer Cassandra-Datenbank in einem sogenannten Metadaten-Speicher gespeichert. Drei Kopien von Objekt-Metadaten werden automatisch an jedem Standort aufbewahrt, um die Daten vor Verlust zu schützen.

Elemente einer ILM-Regel

Eine ILM-Regel besteht aus drei Elementen:

- **Filterkriterien**: Die Basis- und erweiterten Filter einer Regel definieren, für welche Objekte die Regel gilt. Wenn ein Objekt allen Filtern entspricht, wendet StorageGRID die Regel an und erstellt die Objektkopien, die in den Platzierungsanweisungen der Regel angegeben sind.
- **Platzierungsanweisungen**: Die Platzierungsanweisungen einer Regel definieren die Zahl, den Typ und den Ort von Objektkopien. Jede Regel kann eine Reihe von Anweisungen zur Platzierung enthalten, um die Anzahl, den Typ und den Standort der Objektkopien im Laufe der Zeit zu ändern. Wenn der Zeitraum für eine Platzierung abgelaufen ist, werden die Anweisungen in der nächsten Platzierung automatisch bei der nächsten ILM-Bewertung angewendet.
- **Ingest Behavior**: Das Ingest Behavior einer Regel erlaubt Ihnen zu wählen, wie die Objekte, die durch die Regel gefiltert werden, geschützt werden, wenn sie aufgenommen werden (wenn ein S3- oder Swift-Client ein Objekt im Grid speichert).

ILM-Regelfilterung

Wenn Sie eine ILM-Regel erstellen, geben Sie Filter an, um zu identifizieren, für welche Objekte die Regel gilt.

Im einfachsten Fall verwendet eine Regel möglicherweise keine Filter. Alle Regeln, die keine Filter verwenden, gelten für alle Objekte. Daher muss es sich um die letzte (standardmäßige) Regel in einer ILM-Richtlinie handelt. Die Standardregel enthält Speicheranweisungen für Objekte, die nicht mit den Filtern einer anderen Regel übereinstimmen.

- Grundlegende Filter ermöglichen es Ihnen, unterschiedliche Regeln auf große, unterschiedliche Objektgruppen anzuwenden. Mit diesen Filtern können Sie eine Regel auf bestimmte Mandantenkonten, bestimmte S3-Buckets oder Swift-Container oder beides anwenden.

  Grundlegende Filter geben Ihnen eine einfache Möglichkeit, verschiedene Regeln auf eine große Anzahl von Objekten anzuwenden. So müssen beispielsweise die Finanzdaten Ihres Unternehmens möglicherweise gespeichert werden, um gesetzliche Vorgaben einzuhalten. Daten aus der Marketing-Abteilung müssen möglicherweise gespeichert werden, um den täglichen Betrieb zu erleichtern. Nach der

Erstellung separater Mandantenkonten für jede Abteilung oder nach Trennung von Daten aus den verschiedenen Abteilungen in separate S3 Buckets können Sie problemlos eine Regel erstellen, die für alle Finanzdaten und eine zweite Regel gilt für alle Marketingdaten.

- Erweiterte Filter geben Ihnen eine präzise Kontrolle. Sie können Filter erstellen, um Objekte anhand der folgenden Objekteigenschaften auszuwählen:
  - Aufnahmezeit
  - Zeitpunkt des letzten Zugriffs
  - Der Objektname (Schlüssel) ganz oder teilweise
  - Speicherortbeschränkung (nur S3)
  - Objektgröße
  - Benutzer-Metadaten
  - Objekt-Tag (nur S3)

Sie können Objekte nach sehr spezifischen Kriterien filtern. So können beispielsweise Objekte, die von der Bildgebungsabteilung eines Krankenhauses gespeichert sind, häufig verwendet werden, wenn sie weniger als 30 Tage alt und selten danach sind, während Objekte, die Angaben zu Patientenbesuchen enthalten, möglicherweise in die Rechnungsabteilung des Gesundheitsnetzwerks kopiert werden müssen. Sie können Filter erstellen, die jeden Objekttyp anhand von Objektnamen, -Größe, S3-Objekt-Tags oder anderen relevanten Kriterien identifizieren. Anschließend können separate Regeln erstellt werden, um jeden Objektsatz entsprechend zu speichern.

Sie können Filter nach Bedarf in einer einzigen Regel kombinieren. Beispielsweise möchte die Marketingabteilung große Bilddateien anders speichern als die Lieferantendaten, während die Personalabteilung Personaldatensätze in einer bestimmten Region und in einer bestimmten Richtlinie zentral speichern muss. In diesem Fall können Sie Regeln erstellen, die nach Mandantenkonto filtern, um die Datensätze von jeder Abteilung zu trennen, während Sie in jeder Regel Filter verwenden, um den spezifischen Objekttyp zu identifizieren, auf den die Regel angewendet wird.

Anweisungen zur Platzierung von ILM-Regeln

Eine Anleitung zur Platzierung bestimmt, wo, wann und wie Objektdaten gespeichert werden. Eine ILM-Regel kann eine oder mehrere Anweisungen zur Platzierung enthalten. Jede Einstufungsanweisung gilt für einen einzelnen Zeitraum.

Wenn Sie Anweisungen zur Platzierung erstellen:

- Sie beginnen mit der Angabe der Referenzzeit, die bestimmt, wann die Platzierungsanweisungen beginnen. Die Referenzzeit kann sein, wenn ein Objekt aufgenommen wird, wenn auf ein Objekt zugegriffen wird, wenn ein versioniertes Objekt nicht mehr aktuell wird oder eine benutzerdefinierte Zeit.
- Als Nächstes geben Sie an, wann die Platzierung in Bezug auf die Referenzzeit gelten soll. Beispielsweise kann eine Platzierung am Tag 0 beginnen und 365 Tage lang fortgesetzt werden, relativ zu dem Zeitpunkt, zu dem das Objekt aufgenommen wurde.
- Schließlich geben Sie die Art der Kopien (Replizierung oder Erasure Coding) und den Speicherort der Kopien an. So können Sie beispielsweise zwei replizierte Kopien an zwei unterschiedlichen Standorten speichern.

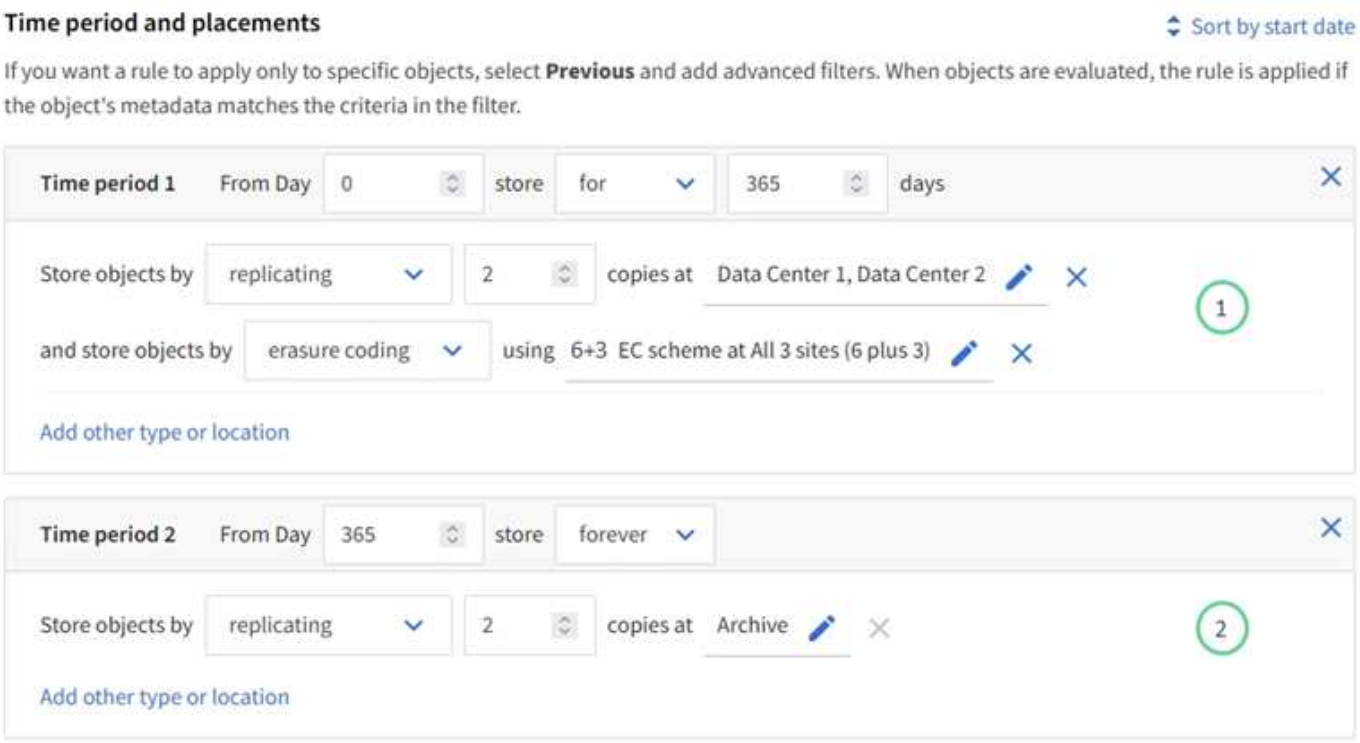
Jede Regel kann mehrere Platzierungen für einen einzigen Zeitraum und verschiedene Platzierungen für unterschiedliche Zeiträume definieren.

- Um Objekte in einem Zeitraum an mehreren Orten zu platzieren, wählen Sie **anderen Typ oder Standort**

hinzufügen, um mehr als eine Zeile für diesen Zeitraum hinzuzufügen.

- Um Objekte an verschiedenen Orten in verschiedenen Zeiträumen zu platzieren, wählen Sie **weiteren Zeitraum hinzufügen**, um den nächsten Zeitraum hinzuzufügen. Geben Sie dann eine oder mehrere Zeilen innerhalb des Zeitraums an.

Das Beispiel zeigt zwei Platzierungsanweisungen auf der Seite Platzierungen definieren des Assistenten zum Erstellen einer ILM-Regel.



Die erste Platzierungsanweisung (1) Hat zwei Linien für das erste Jahr:

- In der ersten Zeile werden zwei replizierte Objektkopien an zwei Datacenter-Standorten erstellt.
- Die zweite Zeile erstellt eine Kopie mit 6 und 3 zur Fehlerkorrektur codierten Kopien unter Verwendung von drei Datacenter-Standorten.

Die zweite Platzierungsanweisung (2) Erstellt zwei archivierte Kopien nach einem Jahr und speichert diese Kopien für immer.

Wenn Sie den Satz von Anweisungen zur Platzierung für eine Regel definieren, müssen Sie sicherstellen, dass mindestens eine Platzierungsanweisung an Tag 0 beginnt, dass zwischen den von Ihnen definierten Zeiträumen keine Lücken bestehen. Und dass die abschließende Anweisung zum Platzieren entweder für immer oder bis Sie keine Objektkopien mehr benötigen.

Da jeder Zeitraum in der Regel abläuft, werden die Anweisungen zur Inhaltsplatzierung für den nächsten Zeitraum angewendet. Neue Objektkopien werden erstellt und nicht benötigte Kopien werden gelöscht.

ILM-Regel Aufnahme-Verhalten

Das Aufnahmeverhalten steuert, ob Objektkopien sofort nach den Anweisungen in der Regel platziert werden oder ob zwischenzeitliche Kopien erstellt und die Speicheranweisungen später angewendet werden. Die folgenden Aufnahmeverhalten stehen für ILM-Regeln zur Verfügung:

- **Ausgewogen**: StorageGRID versucht bei der Aufnahme alle in der ILM-Regel festgelegten Kopien zu erstellen; wenn dies nicht möglich ist, werden Zwischenkopien erstellt und der Erfolg an den Client zurückgesendet. Die Kopien, die in der ILM-Regel angegeben sind, werden, wenn möglich gemacht.
- **Streng**: Alle in der ILM-Regel angegebenen Kopien müssen erstellt werden, bevor der Erfolg an den Client zurückgesendet wird.
- **Dual Commit**: StorageGRID erstellt sofort Zwischenkopien des Objekts und gibt den Erfolg an den Client zurück. Kopien, die in der ILM-Regel angegeben sind, werden nach Möglichkeit erstellt.

Verwandte Informationen

- "Aufnahmeoptionen"
- "Vorteile, Nachteile und Einschränkungen der Aufnahmsoptionen"
- "Konsistenzkontrollen und ILM-Regeln interagieren, um die Datensicherung zu beeinträchtigen"

Beispiel für eine ILM-Regel

Eine ILM-Regel könnte beispielsweise Folgendes angeben:

- Nur auf die Objekte anwenden, die zu Mandant A gehören
- Erstellen Sie zwei replizierte Kopien dieser Objekte und speichern Sie jede Kopie an einem anderen Standort.
- Behalten Sie die beiden Kopien „`Forever,`“ bei, was bedeutet, dass StorageGRID sie nicht automatisch löscht. Stattdessen behält StorageGRID diese Objekte so lange bei, bis sie von einer Löschanfrage eines Clients oder nach Ablauf eines Bucket-Lebenszyklus gelöscht werden.
- Verwenden Sie die ausgewogene Option für das Aufnahmeverhalten: Die Anweisung zur Platzierung von zwei Standorten wird angewendet, sobald Mandant A ein Objekt in StorageGRID speichert, es sei denn, es ist nicht möglich, sofort beide erforderlichen Kopien zu erstellen.

  Wenn z. B. Standort 2 nicht erreichbar ist, wenn Mandant A ein Objekt speichert, erstellt StorageGRID zwei Zwischenkopien auf Storage-Nodes an Standort 1. Sobald Standort 2 verfügbar wird, erstellt StorageGRID die erforderliche Kopie an diesem Standort.

Verwandte Informationen

- "Was ist ein Speicherpool?"
- "Was ist ein Cloud-Storage-Pool?"

Greifen Sie auf den Assistenten zum Erstellen einer ILM-Regel zu

ILM-Regeln ermöglichen es Ihnen, die Platzierung von Objektdaten im Laufe der Zeit zu managen. Zum Erstellen einer ILM-Regel verwenden Sie den Assistenten zum Erstellen einer ILM-Regel.

> Wenn Sie die Standard-ILM-Regel für eine Richtlinie erstellen möchten, befolgen Sie die Anweisungen unter "Anweisungen zum Erstellen einer standardmäßigen ILM-Regel" Stattdessen.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.

- Wenn Sie angeben möchten, für welche Mandantenkonten diese Regel gilt, verfügen Sie über die Berechtigung für die Mandantenkonten oder Sie kennen die Konto-ID für jedes Konto.
- Wenn die Regel Objekte nach Metadaten der Uhrzeit des letzten Zugriffs filtern soll, müssen die Updates der Uhrzeit des letzten Zugriffs für Bucket für S3 oder für Container für Swift aktiviert werden.
- Sie haben alle Cloud-Storage-Pools konfiguriert, die Sie verwenden möchten. Siehe "Cloud Storage Pool Erstellen".
- Sie kennen das "Aufnahmeoptionen".
- Wenn Sie eine konforme Regel für die Verwendung mit S3 Object Lock erstellen müssen, kennen Sie die "Anforderungen für die S3-Objektsperre".
- Optional haben Sie sich das Video angesehen: "Video: Information Lifecycle Management Regeln in StorageGRID 11.7".

Über diese Aufgabe

Wenn ILM-Regeln erstellt werden:

- Dabei sind die Topologie und Storage-Konfigurationen des StorageGRID Systems zu berücksichtigen.
- Es sollte berücksichtigt werden, welche Arten von Objektkopien Sie erstellen möchten (replizierte oder Erasure Coding) und wie viele Kopien der einzelnen Objekte erforderlich sind.
- Legen Sie fest, welche Typen von Objekt-Metadaten in den Applikationen verwendet werden, die sich mit dem StorageGRID System verbinden. ILM-Regeln filtern Objekte auf Basis ihrer Metadaten.
- Dabei sollten Sie berücksichtigen, wo Sie Objektkopien über einen längeren Zeitraum ablegen möchten.
- Entscheiden Sie, welche Aufnahmeoption verwendet werden soll (ausgeglichen, streng oder doppelte Übertragung).

Schritte

1. Wählen Sie **ILM** > **Regeln**.

   Basierend auf der Anzahl der Standorte in der Tabelle wird die Regel 2 Kopien erstellen oder die Regel 1 Kopie pro Standort in der Regelliste angezeigt.

   Wenn die globale S3-Objektsperre für das StorageGRID-System aktiviert wurde, enthält die Übersichtstabelle eine Spalte **konform**, und die Details für die ausgewählte Regel enthalten ein Feld **konform**.

2. Wählen Sie **Erstellen**. "Schritt 1 (Details eingeben)" Des Assistenten zum Erstellen einer ILM-Regel wird angezeigt.

Schritt 1 von 3: Details eingeben

Im Schritt **Details eingeben** des Assistenten zum Erstellen einer ILM-Regel können Sie

einen Namen und eine Beschreibung für die Regel eingeben und Filter für die Regel definieren.

Die Eingabe einer Beschreibung und das Definieren von Filtern für die Regel sind optional.

Über diese Aufgabe

Bei der Auswertung eines Objekts mit einem "ILM-Regel", StorageGRID vergleicht die Objektmetadaten mit den Filtern der Regel. Wenn die Objektmetadaten mit allen Filtern übereinstimmen, verwendet StorageGRID die Regel, um das Objekt abzulegen. Sie können eine Regel für alle Objekte entwerfen oder grundlegende Filter angeben, z. B. ein oder mehrere Mandantenkonten und Bucket-Namen oder erweiterte Filter, wie z. B. Größe des Objekts oder Benutzermetadaten.

Schritte

1. Geben Sie im Feld **Name** einen eindeutigen Namen für die Regel ein.
2. Geben Sie optional im Feld **Beschreibung** eine kurze Beschreibung für die Regel ein.

   Sie sollten den Zweck oder die Funktion der Regel beschreiben, damit Sie die Regel später erkennen können.

3. Wählen Sie optional ein oder mehrere S3- oder Swift-Mandantenkonten aus, für die diese Regel gilt. Wenn diese Regel für alle Mandanten gilt, lassen Sie dieses Feld leer.

   Wenn Sie weder über die Berechtigung für den Root-Zugriff noch über die Berechtigung für die Mandantenkonten verfügen, können Sie keine Mandanten aus der Liste auswählen. Geben Sie stattdessen die Mandanten-ID ein, oder geben Sie mehrere IDs als durch Komma getrennte Zeichenfolge ein.

4. Geben Sie optional die S3-Buckets oder Swift-Container an, für die diese Regel gilt.

   Wenn **entspricht allen** ausgewählt ist (Standard), gilt die Regel für alle S3-Buckets oder Swift-Container.

5. Wählen Sie für S3-Mandanten optional **Yes** aus, um die Regel nur auf ältere Objektversionen in S3-Buckets anzuwenden, für die die Versionierung aktiviert ist.

   Wenn Sie **Ja** auswählen, wird automatisch „`nicht aktuelle Zeit`“ für die Referenzzeit in ausgewählt "Schritt 2 des Assistenten zum Erstellen einer ILM-Regel".

   > Die nicht aktuelle Zeit gilt nur für S3 Objekte in versionierungsfähigen Buckets. Siehe "Operationen für Buckets, PUT Bucket-Versionierung" Und "Objekte managen mit S3 Object Lock".

   Mit dieser Option können Sie die Auswirkungen versionierter Objekte auf den Speicher reduzieren, indem Sie nach nicht aktuellen Objektversionen filtern. Siehe "Beispiel 4: ILM-Regeln und -Richtlinie für versionierte Objekte mit S3".

6. Wählen Sie optional **Erweiterten Filter hinzufügen**, um weitere Filter festzulegen.

   Wenn Sie keine erweiterte Filterung konfigurieren, gilt die Regel für alle Objekte, die den Grundfiltern entsprechen. Weitere Informationen zum erweiterten Filtern finden Sie unter Verwenden Sie erweiterte Filter in ILM-Regeln Und Geben Sie mehrere Metadatentypen und -Werte an.

7. Wählen Sie **Weiter**. "Schritt 2 (Platzierungen definieren)" Des Assistenten zum Erstellen einer ILM-Regel wird angezeigt.

Verwenden Sie erweiterte Filter in ILM-Regeln

Mit der erweiterten Filterung können Sie ILM-Regeln erstellen, die sich nur auf bestimmte Objekte anwenden lassen, basierend auf ihren Metadaten. Wenn Sie die erweiterte Filterung für eine Regel einrichten, wählen Sie den Metadatentyp aus, der übereinstimmen soll, wählen Sie einen Operator aus und geben einen Metadatenwert an. Wenn Objekte ausgewertet werden, wird die ILM-Regel nur auf Objekte angewendet, die Metadaten enthalten, die dem erweiterten Filter entsprechen.

Die Tabelle zeigt die Metadatentypen, die Sie in den erweiterten Filtern angeben können, die Operatoren, die Sie für jeden Metadatentyp verwenden können, und die erwarteten Metadaten.

Metadatentyp	Unterstützte Operatoren	Metadatenwert
Aufnahmezeit	• Ist • Ist es nicht • Ist vorher • Ist ein oder vorher • Ist nachher • Ist ein oder nach	Uhrzeit und Datum, an dem das Objekt aufgenommen wurde. **Hinweis:** um Ressourcenprobleme bei der Aktivierung einer neuen ILM-Richtlinie zu vermeiden, können Sie den erweiterten Filter für die Einspielzeit in jeder Regel verwenden, die den Speicherort einer großen Anzahl vorhandener Objekte ändern könnte. Legen Sie für die Aufnahme-Zeit den Wert fest, der ungefähr der Zeit entspricht, zu der die neue Richtlinie in Kraft tritt, um sicherzustellen, dass vorhandene Objekte nicht unnötig verschoben werden.
Taste	• Gleich • Ist nicht gleich • Enthält • Enthält nicht • Beginnt mit • Startet nicht mit • Endet mit • Endet nicht mit	Der gesamte Objektschlüssel oder Teil eines eindeutigen S3- oder Swift-Objektschlüssels. Beispielsweise können Sie Objekte, die mit enden, aufeinander abstimmen `.txt` Oder beginnen Sie mit `test-object/`.
Zeitpunkt des letzten Zugriffs	• Ist • Ist es nicht • Ist vorher • Ist ein oder vorher • Ist nachher • Ist ein oder nach	Uhrzeit und Datum, an dem das Objekt zuletzt abgerufen wurde (gelesen oder angezeigt). **Hinweis:** Wenn Sie Vorhaben "Letzte Zugriffszeit verwenden" Als erweiterter Filter müssen die Updates der Uhrzeit des letzten Zugriffs für den S3-Bucket oder Swift-Container aktiviert sein.

Metadatentyp	Unterstützte Operatoren	Metadatenwert
Speicherortbeschränkung (nur S3)	• Gleich • Ist nicht gleich	Die Region, in der ein S3-Bucket erstellt wurde. Verwenden Sie **ILM** > **Regionen**, um die angezeigten Regionen zu definieren. **Hinweis:** Ein Wert von US-East-1 entspricht Objekten in Eimern, die in der Region US-East-1 erstellt wurden, sowie Objekten in Buckets, die keine Region angegeben haben. Siehe "Regionen konfigurieren (nur optional und S3)".
Objektgröße	• Gleich • Ist nicht gleich • Kleiner als • Kleiner als oder gleich • Größer als • Größer als oder gleich	Die Größe des Objekts. Das Verfahren zur Einhaltung von Datenkonsistenz eignet sich am besten für Objekte mit einer Größe von mehr als 1 MB. Verwenden Sie kein Erasure Coding für Objekte, die kleiner als 200 KB sind, um zu vermeiden, dass man sehr kleine Fragmente, die zur Fehlerkorrektur codiert wurden, managen muss. **Hinweis:** um nach Objektgrößen kleiner als 1 MB zu filtern, geben Sie einen Dezimalwert ein. Der Browsertyp und die Ländereinstellungen steuern, ob Sie einen Punkt oder ein Komma als Dezimaltrennzeichen verwenden müssen.
Benutzer-Metadaten	• Enthält • Endet mit • Gleich • Vorhanden • Enthält nicht • Endet nicht mit • Ist nicht gleich • Nicht vorhanden • Startet nicht mit • Beginnt mit	Schlüssel-Wert-Paar, wobei **Benutzer-Metadaten-Name** der Schlüssel und **Metadaten-Wert** der Wert ist. Zum Beispiel nach Objekten mit Benutzer-Metadaten von filtern `color=blue`, Spezifizieren `color` Für **Name der Metadaten des Benutzers**, `equals` Für den Bediener, und `blue` Für **Metadatenwert**. **Hinweis:** Benutzer-Metadaten-Namen sind nicht zwischen Groß- und Kleinschreibung zu beachten; Benutzer-Metadaten-Werte sind Groß- und Kleinschreibung zu beachten.

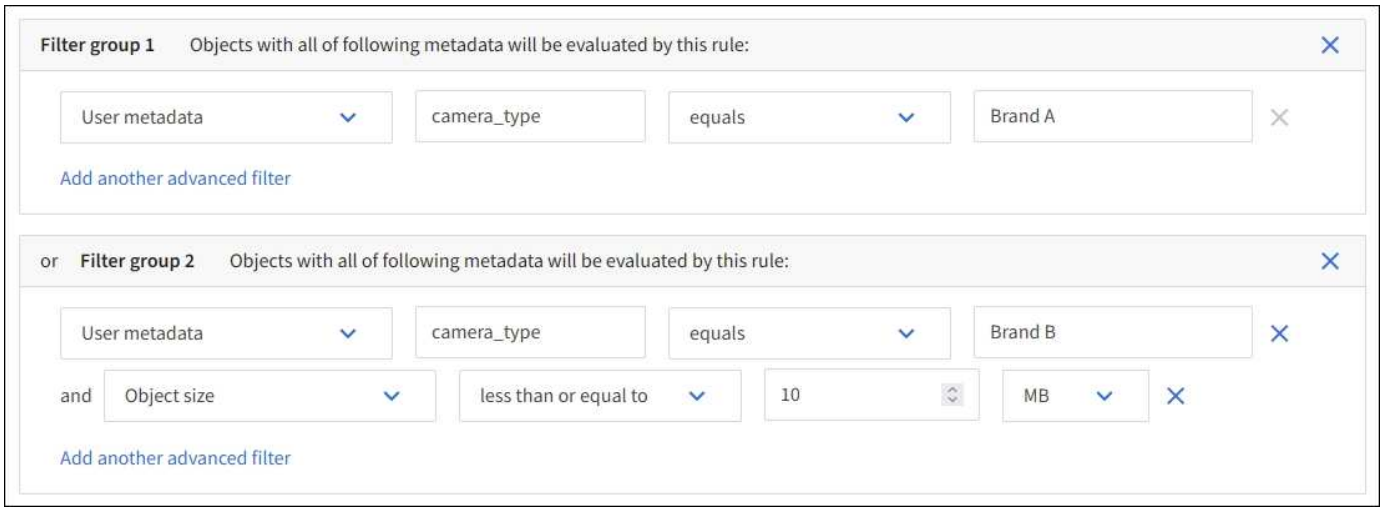
Metadatentyp	Unterstützte Operatoren	Metadatenwert
Objekt-Tag (nur S3)	• Enthält • Endet mit • Gleich • Vorhanden • Enthält nicht • Endet nicht mit • Ist nicht gleich • Nicht vorhanden • Startet nicht mit • Beginnt mit	Schlüssel-Wert-Paar, wobei **Objekt-Tag-Name** der Schlüssel und **Objekt-Tag-Wert** der Wert ist. Zum Beispiel, um nach Objekten zu filtern, die ein Objekt-Tag von haben `Image=True`, Spezifizieren `Image` Für **Objekt-Tag-Name**, `equals` Für den Bediener, und `True` Für **Objekt Tag Wert**. **Hinweis:** Objekt-Tag-Namen und Objekt-Tag-Werte sind Groß- und Kleinschreibung. Sie müssen diese Elemente genau so eingeben, wie sie für das Objekt definiert wurden.

Geben Sie mehrere Metadatentypen und -Werte an

Wenn Sie die erweiterte Filterung definieren, können Sie mehrere Metadatentypen und mehrere Metadatenwerte angeben. Wenn Sie beispielsweise eine Regel mit Objekten zwischen 10 MB und 100 MB Größe vergleichen möchten, wählen Sie den Metadatentyp **Objektgröße** aus und geben zwei Metadatenwerte an.

- Der erste Metadatenwert gibt Objekte an, die größer oder gleich 10 MB sind.
- Der zweite Metadatenwert gibt Objekte an, die kleiner als oder gleich 100 MB sind.

Durch die Verwendung mehrerer Einträge können Sie genau steuern, welche Objekte abgeglichen werden. Im folgenden Beispiel gilt die Regel für Objekte, die einen Brand A oder eine Marke B als Wert der Camera_type-Benutzermetadaten haben. Die Regel gilt jedoch nur für Objekte der Marke B, die kleiner als 10 MB sind.



Schritt 2 von 3: Definieren von Platzierungen

Im Schritt **Platzierungen definieren** des Assistenten zum Erstellen von ILM-Regeln können Sie die Platzierungsanweisungen definieren, die festlegen, wie lange Objekte gespeichert werden, welche Art von Kopien (repliziert oder Erasure codiert), den Speicherort und die Anzahl der Kopien.

Über diese Aufgabe

Eine ILM-Regel kann eine oder mehrere Anweisungen zur Platzierung enthalten. Jede Einstufungsanweisung gilt für einen einzelnen Zeitraum. Wenn Sie mehrere Befehle verwenden, müssen die Zeiträume zusammenhängend sein, und mindestens eine Anweisung muss am Tag 0 beginnen. Die Anweisungen können entweder für immer fortgesetzt werden oder bis Sie keine Objektkopien mehr benötigen.

Jede Anweisung für die Platzierung kann mehrere Zeilen haben, wenn Sie verschiedene Arten von Kopien erstellen oder verschiedene Standorte während dieses Zeitraums verwenden möchten.

In diesem Beispiel speichert die ILM-Regel eine replizierte Kopie an Standort 1 und eine replizierte Kopie am Standort 2 im ersten Jahr. Nach einem Jahr wird eine 2+1-Kopie mit Erasure-Coding-Verfahren an nur einem Standort erstellt und gespeichert.

Schritte

1. Wählen Sie unter **Referenzzeit** den Zeittyp aus, der bei der Berechnung der Startzeit für eine Platzierungsanweisung verwendet werden soll.

Option	Beschreibung
Aufnahmezeit	Die Zeit, zu der das Objekt aufgenommen wurde.
Zeitpunkt des letzten Zugriffs	Die Zeit, zu der das Objekt zuletzt abgerufen (gelesen oder angezeigt) wurde. **Hinweis:** um diese Option nutzen zu können, müssen die Updates für die Uhrzeit des letzten Zugriffs für den S3-Bucket oder Swift-Container aktiviert sein. Siehe "Verwenden Sie die letzte Zugriffszeit in ILM-Regeln".

Option	Beschreibung
Benutzerdefinierte Erstellungszeit	Eine in benutzerdefinierten Metadaten angegebene Zeit.
Nicht aktuelle Zeit	„`nicht aktuelle Zeit`“ wird automatisch ausgewählt, wenn Sie für die Frage „`Diese Regel nur auf ältere Objektversionen anwenden (in S3 Buckets mit aktivierter Versionierung)?`“ ausgewählt haben. Zoll "Schritt 1 des Assistenten zum Erstellen einer ILM-Regel".

Wenn Sie eine konforme Regel erstellen möchten, müssen Sie **Ingest Time** auswählen. Siehe "Objekte managen mit S3 Object Lock".

2. Geben Sie im Abschnitt **Zeitraum und Platzierungen** eine Startzeit und eine Dauer für den ersten Zeitraum ein.

   Sie können beispielsweise festlegen, wo Objekte für das erste Jahr gespeichert werden sollen (*von Tag 0 für 365 Tage*). Mindestens eine Anweisung muss am Tag 0 beginnen.

3. So erstellen Sie replizierte Kopien:
   a. Wählen Sie aus der Dropdown-Liste **Objekte speichern nach** die Option **Replizieren** aus.
   b. Wählen Sie die Anzahl der Kopien aus, die Sie erstellen möchten.

      Wenn Sie die Anzahl der Kopien in 1 ändern, wird eine Warnung angezeigt. Eine ILM-Regel, die immer nur eine replizierte Kopie erstellt, gefährdet Daten permanent. Siehe "Warum sollten Sie keine Replizierung mit nur einer Kopie verwenden".

      Um dieses Risiko zu vermeiden, führen Sie einen oder mehrere der folgenden Schritte aus:

      - Erhöhen Sie die Anzahl der Kopien für den Zeitraum.
      - Fügen Sie Kopien zu anderen Speicherpools oder zu einem Cloud-Speicherpool hinzu.
      - Wählen Sie **Erasure Coding** anstelle von **replizierung**.

        Sie können diese Warnung ohne Bedenken ignorieren, wenn diese Regel bereits mehrere Kopien für alle Zeiträume erstellt.

   c. Wählen Sie im Feld **copies at** die Speicherpools aus, die Sie hinzufügen möchten.

      Wenn Sie nur einen Speicherpool angeben, beachten Sie, dass StorageGRID nur eine replizierte Kopie eines Objekts auf einem beliebigen Speicherknoten speichern kann. Wenn Ihr Raster drei Storage-Nodes enthält und Sie 4 als Anzahl der Kopien auswählen, werden nur drei Kopien erstellt—eine Kopie für jeden Storage-Node.

      Die Warnung **ILM-Platzierung unerreichbar** wird ausgelöst, um anzuzeigen, dass die ILM-Regel nicht vollständig angewendet werden konnte.

      Wenn Sie mehr als einen Speicherpool angeben, beachten Sie folgende Regeln:

      - Die Anzahl der Kopien darf nicht größer sein als die Anzahl der Speicherpools.
      - Wenn die Anzahl der Kopien der Anzahl der Storage-Pools entspricht, wird in jedem Storage-Pool

eine Kopie des Objekts gespeichert.

- Wenn die Anzahl der Kopien geringer ist als die Anzahl der Storage-Pools, wird eine Kopie am Aufnahmeport gespeichert, und das System verteilt die restlichen Kopien, um die Festplattennutzung unter den Pools gleichmäßig zu halten. Dabei wird sichergestellt, dass kein Standort mehr als eine Kopie eines Objekts erhält.
- Wenn sich die Speicherpools überschneiden (die gleichen Storage-Nodes enthalten), werden möglicherweise alle Kopien des Objekts an nur einem Standort gespeichert. Geben Sie daher nicht den Speicherpool Alle Speicherknoten (StorageGRID 11.6 und früher) und einen anderen Speicherpool an.

4. Wenn Sie eine Kopie mit Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) erstellen möchten:
   a. Wählen Sie aus der Dropdown-Liste **Objekte speichern nach** die Option **Erasure Coding** aus.

      Das Verfahren zur Einhaltung von Datenkonsistenz eignet sich am besten für Objekte mit einer Größe von mehr als 1 MB. Verwenden Sie kein Erasure Coding für Objekte, die kleiner als 200 KB sind, um zu vermeiden, dass man sehr kleine Fragmente, die zur Fehlerkorrektur codiert wurden, managen muss.

   b. Wenn Sie keinen Filter für die Objektgröße für einen Wert größer als 0.2 MB hinzugefügt haben, wählen Sie **Zurück**, um zu Schritt 1 zurückzukehren. Wählen Sie dann **Erweiterten Filter hinzufügen** und setzen Sie einen **Objektgröße**-Filter auf einen Wert größer als 0.2 MB.
   c. Wählen Sie den Speicherpool aus, den Sie hinzufügen möchten, und das Erasure-Coding-Schema, das Sie verwenden möchten.

      Der Speicherort für eine Kopie, die nach der Fehlerkorrektur codiert wurde, enthält den Namen des Erasure Coding-Schemas und den Namen des Storage-Pools.

5. Optional:
   a. Wählen Sie **anderen Typ oder Speicherort hinzufügen**, um weitere Kopien an verschiedenen Standorten zu erstellen.
   b. Wählen Sie **weiteren Zeitraum hinzufügen**, um verschiedene Zeiträume hinzuzufügen.

      Objekte werden am Ende des Endzeitzeitraums automatisch gelöscht, es sei denn, der Endzeitraum endet mit **forever**.

6. Wenn Sie Objekte in einem Cloud-Speicherpool speichern möchten:
   a. Wählen Sie in der Dropdown-Liste **Objekte speichern nach Replizieren** aus.
   b. Wählen Sie das Feld **copies at** aus, und wählen Sie dann einen Cloud-Speicherpool aus.

      Beachten Sie bei der Verwendung von Cloud-Storage-Pools folgende Regeln:

      - Sie können nicht mehr als einen Cloud Storage-Pool in einer einzelnen Anweisung auswählen. Ebenso können Sie keinen Cloud-Storage-Pool und keinen Storage-Pool in derselben Anweisung auswählen.
      - Sie können nur eine Kopie eines Objekts in einem beliebigen Cloud Storage Pool speichern. Wenn Sie **Copies** auf 2 oder mehr setzen, wird eine Fehlermeldung angezeigt.
      - Es können nicht mehr als eine Objektkopie gleichzeitig in einem Cloud-Storage-Pool gespeichert werden. Eine Fehlermeldung wird angezeigt, wenn mehrere Platzierungen, die einen Cloud-Speicher-Pool verwenden, sich überschneidende Daten aufweisen oder wenn mehrere Zeilen

derselben Platzierung einen Cloud-Storage-Pool verwenden.

- Ein Objekt kann in einem Cloud-Storage-Pool gleichzeitig gespeichert werden, als replizierte oder als Erasure Coding-Kopie in StorageGRID. Sie müssen jedoch für den Zeitraum mehr als eine Zeile in die Platzierungsanweisung aufnehmen, damit Sie die Anzahl und die Typen der Kopien für jeden Speicherort angeben können.

7. Bestätigen Sie im Aufbewahrungsdiagramm Ihre Platzierungsanweisungen.

   Jede Zeile im Diagramm zeigt an, wo und wann Objektkopien platziert werden. Die Farbe einer Linie steht für den Kopiertyp:

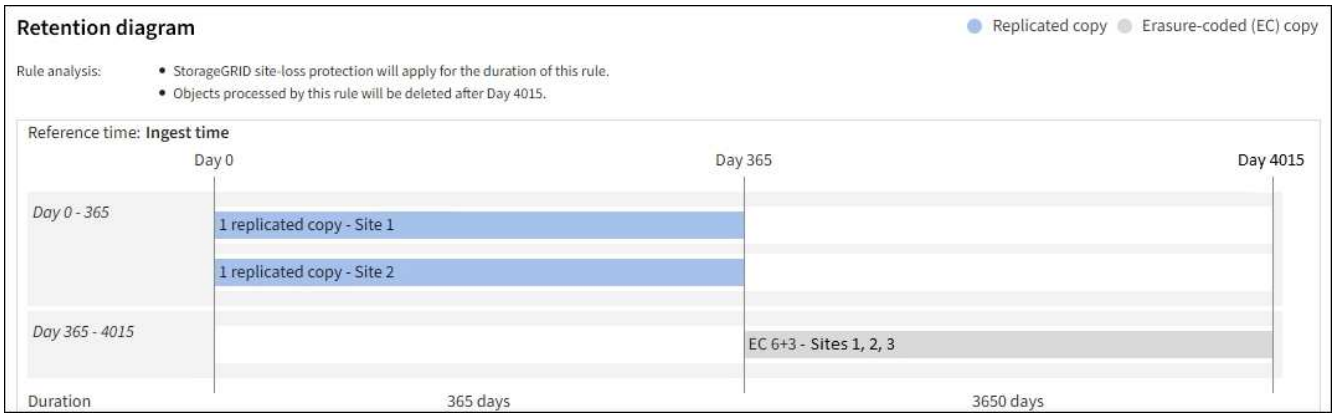
	Replizierte Kopie
	Kopie mit Erasure Coding – eine Kopie
	Cloud-Storage-Pool-Kopie

   In diesem Beispiel speichert die ILM-Regel eine replizierte Kopie an Standort 1 und eine replizierte Kopie am Standort 2 im ersten Jahr. Nach einem Jahr und für weitere 10 Jahre wird eine 6+3 Erasure-coded Kopie an drei Standorten gespeichert. Nach insgesamt 11 Jahren werden die Objekte aus StorageGRID gelöscht.

   Im Abschnitt Regelanalyse des Aufbewahrungsdiagramms steht Folgendes:

   - Für die Dauer dieser Regel gilt eine StorageGRID-Sicherung gegen vor-Ort-Verlust.
   - Durch diese Regel verarbeitete Objekte werden nach Tag 4015 gelöscht.

   Siehe "Schutz vor Standortausfällen"



8. Wählen Sie **Weiter**. "Schritt 3 (Aufnahmeverhalten auswählen)" Des Assistenten zum Erstellen einer ILM-Regel wird angezeigt.

Verwenden Sie die letzte Zugriffszeit in ILM-Regeln

Sie können die Uhrzeit des letzten Zugriffs als Referenzzeit in einer ILM-Regel verwenden. Sie möchten beispielsweise Objekte, die in den letzten drei Monaten auf lokalen Speicherknoten angezeigt wurden, während Sie Objekte verschieben, die noch nicht in letzter Zeit an einen externen Standort betrachtet wurden. Sie können die Uhrzeit

des letzten Zugriffs auch als erweiterten Filter verwenden, wenn eine ILM-Regel nur auf Objekte angewendet werden soll, auf die an einem bestimmten Datum zuletzt zugegriffen wurde.

Über diese Aufgabe

Bevor Sie die letzte Zugriffszeit in einer ILM-Regel verwenden, sollten Sie die folgenden Überlegungen durchgehen:

- Wenn Sie die Uhrzeit des letzten Zugriffs als Referenzzeit verwenden, beachten Sie, dass die Änderung der Uhrzeit des letzten Zugriffs für ein Objekt keine sofortige ILM-Bewertung auslöst. Stattdessen werden die Platzierungen des Objekts bewertet und das Objekt nach Bedarf verschoben, wenn im Hintergrund ILM das Objekt bewertet wird. Dies kann zwei Wochen oder länger dauern, nachdem auf das Objekt zugegriffen wurde.

  Berücksichtigen Sie diese Latenz bei der Erstellung von ILM-Regeln auf der Grundlage der letzten Zugriffszeit und vermeiden Sie Platzierungen, die kurze Zeiträume (weniger als einen Monat) verwenden.

