StorageGRID verwalten

StorageGRID software

NetApp
October 21, 2025

Inhalt

StorageGRID verwalten . . . 1
StorageGRID verwalten . . . 1
Zu dieser Anleitung . . . 1
Bevor Sie beginnen . . . 1
Erste Schritte mit Grid Manager . . . 1
Anforderungen an den Webbrowser . . . 1
Sign in . . . 2
Vom Grid Manager abmelden . . . 6
Ändern Sie Ihr Passwort . . . 7
StorageGRID Lizenzinformationen anzeigen . . . 7
Aktualisieren Sie die StorageGRID -Lizenzinformationen . . . 8
Verwenden der API . . . 9
Kontrollieren Sie den Zugriff auf StorageGRID . . . 31
Steuern Sie den StorageGRID Zugriff . . . 31
Ändern der Bereitstellungspassphrase . . . 32
Ändern der Knotenkonsolenkennwörter . . . 33
SSH-Zugriffskennwörter für Admin-Knoten ändern . . . 35
Verwenden der Identitätsföderation . . . 37
Verwalten von Administratorgruppen . . . 42
Berechtigungen der Administratorgruppe . . . 45
Benutzer verwalten . . . 49
Verwenden Sie Single Sign-On (SSO). . . . 52
Grid-Föderation verwenden . . . 82
Was ist Grid-Föderation? . . . 82
Was ist ein Kontoklon? . . . 85
Was ist Cross-Grid-Replikation? . . . 88
Vergleichen Sie Cross-Grid-Replikation und CloudMirror-Replikation . . . 93
Erstellen von Grid-Föderationsverbindungen . . . 95
Grid-Föderationsverbindungen verwalten . . . 99
Verwalten der zulässigen Mandanten für die Grid-Föderation . . . 104
Beheben von Grid-Föderationsfehlern . . . 109
Identifizieren und wiederholen Sie fehlgeschlagene Replikationsvorgänge . . . 115
Verwalten der Sicherheit . . . 119
Verwalten der Sicherheit . . . 119
Überprüfen Sie die Verschlüsselungsmethoden von StorageGRID . . . 120
Zertifikate verwalten . . . 123
Konfigurieren der Sicherheitseinstellungen . . . 156
Konfigurieren von Schlüsselverwaltungsservern . . . 161
Proxy-Einstellungen verwalten . . . 180
Kontrollieren Sie Firewalls . . . 182
Mandanten verwalten . . . 189
Was sind Mieterkonten? . . . 189
Erstellen Sie ein Mieterkonto . . . 191

Mieterkonto bearbeiten . . . 196
Ändern Sie das Kennwort für den lokalen Root-Benutzer des Mandanten . . . 198
Mieterkonto löschen . . . 199
Plattformdienste verwalten . . . 200
Verwalten von S3 Select für Mandantenkonten . . . 207
Konfigurieren von Clientverbindungen . . . 208
Konfigurieren von S3-Clientverbindungen . . . 208
Sicherheit für S3-Clients . . . 211
Verwenden Sie den S3-Setup-Assistenten . . . 212
Verwalten von HA-Gruppen . . . 222
Verwalten des Lastenausgleichs . . . 233
Konfigurieren von S3-Endpunktdomänennamen . . . 248
Zusammenfassung: IP-Adressen und Ports für Clientverbindungen . . . 250
Netzwerke und Verbindungen verwalten . . . 252
Konfigurieren der Netzwerkeinstellungen . . . 252
Richtlinien für StorageGRID -Netzwerke . . . 252
IP-Adressen anzeigen . . . 254
Konfigurieren von VLAN-Schnittstellen . . . 255
Verwalten von Richtlinien zur Datenverkehrsklassifizierung . . . 259
Unterstützte Verschlüsselungen für ausgehende TLS-Verbindungen . . . 267
Vorteile aktiver, inaktiver und gleichzeitiger HTTP-Verbindungen . . . 267
Linkkosten verwalten . . . 270
Verwenden Sie AutoSupport . . . 272
Was ist AutoSupport? . . . 272
Konfigurieren Sie AutoSupport . . . 277
Manuelles Auslösen eines AutoSupport -Pakets . . . 281
Fehlerbehebung bei AutoSupport -Paketen . . . 282
Senden Sie E-Series AutoSupport -Pakete über StorageGRID . . . 283
Speicherknoten verwalten . . . 287
Speicherknoten verwalten . . . 287
Speicheroptionen verwenden . . . 287
Verwalten des Objektmetadatenspeichers . . . 291
Einstellung für reservierten Metadatenspeicher erhöhen . . . 298
Gespeicherte Objekte komprimieren . . . 300
Vollständige Speicherknoten verwalten . . . 301
Admin-Knoten verwalten . . . 301
Verwenden Sie mehrere Admin-Knoten . . . 301
Identifizieren Sie den primären Admin-Knoten . . . 303
Benachrichtigungsstatus und Warteschlangen anzeigen . . . 303

StorageGRID verwalten

StorageGRID verwalten

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

Zu dieser Anleitung

Die wichtigsten Aufgaben zur Konfiguration und Verwaltung von StorageGRID ermöglichen Ihnen:

- Verwenden Sie den Grid Manager, um Gruppen und Benutzer einzurichten
- Erstellen Sie Mandantenkonten, um S3-Clientanwendungen das Speichern und Abrufen von Objekten zu ermöglichen
- Konfigurieren und Verwalten von StorageGRID -Netzwerken
- Konfigurieren Sie AutoSupport
- Knoteneinstellungen verwalten

Bevor Sie beginnen

- Sie verfügen über ein allgemeines Verständnis des StorageGRID -Systems.
- Sie verfügen über ziemlich detaillierte Kenntnisse zu Linux-Befehlsshells, Netzwerken sowie der Einrichtung und Konfiguration von Serverhardware.

Erste Schritte mit Grid Manager

Anforderungen an den Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	Mindestens unterstützte Version
Google Chrome	119
Microsoft Edge	119
Mozilla Firefox	119

Sie sollten das Browserfenster auf eine empfohlene Breite einstellen.

Browserbreite	Pixel
Minimum	1024
Optimum	1280

Sign in

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

Jedes StorageGRID -System umfasst einen primären Admin-Knoten und eine beliebige Anzahl nicht-primärer Admin-Knoten. Sie können sich auf jedem Admin-Knoten beim Grid Manager anmelden, um das StorageGRID -System zu verwalten. Einige Wartungsvorgänge können jedoch nur vom primären Admin-Knoten aus durchgeführt werden.

Mit HA-Gruppe verbinden

Wenn Admin-Knoten in einer Hochverfügbarkeitsgruppe (HA) enthalten sind, stellen Sie die Verbindung über die virtuelle IP-Adresse der HA-Gruppe oder einen vollqualifizierten Domänennamen her, der der virtuellen IP-Adresse zugeordnet ist. Der primäre Admin-Knoten sollte als primäre Schnittstelle der Gruppe ausgewählt werden, sodass Sie beim Zugriff auf den Grid Manager über den primären Admin-Knoten darauf zugreifen, es sei denn, der primäre Admin-Knoten ist nicht verfügbar. Sehen "Verwalten von Hochverfügbarkeitsgruppen" .

Verwenden von SSO

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

Sign in

Bevor Sie beginnen

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

  Um auf den Grid Manager über einen anderen Port als den Standardport für HTTPS (443) zuzugreifen, fügen 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 eine Sicherheitswarnung angezeigt wird, installieren Sie das Zertifikat mithilfe des Installationsassistenten des Browsers. Sehen "Sicherheitszertifikate verwalten" .

4. Sign in .

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

Kein SSO verwenden

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

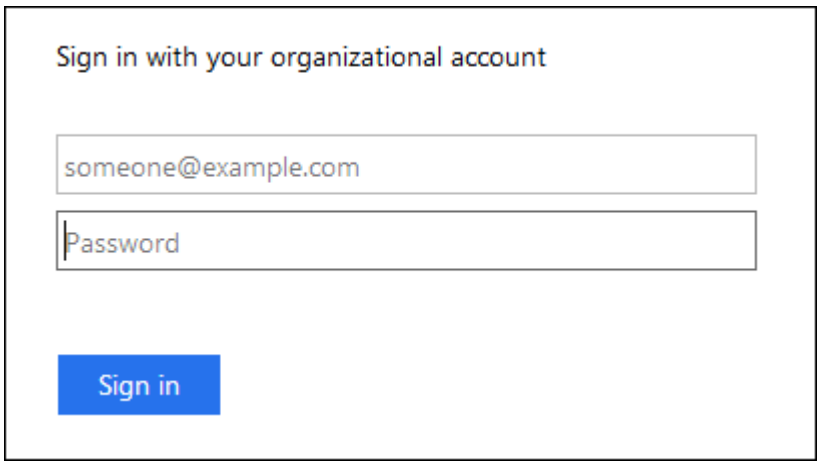
b. Wählen Sie **Anmelden**.