- Wenn Sie die letzte Zugriffszeit als erweiterten Filter oder als Referenzzeit verwenden, müssen Sie die Updates der letzten Zugriffszeit für S3-Buckets aktivieren. Sie können das verwenden "Mandanten-Manager" Oder im "Mandantenmanagement-API".

  Updates der letzten Zugriffszeit sind immer für Swift Container aktiviert. Für S3 Buckets sind sie jedoch standardmäßig deaktiviert.

  Beachten Sie, dass eine Aktualisierung der letzten Zugriffszeit die Performance beeinträchtigen kann, insbesondere bei Systemen mit kleinen Objekten. Die Auswirkungen auf die Performance werden dadurch erzielt, dass StorageGRID die Objekte bei jedem Abruf mit neuen Zeitstempel aktualisieren muss.

In der folgenden Tabelle wird zusammengefasst, ob die Uhrzeit des letzten Zugriffs für alle Objekte im Bucket für verschiedene Arten von Anforderungen aktualisiert wird.

Art der Anfrage	Gibt an, ob die letzte Zugriffszeit aktualisiert wird, wenn die Updates der letzten Zugriffszeit deaktiviert sind	Gibt an, ob die letzte Zugriffszeit aktualisiert wird, wenn die Updates der letzten Zugriffszeit aktiviert sind
Anforderung zum Abrufen eines Objekts, seiner Zugriffssteuerungsliste oder seiner Metadaten	Nein	Ja.
Anforderung zum Aktualisieren der Metadaten eines Objekts	Ja.	Ja.
Anforderung zum Kopieren eines Objekts von einem Bucket in einen anderen	• Nein, für die Quellkopie • Ja, für die Zielkopie	• Ja, für die Quellkopie • Ja, für die Zielkopie

Art der Anfrage	Gibt an, ob die letzte Zugriffszeit aktualisiert wird, wenn die Updates der letzten Zugriffszeit deaktiviert sind	Gibt an, ob die letzte Zugriffszeit aktualisiert wird, wenn die Updates der letzten Zugriffszeit aktiviert sind
Anforderung zum Abschließen eines mehrteiligen Uploads	Ja, für das zusammengesetzte Objekt	Ja, für das zusammengesetzte Objekt

Schritt 3 von 3: Wählen Sie Ingest Behavior

Im Schritt **Einspielverhalten auswählen** des Assistenten zum Erstellen von ILM-Regeln können Sie festlegen, wie die von dieser Regel gefilterten Objekte bei der Aufnahme geschützt werden.

Über diese Aufgabe

StorageGRID erstellt Zwischenkopien und stellt die Objekte später zur ILM-Evaluierung in einen Warteschleife. Außerdem kann es Kopien erstellen, um sofort die Anweisungen zur Platzierung der Regel zu erfüllen.

Schritte

1. Wählen Sie die aus "Aufnahmeverhalten" Zu verwenden.

   Weitere Informationen finden Sie unter "Vorteile, Nachteile und Einschränkungen der Aufnahmsoptionen".

   > Sie können die Option „ausgeglichen“ oder „streng“ nicht verwenden, wenn die Regel eine dieser Platzierungen verwendet:
   >
   > - Ein Cloud-Storage-Pool am Tag 0
   > - Ein Archiv-Node am Tag 0
   > - Ein Cloud-Speicherpool oder ein Archivknoten, wenn die Regel eine benutzerdefinierte Erstellungszeit als Referenzzeit verwendet
   >
   > Siehe "Beispiel 5: ILM-Regeln und Richtlinie für striktes Ingest-Verhalten".

2. Wählen Sie **Erstellen**.

   Die ILM-Regel wird erstellt. Die Regel wird erst aktiv, wenn sie zu einem hinzugefügt wird "ILM-Richtlinie" Und diese Richtlinie ist aktiviert.

   Um die Details der Regel anzuzeigen, wählen Sie den Namen der Regel auf der Seite ILM-Regeln aus.

Erstellen einer Standard-ILM-Regel

Bevor Sie eine ILM-Richtlinie erstellen, müssen Sie eine Standardregel erstellen, um Objekte zu platzieren, die nicht mit einer anderen Regel in der Richtlinie übereinstimmt. Die Standardregel kann keine Filter verwenden. Die Lösung muss für alle Mandanten, alle Buckets und alle Objektversionen gelten.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".

- Sie haben spezifische Zugriffsberechtigungen.

Über diese Aufgabe

Die Standardregel ist die letzte Regel, die in einer ILM-Richtlinie evaluiert werden muss, sodass keine Filter verwendet werden können. Die Platzierungsanweisungen für die Standardregel werden auf alle Objekte angewendet, die nicht mit einer anderen Regel in der Richtlinie übereinstimmen.

In diesem Beispiel gilt die erste Regel nur für Objekte, die zu Test-Tenant-1 gehören. Die letzte Standardregel gilt für Objekte, die zu allen anderen Mandantenkonten gehören.

Beachten Sie beim Erstellen der Standardregel die folgenden Anforderungen:

- Die Standardregel wird automatisch als letzte Regel in der Richtlinie gesetzt.
- Die Standardregel kann keine einfachen oder erweiterten Filter verwenden.
- Die Standardregel muss auf alle Objektversionen angewendet werden.
- Die Standardregel sollte replizierte Kopien erstellen.

> Verwenden Sie keine Regel, die Kopien, die nach der Löschung codiert wurden, als Standardregel für eine Richtlinie erstellt. Für Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) sollte ein erweiterter Filter verwendet werden, um zu verhindern, dass bei kleineren Objekten die Codierung von Datenkonsistenz erfolgt.

- Im Allgemeinen sollte die Standardregel Objekte für immer aufbewahren.
- Wenn Sie die globale S3-Objektsperre verwenden (oder diese aktivieren möchten), muss die Standardregel für die aktive oder vorgeschlagene Richtlinie konform sein.

Schritte

1. Wählen Sie **ILM** > **Regeln**.

2. Wählen Sie **Erstellen**.

   Schritt 1 (Details eingeben) des Assistenten zum Erstellen von ILM-Regeln wird angezeigt.

3. Geben Sie einen eindeutigen Namen für die Regel in das Feld **Regelname** ein.
4. Geben Sie optional im Feld **Beschreibung** eine kurze Beschreibung für die Regel ein.
5. Lassen Sie das Feld **Tenant Accounts** leer.

   Die Standardregel muss auf alle Mandantenkonten angewendet werden.

6. Lassen Sie die Dropdown-Liste „Bucket Name“ als **Matches all** ausgewählt.

   Die Standardregel muss auf alle S3-Buckets und Swift-Container angewendet werden.

7. Behalten Sie die Standardantwort **Nein** für die Frage „`Diese Regel nur auf ältere Objektversionen anwenden (in S3 Buckets mit aktivierter Versionierung)?`“ bei.
8. Fügen Sie keine erweiterten Filter hinzu.

   Die Standardregel kann keine Filter angeben.

9. Wählen Sie **Weiter**.

   Schritt 2 (Platzierungen definieren) wird angezeigt.

10. Wählen Sie für Referenzzeit eine beliebige Option aus.

    Wenn Sie die Standardantwort **Nein** für die Frage beibehalten haben, “Diese Regel nur auf ältere Objektversionen anwenden?” Nicht aktuelle Zeit wird nicht in die Pulldown-Liste aufgenommen. Die Standardregel muss alle Objektversionen anwenden.

11. Legen Sie die Anweisungen für die Platzierung der Standardregel fest.
    - Die Standardregel sollte Objekte für immer aufbewahren. Wenn die Standardregel Objekte nicht dauerhaft enthält, wird eine Warnung angezeigt, wenn Sie eine neue Richtlinie aktivieren. Sie müssen bestätigen, dass dies das Verhalten ist, das Sie erwarten.
    - Die Standardregel sollte replizierte Kopien erstellen.

      > Verwenden Sie keine Regel, die Kopien, die nach der Löschung codiert wurden, als Standardregel für eine Richtlinie erstellt. Die Regeln für das Erasure Coding sollten den erweiterten Filter **Object size (MB) größer als 0.2** enthalten, um zu verhindern, dass kleinere Objekte Erasure Coded werden.

    - Wenn Sie die globale S3-Objektsperre verwenden (oder diese aktivieren möchten), muss die Standardregel konform sein:
      - Die IT muss mindestens zwei replizierte Objektkopien oder eine Kopie mit Verfahren zur Fehlerkorrektur erstellen.
      - Diese Kopien müssen auf Storage-Nodes während der gesamten Dauer jeder Zeile in der Plazierung vorhanden sein.
      - Objektkopien können nicht in einem Cloud-Storage-Pool gespeichert werden.
      - Objektkopien können nicht auf Archivknoten gespeichert werden.
      - Mindestens eine Zeile der Platzierungsanweisungen muss am Tag 0 beginnen, wobei die

Einspielzeit als Referenzzeit verwendet wird.

- Mindestens eine Zeile der Platzierungsanweisungen muss „`Forever`“ sein.

12. Sehen Sie sich das Aufbewahrungsdiagramm an, um Ihre Platzierungsanweisungen zu bestätigen.
13. Wählen Sie **Weiter**.

    Schritt 3 (Aufnahmeverhalten auswählen) wird angezeigt.

14. Wählen Sie die zu verwendende Ingest-Option und dann **Create**.

ILM-Richtlinie erstellen

Erstellen Sie eine ILM-Richtlinie: Überblick

Eine Information Lifecycle Management-Richtlinie (ILM) ist ein bestellter Satz von ILM-Regeln, die bestimmen, wie das StorageGRID System Objektdaten über einen längeren Zeitraum managt.

Bei der Erstellung einer ILM-Richtlinie wählen Sie zunächst die ILM-Regeln aus und ordnen sie an. Anschließend überprüfen Sie das Verhalten Ihrer vorgeschlagenen Richtlinie, indem Sie sie mit zuvor aufgenommenen Objekten simulieren. Wenn Sie damit zufrieden sind, dass die vorgeschlagene Richtlinie wie vorgesehen funktioniert, können Sie sie aktivieren, um die aktive Richtlinie zu erstellen.

> Eine falsch konfigurierte ILM-Richtlinie kann zu nicht wiederherstellbaren Datenverlusten führen. Prüfen Sie vor der Aktivierung einer ILM-Richtlinie die ILM-Richtlinie und ihre ILM-Regeln sorgfältig und simulieren Sie anschließend die ILM-Richtlinie. Vergewissern Sie sich immer, dass die ILM-Richtlinie wie vorgesehen funktioniert.

Standardmäßige ILM-Richtlinie

Wenn Sie StorageGRID installieren und Standorte hinzufügen, wird automatisch eine standardmäßige ILM-Richtlinie erstellt. Wenn Ihr Raster einen Standort enthält, enthält die Standardrichtlinie eine Standardregel, die zwei Kopien jedes Objekts an diesem Standort repliziert. Wenn Ihr Raster mehr als einen Standort enthält, repliziert die Standardregel eine Kopie jedes Objekts an jedem Standort.

Entspricht die Standardrichtlinie nicht Ihren Storage-Anforderungen, können Sie eigene Regeln und Richtlinien erstellen. Siehe "Was ist eine ILM-Regel" Und "Erstellen einer vorgeschlagenen ILM-Richtlinie".

Wie evaluiert eine ILM-Richtlinie Objekte?

Die aktive ILM-Richtlinie für Ihr StorageGRID System steuert die Platzierung, Dauer und Datensicherung aller Objekte.

Wenn Clients Objekte in StorageGRID speichern, werden die Objekte anhand der bestellten ILM-Regeln in der aktiven Richtlinie bewertet:

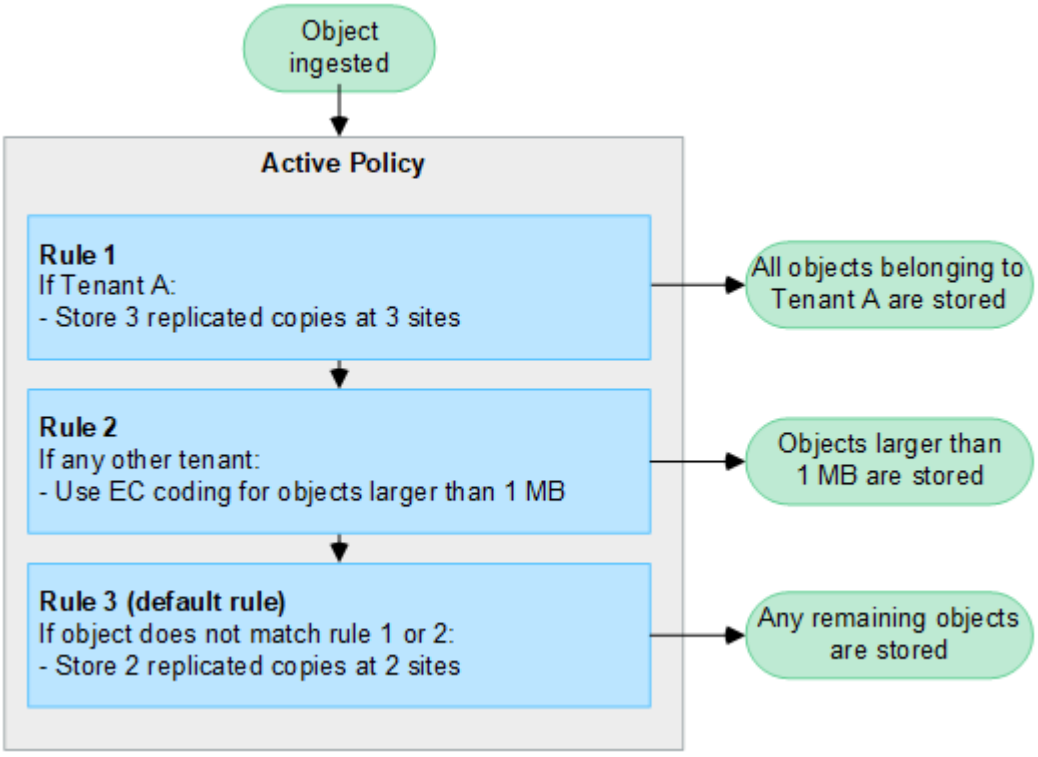
1. Wenn die Filter für die erste Regel in der Richtlinie mit einem Objekt übereinstimmen, wird das Objekt gemäß dem Aufnahmeverhalten der Regel aufgenommen und gemäß den Anweisungen zur Platzierung dieser Regel gespeichert.
2. Wenn die Filter für die erste Regel nicht mit dem Objekt übereinstimmen, wird das Objekt anhand jeder nachfolgenden Regel in der Richtlinie bewertet, bis eine Übereinstimmung vorgenommen wird.
3. Stimmen keine Regeln mit einem Objekt überein, werden das Aufnahmeverhalten und die Anweisungen

zur Platzierung der Standardregel in der Richtlinie angewendet. Die Standardregel ist die letzte Regel in einer Richtlinie. Die Standardregel muss für alle Mandanten, alle Buckets und alle Objektversionen gelten und kann keine erweiterten Filter verwenden.

Beispiel für eine ILM-Richtlinie

Eine ILM-Richtlinie könnte beispielsweise drei ILM-Regeln enthalten, die Folgendes angeben:

- **Regel 1: Replizierte Kopien für Mandant A**
  - Alle Objekte, die zu Mandant A gehören, abgleichen
  - Speichern Sie diese Objekte als drei replizierte Kopien an drei Standorten.
  - Objekte, die zu anderen Mandanten gehören, werden nicht mit Regel 1 abgeglichen, daher werden sie mit Regel 2 verglichen.
- **Regel 2: Erasure Coding für Objekte größer als 1 MB**
  - Alle Objekte von anderen Mandanten abgleichen, aber nur, wenn sie größer als 1 MB sind. Diese größeren Objekte werden mithilfe von 6+3 Erasure Coding an drei Standorten gespeichert.
  - Entspricht nicht Objekten mit einer Größe von 1 MB oder weniger, daher werden diese Objekte mit Regel 3 verglichen.
- **Regel 3: 2 Exemplare 2 Rechenzentren** (Standard)
  - Ist die letzte und Standardregel in der Richtlinie. Verwendet keine Filter.
  - Erstellen Sie zwei replizierte Kopien aller Objekte, die nicht mit Regel 1 oder Regel 2 übereinstimmen (Objekte, die nicht zu Mandant A gehören und mindestens 1 MB groß sind).



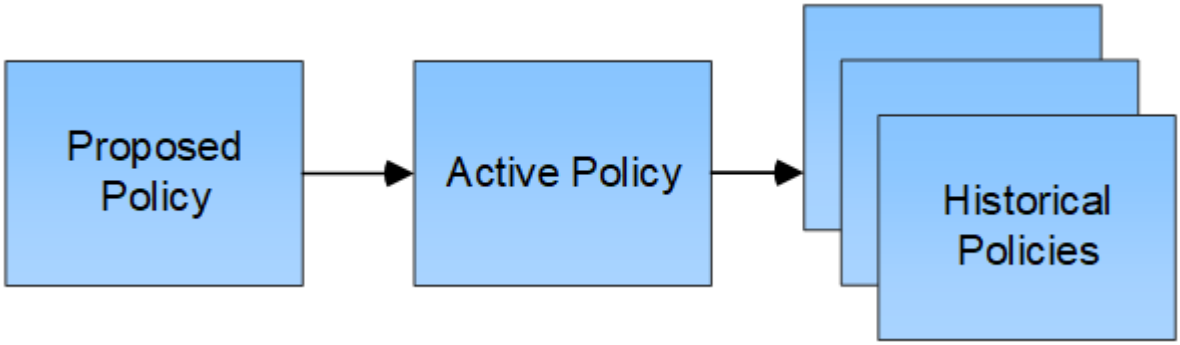
Was sind vorgeschlagene, aktive und historische Politiken?

Jedes StorageGRID System muss über eine aktive ILM-Richtlinie verfügen. Ein StorageGRID System kann auch über eine vorgeschlagene ILM-Richtlinie und eine beliebige Anzahl an historischen Richtlinien verfügen.

Beim ersten Erstellen einer ILM-Richtlinie erstellen Sie eine vorgeschlagene Richtlinie, indem Sie eine oder mehrere ILM-Regeln auswählen und in einer bestimmten Reihenfolge anordnen. Nachdem Sie die vorgeschlagene Richtlinie simuliert haben, um ihr Verhalten zu bestätigen, aktivieren Sie sie, um die aktive Richtlinie zu erstellen.

Bei der Aktivierung einer neuen ILM-Richtlinie verwendet StorageGRID diese Richtlinie, um alle Objekte, einschließlich vorhandener Objekte und neu aufgenommener Objekte, zu managen. Vorhandene Objekte können an neue Standorte verschoben werden, wenn die ILM-Regeln der neuen Richtlinie implementiert werden.

Die Aktivierung der vorgeschlagenen Richtlinie führt dazu, dass die zuvor aktive Richtlinie zu einer historischen Politik wird. Historische ILM-Richtlinien können nicht gelöscht werden.



Überlegungen bei der Erstellung einer ILM-Richtlinie

- Verwenden Sie die vom System bereitgestellte Richtlinie, Richtlinie für Baseline 2 Kopien, nur in Testsystemen. Für StorageGRID 11.6 und frühere Versionen verwendet die Regel 2 Kopien erstellen in dieser Richtlinie den Speicherpool Alle Speicherknoten, der alle Standorte enthält. Wenn Ihr StorageGRID System über mehrere Standorte verfügt, können zwei Kopien eines Objekts an demselben Standort platziert werden.

> Der Speicherpool Alle Speicherknoten wird automatisch während der Installation von StorageGRID 11.6 und früher erstellt. Wenn Sie ein Upgrade auf eine höhere Version von StorageGRID durchführen, ist der Pool Alle Storage-Nodes weiterhin vorhanden. Wenn Sie StorageGRID 11.7 oder höher als neue Installation installieren, wird der Pool Alle Speicherknoten nicht erstellt.

- Berücksichtigen Sie beim Entwurf einer neuen Richtlinie alle unterschiedlichen Objekttypen, die in das Grid aufgenommen werden können. Stellen Sie sicher, dass die Richtlinie Regeln enthält, die mit diesen Objekten übereinstimmen und sie nach Bedarf platziert werden können.
- Halten Sie die ILM-Richtlinie so einfach wie möglich. Dadurch werden potenziell gefährliche Situationen vermieden, in denen Objektdaten nicht wie vorgesehen geschützt werden, wenn im Laufe der Zeit Änderungen am StorageGRID System vorgenommen werden.
- Stellen Sie sicher, dass die Regeln in der Richtlinie in der richtigen Reihenfolge sind. Wenn die Richtlinie aktiviert ist, werden neue und vorhandene Objekte anhand der Regeln in der angegebenen Reihenfolge bewertet, die oben beginnen. Wenn z. B. die erste Regel in einer Richtlinie mit einem Objekt übereinstimmt, wird dieses Objekt nicht von einer anderen Regel bewertet.
- Die letzte Regel in jeder ILM-Richtlinie ist die standardmäßige ILM-Regel, die keine Filter verwenden kann. Wenn ein Objekt nicht mit einer anderen Regel übereinstimmt, steuert die Standardregel, wo das Objekt platziert wird und wie lange es aufbewahrt wird.
- Überprüfen Sie vor der Aktivierung einer neuen Richtlinie alle Änderungen, die die Richtlinie an der Platzierung vorhandener Objekte vornimmt. Das Ändern des Speicherorts eines vorhandenen Objekts

kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

Erstellen einer vorgeschlagenen ILM-Richtlinie

Sie können eine vorgeschlagene ILM-Richtlinie von Grund auf erstellen oder die aktuelle aktive Richtlinie klonen, wenn Sie mit demselben Regelsatz beginnen möchten.

Bevor Sie eine eigene Richtlinie erstellen, überprüfen Sie, ob die "Standardmäßige ILM-Richtlinie" Erfüllt Ihre Storage-Anforderungen nicht.

> Wenn der "Die Einstellung für die globale S3-Objektsperre wurde aktiviert", Sie müssen sicherstellen, dass die ILM-Richtlinie den Anforderungen von Buckets entspricht, für die S3 Object Lock aktiviert ist. Befolgen Sie in diesem Abschnitt die Anweisungen, die erwähnen, dass S3 Object Lock aktiviert ist.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Erforderliche Zugriffsberechtigungen".
- Das ist schon "ILM-Regeln wurden erstellt" Basierend darauf, ob S3 Object Lock aktiviert ist.

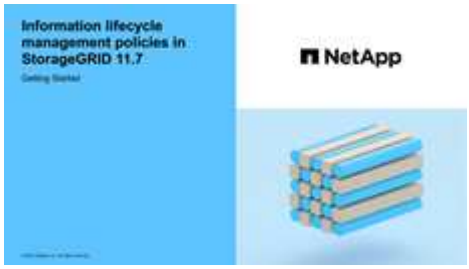
S3 Objektsperre nicht aktiviert

- Das ist schon "ILM-Regeln erstellt" Sie möchten der vorgeschlagenen Richtlinie hinzufügen. Bei Bedarf können Sie eine vorgeschlagene Richtlinie speichern, zusätzliche Regeln erstellen und die vorgeschlagene Richtlinie bearbeiten, um die neuen Regeln hinzuzufügen.
- Das ist schon "Eine Standard-ILM-Regel wurde erstellt" Das keine Filter enthält.

S3-Objektsperre aktiviert

- Der "Die Einstellung für die globale S3-Objektsperre ist bereits aktiviert" Für das StorageGRID-System.
- Das ist schon "Erstellung der konformen und nicht konformen ILM-Regeln" Sie möchten der vorgeschlagenen Richtlinie hinzufügen. Bei Bedarf können Sie eine vorgeschlagene Richtlinie speichern, zusätzliche Regeln erstellen und die vorgeschlagene Richtlinie bearbeiten, um die neuen Regeln hinzuzufügen.
- Das ist schon "Eine Standard-ILM-Regel wurde erstellt" Für die Richtlinie, die konform ist.

- Optional haben Sie sich das Video angesehen: "Video: Information Lifecycle Management Policies in StorageGRID 11.7"



Siehe auch "Erstellen Sie eine ILM-Richtlinie: Überblick".

Über diese Aufgabe

Typische Gründe für die Erstellung einer vorgeschlagenen ILM-Richtlinie sind:

- Sie haben einen neuen Standort hinzugefügt und müssen neue ILM-Regeln verwenden, um Objekte an diesem Standort zu platzieren.
- Sie müssen einen Standort stilllegen und alle ILM-Regeln entfernen, die sich auf den Standort beziehen.
- Sie haben einen neuen Mandanten mit besonderen Anforderungen an die Datensicherheit hinzugefügt.
- Sie haben damit begonnen, einen Cloud-Storage-Pool zu verwenden.

> Verwenden Sie die vom System bereitgestellte Richtlinie, Richtlinie für Baseline 2 Kopien, nur in Testsystemen. Für StorageGRID 11.6 und früher verwendet die Standardregel in dieser Richtlinie den Speicherpool Alle Speicherknoten, der alle Standorte enthält. Wenn Ihr StorageGRID System über mehrere Standorte verfügt, können zwei Kopien eines Objekts an demselben Standort platziert werden.

Schritte

1. Wählen Sie **ILM** > **Richtlinien**.

   Wenn die globale S3 Object Lock-Einstellung aktiviert ist, gibt die Seite ILM-Richtlinien an, welche ILM-Regeln konform sind.

2. Legen Sie fest, wie Sie die vorgeschlagene ILM-Richtlinie erstellen möchten.

Beginnen Sie von vorne

1. Wenn derzeit eine vorgeschlagene ILM-Richtlinie vorhanden ist, wählen Sie **vorgeschlagene Richtlinie** > **Aktionen** > **Entfernen** aus.

   Sie können keine neue vorgeschlagene Richtlinie erstellen, wenn bereits eine vorgeschlagene Richtlinie vorhanden ist.

2. Wählen Sie **vorgeschlagene Richtlinie erstellen** > **Neue Richtlinie erstellen**.

Beginnen Sie mit Regeln aus der aktiven Richtlinie

1. Wenn derzeit eine vorgeschlagene ILM-Richtlinie vorhanden ist, wählen Sie **vorgeschlagene Richtlinie** > **Aktionen** > **Entfernen** aus.

   Sie können die aktive Richtlinie nicht klonen, wenn bereits eine vorgeschlagene Richtlinie vorhanden ist.

2. Wählen Sie **vorgeschlagene Richtlinie erstellen** > **aktive Richtlinie klonen**.

Vorhandene vorgeschlagene Richtlinie bearbeiten

1. Wählen Sie **vorgeschlagene Richtlinie** > **Aktionen** > **Bearbeiten**.

1. Geben Sie im Feld **vorgeschlagener Richtlinienname** einen eindeutigen Namen für die vorgeschlagene Richtlinie ein.
2. Geben Sie im Feld **Grund für Änderung** den Grund ein, aus dem Sie eine neue vorgeschlagene Richtlinie erstellen.
3. Um der Richtlinie Regeln hinzuzufügen, wählen Sie **Regeln auswählen**. Wählen Sie einen Regelnamen

aus, um die Einstellungen für diese Regel anzuzeigen.

> In regelmäßigen Abständen wird die Liste der Regeln automatisch aktualisiert, um Hinzufügungen oder Entnahmen zu berücksichtigen. Wenn eine Regel entfernt wird, nachdem Sie sie ausgewählt haben, wird eine Fehlermeldung angezeigt.

Beim Klonen einer Richtlinie:

- Die von der Richtlinie, die Sie klonen, verwendeten Regeln sind ausgewählt.
- Wenn die Richtlinie, die Sie klonen, Regeln ohne Filter verwendet hat, die nicht die Standardregel waren, werden Sie aufgefordert, alle Regeln außer einer dieser Regeln zu entfernen.
- Wenn die Standardregel einen Filter verwendet hat, werden Sie aufgefordert, eine neue Standardregel auszuwählen.
- Wenn die Standardregel nicht die letzte Regel war, können Sie die Regel an das Ende der neuen Richtlinie verschieben.

S3 Objektsperre nicht aktiviert

1. Wählen Sie eine Standardregel für die vorgeschlagene Richtlinie aus. Um eine neue Standardregel zu erstellen, wählen Sie **ILM-Regelseite** aus.

   Die Standardregel gilt für alle Objekte, die nicht mit einer anderen Regel in der Richtlinie übereinstimmen. Die Standardregel kann keine Filter verwenden und wird immer zuletzt ausgewertet.

   > Verwenden Sie nicht die Regel 2 Kopien erstellen als Standardregel für eine Richtlinie. Die Regel 2 Kopien erstellen verwendet einen einzelnen Speicherpool, alle Speicherknoten, der alle Standorte enthält. Wenn Ihr StorageGRID System über mehrere Standorte verfügt, können zwei Kopien eines Objekts an demselben Standort platziert werden.

S3-Objektsperre aktiviert

1. Wählen Sie eine Standardregel für die vorgeschlagene Richtlinie aus. Um eine neue Standardregel zu erstellen, wählen Sie **ILM-Regelseite** aus.

   Die Liste der Regeln enthält nur die Regeln, die konform sind und keine Filter verwenden.

   > Verwenden Sie nicht die Regel 2 Kopien erstellen als Standardregel für eine Richtlinie. Die Regel 2 Kopien erstellen verwendet einen einzelnen Speicherpool, alle Speicherknoten, der alle Standorte enthält. Wenn Sie diese Regel verwenden, können mehrere Kopien eines Objekts auf demselben Standort platziert werden.

2. Wenn Sie eine andere “default”-Regel für Objekte in nicht konformen S3-Buckets benötigen, wählen Sie **eine Regel ohne Filter für nicht konforme S3-Buckets** aus und wählen Sie eine nicht konforme Regel aus, die keinen Filter verwendet.

   Sie können beispielsweise einen Cloud-Storage-Pool verwenden, um Objekte in Buckets zu speichern, für die die S3-Objektsperre nicht aktiviert ist.

   > Sie können nur eine nicht kompatible Regel auswählen, die keinen Filter verwendet.

Siehe auch "Beispiel 7: Konforme ILM-Richtlinie für S3 Object Lock".

1. Wenn Sie mit der Auswahl der Standardregel fertig sind, wählen Sie **Weiter**.
2. Wählen Sie für den Schritt andere Regeln alle anderen Regeln aus, die Sie der Richtlinie hinzufügen möchten. Diese Regeln verwenden mindestens einen Filter (Mandantenkonto, Bucket-Name, erweiterter Filter oder nicht aktuelle Referenzzeit). Wählen Sie dann **Select**.

   Im Fenster vorgeschlagene Richtlinie erstellen werden nun die ausgewählten Regeln aufgelistet. Die Standardregel ist am Ende, mit den anderen Regeln darüber.

   Wenn S3 Object Lock aktiviert ist und Sie außerdem eine nicht konforme Regel „`default`“ ausgewählt haben, wird diese Regel als die zweitrangige Regel in der Richtlinie hinzugefügt.

Eine Warnung wird angezeigt, wenn eine Regel Objekte nicht für immer behält. Wenn Sie diese Richtlinie aktivieren, müssen Sie bestätigen, dass StorageGRID Objekte löschen soll, wenn die Platzierungsanweisungen für die Standardregel abgelaufen sind (es sei denn, ein Bucket-Lebenszyklus hält die Objekte für einen längeren Zeitraum).

3. Ziehen Sie die Zeilen für die nicht standardmäßigen Regeln, um die Reihenfolge zu bestimmen, in der diese Regeln ausgewertet werden.

   Sie können die Standardregel nicht verschieben. Wenn S3 Object Lock aktiviert ist, können Sie die nicht konforme Regel „`default`“ auch nicht verschieben, wenn eine ausgewählt wurde.

   Sie müssen sich vergewissern, dass die ILM-Regeln in der richtigen Reihenfolge sind. Wenn die Richtlinie aktiviert ist, werden neue und vorhandene Objekte anhand der Regeln in der angegebenen Reihenfolge bewertet, die oben beginnen.

4. Wählen Sie bei Bedarf **Regeln auswählen**, um Regeln hinzuzufügen oder zu entfernen.
5. Wenn Sie fertig sind, wählen Sie **Speichern**.
6. Gehen Sie zu "Simulation einer ILM-Richtlinie". Sie sollten eine vorgeschlagene Richtlinie immer simulieren, bevor Sie sie aktivieren, um sicherzustellen, dass sie wie erwartet funktioniert.

Simulation einer ILM-Richtlinie

Simulieren Sie eine vorgeschlagene Richtlinie für Testobjekte, bevor Sie die Richtlinie aktivieren und auf Ihre Produktionsdaten anwenden. Das Simulationsfenster bietet eine eigenständige Umgebung, die zum Testen von Richtlinien sicher ist, bevor sie aktiviert und auf Daten in der Produktionsumgebung angewendet werden.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die "Erforderliche Zugriffsberechtigungen".
- Für jedes zu testende Objekt ist der S3-Bucket/Objektschlüssel oder der Swift-Container-/Objektname bekannt.

Über diese Aufgabe

Wählen Sie sorgfältig die Objekte aus, die die vorgeschlagene Richtlinie testen soll. Um eine Richtlinie gründlich zu simulieren, sollten Sie mindestens ein Objekt für jeden Filter in jeder Regel testen.

Wenn eine Richtlinie beispielsweise eine Regel enthält, mit der Objekte in Bucket A und eine andere Regel übereinstimmen, um Objekte in Bucket B zu entsprechen, müssen Sie mindestens ein Objekt aus Bucket A und ein Objekt aus Bucket B auswählen, um die Richtlinie gründlich zu testen. Sie müssen außerdem mindestens ein Objekt aus einem anderen Bucket auswählen, um die Standardregel zu testen.

Bei der Simulation einer Richtlinie gelten folgende Überlegungen:

- Nachdem Sie Änderungen an einer Richtlinie vorgenommen haben, speichern Sie die vorgeschlagene Richtlinie. Dann simulieren Sie das Verhalten der gespeicherten vorgeschlagenen Richtlinie.
- Wenn Sie eine Richtlinie simulieren, filtern die ILM-Regeln in der Richtlinie die Testobjekte ab, sodass Sie sehen können, welche Regel auf jedes Objekt angewendet wurde. Es werden jedoch keine Objektkopien erstellt und keine Objekte abgelegt. Wenn Sie eine Simulation ausführen, ändern Sie Ihre Daten, Regeln oder Richtlinien in keiner Weise.

- Das Fenster vorgeschlagene Richtlinie simulieren behält die getesteten Objekte bei, bis Sie entweder **Alle löschen** oder das Symbol entfernen auswählen ✕ Für jedes Objekt in der Liste Simulationsergebnisse.
- Simulation gibt den Namen der übereinstimmenden Regel zurück. Um zu ermitteln, welches Profil für den Speicherpool oder die Erasure Coding-Funktion verwendet wird, wählen Sie den Namen der Regel aus, um auf die Seite mit den Regeldetails zu gelangen. Dort können Sie das Aufbewahrungsdiagramm sowie weitere Details zur Regel anzeigen.
- Wenn die S3-Versionierung aktiviert ist, können Sie die Versions-ID für die Version des Objekts eingeben, das Sie für die Simulation verwenden möchten.

Schritte

1. "Erstellen Sie eine vorgeschlagene Richtlinie".
2. Verwenden eines S3- oder Swift-Clients oder des "Experimentelle S3 Konsole", Die im Tenant Manager für jeden Mandanten verfügbar ist, geben Sie die Objekte ein, die zum Testen jeder Regel erforderlich sind.
3. Wählen Sie auf der ILM-Richtlinienseite, Registerkarte vorgeschlagene Richtlinie, **Simulate** aus.
4. Geben Sie im Feld **Objekt** das S3 ein `bucket/object-key` Oder den Swift `container/object-name` Für ein Testobjekt. Beispiel: `bucket-01/filename.png`.
5. Geben Sie optional eine Versions-ID für das Objekt in das Feld **Versions-ID** ein.
6. Wählen Sie **Simulieren**.
7. Bestätigen Sie im Abschnitt Simulationsergebnisse, dass jedes Objekt mit der richtigen Regel abgeglichen wurde.

Beispiel 1: Überprüfung der Regeln bei der Simulation einer vorgeschlagenen ILM-Richtlinie

In diesem Beispiel wird beschrieben, wie Regeln bei der Simulation einer vorgeschlagenen Richtlinie überprüft werden.

In diesem Beispiel wird die **Beispiel ILM-Richtlinie** für die aufgenommene Objekte in zwei Buckets simuliert. Die Richtlinie umfasst drei Regeln:

- Die erste Regel, **zwei Kopien, zwei Jahre für Eimer-A**, gilt nur für Objekte in Eimer-a.
- Die zweite Regel, **EC-Objekte > 1 MB**, gilt für alle Buckets, aber für Filter auf Objekten größer als 1 MB.
- Die dritte Regel, **zwei Kopien, zwei Rechenzentren**, ist die Standardregel. Er enthält keine Filter und verwendet keine nicht aktuelle Referenzzeit.

Bestätigen Sie nach der Simulation der Richtlinie, dass jedes Objekt mit der richtigen Regel abgeglichen wurde.

In diesem Beispiel:

- `bucket-a/bucket-a object.pdf` Die erste Regel, die nach Objekten in filtert, wurde richtig zugeordnet `bucket-a`.
- `bucket-b/test object greater than 1 MB.pdf` Ist in `bucket-b`, So dass es nicht mit der ersten Regel. Stattdessen wurde sie durch die zweite Regel korrekt abgeglichen, die nach Objekten mit einer Größe von mehr als 1 MB filtert.
- `bucket-b/test object less than 1 MB.pdf` Stimmt nicht mit den Filtern in den ersten beiden Regeln überein, so wird sie durch die Standardregel platziert, die keine Filter enthält.

Beispiel 2: Neuanordnung von Regeln bei der Simulation einer vorgeschlagenen ILM-Richtlinie

Dieses Beispiel zeigt, wie Sie Regeln neu anordnen können, um die Ergebnisse bei der Simulation einer Richtlinie zu ändern.

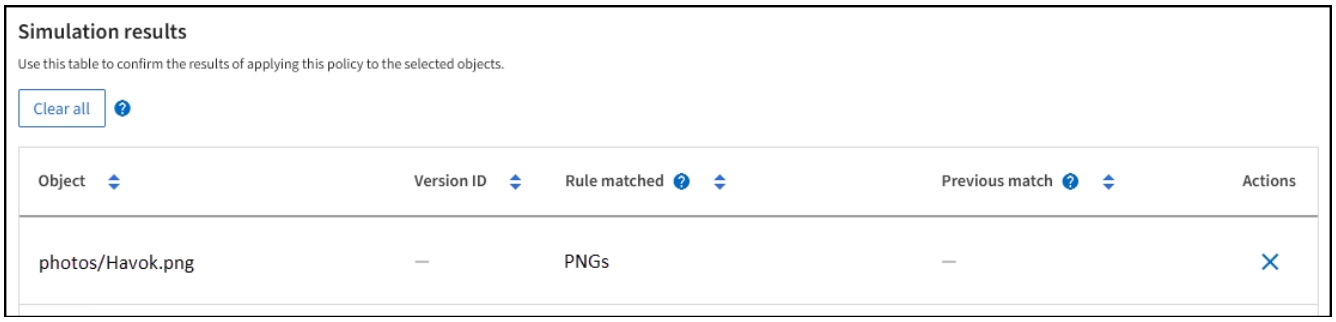
In diesem Beispiel wird die **Demo**-Richtlinie simuliert. Diese Richtlinie, die zum Auffinden von Objekten mit Metadaten für Benutzer der Serie=x-men bestimmt ist, enthält drei Regeln:

- Die erste Regel, **PNGs**, filtert nach Schlüsselnamen, die enden `.png`.
- Die zweite Regel, **X-Men**, gilt nur für Objekte für Mieter A und Filter für `series=x-men` Benutzer-Metadaten:
- Die letzte Regel, **two copies two Data Centers**, ist die Standardregel, die allen Objekten entspricht, die nicht den ersten beiden Regeln entsprechen.

Schritte

1. Nachdem Sie die Regeln hinzugefügt und die Richtlinie gespeichert haben, wählen Sie **Simulieren**.
2. Geben Sie im Feld **Object** den S3-Bucket/Object-Key oder den Swift-Container/Object-Name für ein Testobjekt ein und wählen Sie **Simulate** aus.

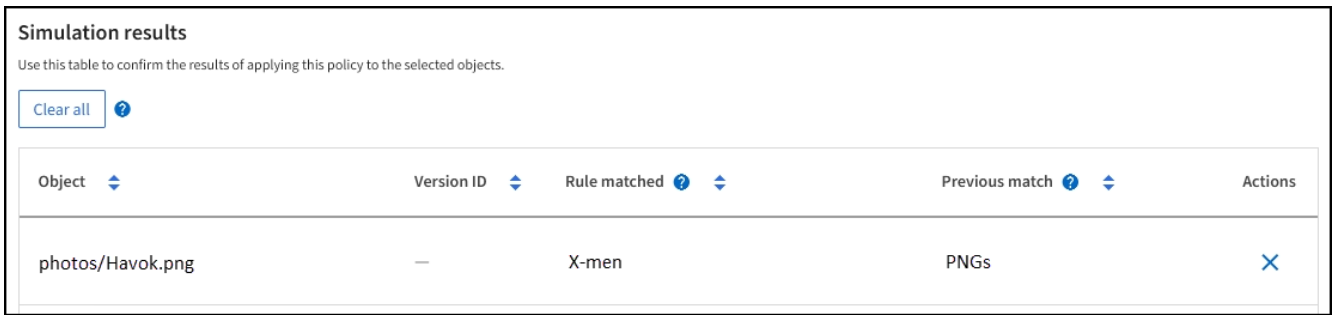
   Die Simulationsergebnisse werden angezeigt und zeigen an, dass der `Havok.png` Das Objekt wurde durch die **PNGs**-Regel abgeglichen.



Jedoch `Havok.png` Sollte die **X-Men**-Regel testen.

3. Um das Problem zu lösen, ordnen Sie die Regeln neu an.
   a. Wählen Sie **Finish**, um das Fenster ILM-Richtlinie simulieren zu schließen.
   b. Wählen Sie **actions** > **Edit**, um die Richtlinie zu bearbeiten.
   c. Ziehen Sie die **X-Men**-Regel an den Anfang der Liste.
   d. Wählen Sie **Speichern**.
4. Wählen Sie **Simulieren**.

   Die zuvor getesteten Objekte werden anhand der aktualisierten Richtlinie neu bewertet und die neuen Simulationsergebnisse angezeigt. In dem Beispiel zeigt die Spalte „Regelabgleichung“, dass der `Havok.png` Das Objekt entspricht jetzt wie erwartet der X-Men-Metadatenregel. In der Spalte Vorheriger Abgleich wird angezeigt, dass die PNGs-Regel mit dem Objekt in der vorherigen Simulation übereinstimmt.

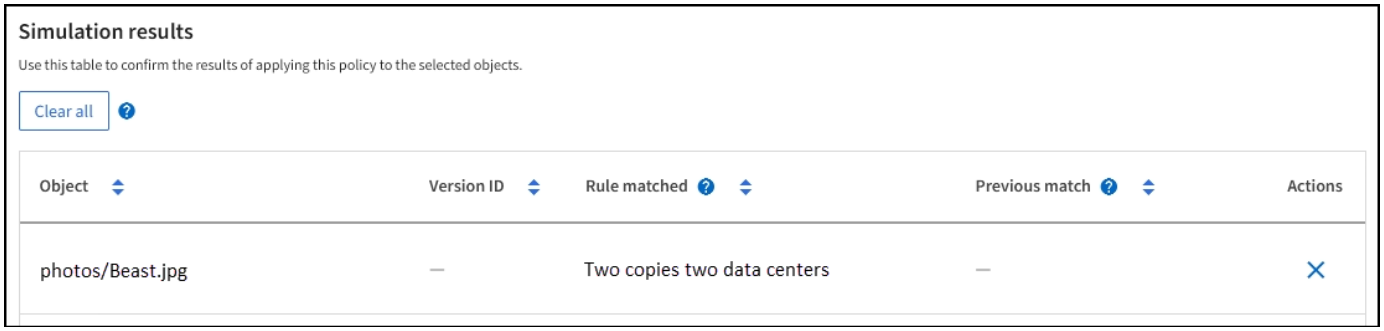


Wenn Sie auf der Registerkarte vorgeschlagene Richtlinie bleiben, können Sie eine Richtlinie neu simulieren, nachdem Sie Änderungen vorgenommen haben, ohne die Namen der Testobjekte erneut eingeben zu müssen.

Beispiel 3: Korrigieren Sie eine Regel bei der Simulation einer vorgeschlagenen ILM-Richtlinie

Dieses Beispiel zeigt, wie eine Richtlinie simuliert, eine Regel in der Richtlinie korrigiert und die Simulation fortgesetzt wird.

In diesem Beispiel wird die **Demo**-Richtlinie simuliert. Diese Richtlinie dient zum Suchen von Objekten, die über solche verfügen `series=x-men` Benutzer-Metadaten: Bei der Simulation dieser Richtlinie gegen die traten jedoch unerwartete Ergebnisse auf `Beast.jpg` Objekt: Anstatt die X-Men-Metadatenregel zu entsprechen, kopiert das Objekt die Standardregel. Zwei Rechenzentren werden kopiert.



Wenn ein Testobjekt nicht mit der erwarteten Regel in der Richtlinie übereinstimmt, müssen Sie jede Regel in der Richtlinie überprüfen und eventuelle Fehler korrigieren.

Schritte

1. Wählen Sie **Fertig**, um das Dialogfeld Richtlinie simulieren zu schließen. Wählen Sie auf der Registerkarte vorgeschlagene Richtlinie **Aufbewahrungsdiagramm** aus. Wählen Sie dann **Alle erweitern** oder **Details anzeigen** für jede Regel nach Bedarf aus.
2. Prüfen Sie das Mandantenkonto der Regel, die Referenzzeit und die Filterkriterien.

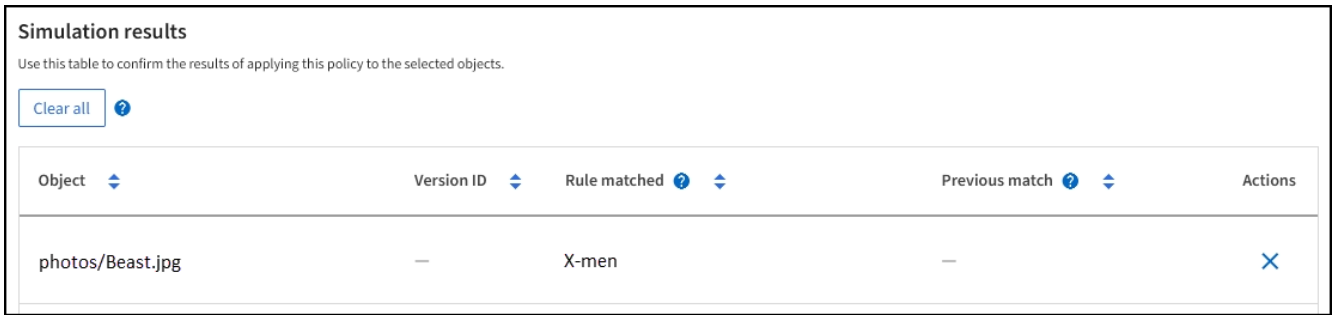
   Angenommen, die Metadaten für die X-men-Regel wurden als „`x-men01`“ anstelle von „`x-men`“ `eingegeben.`“
3. Um den Fehler zu beheben, korrigieren Sie die Regel wie folgt:
   - Wenn die Regel Teil der vorgeschlagenen Richtlinie ist, können Sie entweder die Regel klonen oder die Regel aus der Richtlinie entfernen und sie dann bearbeiten.
   - Wenn die Regel Teil der aktiven Richtlinie ist, müssen Sie die Regel klonen. Sie können keine Regel aus der aktiven Richtlinie bearbeiten oder entfernen.

Option	Schritte
Die Regel klonen	i. Wählen Sie **ILM** > **Regeln**. ii. Wählen Sie die falsche Regel aus, und wählen Sie **Clone**. iii. Geben Sie einen Namen für die neue Regel ein, ändern Sie dann die falschen Informationen und wählen Sie **Create**. iv. Wählen Sie **ILM** > **Richtlinien** > **vorgeschlagene Richtlinie** aus. v. Wählen Sie **Actions** > **Edit**. vi. Wählen Sie **Regeln auswählen**, und wählen Sie dann **Weiter**, um dieselbe Standardregel zu akzeptieren. vii. Aktivieren Sie im Schritt andere Regeln auswählen das Kontrollkästchen für die neue Regel, deaktivieren Sie das Kontrollkästchen für die ursprüngliche Regel und wählen Sie **Auswählen**. viii. Ordnen Sie die Regeln bei Bedarf neu an, indem Sie die neue Regel an die richtige Stelle ziehen. ix. Wählen Sie **Speichern**.

Option	Schritte
Bearbeiten Sie die Regel	i. Wählen Sie **ILM** > **Richtlinien** > **vorgeschlagene Richtlinie** und entfernen Sie die Regel, die Sie bearbeiten möchten. ii. Wählen Sie **ILM** > **Regeln**. iii. Wählen Sie die Regel aus, die Sie bearbeiten möchten, und wählen Sie **Bearbeiten**. Oder aktivieren Sie das Kontrollkästchen für die Regel und wählen Sie **Aktionen** > **Bearbeiten**. iv. Ändern Sie die falschen Informationen für jeden Teil des Assistenten, und wählen Sie dann **Update**. v. Wählen Sie **ILM** > **Richtlinien** > **vorgeschlagene Richtlinie** aus. vi. Wählen Sie **Actions** > **Edit**. vii. Wählen Sie **Regeln auswählen**, und wählen Sie dann **Weiter**, um dieselbe Standardregel zu akzeptieren. viii. Aktivieren Sie im Dialogfeld andere Regeln auswählen das Kontrollkästchen für die korrigierte Regel, wählen Sie **Auswählen** und dann **Speichern**. ix. Ziehen Sie die Zeilen für die nicht standardmäßigen Regeln, um die Reihenfolge zu bestimmen, in der diese Regeln ausgewertet werden.

4. Führen Sie die Simulation erneut aus.

   In diesem Beispiel entspricht die korrigierte X-Men-Regel nun dem `Beast.jpg` Objekt auf Grundlage des `series=x-men` Benutzer-Metadaten, wie erwartet.



Aktivieren Sie die ILM-Richtlinie

Wenn Sie einer vorgeschlagenen ILM-Richtlinie ILM-Regeln hinzufügen, die Richtlinie simulieren und bestätigen, dass es sich wie erwartet verhält, sind Sie bereit, die vorgeschlagene Richtlinie zu aktivieren.

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Das ist schon "Bestimmte Zugriffsberechtigungen".
- Sie haben die vorgeschlagene ILM-Richtlinie gespeichert und simuliert.

Fehler in einer ILM-Richtlinie können zu nicht wiederherstellbaren Datenverlusten führen. Prüfen und simulieren Sie die Richtlinie sorgfältig, bevor Sie sie aktivieren, um sicherzustellen, dass sie wie vorgesehen funktioniert. + Wenn Sie eine neue ILM-Richtlinie aktivieren, verwendet StorageGRID sie für die Verwaltung aller Objekte, einschließlich vorhandener und neu aufgenommenen Objekte. Prüfen Sie vor der Aktivierung einer neuen ILM-Richtlinie alle Änderungen an der Platzierung vorhandener replizierter und Erasure Coding-Objekte. Das Ändern des Speicherorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

Über diese Aufgabe

Wenn Sie eine ILM-Richtlinie aktivieren, verteilt das System die neue Richtlinie auf alle Nodes. Die neue aktive Richtlinie tritt jedoch möglicherweise erst in Kraft, wenn alle Grid-Nodes zur Verfügung stehen, um die neue Richtlinie zu erhalten. In einigen Fällen wartet das System auf die Implementierung einer neuen aktiven Richtlinie, um sicherzustellen, dass Grid-Objekte nicht versehentlich entfernt werden.

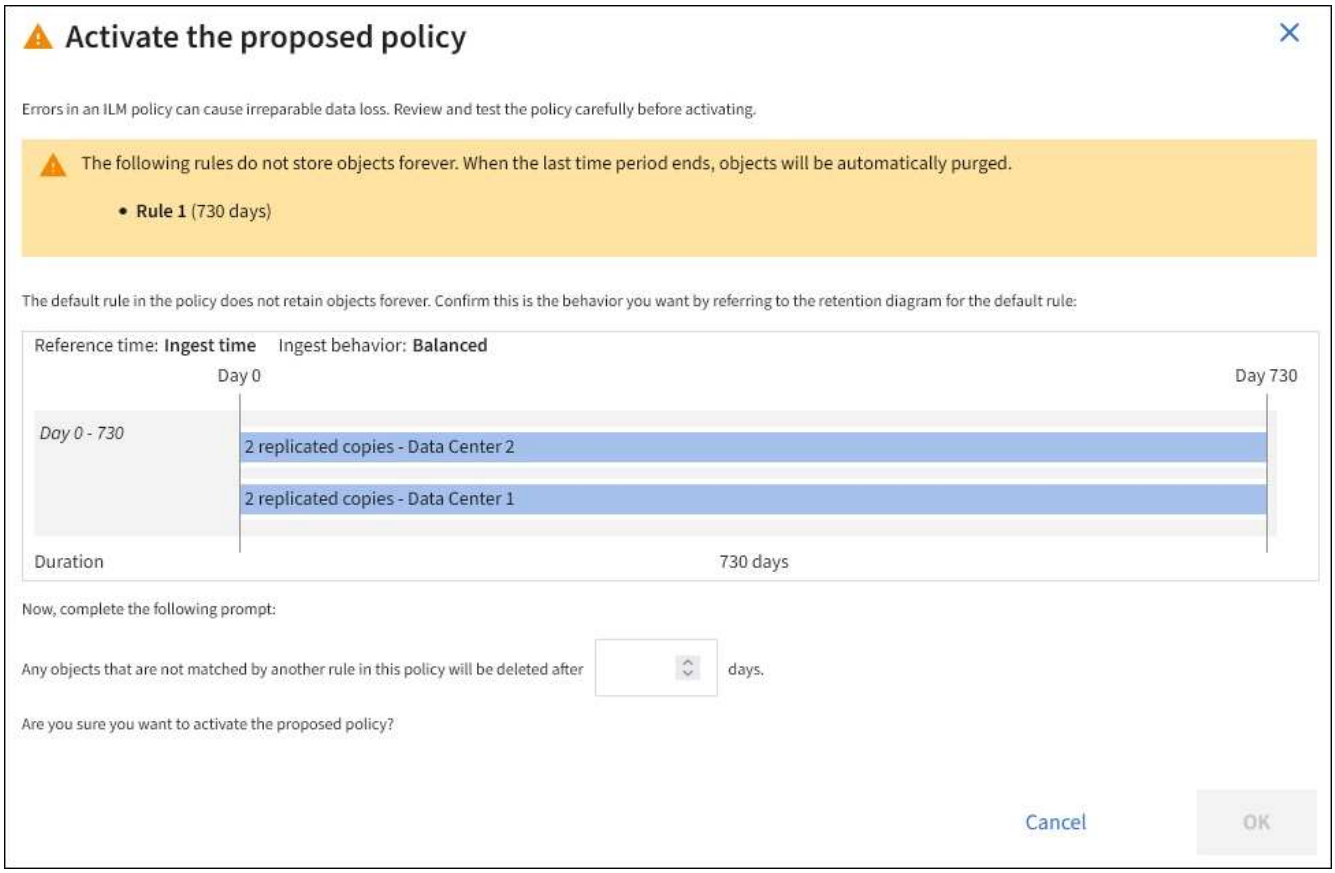
- Nehmen Richtlinienänderungen vor, die die Datenredundanz oder Aufbewahrungszeit verbessern, werden diese Änderungen sofort implementiert. Wenn Sie beispielsweise eine neue Richtlinie aktivieren, die eine Regel mit drei Kopien anstelle einer Regel mit zwei Kopien enthält, wird diese Richtlinie sofort implementiert, da sie die Datenredundanz erhöht.
- Bei Richtlinienänderungen, die Datenredundanz oder -Langlebigkeit verringern könnten, werden diese Änderungen erst implementiert, wenn alle Grid-Nodes verfügbar sind. Wenn Sie beispielsweise eine neue Richtlinie aktivieren, die eine Regel mit zwei Kopien anstelle einer Regel mit drei Kopien verwendet, wird die neue Richtlinie auf der Registerkarte „Aktive Richtlinie“ angezeigt. Sie wird jedoch erst wirksam, wenn alle Nodes online und verfügbar sind.

Schritte

1. Wenn Sie bereit sind, eine vorgeschlagene Richtlinie zu aktivieren, wählen Sie **ILM-Richtlinien** > **vorgeschlagene Richtlinie** aus, und wählen Sie dann **Aktivieren** aus.

   Es wird eine Warnmeldung angezeigt, in der Sie aufgefordert werden, zu bestätigen, dass Sie die vorgeschlagene Richtlinie aktivieren möchten.

   In der Warnmeldung wird eine Eingabeaufforderung angezeigt, wenn die Standardregel Objekte nicht für immer behält. In diesem Beispiel zeigt das Aufbewahrungsdiagramm, dass die Standardregel Objekte nach 730 Tagen (2 Jahre) löscht. Sie müssen **730** in das Textfeld eingeben, um zu bestätigen, dass alle Objekte, die nicht mit einer anderen Regel in der Richtlinie übereinstimmen, nach 730 Tagen aus StorageGRID entfernt werden.



2. Wählen Sie **OK**.

Ergebnis

Wenn eine neue ILM-Richtlinie aktiviert wurde:

- Die Richtlinie wird auf der Registerkarte Aktive Richtlinie angezeigt. Der Eintrag Startdatum zeigt das Datum und die Uhrzeit an, zu der die Richtlinie aktiviert wurde.
- Die zuvor aktive Richtlinie wird auf der Registerkarte Richtlinienverlauf angezeigt. Die Einträge für das Start- und Enddatum geben an, wann die Richtlinie aktiv wurde und wann sie nicht mehr in Kraft war.

Verwandte Informationen

"Beispiel 6: Ändern einer ILM-Richtlinie"

Überprüfen einer ILM-Richtlinie mit Objekt-Metadaten-Lookup

Sobald Sie eine ILM-Richtlinie aktiviert haben, sollten Sie repräsentative Testobjekte in das StorageGRID System aufnehmen. Anschließend sollten Sie eine Objektmetadaten abfragen durchführen, um zu bestätigen, ob Kopien wie vorgesehen erstellt und an den richtigen Orten platziert werden.

Bevor Sie beginnen

- Sie haben eine Objektkennung, die einer der folgenden sein kann:
  - **UUID**: Der Universally Unique Identifier des Objekts. Geben Sie die UUID in allen Großbuchstaben ein.
  - **CBID**: Die eindeutige Kennung des Objekts in StorageGRID. Sie können die CBID eines Objekts aus dem Prüfprotokoll abrufen. Geben Sie die CBID in allen Großbuchstaben ein.

- **S3-Bucket und Objektschlüssel**: Bei Aufnahme eines Objekts über die S3-Schnittstelle verwendet die Client-Applikation eine Bucket- und Objektschlüsselkombination, um das Objekt zu speichern und zu identifizieren. Wenn der S3-Bucket versioniert ist und Sie eine bestimmte Version eines S3-Objekts mithilfe des Bucket und Objektschlüssels nachsehen möchten, steht Ihnen die **Version-ID** zur Verfügung.
- **Swift Container und Objektname**: Wenn ein Objekt über die Swift-Schnittstelle aufgenommen wird, verwendet die Client-Anwendung eine Container- und Objektname-Kombination, um das Objekt zu speichern und zu identifizieren.

Schritte

1. Aufnahme des Objekts.
2. Wählen Sie **ILM** > **Object Metadata Lookup**.
3. Geben Sie die Kennung des Objekts in das Feld **Kennung** ein. Sie können eine UUID, CBID, S3 Bucket/Objektschlüssel oder Swift Container/Objektname eingeben.
4. Optional können Sie eine Version-ID für das Objekt eingeben (nur S3).

5. Wählen Sie **Look Up**.

   Die Ergebnisse der Objektmetadaten werden angezeigt. Auf dieser Seite werden die folgenden Informationstypen aufgeführt:

   - Systemmetadaten, einschließlich Objekt-ID (UUID), Objektname, Name des Containers, Mandantenkontenname oder -ID, logische Größe des Objekts, Datum und Uhrzeit der ersten Erstellung des Objekts sowie Datum und Uhrzeit der letzten Änderung des Objekts.
   - Alle mit dem Objekt verknüpften Schlüssel-Wert-Paare für benutzerdefinierte Benutzer-Metadaten.
   - Bei S3-Objekten sind alle dem Objekt zugeordneten Objekt-Tag-Schlüsselwert-Paare enthalten.
   - Der aktuelle Storage-Standort jeder Kopie für replizierte Objektkopien
   - Für Objektkopien mit Erasure-Coding-Verfahren wird der aktuelle Speicherort der einzelnen Fragmente gespeichert.
   - Bei Objektkopien in einem Cloud Storage Pool befindet sich der Speicherort des Objekts, einschließlich des Namens des externen Buckets und der eindeutigen Kennung des Objekts.
   - Für segmentierte Objekte und mehrteilige Objekte, eine Liste von Objektsegmenten einschließlich Segment-IDs und Datengrößen. Bei Objekten mit mehr als 100 Segmenten werden nur die ersten 100 Segmente angezeigt.
   - Alle Objekt-Metadaten im nicht verarbeiteten internen Speicherformat. Diese RAW-Metadaten enthalten interne System-Metadaten, die nicht garantiert werden, dass sie über Release bis Release beibehalten werden.

Das folgende Beispiel zeigt die Ergebnisse für die Suche nach Objektmetadaten für ein S3-Testobjekt, das als zwei replizierte Kopien gespeichert ist.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


6. Vergewissern Sie sich, dass das Objekt am richtigen Ort und an den richtigen Stellen gespeichert ist und dass es sich um den richtigen Kopiertyp handelt.

> Wenn die Option „Audit“ aktiviert ist, können Sie auch das Audit-Protokoll für die Meldung „ORLM-Objektregeln erfüllt“ überwachen. Die ORLM-Audit-Meldung kann Ihnen weitere Informationen über den Status des ILM-Evaluierungsprozesses liefern, kann Ihnen jedoch keine Informationen über die Richtigkeit der Platzierung der Objektdaten oder die Vollständigkeit der ILM-Richtlinie geben. Das müssen Sie selbst beurteilen. Weitere Informationen finden Sie unter "Prüfung von Audit-Protokollen".

Verwandte Informationen

- "S3-REST-API VERWENDEN"
- "Nutzen Sie die Swift REST API"

Arbeiten mit ILM-Richtlinien und ILM-Regeln

Wenn sich Ihre Speicheranforderungen ändern, müssen Sie möglicherweise eine andere Richtlinie implementieren oder die mit dieser Richtlinie verbundenen ILM-Regeln ändern. Sie können ILM-Metriken anzeigen, um die Systemperformance zu ermitteln.

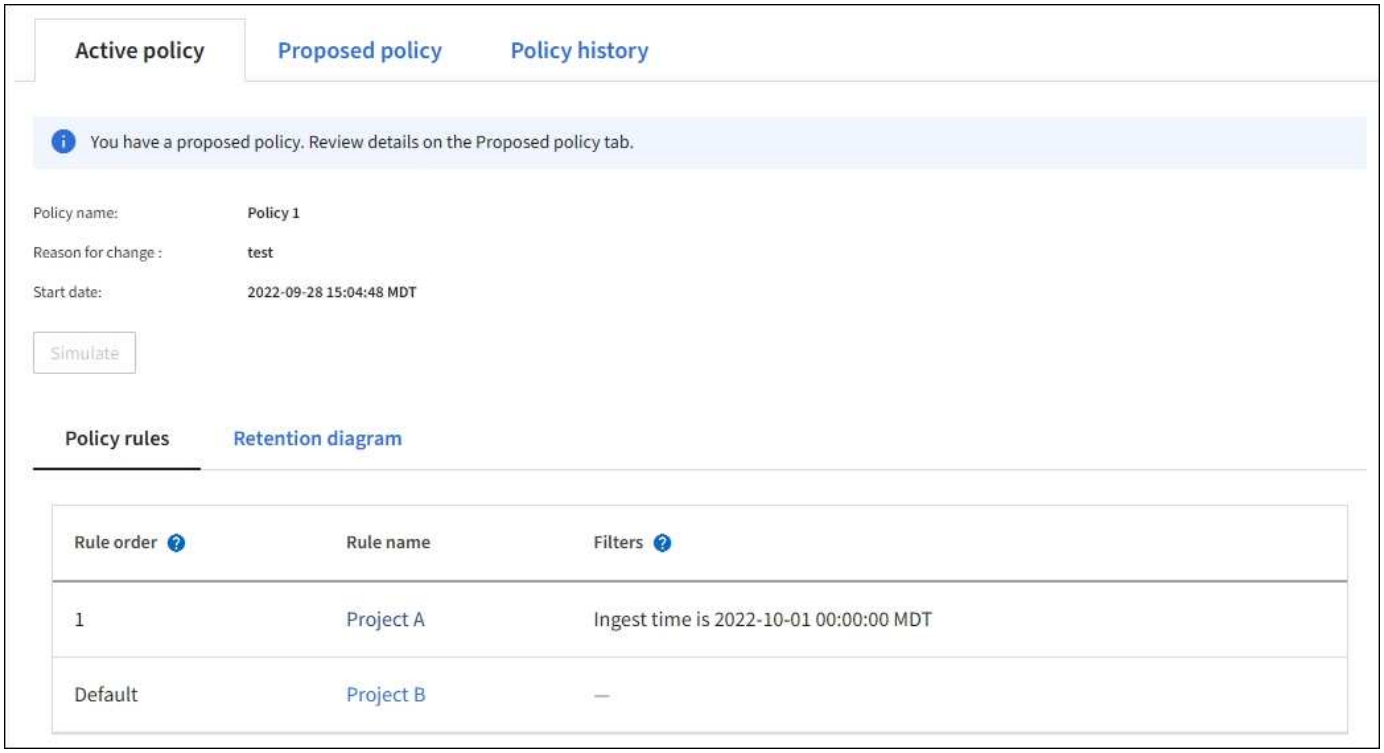
Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.

ILM-Richtlinien anzeigen

So zeigen Sie aktive, vorgeschlagene und historische ILM-Richtlinien an:

1. Wählen Sie **ILM** > **Richtlinien**.
2. Wählen Sie je nach Bedarf **Aktive Richtlinie**, **vorgeschlagene Richtlinie** oder **Richtlinienverlauf** aus, um die Details zu den einzelnen Richtlinien anzuzeigen. Auf jeder Registerkarte können Sie **Policy rules** und **Retention diagram** auswählen.



Klonen einer historischen ILM-Richtlinie

So klonen Sie eine historische ILM-Richtlinie:

1. Wählen Sie **ILM** > **Richtlinien** > **Richtlinienverlauf** aus.
2. Entfernen Sie die vorgeschlagene Richtlinie, falls vorhanden.
3. Aktivieren Sie das Optionsfeld für die Richtlinie, die Sie klonen möchten, und wählen Sie dann **historische Richtlinie klonen** aus.
4. Füllen Sie die erforderlichen Angaben aus, indem Sie den Anweisungen unter folgen "Vorgeschlagene ILM-Richtlinie erstellen".

Eine falsch konfigurierte ILM-Richtlinie kann zu nicht wiederherstellbaren Datenverlusten führen. Prüfen Sie vor der Aktivierung einer ILM-Richtlinie die ILM-Richtlinie und ihre ILM-Regeln sorgfältig und simulieren Sie anschließend die ILM-Richtlinie. Vergewissern Sie sich immer, dass die ILM-Richtlinie wie vorgesehen funktioniert.

Entfernen Sie die vorgeschlagene ILM-Richtlinie

So entfernen Sie die vorgeschlagene Richtlinie:

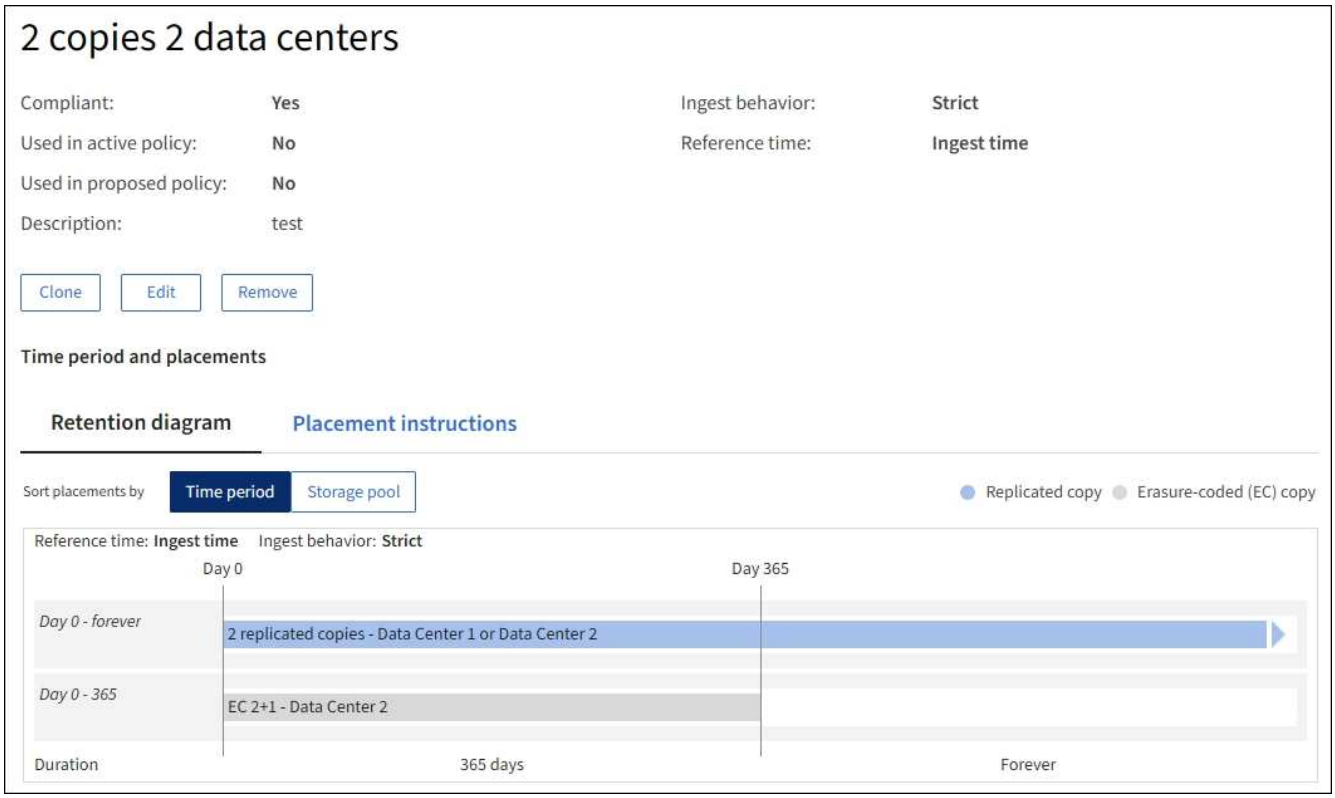
1. Wählen Sie **ILM** > **Richtlinien** > **vorgeschlagene Richtlinie** aus.
2. Wählen Sie **Aktionen** > **Entfernen**.

Die vorgeschlagene Richtlinie und die vorgeschlagene Policy-Registerkarte werden entfernt.

Zeigen Sie Einzelheiten zur ILM-Regel an

So zeigen Sie die Details für eine ILM-Regel an, einschließlich des Aufbewahrungsdiagramms und der Anweisungen zur Platzierung der Regel:

1. Wählen Sie **ILM** > **Regeln**.
2. Wählen Sie die Regel aus, deren Details Sie anzeigen möchten. Beispiel:



Darüber hinaus können Sie auf der Detailseite eine Regel klonen, bearbeiten oder entfernen.

Klonen einer ILM-Regel

Sie können eine Regel nicht bearbeiten, wenn sie in der vorgeschlagenen ILM-Richtlinie oder der aktiven ILM-Richtlinie verwendet wird. Stattdessen können Sie eine Regel klonen und alle erforderlichen Änderungen an der geklonten Kopie vornehmen. Anschließend können Sie die ursprüngliche Regel bei Bedarf aus der

vorgeschlagenen Richtlinie entfernen und durch die geänderte Version ersetzen. Sie können eine ILM-Regel nicht klonen, wenn sie mit StorageGRID Version 10.2 oder früher erstellt wurde.

Bevor Sie einer aktiven ILM-Richtlinie eine geklonte Regel hinzufügen, sollten Sie beachten, dass eine Änderung der Anweisungen zur Platzierung eines Objekts zu einer erhöhten Systemauslastung führen kann.

Schritte

1. Wählen Sie **ILM** > **Regeln**.
2. Aktivieren Sie das Kontrollkästchen für die Regel, die Sie klonen möchten, und wählen Sie dann **Clone** aus. Alternativ wählen Sie den Regelnamen aus, und wählen Sie dann auf der Seite mit den Regeldetails **Clone** aus.
3. Aktualisieren Sie die geklonte Regel, indem Sie die Schritte für befolgen Bearbeiten einer ILM-Regel Und "Verwenden erweiterter Filter in ILM-Regeln".

   Beim Klonen einer ILM-Regel müssen Sie einen neuen Namen eingeben.

Bearbeiten einer ILM-Regel

Möglicherweise müssen Sie eine ILM-Regel bearbeiten, um einen Filter oder eine Platzierungsanweisung zu ändern.

Sie können eine Regel nicht bearbeiten, wenn sie in der aktiven ILM-Richtlinie oder der vorgeschlagenen ILM-Richtlinie verwendet wird. Stattdessen können Sie diese Regeln klonen und erforderliche Änderungen an der geklonten Kopie vornehmen. Sie können auch die vom System bereitgestellte Regel nicht bearbeiten, erstellen Sie 2 Kopien.

> Bevor Sie einer aktiven ILM-Richtlinie eine bearbeitete Regel hinzufügen, müssen Sie beachten, dass eine Änderung der Anweisungen zur Platzierung eines Objekts zu einer erhöhten Systemauslastung führen kann.

Schritte

1. Wählen Sie **ILM** > **Regeln**.
2. Bestätigen Sie, dass die zu bearbeitende Regel nicht in der aktiven ILM-Richtlinie oder der vorgeschlagenen ILM-Richtlinie verwendet wird.
3. Wenn die Regel, die Sie bearbeiten möchten, nicht verwendet wird, aktivieren Sie das Kontrollkästchen für die Regel und wählen Sie **Aktionen** > **Bearbeiten**. Alternativ wählen Sie den Namen der Regel aus, und wählen Sie dann auf der Seite mit den Regeldetails **Bearbeiten** aus.
4. Füllen Sie die Seiten des Assistenten zum Bearbeiten von ILM-Regeln aus. Befolgen Sie bei Bedarf die Schritte für "Erstellen einer ILM-Regel" Und "Verwenden erweiterter Filter in ILM-Regeln".

   Beim Bearbeiten einer ILM-Regel können Sie ihren Namen nicht ändern.

> Wenn Sie eine Regel bearbeiten, die in einer historischen Richtlinie verwendet wird, wird die ⊗ Wenn Sie die Richtlinie anzeigen, wird das Symbol für die Regel angezeigt. Dies bedeutet, dass die Regel zu einer historischen Regel geworden ist.

Entfernen einer ILM-Regel

Um die Liste der aktuellen ILM-Regeln kontrollierbar zu halten, entfernen Sie alle ILM-Regeln, die Sie wahrscheinlich nicht verwenden werden.

Schritte

So entfernen Sie eine ILM-Regel, die derzeit in der aktiven Richtlinie oder in der vorgeschlagenen Richtlinie verwendet wird:

1. Klonen Sie die aktive Richtlinie, oder bearbeiten Sie die vorgeschlagene Richtlinie.
2. Entfernen Sie die ILM-Regel aus der Richtlinie.
3. Speichern, simulieren und aktivieren Sie die neue Richtlinie, um sicherzustellen, dass Objekte wie erwartet geschützt sind.

So entfernen Sie eine derzeit nicht verwendete ILM-Regel:

1. Wählen Sie **ILM** > **Regeln**.
2. Bestätigen Sie, dass die Regel, die Sie entfernen möchten, nicht in der aktiven Richtlinie oder der vorgeschlagenen Richtlinie verwendet wird.
3. Wenn die Regel, die Sie entfernen möchten, nicht verwendet wird, wählen Sie die Regel aus und wählen Sie **Entfernen**. Sie können mehrere Regeln auswählen und alle gleichzeitig entfernen.
4. Wählen Sie **Yes**, um zu bestätigen, dass Sie die ILM-Regel entfernen möchten.

   Die ILM-Regel wird entfernt.

> Wenn Sie eine Regel entfernen, die in einer historischen Richtlinie verwendet wird, wird die ⊗ Wenn Sie die Richtlinie anzeigen, wird das Symbol für die Regel angezeigt. Dies bedeutet, dass die Regel zu einer historischen Regel geworden ist.

Anzeigen von ILM-Metriken

Sie können Metriken für ILM anzeigen, z. B. die Anzahl der Objekte in der Warteschlange und die Evaluierungsrate. Sie können diese Kennzahlen überwachen, um die Systemperformance zu ermitteln. Eine große Warteschlange oder Evaluierungsrate zeigt möglicherweise an, dass das System nicht mit der Aufnahmerate Schritt halten kann, die Auslastung der Client-Applikationen zu hoch ist oder dass ein ungewöhnlicher Zustand vorliegt.

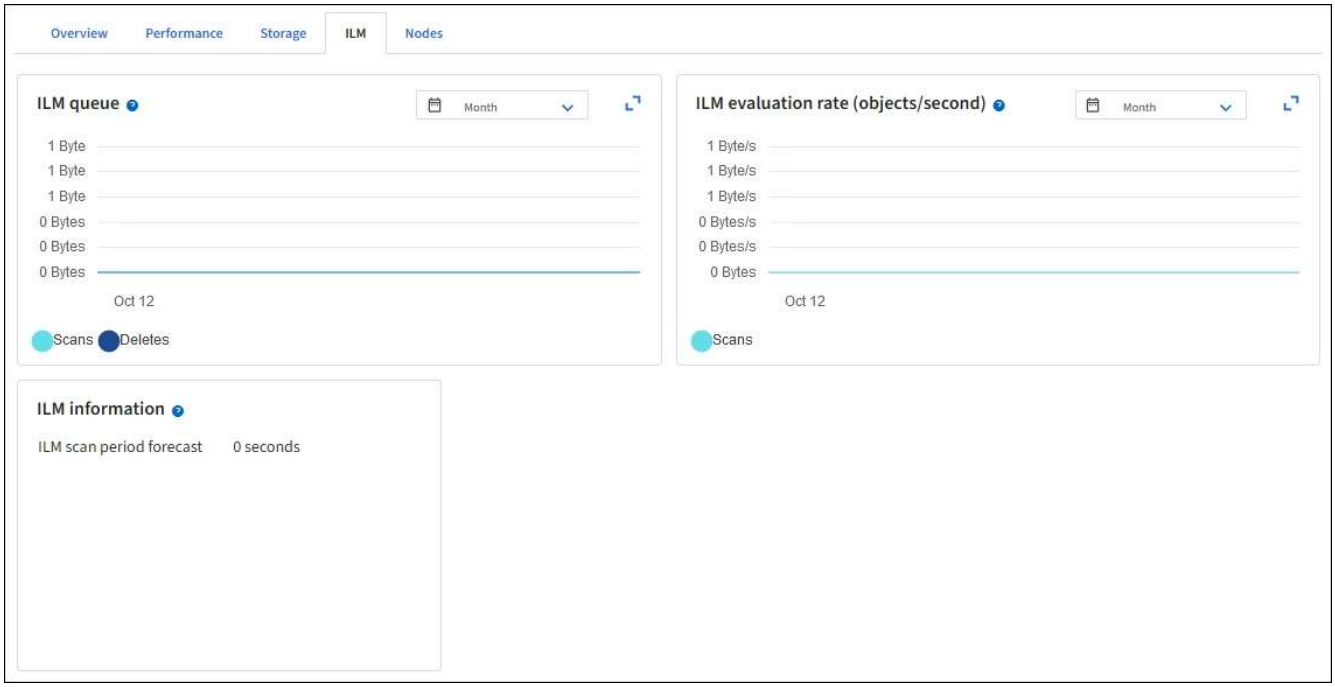
Schritte

1. Wählen Sie **Dashboard** > **ILM**.

> Da das Dashboard angepasst werden kann, ist die Registerkarte ILM möglicherweise nicht verfügbar.

2. Überwachen Sie die Kennzahlen auf der Registerkarte ILM.

   Sie können das Fragezeichen auswählen ? Um eine Beschreibung der Elemente auf der Registerkarte ILM anzuzeigen.



Verwenden Sie die S3-Objektsperre

Objekte managen mit S3 Object Lock

Als Grid-Administrator können Sie S3 Object Lock für Ihr StorageGRID System aktivieren und eine konforme ILM-Richtlinie implementieren. So können Sie sicherstellen, dass Objekte in bestimmten S3 Buckets nicht für einen bestimmten Zeitraum gelöscht oder überschrieben werden.

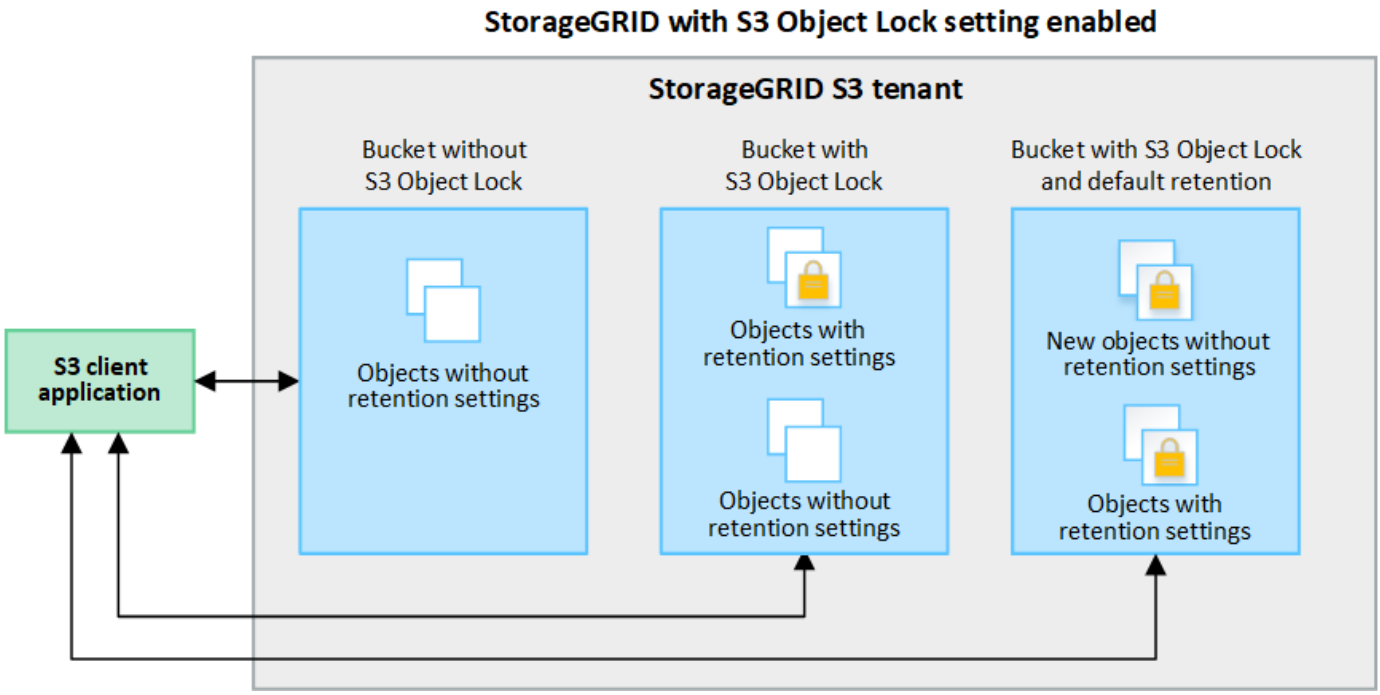
Was ist S3 Object Lock?

Die Funktion StorageGRID S3 Object Lock ist eine Objektschutzlösung, die der S3 Object Lock in Amazon Simple Storage Service (Amazon S3) entspricht.

Wenn die globale S3-Objektsperre für ein StorageGRID-System aktiviert ist, kann ein S3-Mandantenkonto Buckets mit oder ohne aktivierte S3-Objektsperre erstellen. Wenn für einen Bucket die S3 Object Lock aktiviert ist, ist die Bucket-Versionierung erforderlich und wird automatisch aktiviert.

Wenn für einen Bucket die S3 Object Lock aktiviert ist, können S3-Client-Applikationen optional Aufbewahrungseinstellungen für jede Objektversion angeben, die in diesem Bucket gespeichert ist.