Verwenden von SSO

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

  i. Wählen Sie * Sign in*. Die 0 können Sie im Feld Konto stehen lassen.

  ii. Geben Sie Ihre Standard-SSO-Anmeldeinformationen auf der SSO-Anmeldeseite Ihrer Organisation ein. Beispiel:



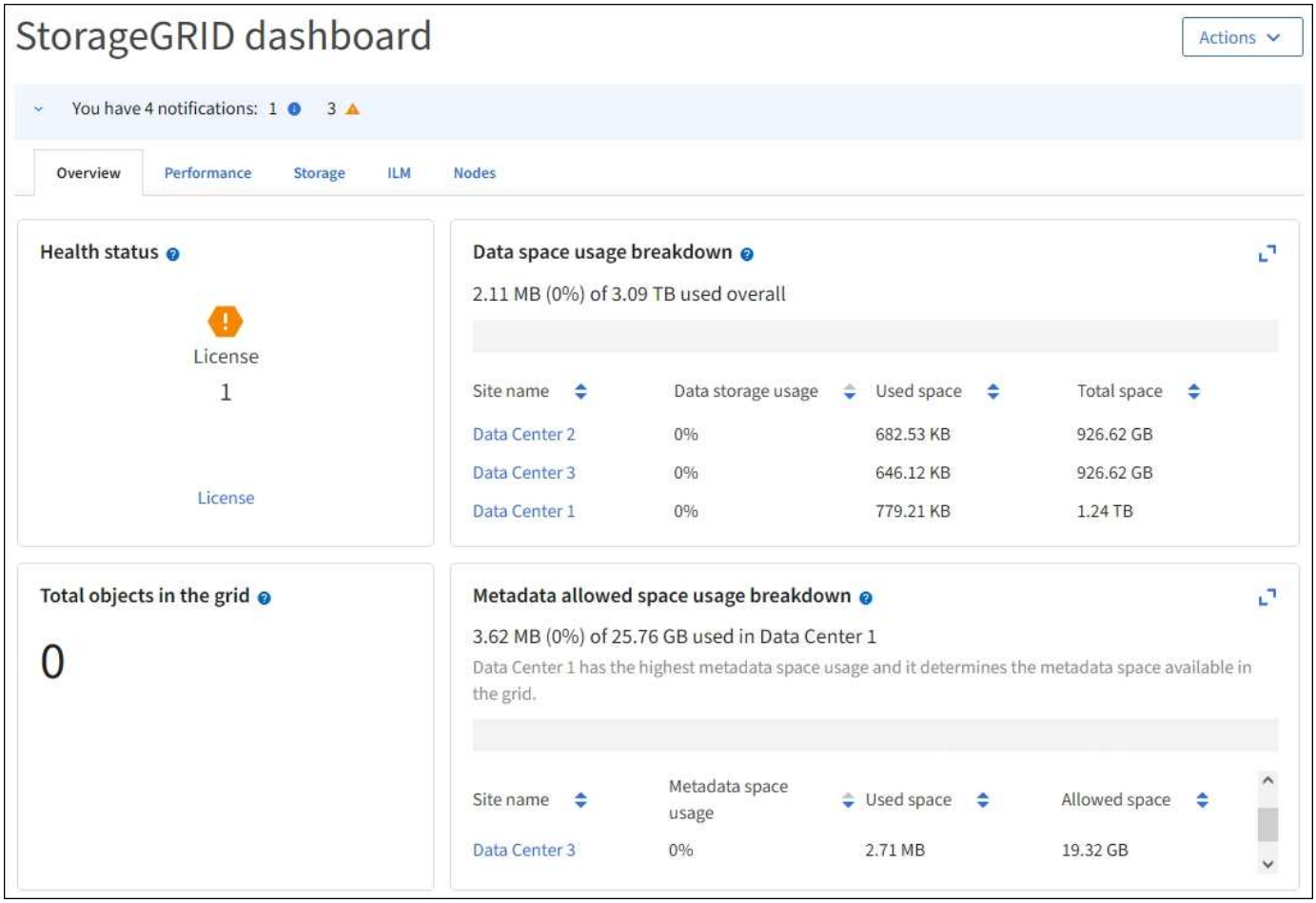
- Wenn StorageGRID SSO verwendet und Sie zuvor auf den Grid Manager oder ein Mandantenkonto zugegriffen haben:

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

ii. Wählen Sie * Sign in*.

iii. Sign in mit Ihren Standard-SSO-Anmeldeinformationen auf der SSO-Anmeldeseite Ihrer Organisation an.

Wenn Sie angemeldet sind, wird die Startseite des Grid Managers angezeigt, die das Dashboard enthält. Um zu erfahren, welche Informationen bereitgestellt werden, siehe"Anzeigen und Verwalten des Dashboards" .



Melden Sie sich bei einem anderen Admin-Knoten an

Befolgen Sie diese Schritte, um sich bei einem anderen Admin-Knoten anzumelden.

Kein SSO verwenden

Schritte

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

Verwenden von SSO

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

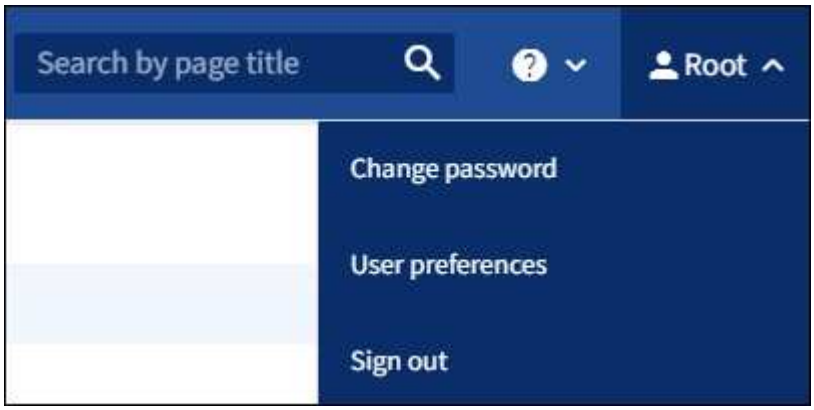
1. Geben Sie den vollqualifizierten Domänennamen oder die IP-Adresse des anderen Admin-Knotens in die Adressleiste des Browsers ein.
2. Wenn Ihre SSO-Sitzung abgelaufen ist, geben Sie Ihre Anmeldeinformationen erneut ein.

Vom Grid Manager abmelden

Wenn Sie mit der Arbeit mit dem Grid Manager fertig sind, müssen Sie sich abmelden, um sicherzustellen, dass nicht autorisierte Benutzer nicht auf das StorageGRID -System zugreifen können. Wenn Sie Ihren Browser schließen, werden Sie je nach den Cookie-Einstellungen Ihres Browsers möglicherweise nicht vom System abgemeldet.

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 Managers wird angezeigt. **Hinweis:** Wenn Sie sich bei mehr als einem Admin-Knoten angemeldet haben, müssen Sie sich von jedem Knoten abmelden.

Option	Beschreibung
SSO aktiviert	Sie sind von allen Admin-Knoten abgemeldet, auf die Sie zugegriffen haben. Die StorageGRID -Anmeldeseite wird angezeigt. **Grid Manager** wird im Dropdown-Menü **Letzte Konten** als Standard aufgeführt und das Feld **Konto-ID** zeigt 0 an. **Hinweis:** Wenn SSO aktiviert ist und Sie auch beim Tenant Manager angemeldet sind, müssen Sie auch"Melden Sie sich vom Mieterkonto ab" Zu"Abmelden von SSO" .

Ändern Sie Ihr Passwort

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

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

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

Schritte

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

   Ihr Passwort muss mindestens 8 und darf nicht mehr als 32 Zeichen enthalten. Bei Passwörtern wird zwischen Groß- und Kleinschreibung unterschieden.

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

StorageGRID Lizenzinformationen anzeigen

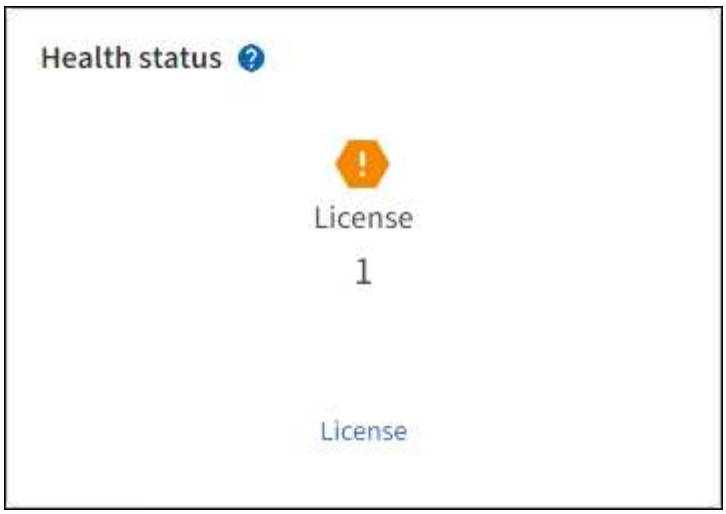
Sie können die Lizenzinformationen für Ihr StorageGRID -System, beispielsweise die maximale Speicherkapazität Ihres Grids, bei Bedarf einsehen.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Wenn ein Problem mit der Softwarelizenz für dieses StorageGRID -System vorliegt, enthält die Integritätsstatuskarte auf dem Dashboard ein Lizenzstatussymbol und einen **Lizenz**-Link. Die Zahl gibt die Anzahl der lizenzbezogenen Probleme an.



Schritte

1. Greifen Sie auf die Lizenzseite zu, indem Sie einen der folgenden Schritte ausführen:
   - Wählen Sie **WARTUNG** > **System** > **Lizenz**.
   - Wählen Sie auf der Gesundheitsstatuskarte im Dashboard das Lizenzstatussymbol oder den Link **Lizenz** aus.