Darüber hinaus kann für einen Bucket, auf dem die S3 Object Lock aktiviert ist, optional ein Standardaufbewahrungsmodus und ein Aufbewahrungszeitraum verwendet werden. Die Standardeinstellungen gelten nur für Objekte, die ohne eigene Aufbewahrungseinstellungen zum Bucket hinzugefügt werden.



Aufbewahrungsmodi

Die Objektsperrfunktion StorageGRID S3 unterstützt zwei Aufbewahrungsmodi, um verschiedene Schutzstufen auf Objekte anzuwenden. Diese Modi entsprechen den Amazon S3 Aufbewahrungsmodi.

- Im Compliance-Modus:
  - Das Objekt kann erst gelöscht werden, wenn das Aufbewahrungsdatum erreicht ist.
  - Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden.
  - Das Aufbewahrungsdatum des Objekts kann erst entfernt werden, wenn dieses Datum erreicht ist.
- Im Governance-Modus:
  - Benutzer mit besonderer Berechtigung können in Anfragen einen Überbrückungskopf verwenden, um bestimmte Aufbewahrungseinstellungen zu ändern.
  - Diese Benutzer können eine Objektversion löschen, bevor das Aufbewahrungsdatum erreicht ist.
  - Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

Aufbewahrungseinstellungen für Objektversionen

Wenn ein Bucket mit aktivierter S3-Objektsperrung erstellt wird, können Benutzer mithilfe der S3-Client-Applikation optional die folgenden Aufbewahrungseinstellungen für jedes Objekt angeben, das dem Bucket hinzugefügt wird:

- **Retention Mode**: Entweder Compliance oder Governance.
- **Rebeat-until-date**: Wenn das Aufbewahrungsdatum einer Objektversion in der Zukunft liegt, kann das Objekt abgerufen, aber nicht gelöscht werden.
- **Legal Hold**: Die Anwendung eines gesetzlichen Hold auf eine Objektversion sperrt diesen Gegenstand sofort. Beispielsweise müssen Sie ein Objekt, das mit einer Untersuchung oder einem Rechtsstreit zusammenhängt, rechtlich festhalten. Eine gesetzliche Aufbewahrungspflichten haben kein Ablaufdatum, bleiben aber bis zur ausdrücklichen Entfernung erhalten. Die gesetzlichen Aufbewahrungspflichten sind unabhängig von der bisherigen Aufbewahrungsfrist.

Befindet sich ein Objekt unter einer Legal Hold-Funktion, kann das Objekt unabhängig vom Aufbewahrungsmodus nicht gelöscht werden.

Weitere Informationen zu den Objekteinstellungen finden Sie unter "Konfigurieren Sie die S3-Objektsperre über die S3-REST-API".

Standardeinstellung für die Aufbewahrung von Buckets

Wenn ein Bucket mit aktivierter S3-Objektsperrung erstellt wurde, können Benutzer optional die folgenden Standardeinstellungen für den Bucket angeben:

- **Default Retention Mode**: Entweder Compliance oder Governance.
- **Default Retention Period**: Wie lange neue Objektversionen, die zu diesem Bucket hinzugefügt wurden, beibehalten werden sollen, beginnend mit dem Tag, an dem sie hinzugefügt werden.

Die Standard-Bucket-Einstellungen gelten nur für neue Objekte, die keine eigenen Aufbewahrungseinstellungen haben. Vorhandene Bucket-Objekte werden nicht beeinflusst, wenn Sie diese Standardeinstellungen hinzufügen oder ändern.

Siehe "Erstellen eines S3-Buckets" Und "Aktualisieren Sie die S3 Object Lock-Standardaufbewahrung".

Vergleich der S3-Objektsperre mit älterer Compliance

Die S3-Objektsperre ersetzt die in früheren StorageGRID-Versionen verfügbare Compliance-Funktion. Da die S3-Objektsperrfunktion den Amazon S3-Anforderungen entspricht, depretiert sie die proprietäre StorageGRID-Compliance-Funktion, die jetzt als „`` Legacy-Compliance“ bezeichnet wird.

Die globale Compliance-Einstellung ist veraltet. Wenn Sie diese Einstellung mit einer früheren Version von StorageGRID aktiviert haben, wird die Einstellung S3 Objektsperre automatisch aktiviert. Sie können die Einstellungen vorhandener konformer Buckets weiterhin mit StorageGRID managen. Es ist jedoch nicht möglich, neue konforme Buckets zu erstellen. Weitere Informationen finden Sie unter "NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5".

Wenn Sie die ältere Compliance-Funktion in einer früheren Version von StorageGRID verwendet haben, lesen Sie die folgende Tabelle, um zu erfahren, wie sie mit der S3-Objektsperrfunktion in StorageGRID verglichen wird.

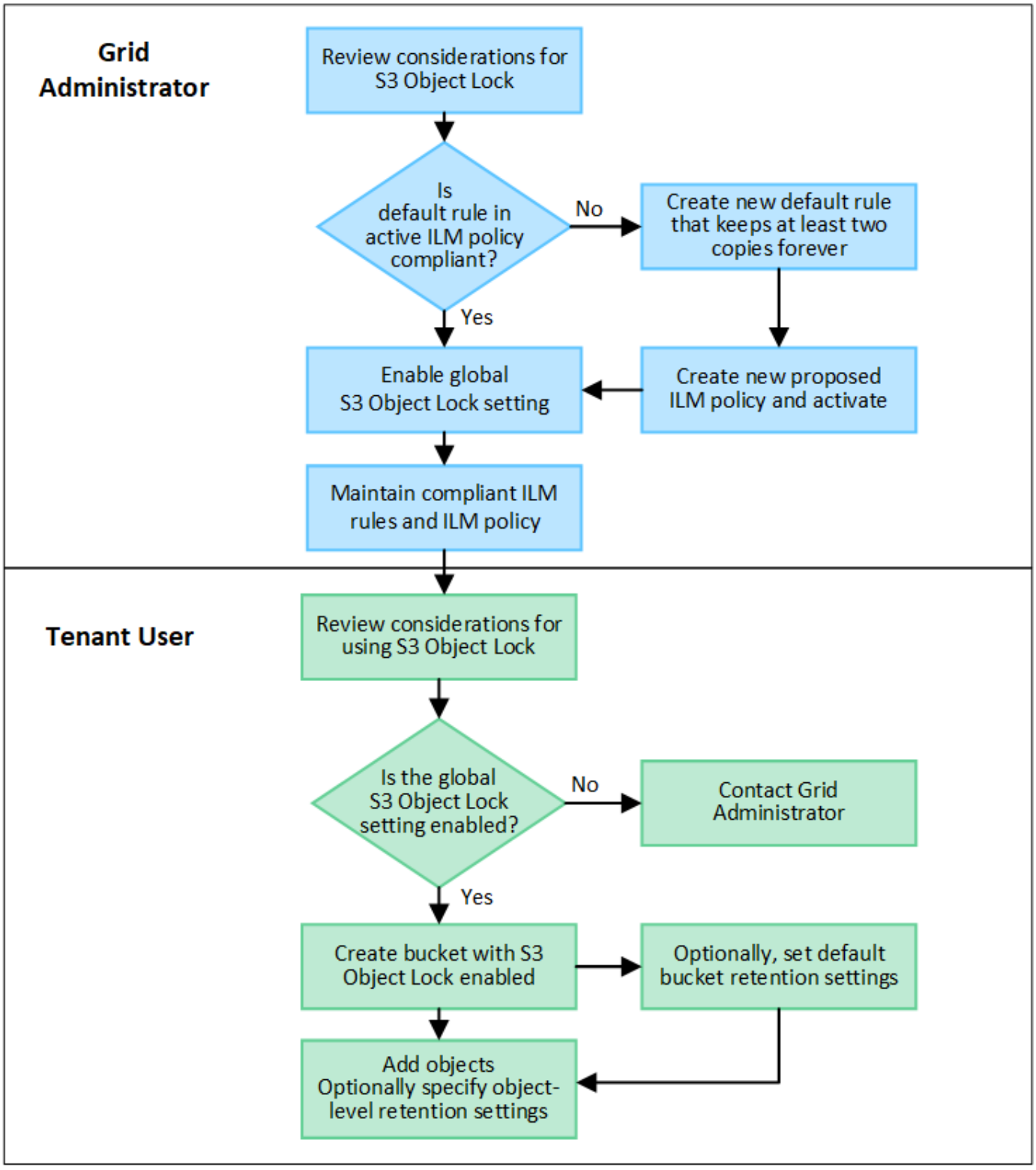
	S3-Objektsperre	Compliance (alt)
Wie wird die Funktion global aktiviert?	Wählen Sie im Grid Manager die Option **KONFIGURATION** > **System** > **S3 Object Lock**.	Wird nicht mehr unterstützt.
Wie wird die Funktion für einen Bucket aktiviert?	Benutzer müssen die S3-Objektsperre aktivieren, wenn ein neuer Bucket mithilfe des Mandantenmanagers, der Mandantenmanagement-API oder der S3-REST-API erstellt wird.	Wird nicht mehr unterstützt.

	S3-Objektsperre	Compliance (alt)
Wird die Bucket-Versionierung unterstützt?	Ja. Die Bucket-Versionierung ist erforderlich und wird automatisch aktiviert, wenn S3 Object Lock für den Bucket aktiviert ist.	Nein
Wie wird die Objektaufbewahrung festgelegt?	Benutzer können für jede Objektversion ein bis-Datum für die Aufbewahrung festlegen oder für jeden Bucket einen Standardaufbewahrungszeitraum festlegen.	Benutzer müssen eine Aufbewahrungsfrist für den gesamten Bucket festlegen. Der Aufbewahrungszeitraum gilt für alle Objekte im Bucket.
Kann der Aufbewahrungszeitraum geändert werden?	• Im Compliance-Modus kann das Aufbewahrungsdatum für eine Objektversion erhöht, aber nicht verringert werden. • Im Governance-Modus können Benutzer mit speziellen Berechtigungen die Aufbewahrungseinstellungen eines Objekts verringern oder sogar entfernen.	Die Aufbewahrungsfrist eines Buckets kann erhöht, aber nie verringert werden.
Wo wird die gesetzliche Aufbewahrungspflichten kontrolliert?	Benutzer können für jede Objektversion im Bucket rechtliche Aufbewahrungspflichten platzieren oder eine gesetzliche Aufbewahrungspflichten aufheben.	Auf dem Bucket werden gesetzliche Aufbewahrungspflichten angebracht, die alle Objekte im Bucket betreffen.
Wann können Objekte gelöscht werden?	• Im Compliance-Modus kann eine Objektversion nach Erreichen des Aufbewahrungsdatums gelöscht werden, vorausgesetzt, das Objekt befindet sich nicht im Legal Hold. • Im Governance-Modus können Benutzer mit speziellen Berechtigungen ein Objekt löschen, bevor das Aufbewahrungsdatum erreicht wird, vorausgesetzt, das Objekt befindet sich nicht unter Legal Hold.	Ein Objekt kann nach Ablauf des Aufbewahrungszeitraums gelöscht werden, sofern der Bucket nicht unter der gesetzlichen Aufbewahrungspflichten liegt. Objekte können automatisch oder manuell gelöscht werden.
Wird die Bucket-Lifecycle-Konfiguration unterstützt?	Ja.	Nein

Workflow für S3 Objektsperre

Als Grid-Administrator müssen Sie sich eng mit den Mandantenbenutzern abstimmen, um sicherzustellen, dass die Objekte so geschützt sind, dass sie ihren Aufbewahrungsanforderungen entsprechen.

Das Workflow-Diagramm zeigt die grundlegenden Schritte zur Verwendung der S3-Objektsperre. Die Schritte werden vom Grid-Administrator und von Mandantenbenutzern durchgeführt.



Den Grid-Administratoren stehen

Wie das Workflow-Diagramm zeigt, muss ein Grid-Administrator zwei übergeordnete Aufgaben durchführen, bevor S3-Mandanten S3-Objektsperre verwenden können:

1. Erstellen Sie mindestens eine kompatible ILM-Regel und stellen Sie diese Regel in der aktiven ILM-Richtlinie zur Standardregel bereit.
2. Aktivieren Sie die globale S3-Objektsperre für das gesamte StorageGRID-System.

Aufgaben für Mandanten

Nach Aktivierung der globalen S3-Objektsperre können Mandanten die folgenden Aufgaben ausführen:

1. Erstellen Sie Buckets, für die S3-Objektsperre aktiviert ist.
2. Optional können Sie Standardaufbewahrungseinstellungen für den Bucket festlegen. Alle Standard-Bucket-Einstellungen werden nur auf neue Objekte angewendet, die keine eigenen Aufbewahrungseinstellungen haben.
3. Fügen Sie diesen Buckets Objekte hinzu und geben Sie optional Aufbewahrungszeiträume auf Objektebene und Einstellungen für Legal Hold an.
4. Aktualisieren Sie nach Bedarf die Standardaufbewahrung für den Bucket oder aktualisieren Sie die Aufbewahrungsfrist oder die Legal Hold-Einstellung für ein einzelnes Objekt.

Anforderungen für die S3-Objektsperre

Sie müssen die Anforderungen für die Aktivierung der globalen S3-Objektsperre, die Anforderungen für die Erstellung konformer ILM-Regeln und ILM-Richtlinien sowie die Einschränkungen prüfen, die StorageGRID für Buckets und Objekte, die S3 Objektsperre verwenden, festlegen.

Anforderungen für die Verwendung der globalen S3-Objektsperre

- Sie müssen die globale S3-Objektsperreneinstellung mithilfe des Grid-Managers oder der Grid-Management-API aktivieren, bevor ein S3-Mandant einen Bucket erstellen kann, dessen S3-Objektsperre aktiviert ist.
- Wenn Sie die globale S3-Objektsperre aktivieren, können alle S3-Mandantenkonten Buckets erstellen, wobei S3-Objektsperre aktiviert ist.
- Nachdem Sie die globale S3-Objektsperrung aktiviert haben, können Sie die Einstellung nicht deaktivieren.
- Die globale S3 Object Lock kann nur aktiviert werden, wenn die Standardregel in der aktiven ILM-Richtlinie „*compliant*“ lautet. (Das heißt, die Standardregel muss die Anforderungen von Buckets mit aktivierter S3 Object Lock erfüllen.)
- Wenn die globale S3-Objektsperrung aktiviert ist, können Sie keine neue vorgeschlagene ILM-Richtlinie erstellen oder eine vorhandene vorgeschlagene ILM-Richtlinie aktivieren, sofern die Standardregel in der Richtlinie nicht konform ist. Nach Aktivierung der globalen S3 Object Lock-Einstellung geben die ILM-Regeln und ILM-Richtlinien-Seiten an, welche ILM-Regeln konform sind.

Anforderungen für konforme ILM-Regeln

Wenn Sie die globale S3-Objektsperre aktivieren möchten, müssen Sie sicherstellen, dass die Standardregel in Ihrer aktiven ILM-Richtlinie konform ist. Eine konforme Regel erfüllt die Anforderungen beider Buckets durch aktivierte S3-Objektsperre und alle vorhandenen Buckets, für die Compliance aktiviert ist:

- Die IT muss mindestens zwei replizierte Objektkopien oder eine Kopie mit Verfahren zur Fehlerkorrektur erstellen.
- Diese Kopien müssen auf Storage-Nodes während der gesamten Dauer jeder Zeile in der Plazierung vorhanden sein.
- Objektkopien können nicht in einem Cloud-Storage-Pool gespeichert werden.
- Objektkopien können nicht auf Archivknoten gespeichert werden.
- Mindestens eine Zeile der Platzierungsanweisungen muss am Tag 0 beginnen, wobei **Ingest time** als Referenzzeit verwendet wird.
- Mindestens eine Zeile der Platzierungsanweisungen muss „`Forever`“ sein.

Anforderungen für aktive und vorgeschlagene ILM-Richtlinien

Wenn die globale S3 Object Lock-Einstellung aktiviert ist, können aktive und vorgeschlagene ILM-Richtlinien sowohl konforme als auch nicht konforme Regeln umfassen.

- Die Standardregel in der aktiven oder einer vorgeschlagenen ILM-Richtlinie muss konform sein.
- Nicht konforme Regeln gelten nur für Objekte in Buckets, für die die S3-Objektsperre nicht aktiviert ist oder die die ältere Compliance-Funktion nicht aktiviert hat.
- Konforme Regeln können auf Objekte in jedem Bucket angewendet werden; S3-Objektsperre oder vorhandene Compliance muss für den Bucket nicht aktiviert werden.

Eine ILM-konforme Richtlinie kann folgende drei Regeln umfassen:

1. Eine konforme Regel, die Erasure-codierte Kopien der Objekte in einem bestimmten Bucket erstellt und bei aktivierter S3-Objektsperre aktiviert ist. Die EC-Kopien werden von Tag 0 bis für immer auf Storage-Nodes gespeichert.
2. Eine nicht konforme Regel, die zwei replizierte Objektkopien auf Storage-Nodes für ein Jahr erstellt und dann eine Objektkopie zu Archivierungs-Nodes verschiebt und die Kopie für immer speichert. Diese Regel gilt nur für Buckets, für die keine S3 Object Lock oder Legacy Compliance aktiviert ist, da nur eine Objektkopie dauerhaft gespeichert und Archive Nodes verwendet werden.
3. Eine konforme Standardregel, die zwei replizierte Objektkopien auf Storage-Nodes von Tag 0 bis für immer erstellt. Diese Regel gilt für alle Objekte in jedem Bucket, die nicht durch die ersten beiden Regeln herausgefiltert wurden.

Anforderungen für Buckets, bei denen die S3-Objektsperre aktiviert ist

- Wenn die globale S3-Objektsperre für das StorageGRID System aktiviert ist, können Sie die Buckets mit aktivierter S3-Objektsperre über den Mandantenmanager, die Mandantenmanagement-API oder die S3-REST-API erstellen.
- Wenn Sie die S3-Objektsperre verwenden möchten, müssen Sie beim Erstellen des Buckets die S3-Objektsperre aktivieren. Sie können die S3-Objektsperre für einen vorhandenen Bucket nicht aktivieren.
- Wenn die S3-Objektsperre für einen Bucket aktiviert ist, ermöglicht StorageGRID automatisch die Versionierung für diesen Bucket. Sie können S3 Object Lock nicht deaktivieren oder die Versionierung für den Bucket nicht unterbrechen.
- Optional können Sie mithilfe von Tenant Manager, der Mandanten-Management-API oder der S3-REST-API für jeden Bucket einen Standardaufbewahrungsmodus und einen Aufbewahrungszeitraum angeben. Die Standardaufbewahrungseinstellungen des Buckets gelten nur für neue Objekte, die dem Bucket hinzugefügt wurden und keine eigenen Aufbewahrungseinstellungen haben. Sie können diese Standardeinstellungen außer Kraft setzen, indem Sie einen Aufbewahrungsmodus und das

Aufbewahrungsdatum für jede Objektversion festlegen, wenn sie hochgeladen wird.

- Die Konfiguration des Bucket-Lebenszyklus wird für Buckets unterstützt, für die S3 Object Lock aktiviert ist.
- Die CloudMirror-Replizierung wird für Buckets nicht unterstützt, wenn S3-Objektsperre aktiviert ist.

Anforderungen für Objekte in Buckets, bei denen die S3-Objektsperre aktiviert ist

- Zum Schutz einer Objektversion können Sie Standardaufbewahrungseinstellungen für den Bucket angeben oder Aufbewahrungseinstellungen für jede Objektversion angeben. Aufbewahrungseinstellungen auf Objektebene können mit der S3-Client-Applikation oder der S3-REST-API angegeben werden.
- Aufbewahrungseinstellungen gelten für einzelne Objektversionen. Eine Objektversion kann sowohl eine Aufbewahrungsfrist als auch eine gesetzliche Haltungseinstellung haben, eine jedoch nicht die andere oder keine. Wenn Sie eine Aufbewahrungsfrist oder eine gesetzliche Aufbewahrungseinstellung für ein Objekt angeben, wird nur die in der Anforderung angegebene Version geschützt. Sie können neue Versionen des Objekts erstellen, während die vorherige Version des Objekts gesperrt bleibt.

Lebenszyklus von Objekten in Buckets, wobei S3 Objektsperre aktiviert ist

Jedes in einem Bucket gespeicherte Objekt mit aktivierter S3 Object Lock durchlaufen die folgenden Phasen:

1. **Objektaufnahme**

   Wenn einem Bucket eine Objektversion hinzugefügt wird, für die S3 Object Lock aktiviert ist, werden die Aufbewahrungseinstellungen wie folgt angewendet:

   - Wenn für das Objekt Aufbewahrungseinstellungen angegeben werden, werden die Einstellungen auf Objektebene angewendet. Alle standardmäßigen Bucket-Einstellungen werden ignoriert.
   - Wenn für das Objekt keine Aufbewahrungseinstellungen angegeben sind, werden die Standard-Bucket-Einstellungen angewendet, sofern diese vorhanden sind.
   - Wenn für das Objekt oder den Bucket keine Aufbewahrungseinstellungen angegeben wurden, ist das Objekt nicht durch S3 Object Lock geschützt.

   Wenn Aufbewahrungseinstellungen angewendet werden, sind sowohl das Objekt als auch alle benutzerdefinierten S3-Metadaten geschützt.

2. **Objektaufbewahrung und -Löschung**

   Von jedem geschützten Objekt werden innerhalb StorageGRID des angegebenen Aufbewahrungszeitraums mehrere Kopien gespeichert. Die genaue Anzahl und Art der Objektkopien sowie der Speicherort werden durch die konformen Regeln der aktiven ILM-Richtlinie bestimmt. Ob ein geschütztes Objekt gelöscht werden kann, bevor das Aufbewahrungsdatum erreicht ist, hängt vom Aufbewahrungsmodus ab.

   - Befindet sich ein Objekt unter einer Legal Hold-Funktion, kann das Objekt unabhängig vom Aufbewahrungsmodus nicht gelöscht werden.

Verwandte Informationen

- "Erstellen eines S3-Buckets"
- "Aktualisieren Sie die S3 Object Lock-Standardaufbewahrung"
- "Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"
- "Beispiel 7: Konforme ILM-Richtlinie für S3 Object Lock"

Aktivieren Sie die S3-Objektsperre global

Falls ein S3-Mandantenkonto Vorschriften beim Speichern von Objektdaten einhalten muss, muss die S3-Objektsperre für Ihr gesamtes StorageGRID System aktiviert werden. Wenn Sie die globale S3-Objektsperre aktivieren, können alle S3-Mandantenbenutzer Buckets und Objekte mit S3 Object Lock erstellen und verwalten.

Bevor Sie beginnen

- Sie haben die Root-Zugriffsberechtigung.
- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben den S3-Objektsperrworkflow überprüft und die Überlegungen verstanden.
- Sie haben bestätigt, dass die Standardregel in der aktiven ILM-Richtlinie konform ist. Siehe "Erstellen einer Standard-ILM-Regel" Entsprechende Details.

Über diese Aufgabe

Ein Grid-Administrator muss die globale S3-Objektsperre aktivieren, damit Mandantenbenutzer neue Buckets erstellen können, für die S3-Objektsperre aktiviert ist. Nachdem diese Einstellung aktiviert ist, kann sie nicht deaktiviert werden.

> Die globale Compliance-Einstellung ist veraltet. Wenn Sie diese Einstellung mit einer früheren Version von StorageGRID aktiviert haben, wird die Einstellung S3 Objektsperre automatisch aktiviert. Sie können die Einstellungen vorhandener konformer Buckets weiterhin mit StorageGRID managen. Es ist jedoch nicht möglich, neue konforme Buckets zu erstellen. Weitere Informationen finden Sie unter "NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5".

Schritte

1. Wählen Sie **KONFIGURATION** > **System** > **S3 Objektsperre**.

   Die Seite Einstellungen für die S3-Objektsperre wird angezeigt.

2. Wählen Sie **S3-Objektsperre aktivieren**.
3. Wählen Sie **Anwenden**.

   Ein Bestätigungsdialogfeld wird angezeigt, in dem Sie daran erinnert werden, dass Sie die S3-Objektsperre nicht deaktivieren können, nachdem sie aktiviert wurde.

4. Wenn Sie sicher sind, dass Sie die S3-Objektsperre für Ihr gesamtes System dauerhaft aktivieren möchten, wählen Sie **OK**.

   Wenn Sie **OK** wählen:

   - Wenn die Standardregel in der aktiven ILM-Richtlinie konform ist, ist S3 Object Lock jetzt für das gesamte Grid aktiviert und kann nicht deaktiviert werden.
   - Wenn die Standardregel nicht kompatibel ist, wird ein Fehler angezeigt. Sie müssen eine neue ILM-Richtlinie erstellen und aktivieren, die eine konforme Regel als Standardregel enthält. Wählen Sie **OK**. Erstellen Sie dann eine neue vorgeschlagene Richtlinie, simulieren Sie sie und aktivieren Sie sie. Siehe "ILM-Richtlinie erstellen" Weitere Anweisungen.

Nachdem Sie fertig sind

Nachdem Sie die globale S3-Objektsperrung aktiviert haben, möchten Sie dies möglicherweise tun "Neue ILM-Richtlinie erstellen". Nach Aktivierung der Einstellung kann die ILM-Richtlinie optional sowohl eine konforme Standardregel als auch eine nicht konforme Standardregel enthalten. Beispielsweise könnte eine nicht konforme Regel verwendet werden, die keine Filter für Objekte in Buckets enthält, für die die S3-Objektsperre nicht aktiviert ist.

Beheben Sie die Konsistenzfehler beim Aktualisieren der S3-Objektsperre oder der alten Compliance-Konfiguration

Wenn ein Datacenter-Standort oder mehrere Storage-Nodes an einem Standort nicht mehr verfügbar sind, müssen Benutzer von S3-Mandanten unter Umständen Änderungen an der S3-Objektsperre oder älterer Compliance-Konfiguration vornehmen.

Mandantenbenutzer, deren Buckets mit aktivierter S3 Object Lock (oder älterer Compliance) vorhanden sind, können bestimmte Einstellungen ändern. Beispielsweise muss ein Mandantenbenutzer, der S3 Object Lock verwendet, eine Objektversion unter die gesetzliche Aufbewahrungspflichten legen.

Wenn ein Mandantenbenutzer die Einstellungen für einen S3-Bucket oder eine Objektversion aktualisiert, versucht StorageGRID, die Bucket- oder Objektmetadaten sofort im Grid zu aktualisieren. Wenn das System die Metadaten nicht aktualisieren kann, weil ein Datacenter-Standort oder mehrere Storage-Nodes nicht verfügbar sind, wird ein Fehler zurückgegeben:

```
503: Service Unavailable
Unable to update compliance settings because the settings can't be
consistently applied on enough storage services. Contact your grid
administrator for assistance.
```

Gehen Sie wie folgt vor, um diesen Fehler zu beheben:

1. Versuchen Sie, alle Storage-Nodes oder -Sites so schnell wie möglich wieder verfügbar zu machen.
2. Wenn Sie nicht in der Lage sind, an jedem Standort ausreichend Storage-Nodes zur Verfügung zu stellen, wenden Sie sich an den technischen Support, der Sie beim Wiederherstellen von Nodes unterstützt und sicherstellt, dass Änderungen konsistent im gesamten Grid angewendet werden.
3. Sobald das zugrunde liegende Problem behoben ist, erinnern Sie den Mandantenbenutzer daran, ihre Konfigurationsänderungen erneut zu versuchen.

Verwandte Informationen

- "Verwenden Sie ein Mandantenkonto"
- "S3-REST-API VERWENDEN"
- "Recovery und Wartung"

Beispiele für ILM-Regeln und -Richtlinien

Beispiel 1: ILM-Regeln und -Richtlinie für Objekt-Storage

Die folgenden Beispielregeln und -Richtlinien dienen als Ausgangspunkt bei der Definition einer ILM-Richtlinie zur Erfüllung der Anforderungen an Objektschutz und -Aufbewahrung.

Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen.

ILM-Regel 1, z. B. 1: Objektdaten an zwei Standorte kopieren

Dieses Beispiel einer ILM-Regel kopiert Objektdaten in Storage-Pools an zwei Standorten.

Regeldefinition	Beispielwert
Speicherpools an einem Standort	Zwei Speicherpools, die jeweils unterschiedliche Standorte mit den Namen Standort 1 und Standort 2 enthalten.
Regelname	Zwei Kopien Zwei Standorte
Referenzzeit	Aufnahmezeit
Platzierungen	Bewahren Sie an Tag 0 bis für immer eine replizierte Kopie an Standort 1 und eine replizierte Kopie an Standort 2 auf.

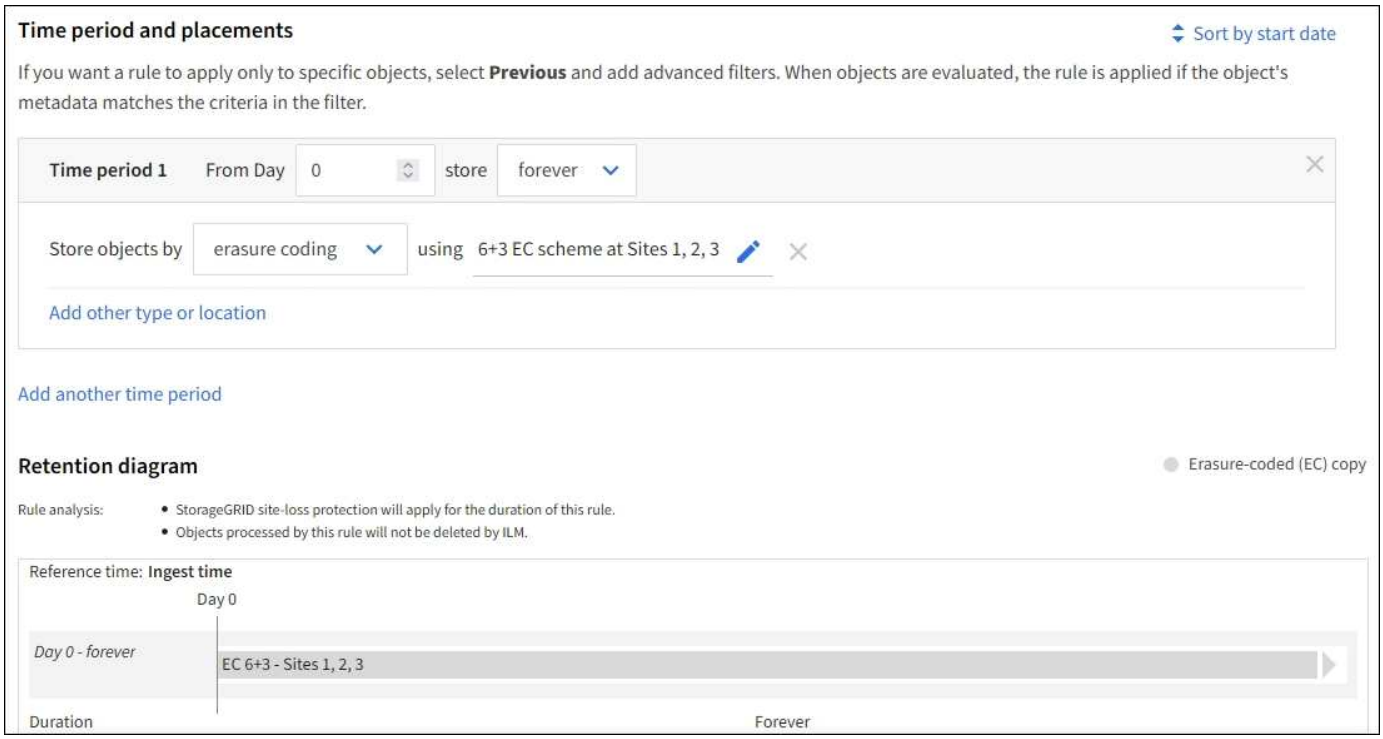
Im Abschnitt Regelanalyse des Aufbewahrungsdiagramms steht Folgendes:

- Für die Dauer dieser Regel gilt eine StorageGRID-Sicherung gegen vor-Ort-Verlust.
- Von dieser Regel verarbeitete Objekte werden nicht durch ILM gelöscht.

ILM-Regel 2, z. B. 1: Profil für Erasure Coding mit Bucket-Matching

Diese Beispielregel verwendet ein Erasure Coding-Profil und einen S3-Bucket, um zu bestimmen, wo und wie lange das Objekt gespeichert ist.

Regeldefinition	Beispielwert
Speicherpool mit mehreren Standorten	• Ein Speicherpool an drei Standorten (Standorte 1, 2, 3) • Verwenden Sie das Erasure Coding-Schema für 6+3
Regelname	S3 Bucket-Finanzdaten
Referenzzeit	Aufnahmezeit
Platzierungen	Erstellen Sie für Objekte in dem S3-Bucket mit dem Namen „Finance-Records“ eine Kopie, die nach Erasure Coding in dem Pool codiert wurde, der vom Profil für Erasure Coding angegeben wurde. Bewahren Sie diese Kopie für immer auf.

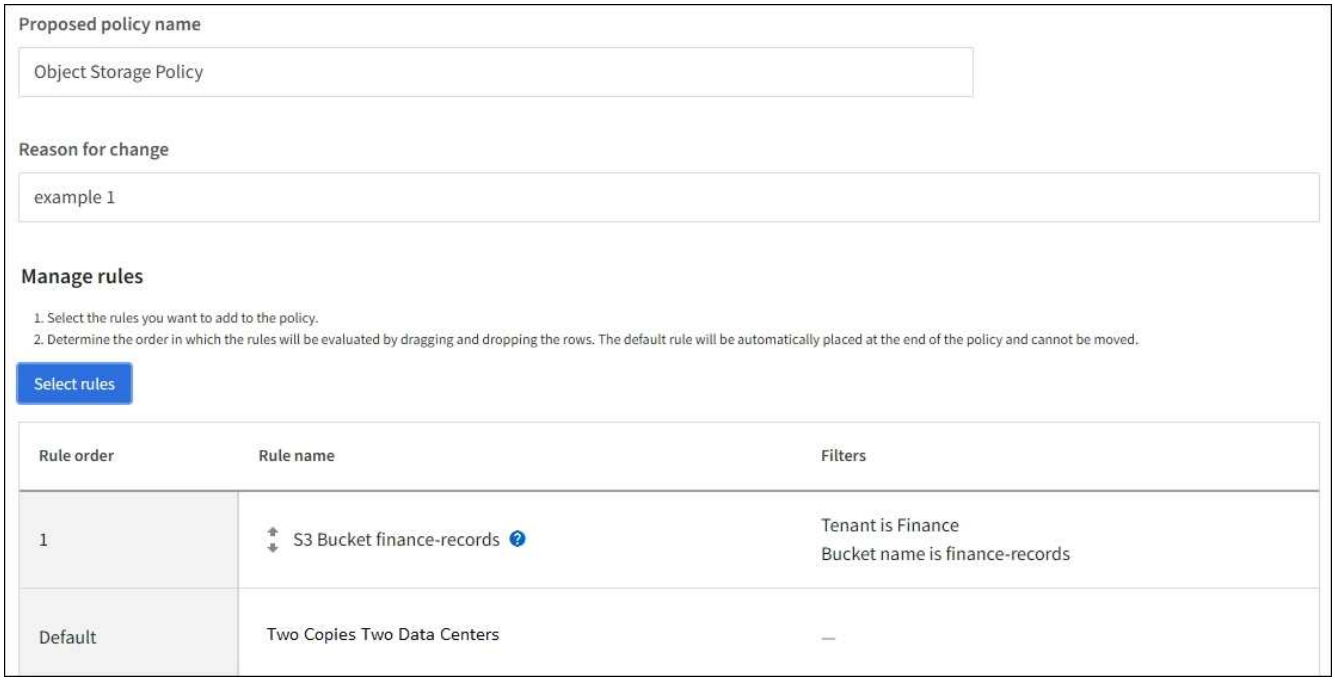


ILM-Richtlinie z. B. 1

In der Praxis sind die meisten ILM-Richtlinien einfach, obwohl das StorageGRID System Ihnen die Entwicklung ausgefeilter und komplexer ILM-Richtlinien ermöglicht.

Eine typische ILM-Richtlinie für ein Grid mit mehreren Standorten kann beispielsweise folgende ILM-Regeln umfassen:

- Speichern Sie bei der Aufnahme alle Objekte, die zum S3-Bucket mit dem Namen gehören `finance-records` In einem Speicherpool, der drei Standorte enthält. Verwenden Sie 6+3 Erasure Coding.
- Wenn ein Objekt nicht mit der ersten ILM-Regel übereinstimmt, verwenden Sie die standardmäßige ILM-Regel der Richtlinie, zwei Kopien von zwei Rechenzentren, um eine Kopie dieses Objekts an Standort 1 und eine Kopie an Standort 2 zu speichern.



Verwandte Informationen

- "Erstellen Sie eine ILM-Richtlinie: Überblick"
- "Erstellen einer vorgeschlagenen ILM-Richtlinie"

Beispiel 2: ILM-Regeln und Richtlinie für EC-Objektgrößen-Filterung

Die folgenden Beispielregeln und -Richtlinien dienen als Ausgangspunkt für die Definition einer ILM-Richtlinie, die nach Objektgröße gefiltert wird, um empfohlene EC-Anforderungen zu erfüllen.

> Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen.

ILM-Regel 1 beispielsweise 2: Verwenden Sie EC für Objekte über 1 MB

In diesem Beispiel werden Objekte mit einer ILM-Regel gelöscht, die größer als 1 MB sind.

> Das Verfahren zur Einhaltung von Datenkonsistenz eignet sich am besten für Objekte mit einer Größe von mehr als 1 MB. Verwenden Sie kein Erasure Coding für Objekte, die kleiner als 200 KB sind, um zu vermeiden, dass man sehr kleine Fragmente, die zur Fehlerkorrektur codiert wurden, managen muss.

Regeldefinition	Beispielwert
Regelname	Nur EC-Objekte > 1 MB
Referenzzeit	Aufnahmezeit

Regeldefinition	Beispielwert
Erweiterter Filter für Objektgröße	Objektgröße größer als 1 MB
Platzierungen	Erstellen Sie eine Kopie mit 2+1-Verfahren zur Fehlerkorrektur mit drei Standorten

ILM-Regel 2 beispielsweise 2: Zwei replizierte Kopien

Diese Beispiel-ILM-Regel erstellt zwei replizierte Kopien und filtert nicht nach Objektgröße. Diese Regel ist die Standardregel für die Richtlinie. Da die erste Regel alle Objekte mit einer Größe von mehr als 1 MB filtert, gilt diese Regel nur für Objekte, die 1 MB oder kleiner sind.

Regeldefinition	Beispielwert
Regelname	Zwei Replizierte Kopien
Referenzzeit	Aufnahmezeit
Erweiterter Filter für Objektgröße	Keine
Platzierungen	Bewahren Sie an Tag 0 bis für immer eine replizierte Kopie an Standort 1 und eine replizierte Kopie an Standort 2 auf.

ILM-Richtlinie beispielsweise 2: Verwenden Sie EC für Objekte über 1 MB

Dieses Beispiel für die ILM-Richtlinie umfasst zwei ILM-Regeln:

- Die erste Löschregel kodiert alle Objekte, die größer als 1 MB sind.
- Die zweite (Standard-) ILM-Regel erstellt zwei replizierte Kopien. Da Objekte größer als 1 MB nach Regel 1 herausgefiltert wurden, gilt Regel 2 nur für Objekte, die 1 MB oder kleiner sind.

Beispiel 3: ILM-Regeln und -Richtlinie für besseren Schutz von Image-Dateien

Mithilfe der folgenden Beispielregeln und -Richtlinie können Sie sicherstellen, dass Bilder mit mehr als 1 MB gelöscht werden und dass zwei Kopien aus kleineren Images erstellt werden.

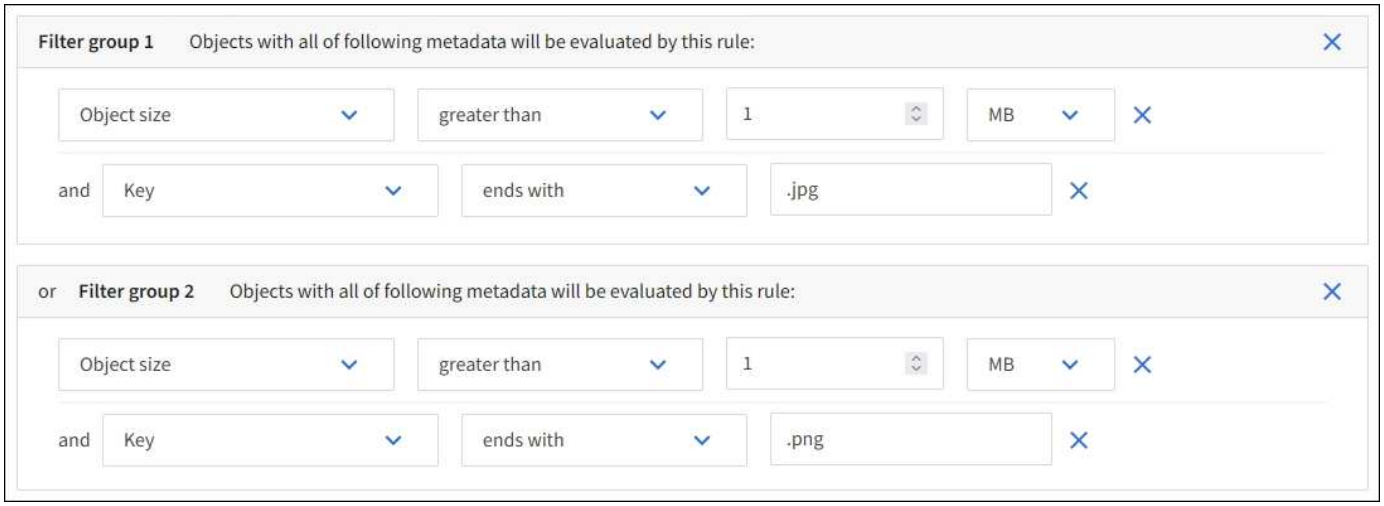
> Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen.

ILM-Regel 1 beispielsweise 3: Verwenden Sie EC für Bilddateien über 1 MB

Diese Beispiel ILM-Regel verwendet erweiterte Filterung zur Löschung von Code aller Bilddateien größer als 1 MB.

> Das Verfahren zur Einhaltung von Datenkonsistenz eignet sich am besten für Objekte mit einer Größe von mehr als 1 MB. Verwenden Sie kein Erasure Coding für Objekte, die kleiner als 200 KB sind, um zu vermeiden, dass man sehr kleine Fragmente, die zur Fehlerkorrektur codiert wurden, managen muss.

Regeldefinition	Beispielwert
Regelname	EC-Bilddateien > 1 MB
Referenzzeit	Aufnahmezeit
Erweiterter Filter für Objektgröße	Objektgröße größer als 1 MB
Erweiterte Filter für Schlüssel	• Endet mit .jpg • Endet mit .png
Platzierungen	Erstellen Sie eine Kopie mit 2+1-Verfahren zur Fehlerkorrektur mit drei Standorten



Da diese Regel als erste Regel in der Richtlinie konfiguriert ist, gilt die Anweisung für die Platzierung von Löschcodes nur für Dateien mit einer Größe von mehr als 1 MB.

ILM-Regel 2 beispielsweise 3: Erstellen Sie 2 replizierte Kopien für alle verbleibenden Image-Dateien

Diese Beispiel-ILM-Regel verwendet erweiterte Filterung, um anzugeben, dass kleinere Bilddateien repliziert werden. Da die erste Regel in der Richtlinie bereits Bilddateien mit einer Größe von mehr als 1 MB übereinstimmt, gilt diese Regel für Bilddateien mit einer Größe von 1 MB.

Regeldefinition	Beispielwert
Regelname	2 Kopien für Bilddateien
Referenzzeit	Aufnahmezeit
Erweiterte Filter für Schlüssel	• Endet mit .jpg • Endet mit .png
Platzierungen	Erstellung von 2 replizierten Kopien in zwei Storage Pools

ILM-Richtlinie beispielsweise 3: Besserer Schutz für Image-Dateien

Dieses Beispiel enthält drei Regeln für die ILM-Richtlinie:

- Die erste Löschregel kodiert alle Bilddateien größer als 1 MB.
- Die zweite Regel erstellt zwei Kopien aller verbleibenden Bilddateien (d. h. Bilder, die 1 MB oder kleiner sind).
- Die Standardregel gilt für alle übrigen Objekte (d. h. alle nicht-Image-Dateien).

Rule order	Rule name	Filters
1	EC image files > 1 MB	Object size is greater than 1 MB
2	2 copies for small images	Object size is less than or equal to 200 KB
Default	Default rule	—

Beispiel 4: ILM-Regeln und -Richtlinie für versionierte Objekte mit S3

Wenn Sie über einen S3-Bucket mit aktivierter Versionierung verfügen, können Sie die aktuellen Objektversionen verwalten, indem Sie Regeln in Ihre ILM-Richtlinie verwenden, die „`noncurrent time`“ als Referenzzeit verwenden.

> Wenn Sie eine begrenzte Aufbewahrungszeit für Objekte angeben, werden diese Objekte nach Erreichen des Zeitraums dauerhaft gelöscht. Stellen Sie sicher, dass Sie verstehen, wie lange die Objekte beibehalten werden.

Wie in diesem Beispiel dargestellt, können Sie den von versionierten Objekten verwendeten Storage mithilfe unterschiedlicher Anweisungen zur Platzierung von nicht aktuellen Objektversionen steuern.

Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen.

Um eine ILM-Richtliniensimulation für eine nicht aktuelle Version eines Objekts durchzuführen, müssen Sie die UUID oder CBID der Objektversion kennen. Um die UUID und die CBID zu finden, verwenden Sie "Objekt-Metadaten-Suche" Solange das Objekt noch aktuell ist.

Verwandte Informationen

- "So werden Objekte gelöscht"

ILM-Regel 1 beispielsweise 4: Speichern Sie drei Kopien für 10 Jahre

Diese ILM-Regel speichert eine Kopie jedes Objekts über einen Zeitraum von 10 Jahren an drei Standorten.

Diese Regel gilt für alle Objekte, unabhängig davon, ob sie versioniert sind.

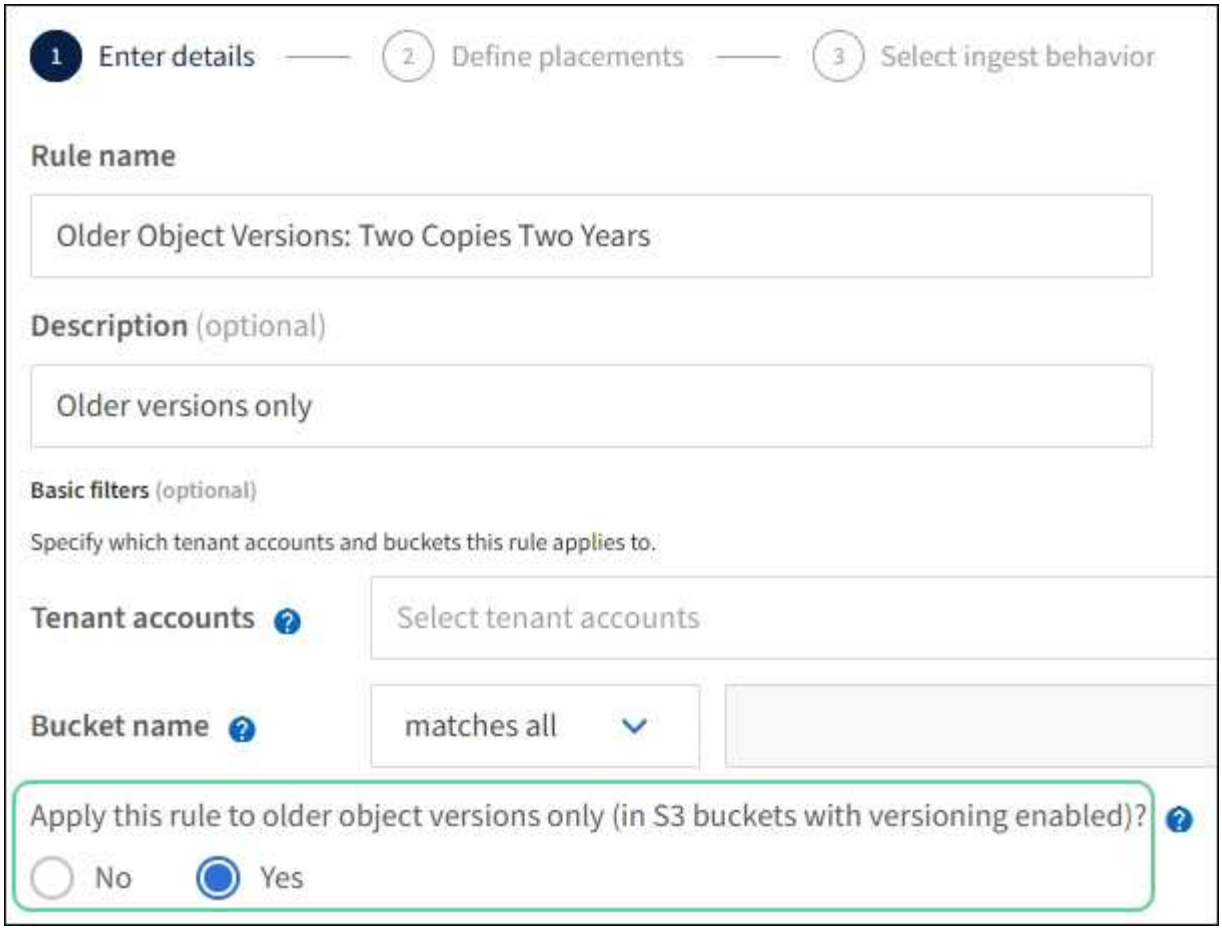
Regeldefinition	Beispielwert
Storage-Pools	Drei Speicherpools, die jeweils aus verschiedenen Rechenzentren mit den Namen Standort 1, Standort 2 und Standort 3 bestehen.
Regelname	Drei Kopien Zehn Jahre
Referenzzeit	Aufnahmezeit
Platzierungen	An Tag 0 sollten Sie drei replizierte Kopien 10 Jahre (3,652 Tage), eine an Standort 1, eine an Standort 2 und eine an Standort 3 aufbewahren. Löschen Sie Ende 10 Jahre alle Kopien des Objekts.

ILM-Regel 2 beispielsweise 4: Speichern Sie zwei Kopien nicht aktueller Versionen für zwei Jahre

In diesem Beispiel wird eine ILM-Regel zwei Kopien der nicht aktuellen Versionen eines versionierten S3 Objekts für zwei Jahre gespeichert.

Da ILM-Regel 1 für alle Versionen des Objekts gilt, müssen Sie eine weitere Regel erstellen, um nicht aktuelle Versionen herauszufiltern.

Um eine Regel zu erstellen, die „`noncurrent time`“ als Referenzzeit verwendet, wählen Sie **Yes** für die Frage „`Diese Regel nur auf ältere Objektversionen anwenden (in S3 Buckets mit aktivierter Versionierung)?`“ aus. Gehen Sie in Schritt 1 (Details eingeben) des Assistenten zum Erstellen einer ILM-Regel vor. Wenn Sie **Yes** auswählen, wird *noncurrent time* automatisch für die Referenzzeit ausgewählt, und Sie können keine andere Referenzzeit auswählen.



In diesem Beispiel werden nur zwei Kopien der nicht aktuellen Versionen gespeichert und diese Kopien für zwei Jahre gespeichert.

Regeldefinition	Beispielwert
Storage-Pools	Zwei Speicherpools, jeweils in verschiedenen Rechenzentren, Standort 1 und Standort 2.
Regelname	Nicht Aktuelle Versionen: Zwei Kopien Zwei Jahre
Referenzzeit	Nicht aktuelle Zeit Wird automatisch ausgewählt, wenn Sie für die Frage „`Diese Regel nur auf ältere Objektversionen anwenden (in S3 Buckets mit aktivierter Versionierung)?`“ auswählen. Im Assistenten zum Erstellen einer ILM-Regel.
Platzierungen	An Tag 0 relativ zur nicht aktuellen Zeit (d. h. ab dem Tag, an dem die Objektversion zur nicht aktuellen Version wird), behalten Sie zwei replizierte Kopien der nicht aktuellen Objektversionen für 2 Jahre (730 Tage), eine in Standort 1 und eine in Standort 2. Löschen Sie Ende 2 Jahre die nicht aktuellen Versionen.

ILM-Richtlinie z. B. 4: S3-versionierte Objekte

Wenn Sie ältere Versionen eines Objekts anders als die aktuelle Version verwalten möchten, müssen Regeln, die „`aktuelle Zeit`“ als Referenzzeit verwenden, in der ILM-Richtlinie vor Regeln erscheinen, die auf die aktuelle Objektversion angewendet werden.

Eine ILM-Richtlinie für S3-versionierte Objekte kann ILM-Regeln wie die folgenden umfassen:

- Bewahren Sie alle älteren (nicht aktuellen) Versionen jedes Objekts für 2 Jahre auf, beginnend mit dem Tag, an dem die Version nicht mehr aktuell wurde.

> Die Regeln „`nicht aktuelle Zeit`“ müssen in der Richtlinie vor den Regeln erscheinen, die für die aktuelle Objektversion gelten. Andernfalls werden die nicht aktuellen Objektversionen niemals mit der Regel „`nicht aktuelle Zeit`“ abgeglichen.

- Bei der Einspeisung können Sie drei replizierte Kopien erstellen und eine Kopie an jedem der drei Standorte speichern. Bewahren Sie 10 Jahre lang Kopien der aktuellen Objektversion auf.

Wenn Sie die Beispielrichtlinie simulieren, erwarten Sie, dass Testobjekte wie folgt bewertet werden:

- Alle nicht aktuellen Objektversionen würden mit der ersten Regel abgeglichen. Wenn eine nicht aktuelle Objektversion älter als zwei Jahre ist, wird diese durch ILM dauerhaft gelöscht (alle Kopien der nicht aktuellen Version, die aus dem Grid entfernt wurde).

> Um nicht aktuelle Objektversionen zu simulieren, müssen Sie die UUID oder CBID dieser Version verwenden. Solange das Objekt noch aktuell ist, können Sie verwenden "Objekt-Metadaten-Suche" Um seine UUID und CBID zu finden.

- Die aktuelle Objektversion würde mit der zweiten Regel abgeglichen. Wenn die aktuelle Objektversion über einen Zeitraum von 10 Jahren gespeichert wurde, fügt der ILM-Prozess eine Löschmarkierung als aktuelle Version des Objekts hinzu und macht die vorherige Objektversion „`noncurrent`“. Bei der nächsten ILM-Evaluierung stimmt diese nicht aktuelle Version mit der ersten Regel überein. Dadurch wird die Kopie an Standort 3 gelöscht und die beiden Kopien an Standort 1 und Standort 2 werden für weitere 2 Jahre gespeichert.

Beispiel 5: ILM-Regeln und Richtlinie für striktes Ingest-Verhalten

Ein Speicherortfilter und das strikte Aufnahmeverhalten in einer Regel verhindern, dass Objekte an einem bestimmten Datacenter-Standort gespeichert werden.

In diesem Beispiel will ein Mieter mit Sitz in Paris aufgrund von regulatorischen Bedenken einige Objekte nicht außerhalb der EU speichern. Andere Objekte, einschließlich aller Objekte aus anderen Mandantenkonten, können entweder im Rechenzentrum von Paris oder im Rechenzentrum der USA gespeichert werden.

> Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen.

Verwandte Informationen

- "Aufnahmeoptionen"
- "Erstellen Sie eine ILM-Regel: Wählen Sie Ingest Behavior aus"

ILM-Regel 1 beispielsweise 5: Strenge Einspeisung für das Pariser Rechenzentrum

In diesem Beispiel verwendet die ILM-Regel das strikte Ingest-Verhalten, um zu gewährleisten, dass Objekte, die von einem in Paris ansässigen Mieter in S3-Buckets gespeichert werden, wobei die Region auf eu-West-3 Region (Paris) eingestellt ist, nie im US-Rechenzentrum gespeichert werden.

Diese Regel gilt für Objekte, die zum Pariser Mieter gehören und die S3-Bucket-Region auf eu-West-3 (Paris) eingestellt ist.

Regeldefinition	Beispielwert
Mandantenkonto	Mieter von Paris
Erweiterter Filter	Die Positionsbeschränkung entspricht eu-West-3
Storage-Pools	Standort 1 (Paris)
Regelname	Strenge Einspeisung für ein Pariser Rechenzentrum
Referenzzeit	Aufnahmezeit
Platzierungen	An Tag 0 bewahren Sie zwei replizierte Kopien für immer in Standort 1 (Paris) auf.
Aufnahmeverhalten	Streng. Verwenden Sie bei der Einspeisung immer die Platzierungen dieser Regel. Die Aufnahme schlägt fehl, wenn es nicht möglich ist, zwei Kopien des Objekts im Pariser Rechenzentrum zu speichern.

ILM-Regel 2 beispielsweise 5: Ausgewogene Aufnahme für andere Objekte

Diese Beispiel-ILM-Regel verwendet das ausgewogene Ingest-Verhalten, um optimale ILM-Effizienz für Objekte zu erzielen, die nicht der ersten Regel zugeordnet sind. Zwei Kopien aller Objekte, die dieser Regel entsprechen, werden gespeichert - eins im US-Rechenzentrum und eins im Pariser Rechenzentrum. Wenn die Regel nicht sofort erfüllt werden kann, werden Zwischenkopien an jedem verfügbaren Ort gespeichert.

Diese Regel gilt für Objekte, die einem beliebigen Mieter und einer beliebigen Region angehören.

Regeldefinition	Beispielwert
Mandantenkonto	Ignorieren
Erweiterter Filter	*Nicht angegeben*
Storage-Pools	Standort 1 (Paris) und Standort 2 (USA)
Regelname	2 Kopien 2 Datacenter
Referenzzeit	Aufnahmezeit

Regeldefinition	Beispielwert
Platzierungen	Am Tag 0 werden zwei replizierte Kopien für immer in zwei Datacentern aufbewahrt
Aufnahmeverhalten	Ausgeglichen. Objekte, die dieser Regel entsprechen, werden nach Möglichkeit gemäß den Anweisungen zur Platzierung der Regel platziert. Andernfalls werden an jedem beliebigen Ort vorläufige Kopien angefertigt.

ILM-Richtlinie z. B. 5: Kombination von Aufnahmeverhalten

Die ILM-Beispielrichtlinie enthält zwei Regeln mit unterschiedlichen Aufnahmeverhalten.

Eine ILM-Richtlinie, die zwei unterschiedliche Aufnahmeverhalten nutzt, kann ILM-Regeln wie die folgenden umfassen:

- Speichern Sie Objekte, die zum Pariser Mieter gehören und die S3-Bucket-Region auf eu-West-3 (Paris) gesetzt ist, nur im Datacenter in Paris. Aufnahme fehlgeschlagen, wenn das Pariser Rechenzentrum nicht verfügbar ist.
- Speichern Sie alle anderen Objekte (einschließlich solcher, die zum Pariser Mieter gehören, jedoch über eine andere Bucket-Region verfügen) sowohl im US-Rechenzentrum als auch im Pariser Rechenzentrum. Erstellen Sie Zwischenkopien an einem beliebigen verfügbaren Speicherort, wenn die Platzierungsanweisung nicht erfüllt werden kann.

Wenn Sie die Beispielrichtlinie simulieren, erwarten Sie, dass Testobjekte wie folgt bewertet werden:

- Alle Objekte, die zum Pariser Mieter gehören und die S3-Bucket-Region auf eu-West-3 gesetzt haben, werden mit der ersten Regel abgeglichen und im Pariser Rechenzentrum gespeichert. Da die erste Regel strenge Einspeisung verwendet, werden diese Objekte nie im US-Rechenzentrum gespeichert. Wenn die Storage-Nodes im Pariser Datacenter nicht verfügbar sind, schlägt die Aufnahme fehl.
- Alle anderen Objekte werden mit der zweiten Regel abgeglichen, einschließlich Objekte, die zum Pariser Mieter gehören und für die die S3-Bucket-Region nicht auf eu-West-3 gesetzt ist. In jedem Datacenter wird eine Kopie jedes Objekts gespeichert. Da die zweite Regel jedoch eine ausgewogene Aufnahme verwendet und ein Datacenter nicht zur Verfügung steht, werden zwei Übergangskopien an jedem verfügbaren Standort gespeichert.

Beispiel 6: Ändern einer ILM-Richtlinie

Wenn Ihr Datenschutz geändert werden muss oder Sie neue Standorte hinzufügen, können Sie eine neue ILM-Richtlinie erstellen und aktivieren.

Vor dem Ändern einer Richtlinie muss verstanden werden, wie Änderungen an ILM-Platzierungen die Gesamt-Performance eines StorageGRID Systems vorübergehend beeinträchtigen können.

In diesem Beispiel wurde eine neue StorageGRID-Site mit einer Erweiterung hinzugefügt, und für die Speicherung von Daten am neuen Standort muss eine neue aktive ILM-Richtlinie implementiert werden. Um eine neue aktive Richtlinie zu implementieren, erstellen Sie zunächst eine vorgeschlagene Richtlinie von einer der beiden "Klonen einer vorhandenen Richtlinie *oder* von Grund auf neu". Danach müssen Sie "Simulieren" Und dann "Aktivieren" Die neue Politik.

Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen.

Wie sich eine Änderung einer ILM-Richtlinie auf die Performance auswirkt

Wenn Sie eine neue ILM-Richtlinie aktivieren, wird die Performance Ihres StorageGRID Systems möglicherweise vorübergehend beeinträchtigt, insbesondere dann, wenn aufgrund der Platzierungsanweisungen in der neuen Richtlinie viele vorhandene Objekte an einen neuen Standort verschoben werden müssen.

Bei der Aktivierung einer neuen ILM-Richtlinie verwendet StorageGRID sie zum Management aller Objekte, einschließlich vorhandener Objekte und neu aufgenommener Objekte. Prüfen Sie vor der Aktivierung einer neuen ILM-Richtlinie alle Änderungen an der Platzierung vorhandener replizierter und Erasure Coding-Objekte. Das Ändern des Speicherorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

Damit eine neue ILM-Richtlinie die Platzierung vorhandener replizierter und Erasure-Coded-Objekte nicht beeinträchtigt, können Sie folgende Möglichkeiten nutzen "Erstellen Sie eine ILM-Regel mit einem Filter für die Aufnahmezeit". Zum Beispiel ist **Ingest time *am oder nach <date and time>***, so dass die neue Regel nur für Objekte gilt, die am oder nach dem angegebenen Datum und der angegebenen Uhrzeit aufgenommen wurden.

Folgende Arten von ILM-Richtlinienänderungen, die vorübergehend Auswirkungen auf die StorageGRID Performance haben:

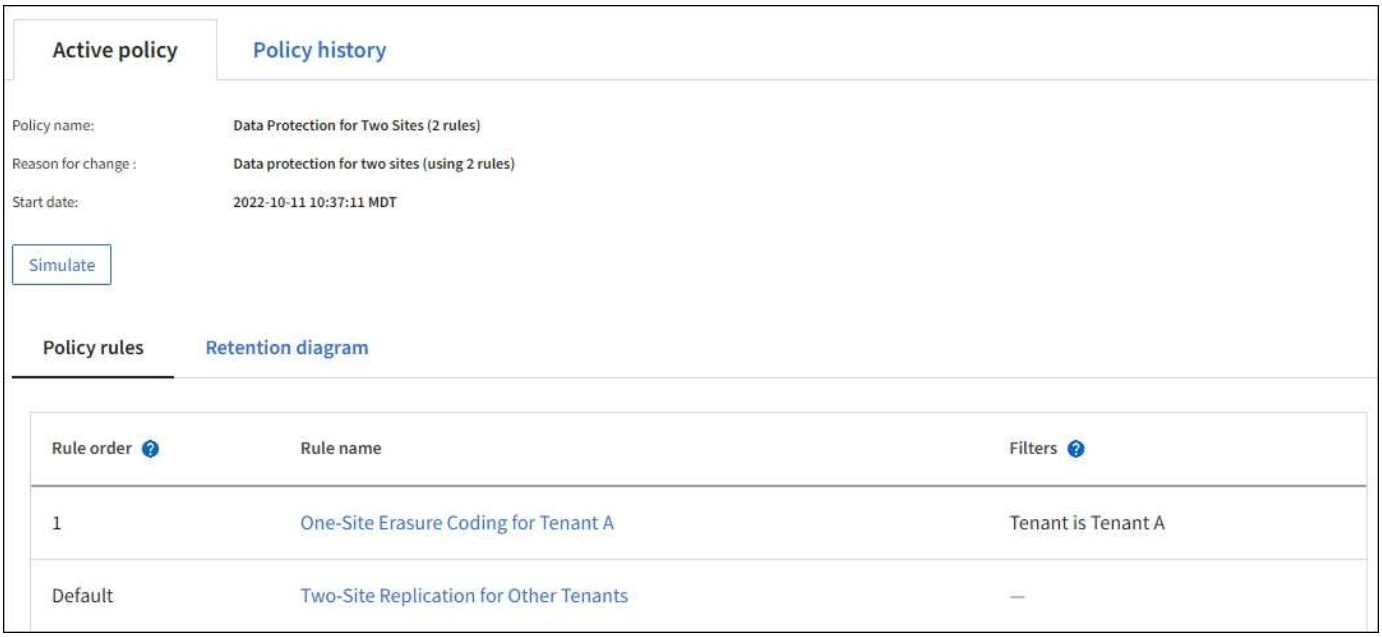
- Anwenden eines anderen Erasure Coding-Profils auf vorhandene Objekte, die zur Fehlerkorrektur codiert wurden

  StorageGRID betrachtet jedes Erasure Coding-Profil als einzigartig und wiederverwendet bei der Verwendung eines neuen Profils keine Fragmente des Erasure Coding.

- Ändern des für vorhandene Objekte erforderlichen Kopientyps; z. B. Konvertieren eines großen Anteils replizierter Objekte in Objekte mit Erasure-Coding-Verfahren.
- Kopien vorhandener Objekte werden an einen völlig anderen Speicherort verschoben, z. B. um eine große Anzahl von Objekten in einen oder aus einem Cloud-Storage-Pool oder an einen Remote-Standort zu verschieben.

Aktive ILM-Richtlinie z. B. 6: Datensicherung an zwei Standorten

In diesem Beispiel wurde die aktive ILM-Richtlinie ursprünglich für ein StorageGRID System mit zwei Standorten konzipiert und verwendet zwei ILM-Regeln.



In dieser ILM-Richtlinie werden Objekte, die von Mandanten A gehören, durch Erasure Coding von 2+1 an einem Standort geschützt, während Objekte, die zu allen anderen Mandanten gehören, durch die Replizierung mit zwei Kopien über zwei Standorte hinweg geschützt sind.

> Die erste Regel in diesem Beispiel verwendet einen erweiterten Filter, um sicherzustellen, dass das Erasure Coding nicht für kleine Objekte verwendet wird. Alle Objekte von Mandant A, die kleiner als 1 MB sind, werden durch die Standardregel geschützt, die Replikation verwendet.

Regel 1: Erasure Coding für einen Standort für Mandant A

Regeldefinition	Beispielwert
Regelname	Erasure Coding für einen Standort für Mandant A
Mandantenkonto	Mandant A
Storage-Pool	Standort 1
Platzierungen	2+1 Erasure Coding in Standort 1 vom Tag 0 bis ewig

Regel 2: Replizierung zwischen zwei Standorten für andere Mandanten

Regeldefinition	Beispielwert
Regelname	Replizierung an zwei Standorten für andere Mandanten
Mandantenkonto	Ignorieren
Storage-Pools	Standort 1 und Standort 2

Regeldefinition	Beispielwert
Platzierungen	Zwei replizierte Kopien von Tag 0 auf ewig: Eine Kopie an Standort 1 und eine Kopie an Standort 2.

Vorgeschlagene ILM-Richtlinie z. B. 6: Datensicherung an drei Standorten

In diesem Beispiel wird die ILM-Richtlinie durch eine neue Richtlinie für ein StorageGRID System mit drei Standorten ersetzt.

Nach einer Erweiterung zum Hinzufügen des neuen Standorts erstellte der Grid-Administrator zwei neue Speicherpools: Einen Speicherpool für Standort 3 und einen Speicherpool mit allen drei Standorten (nicht mit dem Standardspeicherpool Alle Storage-Nodes). Anschließend erstellte der Administrator zwei neue ILM-Regeln und eine neue vorgeschlagene ILM-Richtlinie, die auf den Schutz von Daten an allen drei Standorten ausgelegt ist.

Bei Aktivierung dieser neuen ILM-Richtlinie werden Objekte, die von Mandant A gehören, an drei Standorten durch 2+1 Erasure Coding geschützt, während Objekte, die zu anderen Mandanten gehören (und kleinere Objekte von Mandanten A), durch Replizierung mit 3 Kopien über drei Standorte hinweg gesichert werden.

Regel 1: Erasure Coding für drei Standorte für Mandant A

Regeldefinition	Beispielwert
Regelname	Three-Site Erasure Coding für Mandant A
Mandantenkonto	Mandant A
Storage-Pool	Alle 3 Standorte (einschließlich Standort 1, Standort 2 und Standort 3)
Platzierungen	2+1 Erasure Coding in allen 3 Standorten vom Tag 0 bis für immer

Regel 2: Replizierung an drei Standorten für andere Mandanten

Regeldefinition	Beispielwert
Regelname	Replikation von drei Standorten für andere Mandanten
Mandantenkonto	Ignorieren
Storage-Pools	Standort 1, Standort 2 und Standort 3
Platzierungen	Drei replizierte Kopien von Tag 0 bis ewig: Eine Kopie an Standort 1, eine Kopie an Standort 2 und eine Kopie an Standort 3.

Aktivierung der vorgeschlagenen ILM-Richtlinie beispielsweise 6

Wenn Sie eine neue vorgeschlagene ILM-Richtlinie aktivieren, können vorhandene Objekte an neue Orte verschoben oder neue Objektkopien für vorhandene Objekte erstellt werden, basierend auf den Anweisungen

zur Platzierung in neuen oder aktualisierten Regeln.

> Fehler in einer ILM-Richtlinie können zu nicht wiederherstellbaren Datenverlusten führen. Prüfen und simulieren Sie die Richtlinie sorgfältig, bevor Sie sie aktivieren, um sicherzustellen, dass sie wie vorgesehen funktioniert.

> Bei der Aktivierung einer neuen ILM-Richtlinie verwendet StorageGRID sie zum Management aller Objekte, einschließlich vorhandener Objekte und neu aufgenommener Objekte. Prüfen Sie vor der Aktivierung einer neuen ILM-Richtlinie alle Änderungen an der Platzierung vorhandener replizierter und Erasure Coding-Objekte. Das Ändern des Speicherorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

Was passiert, wenn sich die Anweisungen zur Einhaltung von Datenkonsistenz ändern

In der derzeit aktiven ILM-Richtlinie für dieses Beispiel sind Objekte, die zu Mandant A gehören, durch den Erasure Coding 2+1 an Standort 1 geschützt. In der neuen vorgeschlagenen ILM-Richtlinie werden Objekte von Mandant A durch Erasure Coding 2+1 an Standorten 1, 2 und 3 geschützt.

Wenn die neue ILM-Richtlinie aktiviert ist, werden die folgenden ILM-Vorgänge durchgeführt:

- Neue von Mandanten A aufgenommene Objekte werden in zwei Datenfragmente aufgeteilt und ein Paritätsfragment wird hinzugefügt. Dann wird jedes der drei Fragmente an einem anderen Ort gespeichert.
- Die vorhandenen Objekte, die von Mandant A gehören, werden bei der laufenden ILM-Überprüfung neu bewertet. Da die ILM-Anweisungen ein neues Erasure-Coding-Profil verwenden, werden völlig neue Fragmente erstellt und an die drei Standorte verteilt, die zur Fehlerkorrektur codiert wurden.

> Die vorhandenen 2+1-Fragmente an Standort 1 werden nicht wiederverwendet. StorageGRID betrachtet jedes Erasure Coding-Profil als einzigartig und wiederverwendet bei der Verwendung eines neuen Profils keine Fragmente des Erasure Coding.

Was geschieht, wenn sich Replikationsanweisungen ändern

In der derzeit aktiven ILM-Richtlinie für dieses Beispiel werden Objekte anderer Mandanten mithilfe von zwei replizierten Kopien in Storage Pools an Standorten 1 und 2 geschützt. In der neuen vorgeschlagenen ILM-Richtlinie werden Objekte anderer Mandanten mit drei replizierten Kopien in Storage Pools an Standorten 1, 2 und 3 gesichert.

Wenn die neue ILM-Richtlinie aktiviert ist, werden die folgenden ILM-Vorgänge durchgeführt:

- Wenn ein anderer Mandant als Mandant A ein neues Objekt aufnimmt, erstellt StorageGRID drei Kopien und speichert eine Kopie an jedem Standort.
- Vorhandene Objekte, die zu diesen anderen Mandanten gehören, werden bei der laufenden ILM-Überprüfung neu bewertet. Da die vorhandenen Objektkopien an Standort 1 und Standort 2 weiterhin die Replizierungsanforderungen der neuen ILM-Regel erfüllen, muss StorageGRID nur eine neue Kopie des Objekts für Standort 3 erstellen.

Auswirkungen der Aktivierung dieser Richtlinie auf die Performance

Wenn die vorgeschlagene ILM-Richtlinie in diesem Beispiel aktiviert ist, wird die Gesamtleistung dieses StorageGRID Systems vorübergehend beeinträchtigt. Wenn die Grid-Ressourcen höher als die normalen Level sind, werden neue Fragmente, die nach der Fehlerkorrektur codiert wurden, für vorhandene Objekte von

Mandant A und neue replizierte Kopien an Standort 3 für vorhandene Objekte anderer Mandanten erstellt.

Aufgrund der Änderung der ILM-Richtlinie können Lese- und Schreibanfragen von Clients vorübergehend höhere Latenzen aufweisen als die normalen Latenzen. Die Latenzen kehren wieder auf die normalen Werte zurück, nachdem die Anweisungen zur Platzierung im gesamten Grid vollständig implementiert wurden.

Um Ressourcenprobleme bei der Aktivierung einer neuen ILM-Richtlinie zu vermeiden, können Sie den erweiterten Filter für die Aufnahmezeit in jeder Regel verwenden, die den Speicherort einer großen Anzahl vorhandener Objekte ändern könnte. Legen Sie für die Aufnahme-Zeit den Wert fest, der ungefähr der Zeit entspricht, zu der die neue Richtlinie in Kraft tritt, um sicherzustellen, dass vorhandene Objekte nicht unnötig verschoben werden.

> Wenden Sie sich an den technischen Support, wenn Sie die Verarbeitungsgeschwindigkeit von Objekten nach einer ILM-Richtlinienänderung verlangsamen oder erhöhen müssen.

Beispiel 7: Konforme ILM-Richtlinie für S3 Object Lock

Sie können den S3-Bucket, ILM-Regeln und ILM-Richtlinie in diesem Beispiel als Ausgangspunkt verwenden, wenn Sie eine ILM-Richtlinie definieren, um die Objektschutz- und Aufbewahrungsanforderungen für Objekte in Buckets zu erfüllen, wenn S3-Objektsperre aktiviert ist.

> Wenn Sie die Funktion „ältere Compliance“ in früheren StorageGRID Versionen verwendet haben, können Sie dieses Beispiel auch zur Verwaltung vorhandener Buckets verwenden, in denen die alte Compliance-Funktion aktiviert ist.

> Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen.

Verwandte Informationen

- "Objekte managen mit S3 Object Lock"
- "ILM-Richtlinie erstellen"

Bucket und Objekte für S3 Object Lock Beispiel

In diesem Beispiel hat ein S3-Mandantenkonto mit der Bezeichnung „Bank of ABC“ durch den Mandanten-Manager einen Bucket erstellt, der mit S3-Objektsperre aktiviert wurde, um kritische Bankdatensätze zu speichern.

Bucket-Definition	Beispielwert
Name Des Mandantenkontos	Bank von ABC
Bucket-Name	bankaufzeichnungen
Bucket-Region	US-East-1 (Standard)

Jedes Objekt und jede Objektversion, die dem Bucket für die Bankdatensätze hinzugefügt wird, verwenden die

folgenden Werte für `retain-until-date` Und `legal hold` Einstellungen.

Einstellung für jedes Objekt	Beispielwert
`retain-until-date`	`"2030-12-30T23:59:59Z"` (30. Dezember 2030) Jede Objektversion hat ihre eigene `retain-until-date` Einstellung. Diese Einstellung kann erhöht, aber nicht verringert werden.
`legal hold`	`"OFF"` (Nicht wirksam) Eine gesetzliche Aufbewahrungsphase kann jederzeit während der Aufbewahrungsfrist auf jeder Objektversion platziert oder aufgehoben werden. Befindet sich ein Objekt unter einem Legal Hold, kann das Objekt auch dann nicht gelöscht werden, wenn das `retain-until-date` Wurde erreicht.

ILM-Regel 1 für S3 Object Lock Beispiel: Profil für Erasure Coding mit Bucket-Zuordnung

Diese Beispiel-ILM-Regel gilt nur für das S3-Mandantenkonto namens Bank of ABC. Sie entspricht jedem Objekt im `bank-records` Bucket und anschließend Erasure Coding zur Speicherung des Objekts auf Storage Nodes an drei Datacenter-Standorten mithilfe eines 6+3 Erasure Coding-Profils Diese Regel erfüllt die Anforderungen von Buckets mit aktivierter S3 Object Lock: Eine Kopie wird auf Storage-Nodes vom Tag 0 bis dauerhaft aufbewahrt. Als Referenzzeit wird die Aufnahmezeit verwendet.

Regeldefinition	Beispielwert
Regelname	Konforme Regel: EC-Objekte in Bank-Records Bucket - Bank of ABC
Mandantenkonto	Bank von ABC
Bucket-Name	`bank-records`
Erweiterter Filter	Objektgröße (MB) größer als 1 **Hinweis:** dieser Filter stellt sicher, dass das Erasure Coding nicht für Objekte 1 MB oder kleiner verwendet wird.

Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit
Platzierungen	Ab Tag 0 dauerhaft speichern
Verfahren Zur Einhaltung Von Datenkonsistenz	• Erstellen einer mit Erasure Coding verschlüsselten Kopie auf Storage-Nodes an drei Datacenter-Standorten • Verwendet das Erasure Coding-Schema 6+3

ILM-Regel 2 für S3 Object Lock Beispiel: Nicht konforme Regel

Diese Beispiel-ILM-Regel speichert zunächst zwei replizierte Objektkopien auf Storage Nodes. Nach einem Jahr wird für immer eine Kopie auf einem Cloud-Storage-Pool gespeichert. Da diese Regel einen Cloud-Storage-Pool verwendet, ist diese nicht konform und gilt nicht für Objekte in Buckets, deren S3-Objektsperre aktiviert ist.

Regeldefinition	Beispielwert
Regelname	Nicht konforme Regel: Cloud Storage Pool
Mandantenkonten	Nicht angegeben
Bucket-Name	Nicht angegeben, gilt aber nur für Buckets, für die die S3-Objektsperre (oder die ältere Compliance-Funktion) nicht aktiviert ist.
Erweiterter Filter	Nicht angegeben

Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit
Platzierungen	• Halten Sie am Tag 0 zwei replizierte Kopien auf Storage Nodes in Datacenter 1 und Datacenter 2 für 365 Tage • Nach einem Jahr sollte eine replizierte Kopie immer in einem Cloud-Storage-Pool aufbewahrt werden

ILM-Regel 3 für S3 Object Lock Beispiel: Standardregel

Diese Beispiel-ILM-Regel kopiert Objektdaten in Storage-Pools in zwei Datacentern. Diese konforme Regel wurde als Standardregel in der ILM-Richtlinie konzipiert. Es enthält keine Filter, verwendet keine nicht aktuelle Referenzzeit und erfüllt die Anforderungen von Buckets mit aktivierter S3 Objektsperre: Zwei Objektkopien werden auf Storage-Nodes aufbewahrt von Tag 0 bis für immer und verwenden die Aufnahme als Referenzzeit.

Regeldefinition	Beispielwert
Regelname	Standard-konforme Regel: Zwei Kopien zwei Rechenzentren
Mandantenkonto	Nicht angegeben
Bucket-Name	Nicht angegeben
Erweiterter Filter	Nicht angegeben

Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit

Regeldefinition	Beispielwert
Platzierungen	Halten Sie von Tag 0 bis für immer zwei replizierte Kopien bereit – eins auf Storage-Nodes im Datacenter 1 und eins auf Storage-Nodes im Datacenter 2.

Konforme ILM-Richtlinie für S3 Object Lock Beispiel

Zum Erstellen einer ILM-Richtlinie, die alle Objekte in Ihrem System effektiv schützt, auch in Buckets, deren S3-Objektsperre aktiviert ist, müssen Sie ILM-Regeln auswählen, die die Storage-Anforderungen für alle Objekte erfüllen. Anschließend müssen Sie die vorgeschlagene Richtlinie simulieren und aktivieren.

Fügen Sie der Richtlinie Regeln hinzu

In diesem Beispiel umfasst die ILM-Richtlinie drei ILM-Regeln in der folgenden Reihenfolge:

1. Eine konforme Regel, die Erasure Coding verwendet, um Objekte mit einer Größe von mehr als 1 MB in einem bestimmten Bucket zu schützen. Dabei ist S3 Object Lock aktiviert. Die Objekte werden von Tag 0 bis für immer auf Speicherknoten gespeichert.
2. Eine nicht konforme Regel, die zwei replizierte Objektkopien auf Storage-Nodes für ein Jahr erstellt und dann eine Objektkopie für immer in einen Cloud Storage Pool verschiebt. Diese Regel gilt nicht für Buckets, für die S3-Objektsperre aktiviert ist, da sie einen Cloud-Storage-Pool verwendet.
3. Die standardmäßige, konforme Regel, die zwei replizierte Objektkopien auf Storage-Nodes erstellt, von Tag 0 bis für immer.

Simulieren Sie die vorgeschlagene Richtlinie

Nachdem Sie in Ihrer vorgeschlagenen Richtlinie Regeln hinzugefügt, eine standardkonforme Regel ausgewählt und die anderen Regeln festgelegt haben, sollten Sie die Richtlinie simulieren, indem Sie Objekte aus dem Bucket testen, wobei S3 Object Lock aktiviert ist und aus anderen Buckets. Wenn Sie beispielsweise die Beispielrichtlinie simulieren, erwarten Sie, dass Testobjekte wie folgt bewertet werden:

- Die erste Regel entspricht nur Testobjekten, die mehr als 1 MB in den Bucket-Bankdatensätzen für den Mandanten der Bank of ABC enthalten sind.
- Die zweite Regel entspricht allen Objekten in allen nicht-konformen Buckets für alle anderen Mandantenkonten.
- Die Standardregel stimmt mit den folgenden Objekten überein:
  - Objekte 1 MB oder kleiner in den Bucket-Bankdatensätzen für die Bank of ABC-Mieter.
  - Objekte in jedem anderen Bucket, bei dem die S3-Objektsperre für alle anderen Mandantenkonten aktiviert ist

Aktivieren Sie die Richtlinie

Wenn Sie mit der neuen Richtlinie zufrieden sind, dass Objektdaten wie erwartet geschützt werden, können Sie sie aktivieren.

Systemhärtung

Systemhärtung: Übersicht

Systemhärtung ist der Prozess, bei dem so viele Sicherheitsrisiken wie möglich durch ein StorageGRID System beseitigt werden.

Dieses Dokument bietet einen Überblick über die StorageGRID-spezifischen Härtungsrichtlinien. Diese Richtlinien sind eine Ergänzung zu branchenüblichen Best Practices zur Systemhärtung. In diesen Richtlinien wird beispielsweise davon ausgegangen, dass Sie für StorageGRID starke Passwörter verwenden, HTTPS statt HTTP verwenden und sofern verfügbar die zertifikatbasierte Authentifizierung aktivieren.

Bei der Installation und Konfiguration von StorageGRID können Sie diese Richtlinien nutzen, um alle vorgeschriebenen Sicherheitsziele bezüglich Vertraulichkeit, Integrität und Verfügbarkeit des Informationssystems zu erfüllen.

StorageGRID folgt dem "NetApp Richtlinie zur Bearbeitung von Schwachstellen". Gemeldete Schwachstellen werden gemäß dem Prozess der Reaktion auf Produktsicherheitsvorfälle überprüft und behoben.

Allgemeine Überlegungen zur Erhöhung der StorageGRID-Systeme

Beim Härten eines StorageGRID Systems sind folgende Punkte zu beachten:

- Welches der drei implementierten StorageGRID-Netzwerke ist implementiert? Alle StorageGRID-Systeme müssen das Grid-Netzwerk verwenden, aber Sie können auch das Admin-Netzwerk, das Client-Netzwerk oder beide verwenden. Jedes Netzwerk weist unterschiedliche Sicherheitsüberlegungen auf.
- Die Art der Plattformen, die Sie für die einzelnen Nodes Ihres StorageGRID Systems verwenden. StorageGRID Nodes können auf VMware Virtual Machines innerhalb einer Container-Engine auf Linux-Hosts oder als dedizierte Hardware-Appliances implementiert werden. Jeder Plattformtyp verfügt über eigene Best Practices zur Härtung.
- Wie vertrauenswürdig sind die Mandantenkonten? Wenn Sie ein Service-Provider mit nicht vertrauenswürdigen Mandantenkonten sind, haben Sie andere Sicherheitsbedenken als, wenn Sie nur vertrauenswürdige interne Mandanten verwenden.
- Welche Sicherheitsanforderungen und -Konventionen von Ihrem Unternehmen erfüllt werden? Möglicherweise müssen Sie bestimmte gesetzliche oder unternehmensbezogene Anforderungen einhalten.