     Dieser Link wird nur angezeigt, wenn ein Problem mit der Lizenz vorliegt.
2. Zeigen Sie die schreibgeschützten Details für die aktuelle Lizenz an:
   - StorageGRID -System-ID, die eindeutige Identifikationsnummer für diese StorageGRID Installation
   - Lizenzseriennummer
   - Lizenztyp, entweder **Dauerlizenz** oder **Abonnement**
   - Lizenzierte Speicherkapazität des Netzes
   - Unterstützte Speicherkapazität
   - Enddatum der Lizenz. **N/A** wird für eine unbefristete Lizenz angezeigt.
   - Support-Enddatum

     Dieses Datum wird aus der aktuellen Lizenzdatei gelesen und kann veraltet sein, wenn Sie den Support-Servicevertrag nach Erhalt der Lizenzdatei verlängert oder erneuert haben. Informationen zum Aktualisieren dieses Werts finden Sie unter"Aktualisieren Sie die StorageGRID -Lizenzinformationen" . Sie können das tatsächliche Vertragsende auch mit Active IQ einsehen.
   - Inhalt der Lizenztextdatei

Aktualisieren Sie die StorageGRID -Lizenzinformationen

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

Bevor Sie beginnen

- Sie haben eine neue Lizenzdatei, die Sie auf Ihr StorageGRID -System anwenden können.

- Du hast"spezifische Zugriffsberechtigungen" .
- Sie haben die Bereitstellungspassphrase.

Schritte

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

   Die neue Lizenzdatei wird validiert und angezeigt.
4. Geben Sie die Bereitstellungspassphrase ein.
5. Wählen Sie **Speichern**.

Verwenden der API

Verwenden Sie die Grid Management API

Sie können Systemverwaltungsaufgaben mithilfe der Grid Management REST API anstelle der Grid Manager-Benutzeroberfläche ausführen. Beispielsweise möchten Sie die API möglicherweise verwenden, um Vorgänge zu automatisieren oder mehrere Entitäten, z. B. Benutzer, schneller zu erstellen.

Top-Level-Ressourcen

Die Grid Management API bietet die folgenden Ressourcen der obersten Ebene:

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

API-Anfragen stellen

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

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

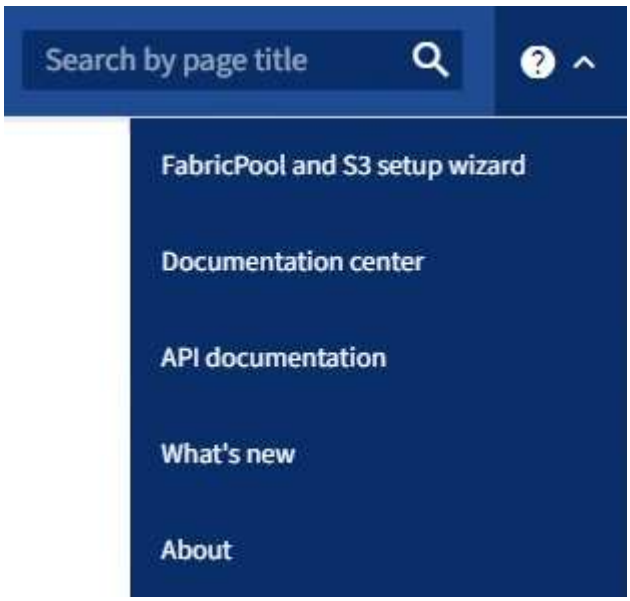
Bevor Sie beginnen

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

Alle API-Operationen, die Sie über die API-Dokumentationswebseite durchführen, sind Live-Operationen. Achten Sie darauf, dass Sie nicht versehentlich Konfigurationsdaten oder andere Daten erstellen, aktualisieren oder löschen.

Schritte

1. Wählen Sie in der Kopfzeile des Grid Managers das Hilfesymbol und dann **API-Dokumentation** aus.



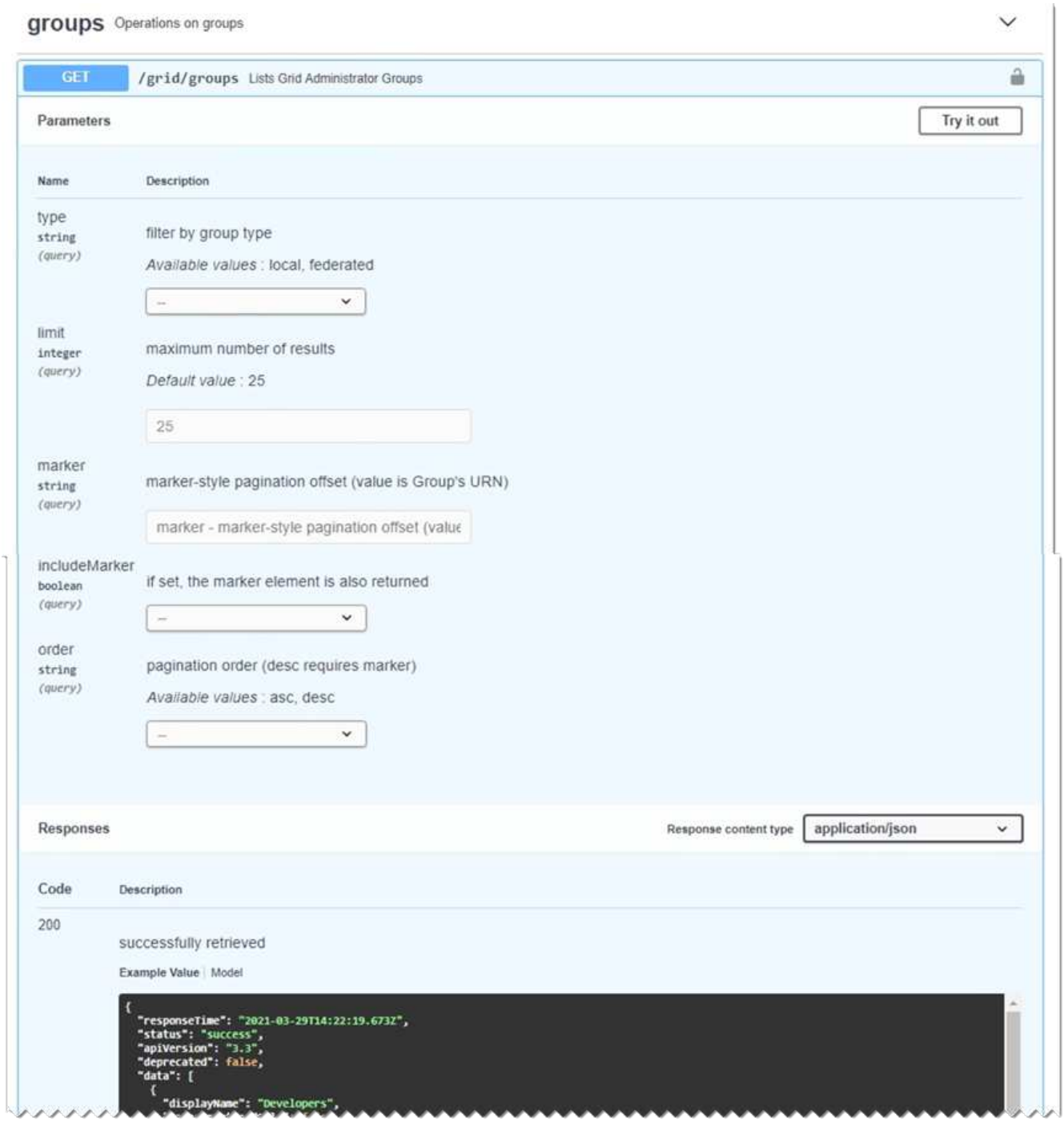
2. Um einen Vorgang mit der privaten API durchzuführen, wählen Sie auf der StorageGRID Management-API-Seite **Zur privaten API-Dokumentation gehen**.

   Die privaten APIs können ohne vorherige Ankündigung geändert werden. Private StorageGRID Endpunkte ignorieren auch die API-Version der Anfrage.

3. Wählen Sie die gewünschte Operation aus.

   Wenn Sie eine API-Operation erweitern, können Sie die verfügbaren HTTP-Aktionen wie GET, PUT, UPDATE und DELETE sehen.

4. Wählen Sie eine HTTP-Aktion aus, um die Anforderungsdetails anzuzeigen, einschließlich der Endpunkt-URL, einer Liste aller erforderlichen oder optionalen Parameter, eines Beispiels des Anforderungstexts (falls erforderlich) und der möglichen Antworten.



5. Stellen Sie fest, ob für die Anforderung zusätzliche Parameter erforderlich sind, beispielsweise eine Gruppen- oder Benutzer-ID. Besorgen Sie sich dann diese Werte. Möglicherweise müssen Sie zuerst eine andere API-Anfrage stellen, um die benötigten Informationen zu erhalten.
6. Stellen Sie fest, ob Sie den Beispielanforderungstext ändern müssen. Wenn ja, können Sie **Modell** auswählen, um die Anforderungen für jedes Feld zu erfahren.
7. Wählen Sie **Ausprobieren**.
8. Geben Sie alle erforderlichen Parameter an oder ändern Sie den Anforderungstext nach Bedarf.
9. Wählen Sie **Ausführen**.
10. Überprüfen Sie den Antwortcode, um festzustellen, ob die Anfrage erfolgreich war.