Hardening-Richtlinien für Software Upgrades

Sie müssen Ihr StorageGRID-System und die zugehörigen Services immer auf dem neuesten Stand halten, um sich gegen Angriffe zu wehren.

Upgrades auf StorageGRID Software

Sofern möglich, sollten Sie ein Upgrade der StorageGRID Software auf das neueste Hauptversion oder auf das vorherige Hauptversion durchführen. Durch die aktuelle Nutzung von StorageGRID lässt sich die Zeit bis zur aktiven Nutzung bekannter Schwachstellen reduzieren und gleichzeitig die Angriffsfläche insgesamt verringern. Darüber hinaus enthalten die neuesten StorageGRID Versionen häufig Funktionen zur Erhöhung der Sicherheit, die in früheren Versionen nicht enthalten sind.

Konsultieren Sie die "NetApp Interoperabilitäts-Matrix-Tool" (IMT), um zu ermitteln, welche Version der StorageGRID-Software Sie verwenden sollen. Wenn ein Hotfix erforderlich ist, priorisiert NetApp die Erstellung von Updates der letzten Versionen. Einige Patches sind möglicherweise nicht mit früheren Versionen kompatibel.

- Die neuesten StorageGRID Versionen und Hotfixes können Sie unter herunterladen "NetApp Downloads: StorageGRID".
- Informationen zum Aktualisieren der StorageGRID-Software finden Sie im "Upgrade-Anweisungen".
- Informationen zum Anwenden eines Hotfix finden Sie im "StorageGRID Hotfix Verfahren".

Upgrades auf externe Dienste

Externe Services können Schwachstellen aufweisen, die StorageGRID indirekt beeinträchtigen. Sie sollten sicherstellen, dass die Services, von denen StorageGRID abhängig sind, immer auf dem neuesten Stand sind. Zu diesen Services gehören LDAP, KMS (oder KMIP Server), DNS und NTP.

Verwenden Sie die "NetApp Interoperabilitäts-Matrix-Tool" Um eine Liste der unterstützten Versionen zu erhalten.

Upgrades auf Hypervisoren

Wenn die StorageGRID-Nodes auf VMware oder einem anderen Hypervisor ausgeführt werden, müssen Sie sicherstellen, dass die Hypervisor-Software und die Firmware auf dem neuesten Stand sind.

Verwenden Sie die "NetApp Interoperabilitäts-Matrix-Tool" Um eine Liste der unterstützten Versionen zu erhalten.

Upgrades auf Linux-Knoten

Wenn Ihre StorageGRID-Knoten Linux-Hostplattformen verwenden, müssen Sie sicherstellen, dass Sicherheitsupdates und Kernel-Updates auf das Host-Betriebssystem angewendet werden. Darüber hinaus müssen Sie Firmware-Updates auf anfällige Hardware anwenden, wenn diese Updates verfügbar sind.

Verwenden Sie die "NetApp Interoperabilitäts-Matrix-Tool" Um eine Liste der unterstützten Versionen zu erhalten.

Hardening Guidelines for StorageGRID Networks

Das StorageGRID System unterstützt bis zu drei Netzwerkschnittstellen pro Grid Node. So können Sie das Netzwerk für jeden einzelnen Grid Node so konfigurieren, dass er Ihren Sicherheits- und Zugriffsanforderungen entspricht.

Ausführliche Informationen zu StorageGRID-Netzwerken finden Sie im "StorageGRID-Netzwerktypen".

Richtlinien für Grid Network

Sie müssen ein Grid-Netzwerk für den gesamten internen StorageGRID-Datenverkehr konfigurieren. Alle Grid-Nodes sind im Grid-Netzwerk und müssen mit allen anderen Nodes kommunizieren können.

Befolgen Sie bei der Konfiguration des Grid-Netzwerks die folgenden Richtlinien:

- Stellen Sie sicher, dass das Netzwerk von nicht vertrauenswürdigen Clients, wie denen im offenen Internet, geschützt ist.
- Wenn möglich, verwenden Sie das Grid-Netzwerk ausschließlich für den internen Datenverkehr. Sowohl das Admin-Netzwerk als auch das Client-Netzwerk haben zusätzliche Firewall-Einschränkungen, die externen Datenverkehr zu internen Diensten blockieren. Die Verwendung des Grid-Netzwerks für externen Client-Datenverkehr wird unterstützt, aber diese Verwendung bietet weniger Schutzebenen.

- Wenn die StorageGRID Implementierung mehrere Datacenter umfasst, verwenden Sie ein virtuelles privates Netzwerk (VPN) oder eine vergleichbare Position im Grid-Netzwerk, um den internen Datenverkehr zusätzlich zu schützen.
- Einige Wartungsverfahren erfordern einen sicheren SSH-Zugriff (Shell) auf Port 22 zwischen dem primären Admin-Node und allen anderen Grid-Nodes. Verwenden Sie eine externe Firewall, um den SSH-Zugriff auf vertrauenswürdige Clients zu beschränken.

Richtlinien für Admin Network

Das Admin-Netzwerk wird normalerweise für administrative Aufgaben verwendet (vertrauenswürdige Mitarbeiter, die den Grid Manager oder SSH verwenden) und für die Kommunikation mit anderen vertrauenswürdigen Services wie LDAP, DNS, NTP oder KMS (oder KMIP Server). StorageGRID ist jedoch nicht intern durchsetzen.

Wenn Sie das Admin-Netzwerk verwenden, befolgen Sie die folgenden Richtlinien:

- Blockieren Sie alle internen Traffic-Ports im Admin-Netzwerk. Siehe "Liste der internen Ports".
- Wenn nicht vertrauenswürdige Clients auf das Admin-Netzwerk zugreifen können, blockieren Sie den Zugriff auf StorageGRID im Admin-Netzwerk mit einer externen Firewall.

Richtlinien für Client Network

Das Client-Netzwerk wird typischerweise für Mandanten und zur Kommunikation mit externen Services wie dem CloudMirror Replikationsservice oder einem anderen Plattformservice verwendet. StorageGRID ist jedoch nicht intern durchsetzen.

Wenn Sie das Client-Netzwerk verwenden, befolgen Sie die folgenden Richtlinien:

- Blockieren Sie alle internen Traffic-Ports im Client-Netzwerk. Siehe "Liste der internen Ports".
- Eingehende Clientdatenverkehr nur an explizit konfigurierten Endpunkten akzeptieren. Weitere Informationen finden Sie unter "Management der Firewall-Kontrollen".

Hardening-Richtlinien für StorageGRID-Knoten

StorageGRID Nodes können auf VMware Virtual Machines innerhalb einer Container-Engine auf Linux-Hosts oder als dedizierte Hardware-Appliances implementiert werden. Jeder Plattformtyp und jeder Node-Typ verfügt über eigene Best Practices zur Härtung.

Firewall-Konfiguration

Im Rahmen des System-Hardening-Prozesses müssen Sie externe Firewall-Konfigurationen überprüfen und ändern, damit der Datenverkehr nur von den IP-Adressen und den Ports akzeptiert wird, von denen er unbedingt benötigt wird.

StorageGRID verfügt über eine interne Firewall auf jedem Node, die die Sicherheit Ihres Grids erhöht, indem Sie den Netzwerkzugriff auf den Node kontrollieren können. Sollten Sie "Interne Firewall-Kontrollen verwalten" Um den Netzwerkzugriff auf allen Ports zu verhindern, mit Ausnahme der Ports, die für Ihre spezifische Grid-Bereitstellung erforderlich sind. Die Konfigurationsänderungen, die Sie auf der Seite Firewall-Steuerung vornehmen, werden für jeden Knoten bereitgestellt.

Sie können insbesondere diese Bereiche managen:

- **Privilegierte Adressen**: Sie können ausgewählten IP-Adressen oder Subnetzen erlauben, auf Ports zuzugreifen, die durch Einstellungen auf der Registerkarte externen Zugriff verwalten geschlossen werden.
- **Externen Zugriff verwalten**: Sie können Ports schließen, die standardmäßig geöffnet sind, oder zuvor geschlossene Ports wieder öffnen.
- **Nicht vertrauenswürdiges Client-Netzwerk**: Sie können angeben, ob ein Knoten eingehenden Datenverkehr vom Client-Netzwerk sowie die zusätzlichen Ports, die geöffnet werden sollen, wenn nicht vertrauenswürdiges Client-Netzwerk konfiguriert ist, anvertraut.

Diese interne Firewall bietet zwar eine zusätzliche Schutzschicht gegen häufig vorgängige Bedrohungen, sie macht aber keine externe Firewall erforderlich.

Eine Liste aller internen und externen Ports, die von StorageGRID verwendet werden, finden Sie unter "Referenz für Netzwerk-Ports".

Deaktivieren Sie nicht verwendete Dienste

Bei allen StorageGRID-Knoten sollten Sie den Zugriff auf nicht genutzte Services deaktivieren oder blockieren. Wenn Sie beispielsweise nicht planen, den Clientzugriff auf die Audit-Freigaben für NFS zu konfigurieren, blockieren oder deaktivieren Sie den Zugriff auf diese Services.

Virtualisierung, Container und gemeinsam genutzte Hardware

Vermeiden Sie bei allen StorageGRID Nodes die Ausführung von StorageGRID auf derselben physischen Hardware wie die nicht vertrauenswürdige Software. Setzen Sie nicht voraus, dass ein Hypervisor-Schutz Malware den Zugriff auf StorageGRID geschützte Daten verhindert, wenn sich sowohl StorageGRID als auch Malware auf derselben physischen Hardware befinden. So nutzen beispielsweise die Meltdown- und Specter-Angriffe kritische Schwachstellen in modernen Prozessoren und ermöglichen Programmen, Daten im Arbeitsspeicher auf demselben Computer zu stehlen.

Schutz von Nodes während der Installation

Erlauben Sie nicht vertrauenswürdigen Benutzern den Zugriff auf StorageGRID-Knoten über das Netzwerk, wenn die Knoten installiert werden. Nodes sind erst dann vollständig sicher, wenn sie sich dem Grid angeschlossen haben.

Richtlinien für Admin-Nodes

Admin Nodes stellen Managementservices wie Systemkonfiguration, Monitoring und Protokollierung bereit. Wenn Sie sich beim Grid Manager oder dem Tenant Manager anmelden, stellen Sie eine Verbindung zu einem Admin-Node her.

Befolgen Sie diese Richtlinien, um die Admin-Knoten in Ihrem StorageGRID-System zu sichern:

- Sichern Sie alle Admin-Knoten von nicht vertrauenswürdigen Clients, wie denen im offenen Internet. Stellen Sie sicher, dass kein nicht vertrauenswürdiger Client auf einen beliebigen Admin-Node im Grid-Netzwerk, auf das Admin-Netzwerk oder auf das Client-Netzwerk zugreifen kann.
- StorageGRID-Gruppen steuern den Zugriff auf Grid Manager- und Mandantenmanager-Funktionen. Gewähren Sie jeder Gruppe von Benutzern die erforderlichen Mindestberechtigungen für ihre Rolle, und verwenden Sie den schreibgeschützten Zugriffsmodus, um zu verhindern, dass Benutzer die Konfiguration ändern.
- Verwenden Sie bei der Verwendung von StorageGRID Load Balancer-Endpunkten Gateway-Nodes anstelle von Admin-Nodes für nicht vertrauenswürdigen Client-Datenverkehr.

- Wenn Sie nicht vertrauenswürdige Mandanten haben, erlauben Sie ihnen keinen direkten Zugriff auf den Mandantenmanager oder die Mandantenmanagement-API. Verwenden Sie stattdessen ein Mandantenportal oder ein externes Mandantenmanagement-System, das mit der Mandantenmanagement-API interagiert.
- Optional können Sie einen Admin-Proxy verwenden, um die AutoSupport-Kommunikation zwischen Admin-Nodes und dem NetApp Support besser zu steuern. Siehe die Schritte für "Erstellen eines Admin-Proxys".
- Verwenden Sie optional die eingeschränkten 8443- und 9443-Ports, um die Kommunikation zwischen Grid Manager und Tenant Manager voneinander zu trennen. Blockieren Sie den gemeinsam genutzten Port 443 und beschränken Sie Mandantenanforderungen auf Port 9443, um zusätzlichen Schutz zu bieten.
- Verwenden Sie optional separate Admin-Nodes für Grid-Administratoren und Mandantenbenutzer.

Weitere Informationen finden Sie in den Anweisungen für "Administration von StorageGRID".

Richtlinien für Storage-Nodes

Storage-Nodes managen und speichern Objektdaten und Metadaten. Befolgen Sie diese Richtlinien, um die Speicherknoten in Ihrem StorageGRID System zu sichern.

- Nicht vertrauenswürdige Clients dürfen keine direkte Verbindung zu Storage-Nodes herstellen. Verwenden Sie einen Load Balancer-Endpunkt, der von einem Gateway-Node oder einem Load Balancer eines Drittanbieters bereitgestellt wird.
- Aktivieren Sie keine ausgehenden Dienste für nicht vertrauenswürdige Mandanten. Wenn Sie beispielsweise das Konto für einen nicht vertrauenswürdigen Mandanten erstellen, erlauben Sie dem Mandanten nicht, seine eigene Identitätsquelle zu verwenden, und erlauben Sie nicht die Nutzung von Plattformdiensten. Siehe die Schritte für "Erstellen eines Mandantenkontos".
- Verwenden Sie einen Drittanbieter-Load-Balancer für nicht vertrauenswürdigen Client-Datenverkehr. Der Lastausgleich von Drittanbietern bietet mehr Kontrolle und zusätzlichen Schutz vor Angriffen.
- Optional können Sie einen Storage Proxy verwenden, um mehr Kontrolle über Cloud Storage Pools und die Kommunikation von Plattform-Services von Storage Nodes zu externen Services zu erhalten. Siehe die Schritte für "Erstellen eines Speicherproxys".
- Optional können Sie über das Client-Netzwerk eine Verbindung zu externen Diensten herstellen. Wählen Sie dann **CONFIGURATION** > **Security** > **Firewall Control** > **UnTrusted Client Networks** aus und geben Sie an, dass das Client-Netzwerk auf dem Storage Node nicht vertrauenswürdig ist. Der Speicherknoten akzeptiert keinen eingehenden Datenverkehr im Client-Netzwerk mehr, aber er erlaubt weiterhin ausgehende Anfragen für Platform Services.

Richtlinien für Gateway-Nodes

Gateway-Knoten stellen eine optionale Schnittstelle zum Lastausgleich bereit, über die Client-Anwendungen eine Verbindung zu StorageGRID herstellen können. Befolgen Sie die folgenden Richtlinien zum Sichern aller Gateway-Knoten in Ihrem StorageGRID System:

- Konfigurieren und verwenden Sie Load Balancer-Endpunkte. Siehe "Überlegungen zum Lastausgleich".
- Verwenden Sie für nicht vertrauenswürdigen Client-Datenverkehr einen Drittanbieter-Load-Balancer zwischen Client und Gateway-Node oder Storage-Nodes. Der Lastausgleich von Drittanbietern bietet mehr Kontrolle und zusätzlichen Schutz vor Angriffen. Wenn Sie einen Load Balancer eines Drittanbieters verwenden, kann der Netzwerk-Traffic optional auch so konfiguriert werden, dass er über einen internen Load Balancer-Endpunkt geleitet oder direkt an Storage Nodes gesendet wird.
- Wenn Sie Load Balancer-Endpunkte verwenden, lassen Sie optional Clients über das Client-Netzwerk verbinden. Wählen Sie dann **CONFIGURATION** > **Security** > **Firewall Control** > **UnTrusted Client**

Networks aus und geben Sie an, dass das Client-Netzwerk auf dem Gateway Node nicht vertrauenswürdig ist. Der Gateway-Node akzeptiert nur eingehenden Datenverkehr an den Ports, die explizit als Load Balancer-Endpunkte konfiguriert wurden.

Richtlinien für die Nodes von Hardware-Appliances

StorageGRID Hardware-Appliances wurden speziell für den Einsatz in einem StorageGRID System entwickelt. Einige Geräte können als Storage-Nodes verwendet werden. Andere Appliances können als Admin-Nodes oder Gateway-Nodes verwendet werden. Appliance-Nodes können mit softwarebasierten Nodes kombiniert oder voll entwickelten All-Appliance-Grids implementiert werden.

Beachten Sie diese Richtlinien zum Schutz aller Hardware-Appliance-Nodes in Ihrem StorageGRID System:

- Wenn die Appliance SANtricity System Manager zum Management des Storage Controllers verwendet, verhindern Sie, dass nicht vertrauenswürdige Clients über das Netzwerk auf SANtricity System Manager zugreifen.
- Wenn die Appliance über einen Baseboard Management Controller (BMC) verfügt, beachten Sie, dass der BMC-Management-Port einen niedrigen Hardwarezugriff ermöglicht. Schließen Sie den BMC-Management-Port nur an ein sicheres, vertrauenswürdiges, internes Management-Netzwerk an. Wenn kein solches Netzwerk verfügbar ist, lassen Sie den BMC-Management-Port unverbunden oder blockiert, es sei denn, eine BMC-Verbindung wird vom technischen Support angefordert.
- Wenn die Appliance die Remote-Verwaltung der Controller-Hardware über Ethernet mit dem IPMI-Standard (Intelligent Platform Management Interface) unterstützt, blockieren Sie den nicht vertrauenswürdigen Datenverkehr auf Port 623.

> ⓘ Sie können den Remote-IPMI-Zugriff für alle Appliances aktivieren oder deaktivieren, die einen BMC enthalten, indem Sie den privaten Endpunkt der Management-API VERWENDEN, PUT /private/bmc.

- Wenn der Storage Controller in der Appliance Laufwerke mit FDE- oder FIPS-Laufwerken umfasst und die Laufwerkssicherheitsfunktion aktiviert ist, konfigurieren Sie die Schlüssel zur Laufwerksicherheit mithilfe von SANtricity. Siehe "Konfiguration von SANtricity System Manager (SG6000 und SG5700)".
- Bei Appliances ohne FDE- oder FIPS-Laufwerke ermöglicht die Node-Verschlüsselung mithilfe eines Key Management Servers (KMS). Siehe "Optional: Node-Verschlüsselung aktivieren".

Härtungsrichtlinien für TLS und SSH

Sie sollten die während der Installation erstellten Standardzertifikate ersetzen und die entsprechende Sicherheitsrichtlinie für TLS- und SSH-Verbindungen auswählen.

Richtlinien für die Härtung von Zertifikaten

Sie sollten die während der Installation erstellten Standardzertifikate durch eigene benutzerdefinierte Zertifikate ersetzen.

Für viele Unternehmen entspricht das selbstsignierte digitale Zertifikat für den StorageGRID-Webzugriff nicht den Richtlinien für die Informationssicherheit. Auf Produktionssystemen sollten Sie ein CA-signiertes digitales Zertifikat zur Verwendung bei der Authentifizierung von StorageGRID installieren.

Sie sollten insbesondere anstelle der folgenden Standardzertifikate benutzerdefinierte Serverzertifikate verwenden:

- **Zertifikat der Verwaltungsschnittstelle**: Zur Sicherung des Zugriffs auf den Grid Manager, den Tenant Manager, die Grid Management API und die Tenant Management API.
- **S3- und Swift-API-Zertifikat**: Dient zum sicheren Zugriff auf Storage-Nodes und Gateway-Nodes, die S3- und Swift-Client-Anwendungen zum Hochladen und Herunterladen von Objektdaten verwenden.

Siehe "Verwalten von Sicherheitszertifikaten" Für Details und Anweisungen.

> StorageGRID managt die für Load Balancer-Endpunkte verwendeten Zertifikate separat. Informationen zum Konfigurieren von Load Balancer-Zertifikaten finden Sie unter "Konfigurieren von Load Balancer-Endpunkten".

Wenn Sie benutzerdefinierte Serverzertifikate verwenden, befolgen Sie die folgenden Richtlinien:

- Zertifikate sollten ein haben `subjectAltName` Das stimmt mit DNS-Einträgen für StorageGRID überein. Weitere Informationen finden Sie in Abschnitt 4.2.1.6, „`SAlternative Name des Subject`“ in "RFC 5280: PKIX-Zertifikat und CRL-Profil".
- Wenn möglich, vermeiden Sie die Verwendung von Platzhalterzertifikaten. Eine Ausnahme dieser Richtlinie ist das Zertifikat für einen S3-Endpunkt im virtuellen Hosted-Stil, der die Verwendung eines Platzhalters erfordert, wenn Bucket-Namen nicht im Voraus bekannt sind.
- Wenn Sie Wildcards in Zertifikaten verwenden müssen, sollten Sie weitere Schritte zur Reduzierung der Risiken Unternehmen. Verwenden Sie ein Platzhalter-Muster z. B. `*.s3.example.com`Und verwenden Sie nicht die `s3.example.com` Suffix für andere Applikationen Dieses Muster funktioniert auch mit Path-Style S3-Zugriff, z. B. `dc1-s1.s3.example.com/mybucket`.
- Legen Sie die Ablaufzeiten für das Zertifikat auf kurz (z. B. 2 Monate) fest, und automatisieren Sie die Zertifikatrotation mithilfe der Grid Management API. Dies ist besonders wichtig für Platzhalterzertifikate.

Darüber hinaus sollten Kunden bei der Kommunikation mit StorageGRID strenge Hostnamen-Kontrollen verwenden.

Richtlinien für die Härtung von TLS- und SSH-Richtlinien

Sie können eine Sicherheitsrichtlinie auswählen, um festzulegen, welche Protokolle und Chiffren zum Aufbau sicherer TLS-Verbindungen mit Clientanwendungen und sicherer SSH-Verbindungen zu internen StorageGRID-Diensten verwendet werden.

Die Sicherheitsrichtlinie steuert, wie TLS und SSH Daten in Bewegung verschlüsseln. Als Best Practice sollten Sie Verschlüsselungsoptionen deaktivieren, die für die Anwendungskompatibilität nicht erforderlich sind. Verwenden Sie die moderne Standardrichtlinie, es sei denn, Ihr System muss Common Criteria-konform sein oder Sie müssen andere Chiffren verwenden.

Siehe "Verwalten Sie die TLS- und SSH-Richtlinie" Für Details und Anweisungen.

Andere Hinweise zur Verhärtung

Beachten Sie zusätzlich die Hinweise zur Verhärtung von StorageGRID-Netzwerken und -Knoten die Härtungsrichtlinien für andere Bereiche des StorageGRID-Systems.

Protokolle und Prüfmeldungen

Sichern Sie StorageGRID-Protokolle und die Ausgabe von Prüfnachrichten sicher. StorageGRID-Protokolle und Audit-Meldungen bieten wertvolle Informationen aus Sicht der Support- und Systemverfügbarkeit. Darüber

hinaus handelt es sich bei den Informationen und Details der StorageGRID-Protokolle und der Ausgabe von Audit-Meldungen in der Regel um sensible Daten.

Konfigurieren Sie StorageGRID, um Sicherheitsereignisse an einen externen Syslog-Server zu senden. Wenn Sie syslog-Export verwenden, wählen Sie TLS und RELP/TLS für die Transportprotokolle aus.

Siehe "Referenz für Protokolldateien" Weitere Informationen zu StorageGRID-Protokollen. Siehe "Audit-Meldungen" Weitere Informationen zu StorageGRID-Überwachungsmeldungen.

NetApp AutoSupport

Mit der AutoSupport Funktion von StorageGRID überwachen Sie proaktiv den Zustand Ihres Systems und senden automatisch Nachrichten und Details an den NetApp Technical Support, das interne Support-Team Ihres Unternehmens oder einen Support-Partner. Standardmäßig werden AutoSupport Meldungen an den technischen Support von NetApp aktiviert, wenn StorageGRID zum ersten Mal konfiguriert wird.

Die AutoSupport-Funktion kann deaktiviert werden. NetApp empfiehlt jedoch die Aktivierung, da AutoSupport die Identifizierung von Problemen und die Behebung von Problemen beschleunigt, wenn es auf Ihrem StorageGRID System zu Problemen kommt.

AutoSupport unterstützt HTTPS, HTTP und SMTP für Transportprotokolle. Aufgrund der sensiblen Eigenschaften von AutoSupport Meldungen empfiehlt NetApp dringend die Verwendung von HTTPS als Standard-Transportprotokoll für das Senden von AutoSupport Meldungen an den NetApp Support.

Cross-Origin Resource Sharing (CORS)

Sie können CORS (Cross-Origin Resource Sharing) für einen S3-Bucket konfigurieren, wenn Webapplikationen in anderen Domänen auf diesen Bucket und die Objekte in diesem Bucket zugreifen sollen. Im Allgemeinen sollten Sie CORS nur aktivieren, wenn dies erforderlich ist. Wenn CORS erforderlich ist, beschränken Sie es auf vertrauenswürdige Herkunft.

Siehe die Schritte für "Konfigurieren der Cross-Origin Resource Sharing (CORS)".

Externe Sicherheitsgeräte

Eine vollständige Härtungslösung muss auch Sicherheitsmechanismen außerhalb von StorageGRID berücksichtigen. Der Einsatz zusätzlicher Infrastrukturgeräte zum Filtern und zur Einschränkung des Zugriffs auf StorageGRID ist eine effektive Möglichkeit, eine anspruchsvolle Sicherheit zu schaffen und zu erhalten. Zu diesen externen Sicherheitsgeräten gehören Firewalls, Intrusion Prevention Systems (IPSs) und andere Sicherheitsgeräte.

Für nicht vertrauenswürdigen Client-Datenverkehr wird ein Load Balancer eines Drittanbieters empfohlen. Der Lastausgleich von Drittanbietern bietet mehr Kontrolle und zusätzlichen Schutz vor Angriffen.

Ransomware-Minderung

Befolgen Sie die Empfehlungen in, um Ihre Objektdaten vor Ransomware-Angriffen zu schützen "Ransomware-Verteidigung mit StorageGRID".

Konfigurieren Sie StorageGRID für FabricPool

Configure StorageGRID for FabricPool: Übersicht

Wenn Sie NetApp ONTAP Software verwenden, können Sie NetApp FabricPool verwenden, um inaktive Daten auf ein NetApp StorageGRID Objekt-Storage-System zu verschieben.

Mithilfe dieser Anweisungen können Sie:

- Erfahren Sie mehr über die Überlegungen und Best Practices bei der Konfiguration von StorageGRID für einen FabricPool-Workload.
- Erfahren Sie, wie Sie ein StorageGRID Objekt-Storage-System zur Verwendung mit FabricPool konfigurieren.
- Erfahren Sie, wie Sie ONTAP die erforderlichen Werte vermitteln, wenn Sie StorageGRID als FabricPool Cloud Tier einbinden.

Schnellstart für die Konfiguration von StorageGRID für FabricPool

Planen Sie Ihre Konfiguration

- Legen Sie fest, welche FabricPool Volume Tiering-Richtlinie Sie für das Tiering inaktiver ONTAP-Daten an StorageGRID verwenden möchten.
- Planen und installieren Sie ein StorageGRID System, um Ihre Storage-Kapazitäts- und Performance-Anforderungen zu erfüllen.
- Machen Sie sich mit der StorageGRID System-Software vertraut, einschließlich der "Grid Manager" Und das "Mandanten-Manager".
- Lesen Sie die FabricPool Best Practices für "HA-Gruppen", "Lastverteilung", "ILM", und "Mehr".
- Lesen Sie diese zusätzlichen Ressourcen mit Details zur Verwendung und Konfiguration von ONTAP und FabricPool:

  "TR-4598: FabricPool Best Practices in ONTAP"

  "ONTAP 9: FabricPool Tier-Management-Überblick mit System Manager"

Durchführung von erforderlichen Aufgaben

Beziehen Sie die "Erforderliche Informationen zum Hinzufügen von StorageGRID als Cloud-Tier", Einschließlich:

- IP-Adressen
- Domain-Namen
- SSL-Zertifikat

Optional konfigurieren "Identitätsföderation" Und "Single Sign On".

Konfigurieren Sie die StorageGRID-Einstellungen

Verwenden Sie StorageGRID, um die Werte zu ermitteln, die ONTAP für die Verbindung mit dem Grid benötigt.

Verwenden der "FabricPool Setup-Assistent" Dies ist die empfohlene und schnellste Methode zum Konfigurieren aller Elemente, Sie können aber auch jede Einheit manuell konfigurieren, falls erforderlich.

4 Konfigurieren Sie ONTAP und DNS

Verwenden Sie ONTAP für "Fügen Sie eine Cloud-Schicht hinzu" Das verwendet die StorageGRID-Werte. Dann, "DNS-Einträge konfigurieren" Um IP-Adressen mit beliebigen Domänennamen zu verknüpfen, die Sie verwenden möchten.

5 Überwachen und verwalten

Führen Sie nach der Inbetriebnahme Ihres Systems fortlaufende Aufgaben in ONTAP und StorageGRID durch, um FabricPool Daten-Tiering über einen längeren Zeitraum zu managen und zu überwachen.

Was ist FabricPool?

FabricPool ist eine ONTAP Hybrid-Storage-Lösung mit einem hochperformanten Flash-Aggregat als Performance-Tier und einem Objektspeicher als Cloud-Tier. Mit FabricPool-fähigen Aggregaten senken Sie die Storage-Kosten, ohne dabei Einbußen bei Performance, Effizienz oder Sicherung hinnehmen zu müssen.

FabricPool ordnet eine Cloud-Tier (einen externen Objektspeicher wie StorageGRID) einer lokalen Tier (ein ONTAP Storage-Aggregat) zu, um eine zusammengesetzte Sammlung von Discs zu erstellen. Volumes innerhalb der FabricPool können dann von dem Tiering profitieren, indem häufig verwendete Daten auf hochperformantem Storage (dem lokalen Tier) bleiben und Tiering für inaktive („kalte“) Daten auf dem externen Objektspeicher (der Cloud-Tier) verschoben werden.

Es sind keine Änderungen an der Architektur erforderlich und die Daten- und Applikationsumgebung lässt sich weiterhin über das zentrale ONTAP Storage-System managen.

Was ist StorageGRID?

NetApp StorageGRID ist eine Storage-Architektur, die Daten als Objekte managt und sich nicht auf andere Storage-Architekturen wie File- oder Block-Storage unterscheidet. Objekte werden in einem einzelnen Container (z. B. Bucket) aufbewahrt und nicht als Dateien in einem Verzeichnis in anderen Verzeichnissen verschachtelt. Obwohl Objekt-Storage im Allgemeinen eine geringere Performance als Datei- oder Block-Storage bietet, ist sie deutlich skalierbarer. StorageGRID Buckets können Daten im Petabyte-Bereich und Milliarden Objekte enthalten.

Vorteile von StorageGRID als Cloud-Tier von FabricPool

FabricPool kann ONTAP-Daten auf eine Reihe von Objekt-Storage-Providern, einschließlich StorageGRID, verschieben. Im Gegensatz zu Public Clouds, bei denen eine maximale Anzahl unterstützter IOPS (Input/Output Operations per Second) auf Bucket- oder Container-Ebene festgelegt werden kann, lässt sich die StorageGRID-Performance mit der Anzahl der Nodes in einem System skalieren. Durch den Einsatz von StorageGRID als FabricPool Cloud-Tier können kalte Daten in Ihrer eigenen Private Cloud vorgehalten werden, um höchste Performance und vollständige Kontrolle über Ihre Daten zu erzielen.

Zudem ist keine FabricPool Lizenz erforderlich, wenn Sie StorageGRID als Cloud-Tier verwenden.

Erforderliche Informationen zum Hinzufügen von StorageGRID als Cloud-Tier

Bevor Sie StorageGRID als Cloud-Tier für FabricPool hinzufügen können, müssen Sie

die Konfigurationsschritte in StorageGRID durchführen und bestimmte Werte für die Verwendung in ONTAP abrufen.

Welche Werte brauche ich?

Die folgende Tabelle zeigt die Werte, die Sie in StorageGRID konfigurieren müssen und wie diese Werte von ONTAP und dem DNS-Server verwendet werden.

Wert	Wobei der Wert konfiguriert ist	Wo Wert verwendet wird
Virtuelle IP-Adressen (VIP)	StorageGRID > HA-Gruppe	DNS-Eintrag
Port	StorageGRID > Endpunkt des Load Balancer	ONTAP System Manager > Cloud Tiering hinzufügen
SSL-Zertifikat	StorageGRID > Endpunkt des Load Balancer	ONTAP System Manager > Cloud Tiering hinzufügen
Servername (FQDN)	StorageGRID > Endpunkt des Load Balancer	DNS-Eintrag
Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel	StorageGRID > Mandant und Bucket	ONTAP System Manager > Cloud Tiering hinzufügen
Bucket/Container-Name	StorageGRID > Mandant und Bucket	ONTAP System Manager > Cloud Tiering hinzufügen

Wie erhalte ich diese Werte?

Je nach Ihren Anforderungen können Sie eine der folgenden Möglichkeiten nutzen, um die benötigten Informationen zu erhalten:

- Verwenden Sie die "FabricPool Setup-Assistent". Der FabricPool Setup-Assistent unterstützt Sie beim schnellen Konfigurieren der erforderlichen Werte in StorageGRID und gibt eine Datei aus, die Sie für die Konfiguration von ONTAP System Manager verwenden können. Der Assistent führt Sie durch die erforderlichen Schritte und stellt sicher, dass Ihre Einstellungen den Best Practices von StorageGRID und FabricPool entsprechen.
- Konfigurieren Sie jedes Element manuell. Geben Sie dann die Werte in ONTAP System Manager oder in die ONTAP CLI ein. Führen Sie hierzu folgende Schritte aus:
  a. "Konfigurieren Sie eine HA-Gruppe (High Availability, Hochverfügbarkeit) für FabricPool".
  b. "Erstellen eines Load Balancer-Endpunkts für FabricPool".
  c. "Erstellen eines Mandantenkontos für FabricPool".
  d. Melden Sie sich beim Mandantenkonto an, und "Erstellen Sie den Bucket und die Zugriffsschlüssel für den Root-Benutzer".
  e. Erstellen Sie eine ILM-Regel für FabricPool-Daten und fügen Sie sie zu Ihrer aktiven ILM-Richtlinie hinzu. Siehe "Konfigurieren Sie ILM für FabricPool-Daten".
  f. Optional "Eine Richtlinie zur Verkehrsklassifizierung für FabricPool erstellen".

Verwenden Sie den FabricPool-Einrichtungsassistenten

Überlegungen und Anforderungen im FabricPool Setup-Assistenten

Mit dem FabricPool-Einrichtungsassistenten können Sie StorageGRID als Objekt-Storage-System für eine FabricPool Cloud-Tier konfigurieren. Nach Abschluss des Setup-Assistenten können Sie die erforderlichen Details in den ONTAP System Manager eingeben.

Wann der FabricPool-Einrichtungsassistent verwendet werden soll

Der FabricPool Setup-Assistent führt Sie durch die einzelnen Schritte der Konfiguration von StorageGRID für die Verwendung mit FabricPool und konfiguriert automatisch bestimmte Einheiten, z. B. ILM- und Traffic-Klassifizierungsrichtlinien. Im Rahmen der Ausführung des Assistenten laden Sie eine Datei herunter, mit der Sie Werte in den ONTAP System Manager eingeben können. Mit dem Assistenten konfigurieren Sie Ihr System schneller und stellen sicher, dass Ihre Einstellungen den Best Practices von StorageGRID und FabricPool entsprechen.

Wenn Sie über die Berechtigung für den Stammzugriff verfügen, können Sie den FabricPool-Einrichtungsassistenten abschließen, wenn Sie den StorageGRID-Grid-Manager verwenden, oder Sie können den Assistenten zu einem späteren Zeitpunkt aufrufen und abschließen. Je nach Ihren Anforderungen können Sie auch einige oder alle erforderlichen Elemente manuell konfigurieren und dann mithilfe des Assistenten die von ONTAP benötigten Werte in einer einzigen Datei zusammenfügen.

> Verwenden Sie den FabricPool Setup-Assistenten, es sei denn, Sie wissen, dass Sie besondere Anforderungen haben oder dass Ihre Implementierung umfangreiche Anpassungen erfordern wird.

Bevor Sie den Assistenten verwenden

Bestätigen Sie, dass Sie die erforderlichen Schritte abgeschlossen haben.

Besprechen der Best Practices

- Sie haben ein allgemeines Verständnis der "Erforderliche Informationen zum Hinzufügen von StorageGRID als Cloud-Tier".
- Sie haben die FabricPool Best Practices für folgende Zwecke überprüft:
  - "Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen"
  - "Lastverteilung"
  - "ILM-Regeln und -Richtlinie"

Beziehen Sie IP-Adressen, und richten Sie VLAN-Schnittstellen ein

Wenn Sie eine HA-Gruppe konfigurieren, wissen Sie, mit welchen Nodes ONTAP eine Verbindung herstellen und welches StorageGRID-Netzwerk verwendet werden soll. Sie wissen auch, welche Werte für das Subnetz CIDR, die Gateway-IP-Adresse und die virtuelle IP (VIP)-Adresse eingegeben werden sollen.

Wenn Sie planen, einen virtuellen LAN zur Trennung des FabricPool-Datenverkehrs zu verwenden, haben Sie die VLAN-Schnittstelle bereits konfiguriert. Siehe "Konfigurieren Sie die VLAN-Schnittstellen".

Konfigurieren Sie Identity Federation und SSO

Wenn Sie planen, Identity Federation oder Single Sign-On (SSO) für Ihr StorageGRID-System zu verwenden, haben Sie diese Funktionen aktiviert. Sie wissen auch, welche föderierte Gruppe Root-Zugriff für das Mandantenkonto haben soll, das ONTAP verwenden wird. Siehe "Verwenden Sie den Identitätsverbund" Und "Konfigurieren Sie Single Sign-On".

Abrufen und Konfigurieren von Domänennamen

- Sie wissen, welcher vollständig qualifizierte Domänenname (FQDN) für StorageGRID verwendet werden soll. DNS-Einträge (Domain Name Server) weisen diesen FQDN den virtuellen IP-Adressen (VIP) der HA-Gruppe zu, die Sie mit dem Assistenten erstellen. Siehe "Konfigurieren Sie den DNS-Server".
- Wenn Sie Anforderungen im virtuellen Hosted-Style von S3 verwenden möchten, haben Sie die Möglichkeit "Domänennamen des S3-Endpunkts wurden konfiguriert". ONTAP verwendet standardmäßig URLs im Pfadstil, es wird jedoch empfohlen, Anforderungen im virtuellen Hosted-Stil zu verwenden.

Anforderungen für Load Balancer und Sicherheitszertifikate prüfen

Wenn Sie den StorageGRID Load Balancer verwenden möchten, haben Sie die allgemeinen Informationen gelesen "Überlegungen zum Lastausgleich". Sie verfügen über die hochgeladenen Zertifikate oder die Werte, die Sie zum Generieren eines Zertifikats benötigen.

Wenn Sie einen externen (Drittanbieter-)Load Balancer-Endpunkt verwenden möchten, verfügen Sie über den vollständig qualifizierten Domänennamen (FQDN), den Port und das Zertifikat für diesen Load Balancer.

Bestätigen Sie die ILM-Speicherpoolkonfiguration

Wenn Sie von einer früheren StorageGRID-Version auf StorageGRID 11.7 aktualisiert haben, haben Sie den zu verwendenden Speicherpool konfiguriert. Im Allgemeinen sollten Sie für jeden StorageGRID-Standort, den Sie zum Speichern von ONTAP-Daten verwenden, einen Speicherpool erstellen.

> Diese Voraussetzung gilt nicht für neue StorageGRID 11.7-Installationen. Wenn Sie StorageGRID 11.7 in einem neuen Grid installieren, werden für jeden Standort automatisch Speicherpools erstellt.

Beziehung zwischen ONTAP und StorageGRID Cloud-Tier

Der FabricPool Assistent führt Sie durch die Erstellung einer einzelnen StorageGRID-Cloud-Tier mit einem StorageGRID-Mandanten, einem Satz an Zugriffsschlüsseln und einem StorageGRID-Bucket. Sie können diese StorageGRID-Cloud-Tier an eine oder mehrere lokale ONTAP-Tiers anbinden.

Die allgemeine Best Practice ist die Anbindung einer einzelnen Cloud-Tier an mehrere lokale Tiers in einem Cluster. Je nach Anforderungen sollten Sie jedoch möglicherweise mehr als einen Bucket oder sogar mehr als einen StorageGRID-Mandanten für die lokalen Tiers in einem einzelnen Cluster verwenden. Die Verwendung verschiedener Buckets und Mandanten ermöglicht die Isolierung von Daten und Datenzugriff zwischen lokalen ONTAP Tiers, allerdings ist die Konfiguration und das Management etwas komplexer.

NetApp empfiehlt, keine einzelne Cloud-Tier an lokale Tiers in mehreren Clustern anzubinden.

> Best Practices für die Verwendung von StorageGRID mit NetApp MetroCluster™ und FabricPool Mirror finden Sie unter "TR-4598: FabricPool Best Practices in ONTAP".

Optional: Verwenden Sie einen anderen Bucket für jeden lokalen Tier

Wenn Sie mehr als einen Bucket für die lokalen Tiers in einem ONTAP-Cluster verwenden möchten, fügen Sie mehr als eine StorageGRID-Cloud-Tier in ONTAP hinzu. Jede Cloud-Tier verwendet dieselbe HA-Gruppe, denselben Load-Balancer-Endpunkt, dieselben Mandanten und Zugriffsschlüssel, verwendet jedoch einen anderen Container (StorageGRID Bucket). Führen Sie die folgenden allgemeinen Schritte aus:

1. Vervollständigen Sie über den StorageGRID Grid Manager den FabricPool-Einrichtungsassistenten für die erste Cloud-Tier.
2. Fügen Sie im ONTAP System Manager eine Cloud-Ebene hinzu und verwenden Sie die von StorageGRID heruntergeladene Datei, um die erforderlichen Werte bereitzustellen.
3. Melden Sie sich über den StorageGRID-Mandantenmanager bei dem Mandanten an, der vom Assistenten erstellt wurde, und erstellen Sie einen zweiten Bucket.
4. Schließen Sie den FabricPool-Assistenten erneut ab. Wählen Sie die vorhandene HA-Gruppe, den Load-Balancer-Endpunkt und den Mandanten aus. Wählen Sie dann den neuen Bucket aus, den Sie manuell erstellt haben. Erstellen einer neuen ILM-Regel für den neuen Bucket und Aktivieren einer ILM-Richtlinie, um diese Regel aufzunehmen
5. Fügen Sie in ONTAP eine zweite Cloud-Tier hinzu, geben Sie aber den neuen Bucket-Namen an.

Optional: Verwenden Sie einen anderen Mandanten und Bucket für jede lokale Tier

Wenn Sie mehr als einen Mandanten und unterschiedliche Zugriffssätze für die lokalen Tiers in einem ONTAP-Cluster verwenden möchten, fügen Sie mehr als ein StorageGRID-Cloud-Tier in ONTAP hinzu. Jede Cloud-Tier verwendet dieselbe HA-Gruppe und denselben Load-Balancer-Endpunkt, verwendet jedoch einen anderen Mandanten, Zugriffsschlüssel und Container (StorageGRID Bucket). Führen Sie die folgenden allgemeinen Schritte aus:

1. Vervollständigen Sie über den StorageGRID Grid Manager den FabricPool-Einrichtungsassistenten für die erste Cloud-Tier.
2. Fügen Sie im ONTAP System Manager eine Cloud-Ebene hinzu und verwenden Sie die von StorageGRID heruntergeladene Datei, um die erforderlichen Werte bereitzustellen.
3. Schließen Sie den FabricPool-Assistenten erneut ab. Wählen Sie die vorhandene HA-Gruppe und den Endpunkt des Load Balancer aus. Erstellen eines neuen Mandanten und Buckets Erstellen einer neuen ILM-Regel für den neuen Bucket und Aktivieren einer ILM-Richtlinie, um diese Regel aufzunehmen
4. Von ONTAP fügen Sie eine zweite Cloud-Tier hinzu, liefern aber den neuen Zugriffsschlüssel, den geheimen Schlüssel und den Bucket-Namen.

Öffnen und Abschließen des FabricPool Setup-Assistenten

Mit dem FabricPool-Einrichtungsassistenten können Sie StorageGRID als Objekt-Storage-System für eine FabricPool Cloud-Tier konfigurieren.

Bevor Sie beginnen

- Sie haben die geprüft "Überlegungen und Anforderungen" Zur Verwendung des FabricPool Setup-Assistenten.

> Wenn Sie StorageGRID für die Verwendung mit einer anderen S3-Client-Anwendung konfigurieren möchten, gehen Sie zu "Verwenden Sie den S3-Einrichtungsassistenten".

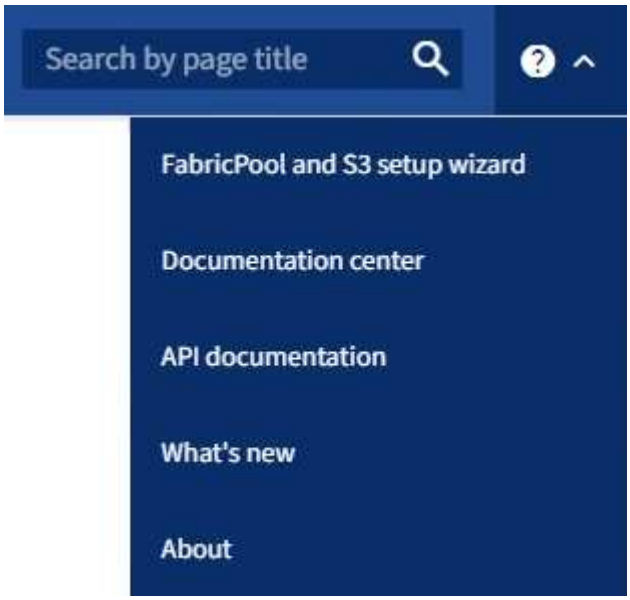
- Sie haben die Root-Zugriffsberechtigung.

Greifen Sie auf den Assistenten zu

Sie können den FabricPool-Einrichtungsassistenten abschließen, wenn Sie den StorageGRID Grid-Manager verwenden, oder Sie können den Assistenten zu einem späteren Zeitpunkt aufrufen und abschließen.

Schritte

1. Melden Sie sich mit einem bei Grid Manager an "Unterstützter Webbrowser".
2. Wenn das Banner **FabricPool and S3 Setup Wizard** auf dem Dashboard angezeigt wird, wählen Sie den Link im Banner aus. Wenn das Banner nicht mehr angezeigt wird, wählen Sie in der Kopfzeile des Grid-Managers das Hilfesymbol aus und wählen Sie **FabricPool und S3-Setup-Assistent** aus.



3. Wählen Sie im Abschnitt FabricPool der Seite mit dem FabricPool- und S3-Setup-Assistenten **Jetzt konfigurieren** aus.

   Schritt 1 von 9: Konfigurieren der HA-Gruppe wird angezeigt.

Schritt 1 von 9: Konfigurieren Sie die HA-Gruppe

Eine HA-Gruppe (High Availability, Hochverfügbarkeit) ist eine Sammlung von Nodes, die jeweils den StorageGRID Lastausgleich enthalten. Eine HA-Gruppe kann Gateway-Nodes, Admin-Nodes oder beides enthalten.

Sie können eine HA-Gruppe verwenden, um FabricPool-Datenverbindungen verfügbar zu halten. Eine HA-Gruppe verwendet virtuelle IP-Adressen (VIPs), um hochverfügbaren Zugriff auf den Load Balancer-Service zu ermöglichen. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle den Workload mit geringen Auswirkungen auf den FabricPool-Betrieb managen

Weitere Informationen zu dieser Aufgabe finden Sie unter "Management von Hochverfügbarkeitsgruppen" Und "Best Practices für Hochverfügbarkeitsgruppen".

Schritte

1. Wenn Sie einen externen Load Balancer verwenden möchten, müssen Sie keine HA-Gruppe erstellen. Wählen Sie **diesen Schritt überspringen** und gehen Sie zu Schritt 2 von 9: Konfigurieren Sie den Load Balancer-Endpunkt.
2. Um den StorageGRID Load Balancer zu verwenden, erstellen Sie eine neue HA-Gruppe oder verwenden

Sie eine vorhandene HA-Gruppe.

Erstellen Sie eine HA-Gruppe

a. Um eine neue HA-Gruppe zu erstellen, wählen Sie **HA-Gruppe erstellen**.

b. Füllen Sie für den Schritt **Enter Details** die folgenden Felder aus.

Feld	Beschreibung
Name DER HA-Gruppe	Ein eindeutiger Anzeigename für diese HA-Gruppe.
Beschreibung (optional)	Die Beschreibung dieser HA-Gruppe.

c. Wählen Sie im Schritt **Schnittstellen hinzufügen** die Knotenschnittstellen aus, die Sie in dieser HA-Gruppe verwenden möchten.

   Verwenden Sie die Spaltenüberschriften, um die Zeilen zu sortieren, oder geben Sie einen Suchbegriff ein, um Schnittstellen schneller zu finden.

   Sie können einen oder mehrere Nodes auswählen, aber Sie können nur eine Schnittstelle für jeden Node auswählen.

d. Bestimmen Sie für den Schritt **priorisiere Schnittstellen** die primäre Schnittstelle und alle Backup-Schnittstellen für diese HA-Gruppe.

   Ziehen Sie Zeilen, um die Werte in der Spalte **Priority order** zu ändern.

   Die erste Schnittstelle in der Liste ist die primäre Schnittstelle. Die primäre Schnittstelle ist die aktive Schnittstelle, sofern kein Fehler auftritt.

   Wenn die HA-Gruppe mehr als eine Schnittstelle enthält und die aktive Schnittstelle ausfällt, werden die virtuellen IP-Adressen (VIP-Adressen) zur ersten Backup-Schnittstelle in der Prioritätsreihenfolge verschoben. Wenn diese Schnittstelle ausfällt, wechseln die VIP-Adressen zur nächsten Backup-Schnittstelle usw. Wenn Ausfälle behoben werden, werden die VIP-Adressen wieder auf die Schnittstelle mit der höchsten Priorität verschoben, die verfügbar ist.

e. Füllen Sie für den Schritt **IP-Adressen eingeben** die folgenden Felder aus.

Feld	Beschreibung
Subnetz-CIDR	Die Adresse des VIP-Subnetzes in CIDR Notation—eine IPv4-Adresse gefolgt von einem Schrägstrich und der Subnetz-Länge (0-32). Die Netzwerkadresse darf keine Host-Bits festgelegt haben. Beispiel: `192.16.0.0/22`.
Gateway-IP-Adresse (optional)	Optional Wenn sich die ONTAP-IP-Adressen, die für den Zugriff auf StorageGRID verwendet werden, nicht im selben Subnetz wie die StorageGRID-VIP-Adressen befinden, geben Sie die IP-Adresse des lokalen StorageGRID-VIP-Gateways ein. Die IP-Adresse des lokalen Gateways muss sich im VIP-Subnetz befinden.

Feld	Beschreibung
Virtuelle IP-Adresse	Geben Sie mindestens eine und nicht mehr als zehn VIP-Adressen für die aktive Schnittstelle in der HA-Gruppe ein. Alle VIP-Adressen müssen sich innerhalb des VIP-Subnetzes befinden, und alle müssen gleichzeitig auf der aktiven Schnittstelle aktiv sein. Mindestens eine Adresse muss IPv4 sein. Optional können Sie weitere IPv4- und IPv6-Adressen angeben.

f. Wählen Sie **HA-Gruppe erstellen** und dann **Fertig stellen**, um zum FabricPool-Setup-Assistenten zurückzukehren.

g. Wählen Sie **Weiter**, um zum Schritt Load Balancer zu gelangen.

Verwenden Sie die vorhandene HA-Gruppe

a. Um eine vorhandene HA-Gruppe zu verwenden, wählen Sie den Namen der HA-Gruppe aus der Dropdown-Liste **Select an HA Group** aus.

b. Wählen Sie **Weiter**, um zum Schritt Load Balancer zu gelangen.

Schritt 2 von 9: Konfigurieren Sie den Load Balancer-Endpunkt

StorageGRID verwendet einen Load Balancer zum Managen des Workloads von Client-Applikationen wie FabricPool. Load Balancing maximiert Geschwindigkeit und Verbindungskapazität über mehrere Storage Nodes hinweg.

Sie können den StorageGRID Load Balancer-Dienst verwenden, der auf allen Gateway- und Admin-Nodes vorhanden ist, oder eine Verbindung zu einem externen Load Balancer (Drittanbieter) herstellen. Die Verwendung des StorageGRID Load Balancer wird empfohlen.

Weitere Informationen zu dieser Aufgabe finden Sie im Abschnitt Allgemein "Überlegungen zum Lastausgleich" Und das "Best Practices für Lastausgleich für FabricPool".

Schritte

1. Wählen oder erstellen Sie einen StorageGRID Load Balancer-Endpunkt oder verwenden Sie einen externen Load Balancer.

Endpunkt erstellen

a. Wählen Sie **Endpunkt erstellen**.

b. Füllen Sie für den Schritt **Enter Endpoint Details** die folgenden Felder aus.

Feld	Beschreibung
Name	Ein beschreibender Name für den Endpunkt.
Port	Der StorageGRID-Port, den Sie für den Lastausgleich verwenden möchten. Dieses Feld ist für den ersten erstellten Endpunkt standardmäßig auf 10433 eingestellt, Sie können jedoch jeden nicht verwendeten externen Port eingeben. Wenn Sie 80 oder 443 eingeben, wird der Endpunkt nur auf Gateway-Nodes konfiguriert, da diese Ports auf Admin-Nodes reserviert sind. **Hinweis:** von anderen Netzdiensten verwendete Ports sind nicht erlaubt. Siehe"Referenz für Netzwerk-Ports".
Client-Typ	Muss **S3** sein.
Netzwerkprotokoll	Wählen Sie **HTTPS**. **Hinweis**: Die Kommunikation mit StorageGRID ohne TLS-Verschlüsselung wird unterstützt, aber nicht empfohlen.

c. Geben Sie für den Schritt **Bindungsmodus auswählen** den Bindungsmodus an. Der Bindungsmodus steuert, wie auf den Endpunkt zugegriffen wird—Verwendung einer beliebigen IP-Adresse oder Verwendung bestimmter IP-Adressen und Netzwerkschnittstellen.

Option	Beschreibung
Global (Standard)	Clients können über die IP-Adresse eines beliebigen Gateway-Node oder Admin-Node, die virtuelle IP-Adresse (VIP) einer beliebigen HA-Gruppe in einem beliebigen Netzwerk oder einen entsprechenden FQDN auf den Endpunkt zugreifen. Verwenden Sie die **Global**-Einstellung (Standard), es sei denn, Sie müssen die Zugriffsmöglichkeiten dieses Endpunkts einschränken.
Virtuelle IPs von HA-Gruppen	Clients müssen eine virtuelle IP-Adresse (oder einen entsprechenden FQDN) einer HA-Gruppe verwenden, um auf diesen Endpunkt zuzugreifen. Endpunkte mit diesem Bindungsmodus können alle dieselbe Portnummer verwenden, solange sich die für die Endpunkte ausgewählten HA-Gruppen nicht überlappen.

Option	Beschreibung
Node-Schnittstellen	Clients müssen die IP-Adressen (oder entsprechende FQDNs) der ausgewählten Knotenschnittstellen verwenden, um auf diesen Endpunkt zuzugreifen.
Node-Typ	Basierend auf dem von Ihnen ausgewählten Knotentyp müssen Clients entweder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Admin-Knotens oder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Gateway-Knotens verwenden, um auf diesen Endpunkt zuzugreifen.

d. Wählen Sie für den Schritt **Tenant Access** eine der folgenden Optionen aus:

Feld	Beschreibung
Alle Mandanten zulassen (Standard)	Alle Mandantenkonten können diesen Endpunkt verwenden, um auf ihre Buckets zuzugreifen. **Alle Mandanten zulassen** ist fast immer die geeignete Option für den für FabricPool verwendeten Load Balancer Endpunkt. Sie müssen diese Option auswählen, wenn Sie den FabricPool-Einrichtungsassistenten für ein neues StorageGRID-System verwenden und noch keine Mandantenkonten erstellt haben.
Ausgewählte Mandanten zulassen	Nur die ausgewählten Mandantenkonten können diesen Endpunkt für den Zugriff auf ihre Buckets verwenden.
Ausgewählte Mandanten blockieren	Die ausgewählten Mandantenkonten können diesen Endpunkt nicht für den Zugriff auf ihre Buckets verwenden. Dieser Endpunkt kann von allen anderen Mandanten verwendet werden.

e. Wählen Sie für den Schritt **Zertifikat anhängen** eine der folgenden Optionen aus:

Feld	Beschreibung
Zertifikat hochladen (empfohlen)	Verwenden Sie diese Option, um ein CA-signiertes Serverzertifikat, einen privaten Zertifikatschlüssel und ein optionales CA-Paket hochzuladen.
Zertifikat wird generiert	Verwenden Sie diese Option, um ein selbstsigniertes Zertifikat zu generieren. Siehe "Konfigurieren von Load Balancer-Endpunkten" Für Details, was eingegeben werden soll.
StorageGRID S3 und Swift-Zertifikat verwenden	Diese Option ist nur verfügbar, wenn Sie bereits eine benutzerdefinierte Version des globalen StorageGRID-Zertifikats hochgeladen oder generiert haben. Siehe "Konfigurieren von S3- und Swift-API-Zertifikaten" Entsprechende Details.

f. Wählen Sie **Fertig**, um zum FabricPool-Setup-Assistenten zurückzukehren.

g. Wählen Sie **Weiter**, um zum Mandanten- und Bucket-Schritt zu gelangen.

> Änderungen an einem Endpunktzertifikat können bis zu 15 Minuten dauern, bis sie auf alle Knoten angewendet werden können.

Verwenden Sie den vorhandenen Endpunkt des Load Balancer

a. Wählen Sie den Namen eines vorhandenen Endpunkts aus der Dropdown-Liste **Select a Load Balancer Endpoint** aus.

b. Wählen Sie **Weiter**, um zum Mandanten- und Bucket-Schritt zu gelangen.

Externen Load Balancer verwenden

a. Füllen Sie die folgenden Felder für den externen Load Balancer aus.

Feld	Beschreibung
FQDN	Der vollständig qualifizierte Domänenname (FQDN) des externen Load Balancer.
Port	Die Portnummer, die FabricPool zur Verbindung mit dem externen Load Balancer verwendet.
Zertifikat	Kopieren Sie das Serverzertifikat für den externen Load Balancer und fügen Sie es in dieses Feld ein.

b. Wählen Sie **Weiter**, um zum Mandanten- und Bucket-Schritt zu gelangen.

Schritt 3 von 9: Mieter und Eimer

Ein Mandant ist eine Einheit, die S3-Applikationen zum Speichern und Abrufen von Objekten in StorageGRID verwenden kann. Jeder Mandant verfügt über eigene Benutzer, Zugriffsschlüssel, Buckets, Objekte und bestimmte Funktionen. Sie müssen einen StorageGRID-Mandanten erstellen, bevor Sie den Bucket erstellen können, den FabricPool verwenden wird.

Ein Bucket ist ein Container, mit dem die Objekte und Objektmetadaten eines Mandanten gespeichert werden können. Obwohl einige Mandanten möglicherweise über mehrere Buckets verfügen, können Sie mit dem Assistenten immer nur einen Mandanten und jeweils nur einen Bucket erstellen oder auswählen. Sie können den Tenant Manager später verwenden, um zusätzliche Buckets hinzuzufügen, die Sie benötigen.

Sie können einen neuen Mandanten und Bucket für die FabricPool-Verwendung erstellen oder einen vorhandenen Mandanten und Bucket auswählen. Wenn Sie einen neuen Mandanten erstellen, erstellt das System automatisch die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel für den Root-Benutzer des Mandanten.

Weitere Informationen zu dieser Aufgabe finden Sie unter "Erstellen eines Mandantenkontos für FabricPool" Und "Erstellen eines S3-Buckets und Abrufen eines Zugriffsschlüssels".

Schritte

Erstellen Sie einen neuen Mandanten und Bucket oder wählen Sie einen vorhandenen Mandanten aus.

Neuer Mandant und Bucket

1. Um einen neuen Mandanten und Bucket zu erstellen, geben Sie einen **Tenant Name** ein. Beispiel: `FabricPool tenant`.
2. Definieren Sie den Root-Zugriff für das Mandantenkonto, je nachdem, ob Ihr StorageGRID-System verwendet "Identitätsföderation", "Single Sign On (SSO)"Oder beides.

Option	Tun Sie das
Wenn die Identitätsföderation nicht aktiviert ist	Geben Sie das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.
Wenn die Identitätsföderation aktiviert ist	a. Wählen Sie eine vorhandene Verbundgruppe aus, um Root-Zugriffsberechtigungen für den Mandanten zu erhalten. b. Geben Sie optional das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.
Wenn sowohl Identitätsföderation als auch Single Sign-On (SSO) aktiviert sind	Wählen Sie eine vorhandene Verbundgruppe aus, um Root-Zugriffsberechtigungen für den Mandanten zu erhalten. Keine lokalen Benutzer können sich anmelden.

3. Geben Sie für **Bucket Name** den Namen des Buckets ein, den FabricPool zum Speichern von ONTAP-Daten verwendet. Beispiel: `fabricpool-bucket`.

   Sie können den Bucket-Namen nach dem Erstellen des Buckets nicht ändern.

4. Wählen Sie die **Region** für diesen Bucket aus.

   Verwenden Sie die Standardregion (US-East-1), es sei denn, Sie möchten ILM zukünftig verwenden, um Objekte basierend auf der Region des Buckets zu filtern.

5. Wählen Sie **Erstellen und Fortfahren**, um den Mandanten und den Bucket zu erstellen und zum Datenschritt Download zu gehen

Wählen Sie Mandant und Bucket aus

Das vorhandene Mandantenkonto muss über mindestens einen Bucket verfügen, für den die Versionierung nicht aktiviert ist. Sie können kein vorhandenes Mandantenkonto auswählen, wenn für diesen Mandanten kein Bucket vorhanden ist.

1. Wählen Sie den vorhandenen Mandanten aus der Dropdown-Liste **Tenant Name** aus.
2. Wählen Sie den vorhandenen Bucket aus der Dropdown-Liste **Bucket Name** aus.

   FabricPool unterstützt keine Objektversionierung, daher werden Buckets mit aktivierter Versionierung nicht angezeigt.

   Wählen Sie keinen Bucket aus, für den die S3-Objektsperrung zur Verwendung mit FabricPool aktiviert ist.

3. Wählen Sie **Weiter**, um zum Schritt Download-Daten zu gelangen.

Schritt 4 von 9: ONTAP-Einstellungen herunterladen

In diesem Schritt laden Sie eine Datei herunter, mit der Sie Werte in den ONTAP System Manager eingeben können.

Schritte

1. Wählen Sie optional das Kopieren-Symbol ( ) Um sowohl die Zugriffsschlüssel-ID als auch den geheimen Zugriffsschlüssel in die Zwischenablage zu kopieren.

   Diese Werte sind in der Download-Datei enthalten, sollten jedoch separat gespeichert werden.

2. Wählen Sie **ONTAP-Einstellungen herunterladen**, um eine Textdatei herunterzuladen, die die bisher eingegebenen Werte enthält.

   Der `ONTAP_FabricPool_settings_bucketname.txt` Datei enthält die Informationen, die Sie benötigen, um StorageGRID als Objekt-Storage-System für eine FabricPool Cloud-Ebene zu konfigurieren, darunter:

   - Verbindungsdetails des Load Balancer, einschließlich des Servernamens (FQDN), des Ports und des Zertifikats
   - Bucket-Name
   - Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel für den Root-Benutzer des Mandantenkontos

3. Speichern Sie die kopierten Schlüssel und die heruntergeladene Datei an einem sicheren Speicherort.

   Schließen Sie diese Seite erst, wenn Sie beide Zugriffsschlüssel kopiert, die ONTAP-Einstellungen heruntergeladen oder beides haben. Die Tasten sind nach dem Schließen dieser Seite nicht mehr verfügbar. Speichern Sie diese Informationen an einem sicheren Ort, da sie zum Abrufen von Daten von Ihrem StorageGRID-System verwendet werden können.

4. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel heruntergeladen oder kopiert haben.
5. Wählen Sie **Weiter**, um zum ILM-Speicherpoolschritt zu gelangen.

Schritt 5 von 9: Wählen Sie einen Speicherpool aus

Ein Speicherpool ist eine Gruppe von Storage-Nodes. Wenn Sie einen Speicherpool auswählen, legen Sie fest, welche Nodes StorageGRID zum Speichern der von ONTAP gestaffelten Daten verwendet.

Weitere Informationen zu diesem Schritt finden Sie unter "Erstellen Sie einen Speicherpool".

Schritte

1. Wählen Sie aus der Drop-down-Liste **Standort** die StorageGRID-Site aus, die Sie für die Daten mit ONTAP-Tiering verwenden möchten.
2. Wählen Sie aus der Dropdown-Liste **Speicherpool** den Speicherpool für diesen Standort aus.

   Der Speicherpool für einen Standort umfasst alle Storage-Nodes an diesem Standort.

3. Wählen Sie **Weiter**, um zum ILM-Regelschritt zu gelangen.

Schritt 6 von 9: Überprüfen Sie die ILM-Regel für FabricPool

Informationen Lifecycle Management-Regeln (ILM) steuern die Platzierung, Dauer und das Aufnahmeverhalten aller Objekte im StorageGRID System.

Der FabricPool-Einrichtungsassistent erstellt automatisch die empfohlene ILM-Regel für die Verwendung mit FabricPool. Diese Regel gilt nur für den von Ihnen angegebenen Bucket. Dabei werden 2+1 Erasure Coding an einem einzigen Standort verwendet, um die aus ONTAP Tiering-Daten zu speichern.

Weitere Informationen zu diesem Schritt finden Sie unter "ILM-Regel erstellen" Und "Best Practices für die Verwendung von ILM mit FabricPool-Daten".

Schritte

1. Überprüfen Sie die Regeldetails.

Feld	Beschreibung
Regelname	Automatisch generiert und kann nicht geändert werden
Beschreibung	Automatisch generiert und kann nicht geändert werden
Filtern	Der Bucket-Name Diese Regel gilt nur für Objekte, die in dem von Ihnen angegebenen Bucket gespeichert wurden.
Referenzzeit	Aufnahmezeit Die Platzierungsanweisung beginnt, wenn Objekte zunächst im Bucket gespeichert werden.
Platzierungsanweisung	Verwenden Sie 2+1 Erasure Coding vom Tag 0 bis für immer

2. Sortieren Sie das Aufbewahrungsdiagramm nach **time period** und **Storage Pool**, um die Platzierungsanweisung zu bestätigen.
   - Der **Zeitraum** für die Regel ist **Tag 0 - für immer**. **Tag 0** bedeutet, dass die Regel angewendet wird, wenn Daten aus ONTAP verschoben werden. **Für immer** bedeutet, dass StorageGRID ILM keine Daten löscht, die aus ONTAP verschoben wurden.
   - Der **Speicherpool** für die Regel ist der von Ihnen ausgewählte Speicherpool. **EC 2+1** bedeutet, dass die Daten mit 2+1 Erasure Coding gespeichert werden. Jedes Objekt wird als zwei Datenfragmente und ein Paritätsfragment gespeichert. Die drei Fragmente für jedes Objekt werden in verschiedenen Storage Nodes an einem einzigen Standort gespeichert.
3. Wählen Sie **Erstellen und Fortfahren**, um diese Regel zu erstellen und zum ILM-Richtlinienschritt zu wechseln.

Schritt 7 von 9: Prüfen und aktivieren Sie die ILM-Richtlinie

Nachdem der FabricPool Setup-Assistent die ILM-Regel für die Verwendung von FabricPool erstellt hat, wird eine vorgeschlagene ILM-Richtlinie erstellt. Sie müssen diese Richtlinie sorgfältig prüfen, bevor Sie sie aktivieren.

Weitere Informationen zu diesem Schritt finden Sie unter "ILM-Richtlinie erstellen" Und "Best Practices für die Verwendung von ILM mit FabricPool-Daten".

> Wenn Sie eine neue ILM-Richtlinie aktivieren, verwendet StorageGRID diese Richtlinie, um die Platzierung, Dauer und Datensicherung aller Objekte im Grid zu managen, einschließlich vorhandener und neu aufgenommenen Objekte. In einigen Fällen kann die Aktivierung einer neuen Richtlinie dazu führen, dass vorhandene Objekte an neue Speicherorte verschoben werden.

> Verwenden Sie zur Vermeidung von Datenverlust keine ILM-Regel, die ausläuft oder die Cloud-Tiering-Daten von FabricPool löscht. Setzen Sie die Aufbewahrungsfrist auf **Forever**, um sicherzustellen, dass FabricPool-Objekte nicht durch StorageGRID ILM gelöscht werden.

Schritte

1. Optional können Sie den vom System generierten **Richtliniennamen** aktualisieren. Standardmäßig hängt das System „`+ FabricPool`“ an den Namen Ihrer aktiven oder vorgeschlagenen Richtlinie an, Sie können jedoch Ihren eigenen Namen angeben.
2. Überprüfen Sie die Liste der Regeln in der vorgeschlagenen Richtlinie.
   - Wenn Ihr Raster keine vorgeschlagene ILM-Richtlinie enthält, erstellt der Assistent eine vorgeschlagene Richtlinie, indem Sie Ihre aktive Richtlinie klonen und die neue Regel oben hinzufügen.
   - Wenn Ihr Raster bereits über eine vorgeschlagene ILM-Richtlinie verfügt und diese Richtlinie dieselben Regeln und dieselbe Reihenfolge wie die aktive ILM-Richtlinie verwendet, fügt der Assistent die neue Regel oben auf der vorgeschlagenen Richtlinie hinzu.
   - Wenn Ihre vorgeschlagene Richtlinie andere Regeln oder eine andere Reihenfolge als die aktive Richtlinie enthält, wird eine Meldung angezeigt. Sie müssen die neue FabricPool-Regel manuell zur ILM-Richtlinie hinzufügen. Befolgen Sie diese Schritte, je nachdem, ob Sie von der aktiven Richtlinie oder der vorgeschlagenen Richtlinie beginnen möchten.

Richtlinie, die von beginnen soll	**Schritte**
Aktive Richtlinie	i. Wählen Sie im linken Menü im Grid Manager **ILM** > **Policies** aus. ii. Wählen Sie die Registerkarte vorgeschlagene Richtlinie aus. iii. Wählen Sie **actions** > **Delete**, um die vorhandene vorgeschlagene Richtlinie zu entfernen. iv. Kehren Sie zum FabricPool-Einrichtungsassistenten zurück. Der Assistent kann jetzt Ihre aktive Richtlinie klonen, um eine neue vorgeschlagene Richtlinie zu erstellen. Die neue FabricPool-Regel wird oben hinzugefügt.

Richtlinie, die von beginnen soll	Schritte
Vorgeschlagene Richtlinie	i. Wählen Sie im linken Menü im Grid Manager **ILM** > **Policies** aus. ii. Wählen Sie die Registerkarte vorgeschlagene Richtlinie aus. iii. Wählen Sie **actions** > **Edit**, um die vorhandene vorgeschlagene Richtlinie zu bearbeiten. iv. Fügen Sie die neue FabricPool-Regel oben hinzu. v. Aktivieren Sie die aktualisierte Richtlinie. vi. Wechseln Sie zum Verkehrsklassifizierung Schritt:

Siehe "Vorgeschlagene ILM-Richtlinie erstellen" Wenn Sie detailliertere Anweisungen benötigen.

3. Überprüfen Sie die Reihenfolge der Regeln in der neuen Richtlinie.

   Da es sich bei der FabricPool-Regel um die erste Regel handelt, werden alle Objekte im FabricPool-Bucket vor die anderen Regeln in der Richtlinie platziert. Objekte in anderen Buckets werden durch nachfolgende Regeln in der Richtlinie platziert.

4. Sehen Sie sich das Aufbewahrungsdiagramm an, um zu erfahren, wie verschiedene Objekte beibehalten werden.
   a. Wählen Sie **Expand all**, um ein Aufbewahrungsdiagramm für jede Regel in der vorgeschlagenen Richtlinie anzuzeigen.
   b. Wählen Sie **time period** und **Storage Pool** aus, um das Aufbewahrungsdiagramm zu überprüfen. Vergewissern Sie sich, dass alle Regeln, die auf den FabricPool-Bucket oder Mandanten zutreffen, Objekte **für immer** behalten.
5. Wenn Sie die vorgeschlagene Richtlinie überprüft haben, wählen Sie **Aktivieren und fortfahren**, um die Richtlinie zu aktivieren und zum Schritt Verkehrsklassifizierung zu wechseln.

> Fehler in einer ILM-Richtlinie können zu irreparablen Datenverlusten führen. Überprüfen Sie die Richtlinie sorgfältig, bevor Sie sie aktivieren.

Schritt 8 von 9: Verkehrsklassifizierungsrichtlinie erstellen

Optional kann der FabricPool-Einrichtungsassistent eine Richtlinie zur Verkehrsklassifizierung erstellen, die Sie zur Überwachung des FabricPool-Workloads verwenden können. Die vom System erstellte Richtlinie verwendet eine übereinstimmende Regel, um den gesamten Netzwerkverkehr in Bezug auf den erstellten Bucket zu identifizieren. Diese Richtlinie überwacht nur den Datenverkehr; sie beschränkt nicht den Datenverkehr für FabricPool oder andere Clients.

Weitere Informationen zu diesem Schritt finden Sie unter "Erstellen einer Traffic-Klassifizierungsrichtlinie für FabricPool".

Schritte

1. Überprüfen Sie die Richtlinie.
2. Wenn Sie diese Verkehrsklassifizierungsrichtlinie erstellen möchten, wählen Sie **Erstellen und fortfahren**.

   Sobald FabricPool mit dem Tiering von Daten in StorageGRID beginnt, können Sie auf der Seite „Richtlinien zur Traffic-Klassifizierung“ die Kennzahlen für den Netzwerk-Traffic für diese Richtlinie

anzeigen. Später können Sie auch Regeln hinzufügen, um andere Workloads einzuschränken und sicherzustellen, dass der FabricPool-Workload den größten Teil der Bandbreite hat.

3. Andernfalls wählen Sie **diesen Schritt überspringen**.

Schritt 9 von 9: Zusammenfassung überprüfen

Die Zusammenfassung enthält Details zu den von Ihnen konfigurierten Elementen, darunter den Namen des Load Balancer, Mandanten und Buckets, die Richtlinie zur Datenklassifizierung und die aktive ILM-Richtlinie.

Schritte

1. Überprüfen Sie die Zusammenfassung.
2. Wählen Sie **Fertig**.

Nächste Schritte

Führen Sie nach Abschluss des FabricPool-Assistenten die folgenden zusätzlichen Schritte aus.

Schritte

1. Gehen Sie zu "Konfigurieren Sie ONTAP System Manager" Um die gespeicherten Werte einzugeben und die ONTAP-Seite der Verbindung abzuschließen. Sie müssen StorageGRID als Cloud-Tier hinzufügen, die Cloud-Tier einer lokalen Tier zuweisen, um eine FabricPool zu erstellen, und Volume-Tiering-Richtlinien festlegen.
2. Gehen Sie zu "Konfigurieren Sie den DNS-Server" Und stellen Sie sicher, dass der DNS einen Datensatz enthält, um den StorageGRID-Servernamen (vollständig qualifizierter Domänenname) jeder verwendeten StorageGRID-IP-Adresse zuzuordnen.
3. Gehen Sie zu "Weitere Best Practices für StorageGRID und FabricPool" Um Best Practices für StorageGRID-Prüfprotokolle und andere globale Konfigurationsoptionen zu erfahren.

Konfigurieren Sie StorageGRID manuell

Erstellen einer HA-Gruppe (High Availability, Hochverfügbarkeit) für FabricPool

Wenn Sie StorageGRID für die Verwendung mit FabricPool konfigurieren, können Sie optional eine oder mehrere HA-Gruppen (High Availability, Hochverfügbarkeit) erstellen. Eine HA-Gruppe ist eine Sammlung von Nodes, die jeweils den StorageGRID Lastausgleich enthalten. Eine HA-Gruppe kann Gateway-Nodes, Admin-Nodes oder beides enthalten.

Sie können eine HA-Gruppe verwenden, um FabricPool-Datenverbindungen verfügbar zu halten. Eine HA-Gruppe verwendet virtuelle IP-Adressen (VIPs), um hochverfügbaren Zugriff auf den Load Balancer-Service zu ermöglichen. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle den Workload mit geringen Auswirkungen auf den FabricPool-Betrieb managen.

Weitere Informationen zu dieser Aufgabe finden Sie unter "Management von Hochverfügbarkeitsgruppen". Um diese Aufgabe mithilfe des FabricPool-Setup-Assistenten abzuschließen, gehen Sie zu "Öffnen und Abschließen des FabricPool Setup-Assistenten".

Bevor Sie beginnen

- Sie haben die geprüft "Best Practices für Hochverfügbarkeitsgruppen ab".
- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".

- Sie haben die Root-Zugriffsberechtigung.
- Wenn Sie ein VLAN verwenden möchten, haben Sie die VLAN-Schnittstelle erstellt. Siehe "Konfigurieren Sie die VLAN-Schnittstellen".

Schritte

1. Wählen Sie **CONFIGURATION** > **Network** > **High Availability groups**.
2. Wählen Sie **Erstellen**.
3. Füllen Sie für den Schritt **Enter Details** die folgenden Felder aus.

Feld	Beschreibung
Name DER HA-Gruppe	Ein eindeutiger Anzeigename für diese HA-Gruppe.
Beschreibung (optional)	Die Beschreibung dieser HA-Gruppe.

4. Wählen Sie im Schritt **Schnittstellen hinzufügen** die Knotenschnittstellen aus, die Sie in dieser HA-Gruppe verwenden möchten.

   Verwenden Sie die Spaltenüberschriften, um die Zeilen zu sortieren, oder geben Sie einen Suchbegriff ein, um Schnittstellen schneller zu finden.

   Sie können einen oder mehrere Nodes auswählen, aber Sie können nur eine Schnittstelle für jeden Node auswählen.

5. Bestimmen Sie für den Schritt **priorisiere Schnittstellen** die primäre Schnittstelle und alle Backup-Schnittstellen für diese HA-Gruppe.

   Ziehen Sie Zeilen, um die Werte in der Spalte **Priority order** zu ändern.

   Die erste Schnittstelle in der Liste ist die primäre Schnittstelle. Die primäre Schnittstelle ist die aktive Schnittstelle, sofern kein Fehler auftritt.

   Wenn die HA-Gruppe mehr als eine Schnittstelle enthält und die aktive Schnittstelle ausfällt, werden die virtuellen IP-Adressen (VIP-Adressen) zur ersten Backup-Schnittstelle in der Prioritätsreihenfolge verschoben. Wenn diese Schnittstelle ausfällt, wechseln die VIP-Adressen zur nächsten Backup-Schnittstelle usw. Wenn Ausfälle behoben werden, werden die VIP-Adressen wieder auf die Schnittstelle mit der höchsten Priorität verschoben, die verfügbar ist.

6. Füllen Sie für den Schritt **IP-Adressen eingeben** die folgenden Felder aus.

Feld	Beschreibung
Subnetz-CIDR	Die Adresse des VIP-Subnetzes in CIDR Notation—eine IPv4-Adresse gefolgt von einem Schrägstrich und der Subnetz-Länge (0-32). Die Netzwerkadresse darf keine Host-Bits festgelegt haben. Beispiel: `192.16.0.0/22`.

Feld	Beschreibung
Gateway-IP-Adresse (optional)	Optional Wenn sich die ONTAP-IP-Adressen, die für den Zugriff auf StorageGRID verwendet werden, nicht im selben Subnetz wie die StorageGRID-VIP-Adressen befinden, geben Sie die IP-Adresse des lokalen StorageGRID-VIP-Gateways ein. Die IP-Adresse des lokalen Gateways muss sich im VIP-Subnetz befinden.
Virtuelle IP-Adresse	Geben Sie mindestens eine und nicht mehr als zehn VIP-Adressen für die aktive Schnittstelle in der HA-Gruppe ein. Alle VIP-Adressen müssen sich innerhalb des VIP-Subnetzes befinden. Mindestens eine Adresse muss IPv4 sein. Optional können Sie weitere IPv4- und IPv6-Adressen angeben.

7. Wählen Sie **HA-Gruppe erstellen** und dann **Fertig stellen**.

Erstellen eines Load Balancer-Endpunkts für FabricPool

StorageGRID verwendet einen Load Balancer zum Managen des Workloads von Client-Applikationen wie FabricPool. Load Balancing maximiert Geschwindigkeit und Verbindungskapazität über mehrere Storage Nodes hinweg.

Wenn Sie StorageGRID für die Verwendung mit FabricPool konfigurieren, müssen Sie einen Load Balancer-Endpunkt konfigurieren und ein Load Balancer-Endpunktzertifikat hochladen oder generieren, das zum Sichern der Verbindung zwischen ONTAP und StorageGRID verwendet wird.

Um diese Aufgabe mithilfe des FabricPool-Setup-Assistenten abzuschließen, gehen Sie zu "Öffnen und Abschließen des FabricPool Setup-Assistenten".

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die Root-Zugriffsberechtigung.
- Sie haben den General überprüft "Überlegungen zum Lastausgleich" Sowie dem "Best Practices für Lastausgleich für FabricPool".

Schritte

1. Wählen Sie **CONFIGURATION** > **Network** > **Load Balancer Endpunkte**.
2. Wählen Sie **Erstellen**.
3. Füllen Sie für den Schritt **Enter Endpoint Details** die folgenden Felder aus.

Feld	Beschreibung
Name	Ein beschreibender Name für den Endpunkt.

Feld	Beschreibung
Port	Der StorageGRID-Port, den Sie für den Lastausgleich verwenden möchten. Dieses Feld ist für den ersten erstellten Endpunkt standardmäßig auf 10433 eingestellt, Sie können jedoch jeden nicht verwendeten externen Port eingeben. Wenn Sie 80 oder 443 eingeben, wird der Endpunkt nur auf Gateway-Nodes konfiguriert. Diese Ports sind für Admin-Nodes reserviert. **Hinweis:** von anderen Netzdiensten verwendete Ports sind nicht erlaubt. Siehe"Referenz für Netzwerk-Ports". Sie geben diese Nummer an ONTAP an, wenn Sie StorageGRID als FabricPool-Cloud-Tier hinzufügen.
Client-Typ	Wählen Sie **S3**.
Netzwerkprotokoll	Wählen Sie **HTTPS**. **Hinweis**: Die Kommunikation mit StorageGRID ohne TLS-Verschlüsselung wird unterstützt, aber nicht empfohlen.

4. Geben Sie für den Schritt **Bindungsmodus auswählen** den Bindungsmodus an. Der Bindungsmodus steuert, wie auf den Endpunkt zugegriffen wird—Verwendung einer beliebigen IP-Adresse oder Verwendung bestimmter IP-Adressen und Netzwerkschnittstellen.

Option	Beschreibung
Global (Standard)	Clients können über die IP-Adresse eines beliebigen Gateway-Node oder Admin-Node, die virtuelle IP-Adresse (VIP) einer beliebigen HA-Gruppe in einem beliebigen Netzwerk oder einen entsprechenden FQDN auf den Endpunkt zugreifen. Verwenden Sie die **Global**-Einstellung (Standard), es sei denn, Sie müssen die Zugriffsmöglichkeiten dieses Endpunkts einschränken.
Virtuelle IPs von HA-Gruppen	Clients müssen eine virtuelle IP-Adresse (oder einen entsprechenden FQDN) einer HA-Gruppe verwenden, um auf diesen Endpunkt zuzugreifen. Endpunkte mit diesem Bindungsmodus können alle dieselbe Portnummer verwenden, solange sich die für die Endpunkte ausgewählten HA-Gruppen nicht überlappen.
Node-Schnittstellen	Clients müssen die IP-Adressen (oder entsprechende FQDNs) der ausgewählten Knotenschnittstellen verwenden, um auf diesen Endpunkt zuzugreifen.

Option	Beschreibung
Node-Typ	Basierend auf dem von Ihnen ausgewählten Knotentyp müssen Clients entweder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Admin-Knotens oder die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Gateway-Knotens verwenden, um auf diesen Endpunkt zuzugreifen.