Grid Management-API-Operationen

Die Grid Management API organisiert die verfügbaren Vorgänge in den folgenden Abschnitten.

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

- **Konten**: Vorgänge zum Verwalten von Speichermandantenkonten, einschließlich Erstellen neuer Konten und Abrufen der Speichernutzung für ein bestimmtes Konto.
- **Alarmverlauf**: Vorgänge für gelöste Alarme.
- **Alarmempfänger**: Vorgänge für Empfänger von Alarmbenachrichtigungen (E-Mail).
- **alert-rules**: Vorgänge für Alarmregeln.
- **alert-silences**: Vorgänge zum Stummschalten von Alarmen.
- **Alarme**: Vorgänge für Alarme.
- **Audit**: Vorgänge zum Auflisten und Aktualisieren der Audit-Konfiguration.
- **auth**: Vorgänge zum Durchführen der Benutzersitzungsauthentifizierung.

  Die Grid Management API unterstützt das Bearer Token Authentication Scheme. Um sich anzumelden, geben Sie im JSON-Text der Authentifizierungsanfrage einen Benutzernamen und ein Kennwort ein (das heißt, `POST /api/v3/authorize`). Wenn der Benutzer erfolgreich authentifiziert wurde, wird ein Sicherheitstoken zurückgegeben. Dieses Token muss im Header nachfolgender API-Anfragen bereitgestellt werden („Authorization: Bearer *token*“). Das Token verfällt nach 16 Stunden.

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

  Informationen zur Verbesserung der Authentifizierungssicherheit finden Sie unter „Schutz vor Cross-Site Request Forgery“.

- **Client-Zertifikate**: Vorgänge zum Konfigurieren von Client-Zertifikaten, sodass mithilfe externer Überwachungstools sicher auf StorageGRID zugegriffen werden kann.
- **config**: Vorgänge im Zusammenhang mit der Produktversion und den Versionen der Grid Management API. Sie können die Produktversion und die Hauptversionen der Grid Management-API auflisten, die von dieser Version unterstützt werden, und Sie können veraltete Versionen der API deaktivieren.
- **deaktivierte Funktionen**: Vorgänge zum Anzeigen von Funktionen, die möglicherweise deaktiviert wurden.
- **DNS-Server**: Vorgänge zum Auflisten und Ändern konfigurierter externer DNS-Server.
- **Laufwerksdetails**: Vorgänge auf Laufwerken für bestimmte Speichergerätemodelle.
- **Endpunktdomänennamen**: Vorgänge zum Auflisten und Ändern von S3-Endpunktdomänennamen.
- **Erasure-Coding**: Operationen an Erasure-Coding-Profilen.
- **Erweiterung**: Operationen zur Erweiterung (Prozedurebene).
- **Expansion-Nodes**: Operationen auf Expansionsebene (Knotenebene).
- **expansion-sites**: Operationen zur Erweiterung (Site-Ebene).
- **grid-networks**: Vorgänge zum Auflisten und Ändern der Grid-Netzwerkliste.

- **grid-passwords**: Vorgänge für die Grid-Passwortverwaltung.
- **Gruppen**: Vorgänge zum Verwalten lokaler Grid-Administratorgruppen und zum Abrufen föderierter Grid-Administratorgruppen von einem externen LDAP-Server.
- **Identitätsquelle**: Vorgänge zum Konfigurieren einer externen Identitätsquelle und zum manuellen Synchronisieren von föderierten Gruppen- und Benutzerinformationen.
- **ilm**: Vorgänge im Bereich Information Lifecycle Management (ILM).
- **in-progress-procedures**: Ruft die Wartungsvorgänge ab, die derzeit ausgeführt werden.
- **Lizenz**: Vorgänge zum Abrufen und Aktualisieren der StorageGRID -Lizenz.
- **logs**: Vorgänge zum Sammeln und Herunterladen von Protokolldateien.v
- **Metriken**: Vorgänge an StorageGRID -Metriken, einschließlich sofortiger Metrikabfragen zu einem bestimmten Zeitpunkt und Bereichsmetrikabfragen über einen bestimmten Zeitraum. Die Grid Management API verwendet das Systemüberwachungstool Prometheus als Backend-Datenquelle. Informationen zum Erstellen von Prometheus-Abfragen finden Sie auf der Prometheus-Website.

> ⓘ Metriken, die Folgendes umfassen:*`private`* in ihren Namen sind nur für den internen Gebrauch bestimmt. Diese Kennzahlen können sich zwischen den StorageGRID Versionen ohne Vorankündigung ändern.

- **Knotendetails**: Operationen an Knotendetails.
- **Knotengesundheit**: Vorgänge zum Knotengesundheitsstatus.
- **node-storage-state**: Vorgänge zum Knotenspeicherstatus.
- **ntp-servers**: Vorgänge zum Auflisten oder Aktualisieren externer Network Time Protocol (NTP)-Server.
- **Objekte**: Operationen an Objekten und Objektmetadaten.
- **Wiederherstellung**: Vorgänge für das Wiederherstellungsverfahren.
- **recovery-package**: Vorgänge zum Herunterladen des Wiederherstellungspakets.
- **Regionen**: Vorgänge zum Anzeigen und Erstellen von Regionen.
- **s3-object-lock**: Vorgänge an globalen S3-Objektsperreinstellungen.
- **Serverzertifikat**: Vorgänge zum Anzeigen und Aktualisieren von Grid Manager-Serverzertifikaten.
- **snmp**: Vorgänge an der aktuellen SNMP-Konfiguration.
- **storage-watermarks**: Wasserzeichen des Speicherknotens.
- **Verkehrsklassen**: Vorgänge für Verkehrsklassifizierungsrichtlinien.
- **untrusted-client-network**: Vorgänge an der nicht vertrauenswürdigen Client-Netzwerkkonfiguration.
- **Benutzer**: Vorgänge zum Anzeigen und Verwalten von Grid Manager-Benutzern.

Grid Management API-Versionierung

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

Diese Anforderungs-URL gibt beispielsweise Version 4 der API an.

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

Die Hauptversion der API wird erhöht, wenn Änderungen vorgenommen werden, die mit älteren Versionen

nicht kompatibel sind. Die Nebenversion der API wird erhöht, wenn Änderungen vorgenommen werden, die mit älteren Versionen *kompatibel* sind. Zu den kompatiblen Änderungen gehört das Hinzufügen neuer Endpunkte oder neuer Eigenschaften.

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

Art der Änderung an der API	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 API aktiviert. Wenn Sie jedoch auf eine neue Funktionsversion von StorageGRID aktualisieren, haben Sie weiterhin Zugriff auf die ältere API-Version für mindestens eine StorageGRID -Funktionsversion.

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

Veraltete Anfragen werden auf folgende Weise als veraltet gekennzeichnet:

- Der Antwortheader lautet „Deprecated: true“
- Der JSON-Antworttext enthält „deprecated“: true
- Zu nms.log wird eine veraltete Warnung hinzugefügt. Beispiel:

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

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

Verwenden Sie die `GET /versions` API-Anforderung zum Zurückgeben einer Liste der unterstützten API-Hauptversionen. Diese Anfrage befindet sich im Abschnitt **config** der Swagger-API-Dokumentation.

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

Angeben einer API-Version für eine Anfrage

Sie können die API-Version mithilfe eines Pfadparameters angeben(`/api/v4`) oder eine Kopfzeile(`Api-Version: 4`). Wenn Sie beide Werte angeben, überschreibt der Header-Wert den Pfadwert.

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

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

Schutz vor Cross-Site Request Forgery (CSRF)

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

Ein Angreifer, der eine Anfrage an eine andere Site auslösen kann (z. B. mit einem HTTP-Formular-POST), kann dafür sorgen, dass bestimmte Anfragen unter Verwendung der Cookies des angemeldeten Benutzers gestellt werden.

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

Um die Funktion zu aktivieren, legen Sie die `csrfToken` Parameter auf `true` während der Authentifizierung. Die Standardeinstellung ist `false` .

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

Wenn dies zutrifft, `GridCsrfToken` Cookie wird mit einem zufälligen Wert für Anmeldungen am Grid Manager gesetzt, und die `AccountCsrfToken` Für die Anmeldung beim Tenant Manager wird ein Cookie mit einem zufälligen Wert gesetzt.

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

- Der `X-Csrf-Token` Header, wobei der Wert des Headers auf den Wert des CSRF-Token-Cookies gesetzt ist.
- Für Endpunkte, die einen formkodierten Textkörper akzeptieren: A `csrfToken` formcodierter Anforderungstextparameter.

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

> Anfragen, für die ein CSRF-Token-Cookie gesetzt ist, erzwingen außerdem den Header „Content-Type: application/json“ für alle Anfragen, die einen JSON-Anforderungstext erwarten, als zusätzlichen Schutz vor CSRF-Angriffen.

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

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

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

Sign in , wenn Single Sign-On aktiviert ist

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

Bevor Sie beginnen

- Sie kennen den SSO-Benutzernamen und das Kennwort für einen Verbundbenutzer, der zu einer StorageGRID -Benutzergruppe gehört.
- Wenn Sie auf die Tenant Management API zugreifen möchten, kennen Sie die Mandantenkonto-ID.

Informationen zu diesem Vorgang

Um ein Authentifizierungstoken zu erhalten, können Sie eines der folgenden Beispiele verwenden:

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

Installationsdateien befindet(`./rpms` für Red Hat Enterprise Linux, `./debs` für Ubuntu oder Debian und `./vsphere` für VMware).

- Ein Beispiel-Workflow für Curl-Anfragen.

  Wenn Sie den Curl-Workflow zu langsam ausführen, kann es zu einer Zeitüberschreitung kommen. Möglicherweise wird der folgende Fehler angezeigt: `A valid SubjectConfirmation was not found on this Response`.

  > Der beispielhafte Curl-Workflow schützt das Kennwort nicht davor, von anderen Benutzern eingesehen zu werden.

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

Schritte

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

   Geben Sie bei entsprechender 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 Mandantenverwaltungs-API zugreifen möchten.

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

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

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

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

   a. Deklarieren Sie die für die Anmeldung erforderlichen Variablen.

```
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 weitergeleitet an `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, jedoch nicht die zusätzliche JSON-Codierungsebene.

```
{
    "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 Clientanforderungs-ID von AD FS enthält.

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

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

Die Antwort enthält die Client-Anforderungs-ID:

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

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

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

f. Senden Sie Ihre Anmeldeinformationen 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 302-Weiterleitung mit zusätzlichen Informationen in den Headern zurück.

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

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

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

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

h. Senden Sie eine GET-Anfrage mit den Cookies aus dem Authentifizierungs-POST an den angegebenen Speicherort.

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

Die Antwortheader enthalten AD FS-Sitzungsinformationen für die spätere Abmeldung und der Antworttext enthält die SAML-Antwort in einem ausgeblendeten 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 versteckten Feld:

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

j. Mit den gespeicherten `SAMLResponse` , erstellen Sie ein StorageGRID`/api/saml-response` Anforderung zum Generieren eines StorageGRID Authentifizierungstokens.

   Für `RelayState` , verwenden Sie die Mandantenkonto-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 enthält das Authentifizierungstoken.

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

a. Speichern Sie das Authentifizierungstoken in der Antwort als `MYTOKEN` .

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

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

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

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

Informationen zu diesem Vorgang

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

Schritte

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

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

Es wird eine Abmelde-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 Abmelde-URL.

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

3. Senden Sie eine Anfrage an die Abmelde-URL, um SLO auszulösen und zurück zu StorageGRID umzuleiten.

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

Die 302-Antwort wird zurückgegeben. Der Umleitungsort ist nicht auf die reine API-Abmeldung anwendbar.

```
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 Bearer-Token.

Das Löschen des StorageGRID Bearer-Tokens funktioniert genauso wie ohne SSO. Wenn „Cookie „sso=true““ nicht angegeben ist, 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 Sie die API, wenn Single Sign-On aktiviert ist (Azure).

Wenn Sie"Single Sign-On (SSO) konfiguriert und aktiviert" und Sie Azure als SSO-Anbieter verwenden, können Sie mithilfe von zwei Beispielskripten ein Authentifizierungstoken erhalten, das für die Grid Management API oder die Tenant Management API gültig ist.

Sign in , wenn Azure Single Sign-On aktiviert ist.

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

Bevor Sie beginnen

- Sie kennen die SSO-E-Mail-Adresse und das Kennwort für einen Verbundbenutzer, der zu einer StorageGRID Benutzergruppe gehört.
- Wenn Sie auf die Tenant Management API zugreifen möchten, kennen Sie die Mandantenkonto-ID.

Informationen zu diesem Vorgang

Um ein Authentifizierungstoken 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 StorageGRID Installationsverzeichnis(`./rpms` für Red Hat Enterprise Linux, `./debs` für Ubuntu oder Debian und `./vsphere` für VMware).

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

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

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

Schritte

1. Installieren Sie die erforderlichen Abhängigkeiten wie folgt:

a. Installieren Sie Node.js (siehe "https://nodejs.org/en/download/").

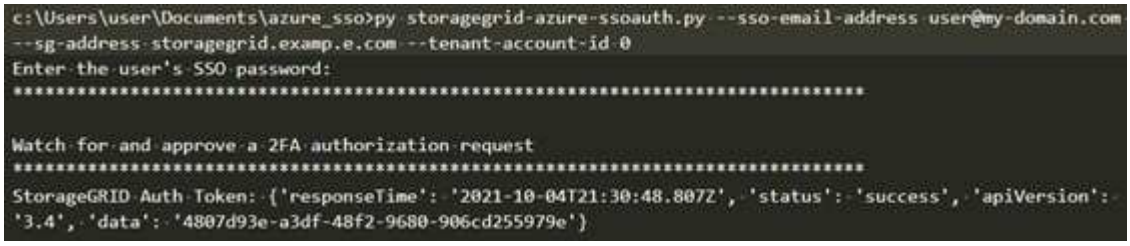
b. Installieren Sie die erforderlichen Node.js-Module (Puppeteer und jsdom):

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

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

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

3. Geben Sie bei entsprechender Aufforderung Werte für die folgenden Argumente ein (oder übergeben Sie sie mithilfe von Parametern):
   - Die SSO-E-Mail-Adresse, die zur Anmeldung bei Azure verwendet wird
   - Die Adresse für StorageGRID
   - Die Mandantenkonto-ID, wenn Sie auf die Mandantenverwaltungs-API zugreifen möchten
4. Geben Sie bei der entsprechenden Aufforderung das Kennwort ein und seien Sie bereit, Azure bei Bedarf eine MFA-Autorisierung bereitzustellen.



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

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

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

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

Sign in , wenn Single Sign-On aktiviert ist

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

Bevor Sie beginnen

- Sie kennen den SSO-Benutzernamen und das Kennwort für einen Verbundbenutzer, der zu einer StorageGRID -Benutzergruppe gehört.
- Wenn Sie auf die Tenant Management API zugreifen möchten, kennen Sie die Mandantenkonto-ID.

Informationen zu diesem Vorgang

Um ein Authentifizierungstoken zu erhalten, können Sie eines der folgenden Beispiele verwenden:

- Der `storagegrid-ssoauth.py` Python-Skript, das sich im Verzeichnis der StorageGRID Installationsdateien befindet(`./rpms` für Red Hat Enterprise Linux, `./debs` für Ubuntu oder Debian und `./vsphere` für VMware).
- Ein Beispiel-Workflow für Curl-Anfragen.

  Wenn Sie den Curl-Workflow zu langsam ausführen, kann es zu einer Zeitüberschreitung kommen. Möglicherweise wird der folgende Fehler angezeigt: `A valid SubjectConfirmation was not found on this Response`.

  > Der beispielhafte Curl-Workflow schützt das Kennwort nicht davor, von anderen Benutzern eingesehen zu werden.

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

Schritte

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

   Geben Sie bei entsprechender Aufforderung Werte für die folgenden Argumente ein:

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

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

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

   Das StorageGRID Autorisierungstoken wird in der Ausgabe bereitgestellt. Sie können das Token jetzt für

andere Anfragen verwenden, ähnlich wie Sie die API verwenden würden, wenn SSO nicht verwendet würde.

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

   a. Deklarieren Sie die für die Anmeldung erforderlichen Variablen.

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

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

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

```
{
    "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 geben Sie die Antwort wieder:

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

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

e. Exportieren Sie den Wert „pf.adapterId“ und geben Sie die Antwort aus:

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

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

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

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

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

g. Exportieren Sie den „Aktionswert“:

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

h. Senden Sie Cookies zusammen mit Anmeldeinformationen:

```
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 versteckten Feld:

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

j. Mit den gespeicherten `SAMLResponse` , erstellen Sie ein StorageGRID`/api/saml-response` Anforderung zum Generieren eines StorageGRID Authentifizierungstokens.

   Für `RelayState` , verwenden Sie die Mandantenkonto-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 enthält das Authentifizierungstoken.

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

a. Speichern Sie das Authentifizierungstoken in der Antwort als `MYTOKEN` .

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

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

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

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

Informationen zu diesem Vorgang

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

Schritte

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

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

Es wird eine Abmelde-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 Abmelde-URL.

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

3. Senden Sie eine Anfrage an die Abmelde-URL, um SLO auszulösen und zurück zu StorageGRID umzuleiten.

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

Die 302-Antwort wird zurückgegeben. Der Umleitungsort ist nicht auf die reine API-Abmeldung anwendbar.

```
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 Bearer-Token.