5. Wählen Sie für den Schritt **Tenant Access** eine der folgenden Optionen aus:

Feld	Beschreibung
Alle Mandanten zulassen (Standard)	Alle Mandantenkonten können diesen Endpunkt verwenden, um auf ihre Buckets zuzugreifen. **Alle Mandanten zulassen** ist fast immer die geeignete Option für den für FabricPool verwendeten Load Balancer Endpunkt. Sie müssen diese Option auswählen, wenn Sie noch keine Mandantenkonten erstellt haben.
Ausgewählte Mandanten zulassen	Nur die ausgewählten Mandantenkonten können diesen Endpunkt für den Zugriff auf ihre Buckets verwenden.
Ausgewählte Mandanten blockieren	Die ausgewählten Mandantenkonten können diesen Endpunkt nicht für den Zugriff auf ihre Buckets verwenden. Dieser Endpunkt kann von allen anderen Mandanten verwendet werden.

6. Wählen Sie für den Schritt **Zertifikat anhängen** eine der folgenden Optionen aus:

Feld	Beschreibung
Zertifikat hochladen (empfohlen)	Verwenden Sie diese Option, um ein CA-signiertes Serverzertifikat, einen privaten Zertifikatschlüssel und ein optionales CA-Paket hochzuladen.
Zertifikat wird generiert	Verwenden Sie diese Option, um ein selbstsigniertes Zertifikat zu generieren. Siehe "Konfigurieren von Load Balancer-Endpunkten" Für Details, was eingegeben werden soll.
StorageGRID S3 und Swift-Zertifikat verwenden	Diese Option ist nur verfügbar, wenn Sie bereits eine benutzerdefinierte Version des globalen StorageGRID-Zertifikats hochgeladen oder generiert haben. Siehe "Konfigurieren von S3- und Swift-API-Zertifikaten" Entsprechende Details.

7. Wählen Sie **Erstellen**.

Änderungen an einem Endpunktzertifikat können bis zu 15 Minuten dauern, bis sie auf alle Knoten angewendet werden können.

Erstellen eines Mandantenkontos für FabricPool

Sie müssen ein Mandantenkonto im Grid Manager for FabricPool Use erstellen.

Mandantenkonten ermöglichen Client-Applikationen, Objekte auf StorageGRID zu speichern und abzurufen. Jedes Mandantenkonto verfügt über eine eigene Account-ID, autorisierte Gruppen und Benutzer, Buckets und Objekte.

Weitere Informationen zu dieser Aufgabe finden Sie unter "Erstellen eines Mandantenkontos". Um diese Aufgabe mithilfe des FabricPool-Setup-Assistenten abzuschließen, gehen Sie zu "Öffnen und Abschließen des FabricPool Setup-Assistenten".

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben spezifische Zugriffsberechtigungen.

Schritte

1. Wählen Sie **MIETER**.
2. Wählen Sie **Erstellen**.
3. Geben Sie für die Schritte zum Eingeben von Details die folgenden Informationen ein.

Feld	Beschreibung
Name	Ein Name für das Mandantenkonto. Mandantennamen müssen nicht eindeutig sein. Wenn das Mandantenkonto erstellt wird, erhält es eine eindeutige, numerische Konto-ID.
Beschreibung (optional)	Eine Beschreibung zur Identifizierung des Mandanten.
Client-Typ	Muss **S3** für FabricPool sein.
Storage-Kontingent (optional)	Lassen Sie dieses Feld für FabricPool leer.

4. Für den Schritt Berechtigungen auswählen:
   a. Wählen Sie nicht **Plattformdienste zulassen**.

      FabricPool Mandanten benötigen in der Regel keine Plattform-Services, wie z. B. CloudMirror-Replizierung.

   b. Wählen Sie optional **eigene Identitätsquelle verwenden**.
   c. Wählen Sie nicht **S3 Select zulassen**.

      FabricPool-Mandanten müssen in der Regel nicht S3 Select verwenden.

   d. Wählen Sie optional **Grid Federation Connection** verwenden, um dem Mandanten die Verwendung eines zu ermöglichen "Netzverbundverbindung" Für Account-Klonen und Grid-übergreifende Replizierung. Wählen Sie dann die zu verwendende Netzverbundverbindung aus.
5. Geben Sie für den Schritt Root-Zugriff definieren an, welcher Benutzer die anfängliche Root-Zugriffsberechtigung für das Mandantenkonto erhält, je nachdem, ob das StorageGRID-System verwendet

"Identitätsföderation", "Single Sign On (SSO)"Oder beides.

Option	Tun Sie das
Wenn die Identitätsföderation nicht aktiviert ist	Geben Sie das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.
Wenn die Identitätsföderation aktiviert ist	a. Wählen Sie eine vorhandene Verbundgruppe aus, um Root-Zugriffsberechtigungen für den Mandanten zu erhalten. b. Geben Sie optional das Kennwort an, das beim Anmelden bei der Serviceeinheit als lokaler Root-Benutzer verwendet werden soll.
Wenn sowohl Identitätsföderation als auch Single Sign-On (SSO) aktiviert sind	Wählen Sie eine vorhandene Verbundgruppe aus, um Root-Zugriffsberechtigungen für den Mandanten zu erhalten. Keine lokalen Benutzer können sich anmelden.

6. Wählen Sie **Create Tenant**.

Erstellen eines S3-Buckets und Abrufen von Zugriffsschlüsseln

Bevor Sie StorageGRID mit einem FabricPool-Workload verwenden, müssen Sie einen S3-Bucket für Ihre FabricPool-Daten erstellen. Außerdem müssen Sie einen Zugriffsschlüssel und einen geheimen Zugriffsschlüssel für das Mandantenkonto erhalten, das Sie für FabricPool verwenden werden.

Weitere Informationen zu dieser Aufgabe finden Sie unter "S3-Bucket erstellen" Und "Erstellen Ihrer eigenen S3-Zugriffsschlüssel". Um diese Aufgabe mithilfe des FabricPool-Setup-Assistenten abzuschließen, gehen Sie zu "Öffnen und Abschließen des FabricPool Setup-Assistenten".

Bevor Sie beginnen

- Sie haben ein Mandantenkonto für die Nutzung von FabricPool erstellt.
- Sie haben Root-Zugriff auf das Mandantenkonto.

Schritte

1. Melden Sie sich beim Tenant Manager an.

   Sie können eine der folgenden Aktionen ausführen:

   - Wählen Sie auf der Seite Mandantenkonten im Grid Manager den Link **Anmelden** für den Mieter aus, und geben Sie Ihre Anmeldedaten ein.
   - Geben Sie die URL für das Mandantenkonto in einem Webbrowser ein, und geben Sie Ihre Anmeldedaten ein.

2. Erstellung eines S3-Buckets für FabricPool-Daten

   Sie müssen für jedes zu verwendende ONTAP Cluster einen eindeutigen Bucket erstellen.

   a. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3)** > **Buckets**.
   b. Wählen Sie **Eimer erstellen**.
   c. Geben Sie den Namen des StorageGRID-Buckets ein, den Sie mit FabricPool verwenden möchten.

Beispiel: `fabricpool-bucket`.

Sie können den Bucket-Namen nach dem Erstellen des Buckets nicht ändern.

d. Wählen Sie die Region für diesen Bucket aus.

Standardmäßig werden alle Buckets im erstellt `us-east-1` Werden.

e. Wählen Sie **Weiter**.

f. Wählen Sie **Eimer erstellen**.

Wählen Sie nicht **enable object Versioning** für den FabricPool Bucket aus. Bearbeiten Sie einen FabricPool-Bucket nicht, um **verfügbar** oder einen nicht standardmäßigen Konsistenzlevel zu verwenden. Die empfohlene Bucket-Konsistenzstufe für FabricPool Buckets ist **Read-after-New-write**, was die Standardeinstellung für einen neuen Bucket ist.

3. Erstellen Sie einen Zugriffsschlüssel und einen geheimen Zugriffsschlüssel.

a. Wählen Sie **STORAGE (S3)** > **Meine Zugriffsschlüssel** aus.

b. Wählen Sie **Schlüssel erstellen**.

c. Wählen Sie **Zugriffsschlüssel erstellen**.

d. Kopieren Sie die Zugriffsschlüssel-ID und den Schlüssel für den geheimen Zugriff an einen sicheren Ort, oder wählen Sie **.csv herunterladen**, um eine Tabellenkalkulationsdatei mit der Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel zu speichern.

Sie geben diese Werte in ONTAP ein, wenn Sie StorageGRID als FabricPool Cloud-Tier konfigurieren.

Wenn Sie in Zukunft in StorageGRID einen neuen Zugriffsschlüssel und einen geheimen Zugriffsschlüssel generieren, geben Sie die neuen Schlüssel in ONTAP ein, bevor Sie die alten Werte aus StorageGRID löschen. Andernfalls könnte ONTAP vorübergehend seinen Zugriff auf StorageGRID verlieren.

Konfigurieren Sie ILM für FabricPool-Daten

Sie können diese einfache Beispielrichtlinie als Ausgangspunkt für Ihre eigenen ILM-Regeln und -Richtlinien verwenden.

Das Beispiel geht davon aus, dass Sie die ILM-Regeln und eine ILM-Richtlinie für ein StorageGRID System mit vier Storage-Nodes in einem einzelnen Datacenter in Denver, Colorado, entwerfen. Die FabricPool-Daten in diesem Beispiel verwenden einen Bucket mit dem Namen `fabricpool-bucket`.

Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen. Weitere Informationen finden Sie unter "Objektmanagement mit ILM".

Verwenden Sie zur Vermeidung von Datenverlust keine ILM-Regel, die ausläuft oder die Cloud-Tiering-Daten von FabricPool löscht. Setzen Sie die Aufbewahrungsfrist auf **Forever**, um sicherzustellen, dass FabricPool-Objekte nicht durch StorageGRID ILM gelöscht werden.

Bevor Sie beginnen

- Sie haben die geprüft "Best Practices für die Verwendung von ILM mit FabricPool-Daten".
- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".
- Sie haben die Berechtigung für den ILM- oder Root-Zugriff.
- Wenn Sie von einer früheren StorageGRID-Version auf StorageGRID 11.7 aktualisiert haben, haben Sie den zu verwendenden Speicherpool konfiguriert. Im Allgemeinen sollten Sie für jeden StorageGRID-Standort einen Speicherpool erstellen.

Diese Voraussetzung gilt nicht für neue StorageGRID 11.7-Installationen. Wenn Sie StorageGRID 11.7 in einem neuen Grid installieren, werden für jeden Standort automatisch Speicherpools erstellt.

Schritte

1. Erstellen einer ILM-Regel, die sich nur auf die Daten in bezieht `fabricpool-bucket`. In dieser Beispielregel werden Kopien mit Verfahren zur Fehlerkorrektur erstellt.

Regeldefinition	Beispielwert
Regelname	2 + 1 Erasure Coding für FabricPool-Daten
Bucket-Name	`fabricpool-bucket` Sie könnten auch nach dem FabricPool-Mandantenkonto filtern.
Erweiterte Filter	Objektgröße größer als 0.2 MB. **Hinweis:** FabricPool schreibt nur 4 MB Objekte, aber Sie müssen einen Objektgrößenfilter hinzufügen, da diese Regel Erasure Coding verwendet.
Referenzzeit	Aufnahmezeit
Zeitraum und Platzierungen	Ab Tag 0 für immer speichern Speichern Sie Objekte durch Erasure Coding mit dem 2+1-EC-Schema in Denver und bewahren Sie diese Objekte für immer in StorageGRID auf. Verwenden Sie zur Vermeidung von Datenverlust keine ILM-Regel, die ausläuft oder die Cloud-Tiering-Daten von FabricPool löscht.
Aufnahmeverhalten	Ausgeglichen

2. Erstellen Sie eine standardmäßige ILM-Regel, die zwei replizierte Kopien von Objekten erstellt, die der ersten Regel nicht zugeordnet sind. Wählen Sie keinen einfachen Filter (Mandantenkonto oder Bucket-Name) oder keine erweiterten Filter aus.

Regeldefinition	Beispielwert
Regelname	Zwei replizierte Kopien
Bucket-Name	*None*
Erweiterte Filter	*None*
Referenzzeit	Aufnahmezeit
Zeitraum und Platzierungen	Ab Tag 0 für immer speichern Speichern Sie Objekte, indem Sie 2 Kopien in Denver replizieren.
Aufnahmeverhalten	Ausgeglichen

3. Erstellen Sie eine vorgeschlagene ILM-Richtlinie und wählen Sie beide Regeln aus. Da die Replikationsregel keine Filter verwendet, kann es sich um die Standardregel (letzte) für die Richtlinie handelt.
4. Aufnahme von Testobjekten in das Raster
5. Simulieren Sie die Richtlinie mit den Testobjekten, um das Verhalten zu überprüfen.
6. Aktivieren Sie die Richtlinie.

Wenn diese Richtlinie aktiviert ist, speichert StorageGRID Objektdaten wie folgt:

- Die Daten-Tiering von FabricPool in `fabricpool-bucket` Wird mithilfe des 2+1-Schemas zur Einhaltung von Datenkonsistenz (Erasure Coding) codiert. Zwei Datenfragmente und ein Paritätsfragment werden auf drei verschiedenen Storage Nodes platziert.
- Alle Objekte in allen anderen Buckets werden repliziert. Es werden zwei Kopien erstellt und auf zwei verschiedenen Speicherknoten platziert.
- Die Kopien werden für immer in StorageGRID aufbewahrt. StorageGRID ILM wird diese Objekte nicht löschen.

Erstellen einer Traffic-Klassifizierungsrichtlinie für FabricPool

Optional können Sie eine StorageGRID Traffic-Klassifizierungsrichtlinie entwerfen, um die Servicequalität für den FabricPool-Workload zu optimieren.

Weitere Informationen zu dieser Aufgabe finden Sie unter "Verwalten von Richtlinien zur Verkehrsklassifizierung". Um diese Aufgabe mithilfe des FabricPool-Setup-Assistenten abzuschließen, gehen Sie zu "Öffnen und Abschließen des FabricPool Setup-Assistenten".

Bevor Sie beginnen

- Sie sind mit einem bei Grid Manager angemeldet "Unterstützter Webbrowser".

- Sie haben die Root-Zugriffsberechtigung.

Über diese Aufgabe

Die Best Practices für das Erstellen einer Traffic-Klassifizierungsrichtlinie für FabricPool hängen vom Workload ab:

- Bei der Planung, primäre FabricPool Workload-Daten auf StorageGRID zu verschieben, sollte sichergestellt werden, dass der FabricPool-Workload den größten Teil der Bandbreite hat. Sie können eine Traffic-Klassifizierungsrichtlinie erstellen, um alle anderen Workloads einzuschränken.

  Im Allgemeinen sind FabricPool-Lesevorgänge wichtiger als Schreibvorgänge.

  Wenn beispielsweise andere S3-Clients dieses StorageGRID-System verwenden, sollten Sie eine Traffic-Klassifizierungsrichtlinie erstellen. Der Netzwerk-Traffic kann für die anderen Buckets, Mandanten, IP-Subnetze oder Load Balancer Endpunkte begrenzt werden.

*Im Allgemeinen sollten Sie keine Quality of Service-Limits für FabricPool-Workloads einführen; Sie sollten nur die anderen Workloads begrenzen.

- Die Einschränkungen, die für andere Workloads gelten, sollten das Verhalten dieser Workloads berücksichtigen. Die auferlegten Einschränkungen hängen auch von der Größe und den Funktionen des Grids und der erwarteten Auslastung ab.

Schritte

1. Wählen Sie **CONFIGURATION** > **Network** > **traffic classification**.
2. Wählen Sie **Erstellen**.
3. Geben Sie einen Namen und eine Beschreibung (optional) für die Richtlinie ein und wählen Sie **Weiter**.
4. Fügen Sie für den Schritt übereinstimmende Regeln hinzufügen mindestens eine Regel hinzu.
   a. Wählen Sie **Regel hinzufügen**
   b. Wählen Sie unter Typ * Load Balancer Endpunkt* aus, und wählen Sie den Load Balancer Endpunkt aus, den Sie für FabricPool erstellt haben.

      Sie können auch das FabricPool-Mandantenkonto oder den Bucket auswählen.

   c. Wenn diese Datenverkehrsrichtlinie den Datenverkehr für die anderen Endpunkte einschränken soll, wählen Sie **inverse Übereinstimmung**.
5. Fügen Sie optional eine oder mehrere Grenzwerte hinzu, um den Netzwerkverkehr zu steuern, der der Regel entspricht.

   StorageGRID sammelt Kennzahlen, auch wenn Sie keine Limits hinzufügen, sodass Sie Verkehrstrends besser verstehen können.

   a. Wählen Sie **Limit hinzufügen**.
   b. Wählen Sie den zu begrenzenden Verkehrstyp und die anzuwählenden Grenzwerte aus.
6. Wählen Sie **Weiter**.
7. Lesen und prüfen Sie die Richtlinie zur Verkehrsklassifizierung. Verwenden Sie die Schaltfläche * Zurück*, um zurückzugehen und Änderungen vorzunehmen. Wenn Sie mit der Richtlinie zufrieden sind, wählen Sie **Speichern und fortfahren**.

Nach dem Ende

"Zeigen Sie Metriken zum Netzwerkverkehr an" Um zu überprüfen, ob die Richtlinien die von Ihnen erwarteten Verkehrsgrenzwerte durchsetzen.

Konfigurieren Sie ONTAP System Manager

Nachdem Sie die erforderlichen StorageGRID Informationen erhalten haben, können Sie auf ONTAP StorageGRID als Cloud-Tier hinzufügen.

Bevor Sie beginnen

- Wenn Sie den FabricPool-Setup-Assistenten abgeschlossen haben, steht Ihnen der zur Verfügung `ONTAP_FabricPool_settings_bucketname.txt` Heruntergeladene Datei.
- Wenn Sie StorageGRID manuell konfiguriert haben, verfügen Sie über den vollständig qualifizierten Domänennamen (FQDN), den Sie für StorageGRID verwenden, oder über die virtuelle IP-Adresse (VIP) für die StorageGRID HA-Gruppe, die Portnummer für den Endpunkt des Load Balancer, das Load Balancer-Zertifikat, Die Zugriffsschlüssel-ID und der geheime Schlüssel für den Root-Benutzer des Mandantenkontos sowie den Namen des Bucket-ONTAP, die in diesem Mandanten verwendet werden.

Zugriff auf ONTAP System Manager

In diesen Anweisungen wird beschrieben, wie Sie StorageGRID mit ONTAP System Manager als Cloud-Tier hinzufügen. Sie können dieselbe Konfiguration mithilfe der ONTAP CLI abschließen. Weitere Anweisungen finden Sie unter "ONTAP 9: FabricPool-Tier-Management mit CLI".

Schritte

1. Greifen Sie auf System Manager für den ONTAP-Cluster zu, den Sie auf StorageGRID Tiering möchten.
2. Melden Sie sich als Administrator für das Cluster an.
3. Navigieren Sie zu **STORAGE** > **Tiers** > **Add Cloud Tier**.
4. Wählen Sie **StorageGRID** aus der Liste der Objektspeicher-Anbieter aus.

Geben Sie StorageGRID-Werte ein

Siehe "ONTAP 9: FabricPool Tier-Management-Überblick mit System Manager" Finden Sie weitere Informationen.

Schritte

1. Füllen Sie das Formular „Cloud-Tiering hinzufügen“ mit der aus `ONTAP_FabricPool_settings_bucketname.txt` Datei oder die Werte, die Sie manuell erhalten haben.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für diese Cloud-Tier ein. Sie können den Standardwert übernehmen.

Feld	Beschreibung
URL-Stil	Wenn Sie "Domänennamen des S3-Endpunkts wurden konfiguriert"Wählen Sie **Virtual Hosted-Style URL**. **Pfad-Stil-URL** ist der Standard für ONTAP, aber die Verwendung von virtuellen Hosted-Stil-Anforderungen wird für StorageGRID empfohlen. Sie müssen **Pfad-Stil-URL** verwenden, wenn Sie eine IP-Adresse anstelle eines Domänennamens für das Feld **Servername (FQDN)** angeben.
Servername (FQDN)	Geben Sie den vollständig qualifizierten Domänennamen (FQDN) ein, den Sie für StorageGRID verwenden, oder die virtuelle IP-Adresse (VIP) für die StorageGRID HA-Gruppe. Beispiel: `s3.storagegrid.company.com`. Beachten Sie Folgendes: • Die hier angegebene IP-Adresse oder der Domänenname muss mit dem Zertifikat übereinstimmen, das Sie für den StorageGRID-Load-Balancer-Endpunkt hochgeladen oder generiert haben. • Wenn Sie einen Domänennamen angeben, muss der DNS-Eintrag jeder IP-Adresse zugeordnet werden, die Sie zur Verbindung mit StorageGRID verwenden. Siehe "Konfigurieren Sie den DNS-Server".
SSL	Aktiviert (Standard).
Objektspeicherzertifikat	Fügen Sie das Zertifikat-PEM ein, das Sie für den StorageGRID Load Balancer-Endpunkt verwenden, einschließlich: `-----BEGIN CERTIFICATE-----` Und `-----END CERTIFICATE-----`. **Hinweis:** Wenn eine Zwischenzertifizierungsstelle das StorageGRID-Zertifikat ausgestellt hat, müssen Sie das Zwischenzertifikat vorlegen. Wenn das StorageGRID-Zertifikat direkt von der Root-CA ausgestellt wurde, müssen Sie das Root-CA-Zertifikat bereitstellen.
Port	Geben Sie den vom Endpunkt des StorageGRID Load Balancer verwendeten Port ein. ONTAP wird diesen Port verwenden, wenn es eine Verbindung zu StorageGRID herstellt. Beispiel: 10433.
Zugriffsschlüssel und geheimer Schlüssel	Geben Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel für den Root-Benutzer des StorageGRID-Mandantenkontos ein. **Tipp**: Wenn Sie in Zukunft einen neuen Zugriffsschlüssel und geheimen Zugriffsschlüssel in StorageGRID generieren, geben Sie die neuen Schlüssel in ONTAP ein, bevor Sie die alten Werte aus StorageGRID löschen. Andernfalls könnte ONTAP vorübergehend seinen Zugriff auf StorageGRID verlieren.
Containername	Geben Sie den Namen des StorageGRID-Buckets ein, den Sie für die Verwendung mit diesem ONTAP-Tier erstellt haben.

2. Schließen Sie die endgültige FabricPool-Konfiguration in ONTAP ab.
    a. Fügen Sie ein oder mehrere Aggregate zur Cloud-Tier hinzu.
    b. Optional können Sie eine Tiering Policy für Volumes erstellen.

Konfigurieren Sie den DNS-Server

Nach der Konfiguration von Hochverfügbarkeitsgruppen, Load Balancer-Endpunkten und S3-Endpunkt-Domänennamen müssen Sie sicherstellen, dass der DNS die erforderlichen Einträge für StorageGRID enthält. Sie müssen einen DNS-Eintrag für jeden Namen im Sicherheitszertifikat und für jede IP-Adresse angeben, die Sie verwenden können.

Siehe "Überlegungen zum Lastausgleich".

DNS-Einträge für den StorageGRID-Servernamen

Fügen Sie DNS-Einträge hinzu, um den Namen des StorageGRID-Servers (vollständig qualifizierter Domänenname) jeder verwendeten StorageGRID-IP-Adresse zuzuordnen. Die im DNS eingegebenen IP-Adressen hängen davon ab, ob Sie eine HA-Gruppe der Load-Balancing-Nodes verwenden:

- Wenn Sie eine HA-Gruppe konfiguriert haben, stellt ONTAP eine Verbindung zu den virtuellen IP-Adressen dieser HA-Gruppe her.
- Wenn Sie keine HA-Gruppe verwenden, kann sich ONTAP mithilfe der IP-Adresse eines beliebigen Gateway-Node oder Admin-Node mit dem StorageGRID Load Balancer-Service verbinden.
- Wenn der Servername auf mehr als eine IP-Adresse aufgelöst wird, baut ONTAP Client-Verbindungen mit allen IP-Adressen auf (bis zu maximal 16 IP-Adressen). Die IP-Adressen werden bei Verbindungsaufbau in einer Round-Robin-Methode erfasst.

DNS-Einträge für Anforderungen im virtuellen Hosted-Stil

Wenn Sie definiert haben "Domänennamen des S3-Endpunkts" Außerdem verwenden Sie Anfragen im virtuellen Hosted-Stil und fügen DNS-Einträge für alle erforderlichen S3-Endpunkt-Domänennamen hinzu, einschließlich aller Platzhalternamen.

StorageGRID Best Practices für FabricPool

Best Practices für Hochverfügbarkeitsgruppen (High Availability groups, HA-Gruppen

Bevor Sie StorageGRID als FabricPool-Cloud-Tier hinzufügen, erfahren Sie mehr über StorageGRID HA-Gruppen (High Availability, Hochverfügbarkeit) und lesen Sie die Best Practices zur Verwendung von HA-Gruppen mit FabricPool durch.

Was ist eine HA-Gruppe?

Eine HA-Gruppe (High Availability, Hochverfügbarkeit) ist eine Sammlung von Schnittstellen aus mehreren StorageGRID Gateway-Nodes, Admin-Nodes oder beidem. Eine HA-Gruppe hilft, Client-Datenverbindungen verfügbar zu halten. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle den Workload mit geringer Auswirkung auf die FabricPool-Vorgänge managen.

Jede HA-Gruppe ermöglicht einen hochverfügbaren Zugriff auf die Shared Services auf den zugehörigen Nodes. Beispielsweise bietet eine HA-Gruppe, die aus Schnittstellen nur auf Gateway-Nodes oder sowohl Admin-Nodes als auch Gateway-Nodes besteht, einen hochverfügbaren Zugriff auf den Shared Load Balancer

Service.

Weitere Informationen zu Hochverfügbarkeitsgruppen finden Sie unter "Managen Sie Hochverfügbarkeitsgruppen (High Availability Groups, HA-Gruppen)".

Verwenden von HA-Gruppen

Die Best Practices für die Erstellung einer StorageGRID HA-Gruppe für FabricPool hängen von den Workloads ab.

- Wenn Sie FabricPool für primäre Workload-Daten verwenden möchten, müssen Sie eine HA-Gruppe erstellen, die mindestens zwei Nodes für Lastausgleich enthält, um eine Unterbrechung des Datenabrufs zu verhindern.
- Wenn Sie eine FabricPool Richtlinie für das reine Volume-Tiering nur für Snapshots oder nicht für lokale Performance-Tiers (z. B. Disaster Recovery-Standorte oder NetApp SnapMirror Ziele) verwenden möchten, können Sie eine HA-Gruppe mit nur einem Node konfigurieren.

Diese Anweisungen beschreiben die Einrichtung einer HA-Gruppe für Active-Backup HA (ein Node ist aktiv und ein Node ist ein Backup). Möglicherweise verwenden Sie jedoch lieber DNS Round Robin oder Active-Active HA. Informationen zu den Vorteilen dieser anderen HA-Konfigurationen finden Sie unter "Konfigurationsoptionen für HA-Gruppen".

Best Practices für Lastausgleich für FabricPool

Bevor Sie StorageGRID als FabricPool-Cloud-Tier einbinden, sollten Sie sich die Best Practices für die Verwendung von Load Balancern mit FabricPool ansehen.

Allgemeine Informationen zum StorageGRID Load Balancer und zum Load Balancer-Zertifikat finden Sie unter "Überlegungen zum Lastausgleich".

Best Practices für den Mandantenzugriff auf den für FabricPool verwendeten Load Balancer-Endpunkt

Sie können steuern, welche Mandanten einen bestimmten Load Balancer-Endpunkt für den Zugriff auf ihre Buckets verwenden können. Sie können alle Mandanten erlauben, einige Mandanten zulassen oder einige Mandanten blockieren. Wenn Sie einen Endpunkt für die Lastverteilung für die FabricPool-Nutzung erstellen, wählen Sie **Alle Mandanten zulassen** aus. ONTAP verschlüsselt die in StorageGRID Buckets gespeicherten Daten, sodass diese zusätzliche Sicherheitsschicht nur wenig zusätzliche Sicherheit bietet.

Best Practices für das Sicherheitszertifikat

Wenn Sie einen StorageGRID Load Balancer-Endpunkt für die Verwendung mit FabricPool erstellen, geben Sie das Sicherheitszertifikat an, mit dem ONTAP sich mit StorageGRID authentifizieren kann.

In den meisten Fällen sollte bei der Verbindung zwischen ONTAP und StorageGRID die TLS-Verschlüsselung (Transport Layer Security) verwendet werden. Die Verwendung von FabricPool ohne TLS-Verschlüsselung wird unterstützt, aber nicht empfohlen. Wenn Sie das Netzwerkprotokoll für den Endpunkt des StorageGRID Load Balancer auswählen, wählen Sie **HTTPS** aus. Stellen Sie dann das Sicherheitszertifikat bereit, mit dem ONTAP sich mit StorageGRID authentifizieren kann.

Weitere Informationen zum Serverzertifikat für einen Lastausgleichsendpunkt:

- "Verwalten von Sicherheitszertifikaten"
- "Überlegungen zum Lastausgleich"

- "Härtungsrichtlinien für Serverzertifikate"

Zertifikat zu ONTAP hinzufügen

Wenn Sie StorageGRID als FabricPool-Cloud-Tier hinzufügen, müssen Sie dasselbe Zertifikat auf dem ONTAP-Cluster installieren, einschließlich des Stammzertifikats und aller untergeordneten Zertifizierungsstellenzertifikate.

Managen Sie den Ablauf des Zertifikats

> Wenn das Zertifikat zur Sicherung der Verbindung zwischen ONTAP und StorageGRID ausläuft, funktioniert FabricPool vorübergehend nicht mehr, und ONTAP verliert vorübergehend den Zugriff auf Daten, die auf StorageGRID-Daten verteilt sind.

Befolgen Sie die folgenden Best Practices, um Probleme mit dem Ablauf von Zertifikaten zu vermeiden:

- Überwachen Sie sorgfältig alle Warnungen, die darauf hinweisen, dass sich das Ablaufdatum des Zertifikats nähert, z. B. das Endpunktzertifikat **Ablauf des Load Balancer** und **Ablauf des globalen Serverzertifikats für S3- und Swift-API**-Warnungen.
- Halten Sie die StorageGRID- und ONTAP-Versionen des Zertifikats immer synchron. Wenn Sie das für einen Load Balancer-Endpunkt verwendete Zertifikat ersetzen oder erneuern, müssen Sie das von ONTAP für die Cloud-Tier verwendete Zertifikat ersetzen oder erneuern.
- Ein öffentlich signiertes CA-Zertifikat verwenden. Wenn Sie ein von einer Zertifizierungsstelle signiertes Zertifikat verwenden, können Sie die Grid-Management-API verwenden, um die Zertifikatrotation zu automatisieren. So können Sie bald abgelaufende Zertifikate unterbrechungsfrei ersetzen.
- Wenn Sie ein selbstsigniertes StorageGRID-Zertifikat generiert haben und dieses Zertifikat kurz vor dem Ablauf steht, müssen Sie das Zertifikat sowohl in StorageGRID als auch in ONTAP manuell ersetzen, bevor das vorhandene Zertifikat abläuft. Wenn ein selbstsigniertes Zertifikat bereits abgelaufen ist, deaktivieren Sie die Zertifikatvalidierung in ONTAP, um einen Zugriffsverlust zu verhindern.

  Siehe "NetApp Knowledge Base: So konfigurieren Sie ein neues selbstsigniertes StorageGRID Serverzertifikat für eine vorhandene ONTAP FabricPool Implementierung" Weitere Anweisungen.

Best Practices für die Verwendung von ILM mit FabricPool-Daten

Wenn Sie FabricPool für das Tiering von Daten für StorageGRID verwenden, müssen Sie die Anforderungen für die Verwendung von StorageGRID Information Lifecycle Management (ILM) mit FabricPool-Daten kennen.

> FabricPool ist nicht mit den StorageGRID ILM-Regeln oder -Richtlinien bekannt. Wenn die StorageGRID ILM-Richtlinie falsch konfiguriert ist, kann es zu Datenverlusten kommen. Ausführliche Informationen finden Sie unter "Erstellen Sie eine ILM-Regel: Überblick" Und "Erstellen Sie eine ILM-Richtlinie: Überblick".

Richtlinien für die Verwendung von ILM mit FabricPool

Bei Verwendung des FabricPool-Einrichtungsassistenten erstellt der Assistent automatisch eine neue ILM-Regel für jeden von Ihnen erstellten S3-Bucket, fügt diese Regel einer vorgeschlagenen Richtlinie hinzu und fordert Sie zur Aktivierung der neuen Richtlinie im Rahmen des Assistenten auf. Die automatisch erstellte Regel folgt den empfohlenen Best Practices: Sie verwendet 2+1 Erasure Coding an einem einzigen Standort.

Wenn Sie StorageGRID manuell konfigurieren und nicht den FabricPool Setup-Assistenten verwenden, lesen Sie diese Richtlinien, um sicherzustellen, dass Ihre ILM-Regeln und ILM-Richtlinien für FabricPool-Daten und Ihre Geschäftsanforderungen geeignet sind. Möglicherweise müssen Sie neue Regeln erstellen und Ihre aktive ILM-Richtlinie aktualisieren, um diese Richtlinien zu erfüllen.

- Sie können jede beliebige Kombination aus Replizierung und Verfahren zur Einhaltung von Datenkonsistenz zum Schutz von Cloud-Tiering-Daten verwenden.

  Die empfohlene Best Practice besteht darin, ein 2+1-Verfahren zur Einhaltung von Datenkonsistenz an einem Standort zu verwenden, um eine kosteneffiziente Datensicherung zu gewährleisten. Das Verfahren zur Einhaltung von Datenkonsistenz benötigt zwar mehr CPU, bietet aber wesentlich weniger Storage-Kapazität als Replizierung. Die Schemata 4+1 und 6+1 benötigen weniger Kapazität als das Schema 2+1. Die Schemata 4+1 und 6+1 sind jedoch weniger flexibel, wenn Sie während der Grid-Erweiterung Storage-Nodes hinzufügen müssen. Weitere Informationen finden Sie unter "Erweitern Sie Storage-Kapazität für Objekte, die nach dem Erasure-Coding-Verfahren codiert wurden".

- Jede auf FabricPool-Daten angewandte Regel muss entweder Erasure Coding verwenden oder mindestens zwei replizierte Kopien erstellen.

  > Eine ILM-Regel, die immer nur eine replizierte Kopie erstellt, gefährdet Daten permanent. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen beträchtlichen Fehler hat. Während Wartungsarbeiten wie Upgrades verlieren Sie auch vorübergehend den Zugriff auf das Objekt.

- Wenn es nötig ist "FabricPool-Daten aus StorageGRID entfernen", Verwenden Sie ONTAP, um alle Daten für das FabricPool-Volume abzurufen und auf die Performance-Tier zu übertragen.

  > Verwenden Sie zur Vermeidung von Datenverlust keine ILM-Regel, die ausläuft oder die Cloud-Tiering-Daten von FabricPool löscht. Legen Sie den Aufbewahrungszeitraum in jeder ILM-Regel auf **Forever** fest, um sicherzustellen, dass FabricPool Objekte nicht durch StorageGRID ILM gelöscht werden.

- Erstellen Sie keine Regeln, um Daten aus FabricPool Cloud-Tiers an einen anderen Speicherort zu verschieben. Sie können keinen Cloud-Speicherpool verwenden, um FabricPool-Daten in einen anderen Objektspeicher zu verschieben. Ebenso können Sie FabricPool-Daten nicht mit einem Archivknoten auf Band archivieren.

  > Die Verwendung von Cloud Storage Pools mit FabricPool wird nicht unterstützt, weil die zusätzliche Latenz zum Abrufen eines Objekts aus dem Cloud-Storage-Pool-Ziel hinzugefügt wird.

- Ab ONTAP 9.8 können Sie optional Objekt-Tags erstellen, um Daten in Tiers zu klassifizieren und zu sortieren und das Management zu erleichtern. Beispielsweise können Sie Tags nur auf FabricPool Volumes festlegen, die an StorageGRID angebunden sind. Wenn Sie dann ILM-Regeln in StorageGRID erstellen, können Sie diese Daten mithilfe des erweiterten Filter Object Tag auswählen und platzieren.

Weitere Best Practices für StorageGRID und FabricPool

Wenn Sie ein StorageGRID-System für die Verwendung mit FabricPool konfigurieren, müssen Sie möglicherweise andere StorageGRID-Optionen ändern. Bevor Sie eine globale Einstellung ändern, überlegen Sie, wie sich die Änderung auf andere S3-

Anwendungen auswirkt.

Überwachungsmeldung und Protokollziele

FabricPool-Workloads verfügen oft über eine hohe Rate an Lesevorgängen, die ein hohes Volumen an Audit-Nachrichten erzeugen können.

- Wenn Sie keine Aufzeichnung von Client-Leseoperationen für FabricPool oder eine andere S3-Anwendung benötigen, gehen Sie optional zu **CONFIGURATION** > **Monitoring** > **Audit und Syslog-Server**. Ändern Sie die Einstellung **Client reads** auf **Error**, um die Anzahl der im Auditprotokoll aufgezeichneten Überwachungsmeldungen zu verringern. Siehe "Konfigurieren von Überwachungsmeldungen und Protokollzielen" Entsprechende Details.
- Wenn Sie über ein großes Grid verfügen, mehrere Arten von S3-Applikationen verwenden oder alle Audit-Daten behalten möchten, konfigurieren Sie einen externen Syslog-Server und speichern Sie Audit-Informationen Remote. Durch die Verwendung eines externen Servers werden die Auswirkungen der Protokollierung von Audit-Nachrichten auf die Performance minimiert, ohne dass die Vollständigkeit der Audit-Daten reduziert wird. Siehe "Überlegungen für externen Syslog-Server" Entsprechende Details.

Objektverschlüsselung

Beim Konfigurieren von StorageGRID können Sie optional den aktivieren "Globale Option für Verschlüsselung gespeicherter Objekte" Falls Datenverschlüsselung für andere StorageGRID Clients erforderlich ist. Die Daten, die von FabricPool zu StorageGRID verschoben werden, sind bereits verschlüsselt, d. h. die Aktivierung der StorageGRID-Einstellung ist nicht erforderlich. Die Client-seitige Verschlüsselung ist Eigentum von ONTAP.

Objektkomprimierung

Aktivieren Sie beim Konfigurieren von StorageGRID nicht das "Globale Option zum Komprimieren gespeicherter Objekte". Die Daten, die von FabricPool zu StorageGRID verschoben werden, werden bereits komprimiert. Durch Verwendung der Option StorageGRID wird die Größe eines Objekts nicht weiter reduziert.

Bucket-Konsistenzstufe

Für FabricPool Buckets ist die empfohlene Bucket-Konsistenzstufe **Read-after-New-write**, was die Standardeinstellung für einen neuen Bucket ist. Bearbeiten Sie FabricPool Buckets nicht, um **verfügbar** oder eine andere Konsistenzstufe zu verwenden.

FabricPool Tiering

Wenn ein StorageGRID Node Storage verwendet, der von einem NetApp ONTAP System zugewiesen wurde, vergewissern Sie sich, dass auf dem Volume keine FabricPool-Tiering-Richtlinie aktiviert ist. Wenn beispielsweise ein StorageGRID Node auf einem VMware Host ausgeführt wird, stellen Sie sicher, dass für das Volume, das den Datastore für den StorageGRID Node unterstützt, keine FabricPool-Tiering-Richtlinie aktiviert ist. Das Deaktivieren von FabricPool Tiering für Volumes, die in Verbindung mit StorageGRID Nodes verwendet werden, vereinfacht die Fehlerbehebung und Storage-Vorgänge.

> ⚠ Verwenden Sie FabricPool niemals, um StorageGRID-bezogene Daten in das Tiering zurück zu StorageGRID selbst zu verschieben. Das Tiering von StorageGRID-Daten zurück in die StorageGRID verbessert die Fehlerbehebung und reduziert die Komplexität von betrieblichen Abläufen.

FabricPool-Daten aus StorageGRID entfernen

Falls Sie die aktuell in StorageGRID gespeicherten FabricPool-Daten entfernen müssen, müssen Sie mithilfe von ONTAP alle Daten des FabricPool Volumes abrufen und in die Performance-Tier verschieben.

Bevor Sie beginnen

- Sie haben die Anweisungen und Überlegungen in geprüft "Daten auf die Performance-Tier übertragen".
- Sie verwenden ONTAP 9.8 oder höher.
- Sie verwenden ein "Unterstützter Webbrowser".
- Sie gehören einer StorageGRID-Benutzergruppe für das FabricPool-Mandantenkonto an, das über den verfügt "Managen aller Buckets oder Root-Zugriffsberechtigungen".

Über diese Aufgabe

Im Folgenden wird erläutert, wie Daten von StorageGRID zurück zu FabricPool verschoben werden. Sie führen dieses Verfahren mit ONTAP und StorageGRID Tenant Manager durch.

Schritte

1. Von ONTAP, geben Sie die `volume modify` Befehl.

   Einstellen `tiering-policy` Bis `none` Um das neue Tiering zu beenden und festzulegen `cloud-retrieval-policy` Bis `promote` Um alle Daten zurückzugeben, die zuvor auf StorageGRID verschoben wurden.

   Siehe "Sämtliche Daten von einem FabricPool Volume auf die Performance-Tier übertragen".

2. Warten Sie, bis der Vorgang abgeschlossen ist.

   Sie können das verwenden `volume object-store` Befehl mit dem `tiering` Option auf "Überprüfen Sie den Status der Performance-Tier-Promotion".

3. Wenn der Hochstufen-Vorgang abgeschlossen ist, melden Sie sich beim StorageGRID-Mandanten-Manager für das FabricPool-Mandanten-Konto an.
4. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3)** > **Buckets**.
5. Vergewissern Sie sich, dass der FabricPool-Bucket jetzt leer ist.
6. Wenn der Eimer leer ist, "Löschen Sie den Bucket".

Nachdem Sie fertig sind

Wenn Sie den Bucket löschen, kann das Tiering von FabricPool zu StorageGRID nicht mehr fortgesetzt werden. Da die lokale Tier jedoch nach wie vor mit dem StorageGRID-Cloud-Tier verbunden ist, gibt ONTAP System Manager Fehlermeldungen aus, die darauf hinweisen, dass der Bucket nicht verfügbar ist.

Um diese Fehlermeldungen zu vermeiden, führen Sie einen der folgenden Schritte aus:

- Verwenden Sie FabricPool Mirror, um ein anderes Cloud-Tier zum Aggregat zu verbinden.
- Verschieben Sie die Daten aus dem FabricPool-Aggregat in ein nicht-FabricPool-Aggregat und löschen Sie dann das ungenutzte Aggregat.

Siehe "ONTAP-Dokumentation für FabricPool" Weitere Anweisungen.

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.