Das Löschen des StorageGRID Bearer-Tokens funktioniert genauso wie ohne SSO. Wenn „Cookie „sso=true““ nicht angegeben ist, 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
```

Funktionen mit der API deaktivieren

Sie können die Grid Management API verwenden, um bestimmte Funktionen im StorageGRID -System vollständig zu deaktivieren. Wenn eine Funktion deaktiviert ist, können niemandem Berechtigungen zum Ausführen der mit dieser Funktion verbundenen Aufgaben zugewiesen werden.

Informationen zu diesem Vorgang

Mit dem System „Deaktivierte Funktionen“ können Sie den Zugriff auf bestimmte Funktionen im StorageGRID -System verhindern. Das Deaktivieren einer Funktion ist die einzige Möglichkeit, den Root-Benutzer oder Benutzer, die zu Administratorgruppen mit der Berechtigung **Root-Zugriff** gehören, daran zu hindern, diese Funktion zu verwenden.

Um zu verstehen, wie nützlich diese Funktionalität sein kann, betrachten Sie das folgende Szenario:

Unternehmen A ist ein Dienstanbieter, der die Speicherkapazität seines StorageGRID -Systems durch die Erstellung von Mieterkonten mietet. Um die Sicherheit der Objekte ihrer Mieter zu gewährleisten, möchte Unternehmen A sicherstellen, dass seine eigenen Mitarbeiter nach der Bereitstellung des Kontos niemals auf ein Mieterkonto zugreifen können.

*Unternehmen A kann dieses Ziel erreichen, indem es das System zum Deaktivieren von Funktionen in der Grid Management-API verwendet. Durch die vollständige Deaktivierung der Funktion **Root-Passwort des Mandanten ändern** im Grid Manager (sowohl in der Benutzeroberfläche als auch in der API) stellt Unternehmen A sicher, dass Administratorbenutzer – einschließlich des Root-Benutzers und Benutzer, die zu Gruppen mit der Berechtigung **Root-Zugriff** gehören – das Passwort für den Root-Benutzer eines Mandantenkontos nicht ändern können.*

Schritte

1. Greifen Sie auf die Swagger-Dokumentation für die Grid Management API zu. Sehen "Verwenden Sie die Grid Management API" .
2. Suchen Sie den Endpunkt „Funktionen deaktivieren“.
3. Um eine Funktion zu deaktivieren, z. B. „Stammkennwort des Mandanten ändern“, senden Sie einen Text wie diesen an die API:

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

   Wenn die Anfrage abgeschlossen ist, wird die Funktion „Stammkennwort des Mandanten ändern“ deaktiviert. Die Verwaltungsberechtigung **Stammkennwort des Mandanten ändern** wird nicht mehr in der Benutzeroberfläche angezeigt und jede API-Anforderung, die versucht, das Stammkennwort für einen Mandanten zu ändern, schlägt mit „403 Forbidden“ fehl.

Deaktivierte Funktionen reaktivieren

Standardmäßig können Sie die Grid Management API verwenden, um eine deaktivierte Funktion wieder zu aktivieren. Wenn Sie jedoch verhindern möchten, dass deaktivierte Funktionen jemals wieder aktiviert werden, können Sie die Funktion **activateFeatures** selbst deaktivieren.

> Die Funktion **activateFeatures** kann nicht erneut aktiviert werden. Wenn Sie sich entscheiden, diese Funktion zu deaktivieren, beachten Sie, dass Sie dadurch dauerhaft die Möglichkeit verlieren, andere deaktivierte Funktionen wieder zu aktivieren. Sie müssen sich an den technischen Support wenden, um verlorene Funktionen wiederherzustellen.

Schritte

1. Greifen Sie auf die Swagger-Dokumentation für die Grid Management API zu.
2. Suchen Sie den Endpunkt „Funktionen deaktivieren“.
3. Um alle Funktionen wieder zu aktivieren, senden Sie einen Text wie diesen an die API:

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

Wenn diese Anforderung abgeschlossen ist, werden alle Funktionen, einschließlich der Funktion „Stammkennwort des Mandanten ändern“, wieder aktiviert. Die Verwaltungsberechtigung **Root-Passwort des Mandanten ändern** wird jetzt in der Benutzeroberfläche angezeigt und jede API-Anforderung, die versucht, das Root-Passwort für einen Mandanten zu ändern, ist erfolgreich, vorausgesetzt, der Benutzer verfügt über die Verwaltungsberechtigung **Root-Zugriff** oder **Root-Passwort des Mandanten ändern**.

Das vorherige Beispiel bewirkt, dass *alle* deaktivierten Funktionen wieder aktiviert werden. Wenn andere Funktionen deaktiviert wurden und deaktiviert bleiben sollen, müssen Sie diese in der PUT-Anforderung explizit angeben. Um beispielsweise die Funktion „Stammkennwort des Mandanten ändern“ erneut zu aktivieren und die Verwaltungsberechtigung „storageAdmin“ weiterhin zu deaktivieren, senden Sie diese PUT-Anfrage:

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

Kontrollieren Sie den Zugriff auf StorageGRID

Steuern Sie den StorageGRID Zugriff

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

Kontrollieren Sie den Zugriff auf den Grid Manager

Sie legen fest, wer auf den Grid Manager und die Grid Management API zugreifen kann, indem Sie Gruppen und Benutzer aus einem Identitätsföderationsdienst importieren oder lokale Gruppen und lokale Benutzer einrichten.

Verwenden"Identitätsföderation" macht das Einrichten"Gruppen" Und"Benutzer" schneller und ermöglicht Benutzern die Anmeldung bei StorageGRID mit vertrauten Anmeldeinformationen. 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 bestimmen, welche Aufgaben jeder Benutzer ausführen kann, indem Sie ihm unterschiedliche"Berechtigungen" zu jeder Gruppe. Beispielsweise möchten Sie möglicherweise, dass Benutzer einer Gruppe ILM-Regeln verwalten können und Benutzer einer anderen Gruppe Wartungsaufgaben ausführen können. Ein Benutzer muss mindestens einer Gruppe angehören, um auf das System zugreifen zu können.

Optional können Sie eine Gruppe so konfigurieren, dass sie schreibgeschützt ist. Benutzer in einer

schreibgeschützten Gruppe können Einstellungen und Funktionen nur anzeigen. Sie können im Grid Manager oder in der Grid Management API keine Änderungen vornehmen oder Vorgänge ausführen.

Aktivieren der einmaligen Anmeldung

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

Bereitstellungspassphrase ändern

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

Ändern der Knotenkonsolenkennwörter

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

Ändern der Bereitstellungspassphrase

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

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

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

Schritte

1. Wählen Sie **KONFIGURATION** > **Zugriffskontrolle** > **Grid-Passwörter**.
2. Wählen Sie unter **Bereitstellungspassphrase ändern** die Option **Änderung vornehmen** aus.
3. Geben Sie Ihre aktuelle Bereitstellungspassphrase ein.
4. Geben Sie die neue Passphrase ein. Die Passphrase muss mindestens 8 und darf nicht mehr als 32 Zeichen enthalten. Bei Passphrasen wird zwischen Groß- und Kleinschreibung unterschieden.

5. Bewahren Sie die neue Bereitstellungspassphrase an einem sicheren Ort auf. Es wird für Installations-, Erweiterungs- und Wartungsverfahren benötigt.
6. Geben Sie die neue Passphrase erneut ein und wählen Sie **Speichern**.

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

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

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

Ändern der Knotenkonsolenkennwörter

Jeder Knoten in Ihrem Grid verfügt über ein eindeutiges Knotenkonsolenkennwort, das Sie zum Anmelden am Knoten benötigen. Verwenden Sie diese Schritte, um jedes eindeutige Knotenkonsolenkennwort für jeden Knoten in Ihrem Raster zu ändern.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Wartungs- oder Root-Zugriffsberechtigung" .
- Sie verfügen über die aktuelle Bereitstellungspassphrase.

Informationen zu diesem Vorgang

Verwenden Sie das Kennwort der Knotenkonsole, um sich per SSH als „Administrator“ bei einem Knoten oder als Root-Benutzer bei einer VM-/physischen Konsolenverbindung anzumelden. Der Prozess zum Ändern des Knotenkonsolenkennworts erstellt neue Kennwörter für jeden Knoten in Ihrem Raster und speichert die Kennwörter in einer aktualisierten `Passwords.txt` Datei im Wiederherstellungspaket. Die Passwörter sind in der Spalte „Passwort“ in der Datei „Passwords.txt“ aufgeführt.

Für die SSH-Schlüssel, die für die Kommunikation zwischen Knoten verwendet werden, gibt es separate SSH-Zugriffskennwörter. Die SSH-Zugangspasswörter werden durch dieses Verfahren nicht geändert.

Zugriff auf den Assistenten

Schritte

1. Wählen Sie **KONFIGURATION** > **Zugriffskontrolle** > **Grid-Passwörter**.
2. Wählen Sie unter **Passwörter der Knotenkonsole ändern** die Option **Änderung vornehmen** aus.

Geben Sie die Bereitstellungspassphrase ein

Schritte

1. Geben Sie die Bereitstellungspassphrase für Ihr Grid ein.
2. Wählen Sie **Weiter**.

Laden Sie das aktuelle Wiederherstellungspaket herunter

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

Schritte

1. Wählen Sie **Wiederherstellungspaket herunterladen**.
2. Kopieren Sie die Wiederherstellungspaketdatei(`.zip`) an zwei sichere und getrennte Orte.

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

3. Wählen Sie **Weiter**.
4. Wenn das Bestätigungsdialogfeld angezeigt wird, wählen Sie **Ja**, wenn Sie bereit sind, mit der Änderung der Knotenkonsolenkennwörter zu beginnen.

   Sie können diesen Vorgang nach dem Start nicht mehr abbrechen.

Ändern der Knotenkonsolenkennwörter

Wenn der Kennwortprozess der Knotenkonsole startet, wird ein neues Wiederherstellungspaket generiert, das die neuen Kennwörter enthält. Anschließend werden die Passwörter auf jedem Knoten aktualisiert.

Schritte

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

   a. Öffnen Sie die `.zip` Datei.

   b. Bestätigen Sie, dass Sie auf die Inhalte zugreifen können, einschließlich der `Passwords.txt` Datei, die die neuen Passwörter für die Knotenkonsole enthält.

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

      Überschreiben Sie nicht das alte Wiederherstellungspaket.

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

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

   Wenn die Passwörter für alle Knoten geändert werden, wird ein grünes Erfolgsbanner angezeigt. Fahren

Sie mit dem nächsten Schritt fort.

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

Wenn die Kennwortaktualisierung für einen oder mehrere Knoten fehlgeschlagen ist:

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

> ⓘ Durch einen erneuten Versuch werden nur die Knotenkonsolenkennwörter auf den Knoten geändert, bei denen bei vorherigen Kennwortänderungsversuchen ein Fehler aufgetreten ist.

6. Nachdem die Passwörter der Knotenkonsole für alle Knoten geändert wurden, löschen Sie dieerstes Wiederherstellungspaket, das Sie heruntergeladen haben .
7. Verwenden Sie optional den Link **Wiederherstellungspaket**, um eine zusätzliche Kopie des neuen Wiederherstellungspakets herunterzuladen.

SSH-Zugriffskennwörter für Admin-Knoten ändern

Durch das Ändern der SSH-Zugriffskennwörter für Admin-Knoten werden auch die eindeutigen Sätze interner SSH-Schlüssel für jeden Knoten im Raster aktualisiert. Der primäre Admin-Knoten verwendet diese SSH-Schlüssel, um mithilfe einer sicheren, passwortlosen Authentifizierung auf Knoten zuzugreifen.

Verwenden Sie einen SSH-Schlüssel, um sich bei einem Knoten anzumelden als `admin` oder an den Root-Benutzer einer VM oder einer physischen Konsolenverbindung.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Wartungs- oder Root-Zugriffsberechtigung" .
- Sie verfügen über die aktuelle Bereitstellungspassphrase.

Informationen zu diesem Vorgang

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

Für die SSH-Schlüssel, die für die Kommunikation zwischen Knoten verwendet werden, gibt es separate SSH-Zugriffskennwörter. Diese werden durch dieses Verfahren nicht verändert.

Zugriff auf den Assistenten

Schritte

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

2. Wählen Sie unter **SSH-Schlüssel ändern** die Option **Änderung vornehmen**.

Laden Sie das aktuelle Wiederherstellungspaket herunter

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

Schritte

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

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

4. Wählen Sie **Weiter**.
5. Wenn das Bestätigungsdialogfeld angezeigt wird, wählen Sie **Ja**, wenn Sie bereit sind, mit der Änderung der SSH-Zugriffsschlüssel zu beginnen.

   Sie können diesen Vorgang nach dem Start nicht mehr abbrechen.

SSH-Zugriffsschlüssel ändern

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

Schritte

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

   a. Öffnen Sie die `.zip` Datei.

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

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

      Überschreiben Sie nicht das alte Wiederherstellungspaket.

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

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

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

Wenn während des Aktualisierungsvorgangs ein Fehler auftritt, wird in einer Bannermeldung die Anzahl der Knoten aufgelistet, deren Schlüssel nicht geändert werden konnten. Das System wiederholt den Vorgang automatisch auf jedem Knoten, dessen Schlüssel nicht geändert werden konnte. Wenn der Vorgang endet und einige Knoten immer noch keinen geänderten Schlüssel haben, wird die Schaltfläche **Wiederholen** angezeigt.

Wenn die Schlüsselaktualisierung für einen oder mehrere Knoten fehlgeschlagen ist:

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

   Durch einen erneuten Versuch werden nur die SSH-Zugriffsschlüssel auf den Knoten geändert, bei denen bei vorherigen Schlüsseländerungsversuchen ein Fehler aufgetreten ist.

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

Verwenden der Identitätsföderation

Durch die Verwendung der Identitätsföderation wird das Einrichten von Gruppen und Benutzern beschleunigt und Benutzer können sich mit vertrauten Anmeldeinformationen bei StorageGRID anmelden.

Konfigurieren der Identitätsföderation für Grid Manager

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

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .
- Sie verwenden Active Directory, Azure AD, OpenLDAP oder Oracle Directory Server als Identitätsanbieter.

  Wenn Sie einen LDAP v3-Dienst verwenden möchten, der nicht aufgeführt ist, wenden Sie sich an den technischen Support.

- Wenn Sie OpenLDAP verwenden möchten, müssen Sie den OpenLDAP-Server konfigurieren. Sehen Richtlinien zum Konfigurieren eines OpenLDAP-Servers .
- Wenn Sie Single Sign-On (SSO) aktivieren möchten, haben Sie die"Anforderungen und Überlegungen für Single Sign-On" .
- Wenn Sie Transport Layer Security (TLS) für die Kommunikation mit dem LDAP-Server verwenden möchten, verwendet der Identitätsanbieter TLS 1.2 oder 1.3. Sehen "Unterstützte Verschlüsselungen für ausgehende TLS-Verbindungen" .

Informationen zu diesem Vorgang

Sie können eine Identitätsquelle für den Grid Manager konfigurieren, wenn Sie Gruppen aus einem anderen

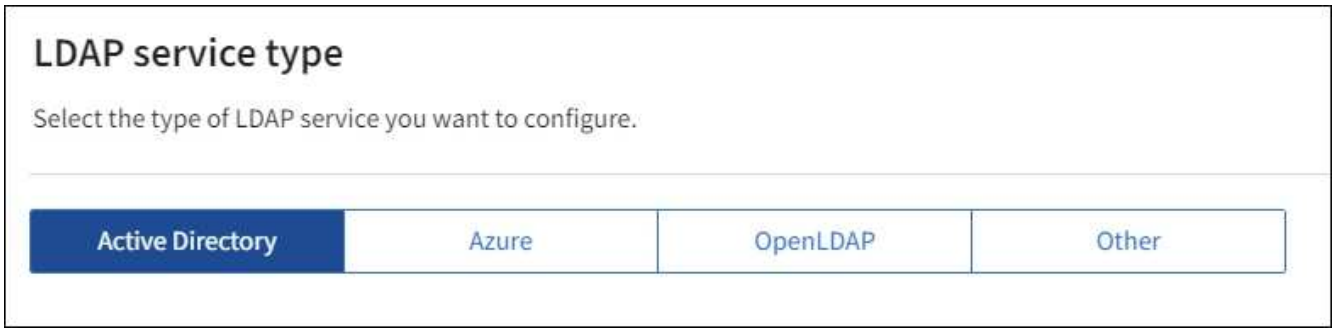
System wie Active Directory, Azure AD, OpenLDAP oder Oracle Directory Server importieren möchten. Sie können die folgenden Gruppentypen importieren:

- Administratorgruppen. Die Benutzer in Administratorgruppen können sich beim Grid Manager anmelden und Aufgaben basierend auf den der Gruppe zugewiesenen Verwaltungsberechtigungen ausführen.
- Mandantenbenutzergruppen für Mandanten, die keine eigene Identitätsquelle verwenden. Benutzer in Mandantengruppen können sich beim Mandantenmanager anmelden und Aufgaben basierend auf den der Gruppe im Mandantenmanager zugewiesenen Berechtigungen ausführen. Sehen"Mieterkonto erstellen" Und"Verwenden eines Mandantenkontos" für Details.

Geben Sie die Konfiguration ein

Schritte

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



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

4. Wenn Sie **Sonstige** ausgewählt haben, füllen Sie die Felder im Abschnitt „LDAP-Attribute“ aus. Andernfalls fahren Sie mit dem nächsten Schritt fort.
   - **Eindeutiger Benutzername**: Der Name des Attributs, das die eindeutige Kennung eines LDAP-Benutzers enthält. Dieses Attribut ist gleichbedeutend mit `sAMAccountName` für Active Directory und `uid` für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `uid` .
   - **Benutzer-UUID**: Der Name des Attributs, das die permanente eindeutige Kennung eines LDAP-Benutzers enthält. Dieses Attribut ist gleichbedeutend mit `objectGUID` für Active Directory und `entryUUID` für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `nsuniqueid` . Der Wert jedes Benutzers für das angegebene Attribut muss eine 32-stellige Hexadezimalzahl im 16-Byte- oder Zeichenfolgenformat sein, wobei Bindestriche ignoriert werden.
   - **Eindeutiger Gruppenname**: Der Name des Attributs, das die eindeutige Kennung einer LDAP-Gruppe enthält. Dieses Attribut ist gleichbedeutend mit `sAMAccountName` für Active Directory und `cn` für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `cn` .
   - **Gruppen-UUID**: Der Name des Attributs, das die permanente eindeutige Kennung einer LDAP-Gruppe enthält. Dieses Attribut ist gleichbedeutend mit `objectGUID` für Active Directory und `entryUUID` für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `nsuniqueid` . Der Wert jeder Gruppe für das angegebene Attribut muss eine 32-stellige Hexadezimalzahl im 16-Byte- oder Zeichenfolgenformat sein, wobei Bindestriche ignoriert werden.
5. Geben Sie für alle LDAP-Diensttypen die erforderlichen LDAP-Server- und

Netzwerkverbindungsinformationen im Abschnitt „LDAP-Server konfigurieren“ ein.

- **Hostname**: Der vollqualifizierte Domänenname (FQDN) oder die IP-Adresse des LDAP-Servers.
- **Port**: Der Port, der für die Verbindung mit dem LDAP-Server verwendet wird.

  > Der Standardport für STARTTLS ist 389 und der Standardport für LDAPS ist 636. Sie können jedoch jeden Port verwenden, solange Ihre Firewall richtig 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 Down-Level-Anmeldenamen oder den Benutzerprinzipalnamen angeben.

  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`
  - **Azurblau**: `accountEnabled` Und `userPrincipalName`

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

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

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

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

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

  > Die Werte für den **Eindeutigen Benutzernamen** müssen innerhalb des **Benutzerbasis-DN**, zu dem sie gehören, eindeutig sein.

- **Bind-Benutzernamenformat** (optional): Das Standardbenutzernamenmuster, das StorageGRID verwenden soll, wenn das Muster nicht automatisch ermittelt werden kann.

  Es wird empfohlen, das **Bind-Benutzernamenformat** anzugeben, da dies Benutzern die Anmeldung ermöglichen kann, wenn StorageGRID keine Bindung mit dem Dienstkonto herstellen kann.

  Geben Sie eines dieser Muster ein:

- **UserPrincipalName-Muster (Active Directory und Azure)**: `[USERNAME]@example.com`
- **Downlevel-Anmeldenamenmuster (Active Directory und Azure)**: `example\[USERNAME]`
- **Muster für eindeutige Namen**: `CN=[USERNAME],CN=Users,DC=example,DC=com`

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

6. Wählen Sie im Abschnitt „Transport Layer Security (TLS)“ eine Sicherheitseinstellung aus.
   - **STARTLS verwenden**: Verwenden Sie STARTTLS, um die Kommunikation mit dem LDAP-Server zu sichern. Dies ist die empfohlene Option für Active Directory, OpenLDAP oder Andere, aber diese Option wird für 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.
   - **TLS nicht verwenden**: Der Netzwerkverkehr zwischen dem StorageGRID -System und dem LDAP-Server wird nicht gesichert. Diese Option wird für Azure nicht unterstützt.

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

7. Wenn Sie STARTTLS oder LDAPS ausgewählt haben, wählen Sie das Zertifikat aus, das zum Sichern der Verbindung verwendet wird.
   - **CA-Zertifikat des Betriebssystems verwenden**: Verwenden Sie das standardmäßig auf dem Betriebssystem installierte 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 und fügen Sie es in das Textfeld „CA-Zertifikat“ ein.

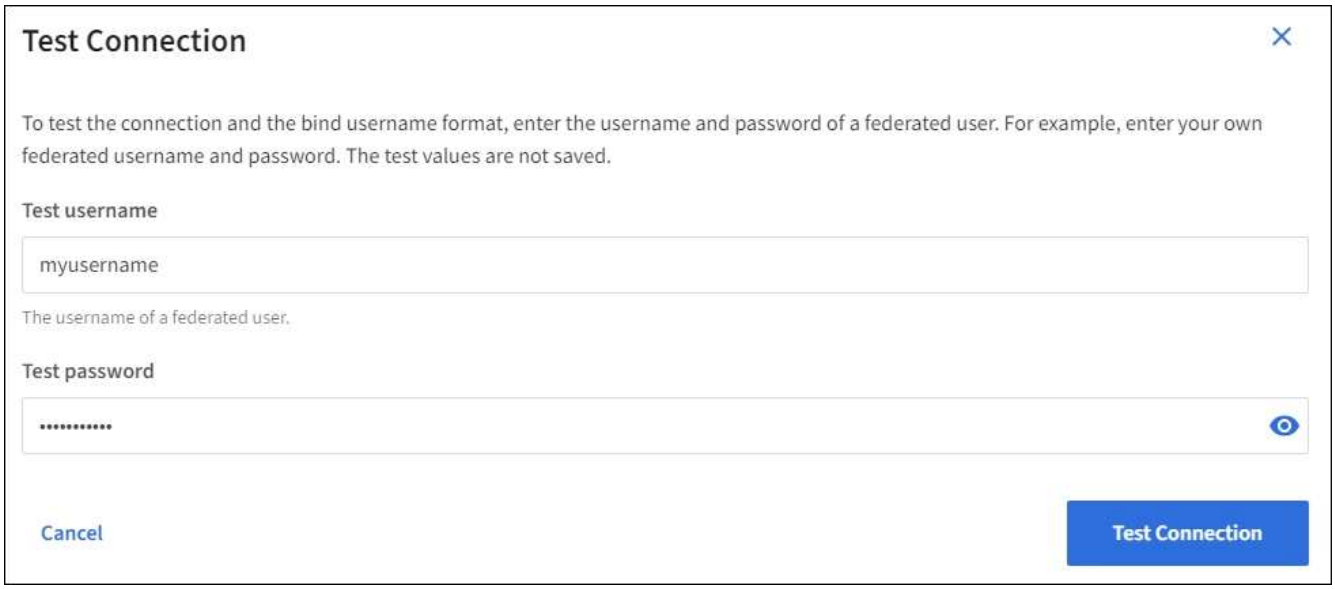
Testen Sie die Verbindung und speichern Sie die Konfiguration

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-Benutzernamenformat, falls Sie eines angegeben haben.

Schritte

1. Wählen Sie **Verbindung testen**.
2. Wenn Sie kein Bind-Benutzernamenformat angegeben haben:
   - Bei gültigen Verbindungseinstellungen wird die Meldung „Verbindungstest erfolgreich“ angezeigt. Wählen Sie **Speichern**, um die Konfiguration zu speichern.
   - Bei ungültigen Verbindungseinstellungen erscheint die Meldung „Testverbindung konnte nicht hergestellt werden“. Wählen Sie **Schließen**. Beheben Sie dann alle Probleme und testen Sie die Verbindung erneut.
3. Wenn Sie ein Bind-Benutzernamenformat angegeben haben, geben Sie den Benutzernamen und das Kennwort eines gültigen Verbundbenutzers ein.

   Geben Sie beispielsweise Ihren eigenen Benutzernamen und Ihr eigenes Passwort ein. Verwenden Sie im Benutzernamen keine Sonderzeichen wie @ oder /.



- Bei gültigen Verbindungseinstellungen wird die Meldung „Verbindungstest erfolgreich“ angezeigt. Wählen Sie **Speichern**, um die Konfiguration zu speichern.
- Wenn die Verbindungseinstellungen, das Bind-Benutzernamenformat oder der Testbenutzername und das Testkennwort ungültig sind, wird eine Fehlermeldung angezeigt. Beheben Sie alle Probleme und testen Sie die Verbindung erneut.

Erzwingen der Synchronisierung mit der Identitätsquelle

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

Schritte

1. Gehen Sie zur Seite „Identitätsföderation“.
2. Wählen Sie oben auf der Seite **Sync-Server** aus.

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

   Die Warnung **Fehler bei der Synchronisierung der Identitätsföderation** wird ausgelöst, wenn beim Synchronisieren föderierter Gruppen und Benutzer aus der Identitätsquelle ein Problem auftritt.

Identitätsföderation deaktivieren

Sie können die Identitätsföderation für Gruppen und Benutzer vorübergehend oder dauerhaft deaktivieren. Wenn die Identitätsföderation deaktiviert ist, findet keine Kommunikation zwischen StorageGRID und der Identitätsquelle statt. Alle von Ihnen konfigurierten Einstellungen bleiben jedoch erhalten, sodass Sie die Identitätsföderation in Zukunft problemlos wieder aktivieren können.

Informationen zu diesem Vorgang

Bevor Sie die Identitätsföderation deaktivieren, sollten Sie Folgendes beachten:

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

Sitzung abläuft, können sich nach Ablauf ihrer Sitzung jedoch nicht mehr anmelden.

- Es findet keine Synchronisierung zwischen dem StorageGRID -System und der Identitätsquelle statt und es werden keine Warnungen für Konten ausgelöst, die nicht synchronisiert wurden.
- Das Kontrollkästchen **Identitätsföderation aktivieren** ist deaktiviert, wenn Single Sign-On (SSO) auf **Aktiviert** oder **Sandbox-Modus** eingestellt ist. Der SSO-Status auf der Single Sign-On-Seite muss **Deaktiviert** sein, bevor Sie die Identitätsföderation deaktivieren können. Sehen "Deaktivieren der einmaligen Anmeldung" .

Schritte

1. Gehen Sie zur Seite „Identitätsföderation“.
2. Deaktivieren Sie das Kontrollkästchen **Identitätsföderation aktivieren**.

Richtlinien zum Konfigurieren 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 für extern deaktivierte Benutzer nicht automatisch. Um den S3-Zugriff zu blockieren, löschen Sie alle S3-Schlüssel für den Benutzer oder entfernen Sie den Benutzer aus allen Gruppen.

Memberof- und Refint-Overlays

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

Indizierung

Sie müssen die folgenden OpenLDAP-Attribute mit den angegebenen Indexschlüsselwörtern 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.

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

Verwalten von Administratorgruppen

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

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .
- Wenn Sie eine föderierte Gruppe importieren möchten, haben Sie die Identitätsföderation konfiguriert und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.

Erstellen einer Administratorgruppe

Mithilfe von Administratorgruppen können Sie festlegen, welche Benutzer auf welche Funktionen und Vorgänge im Grid Manager und der Grid Management API zugreifen können.

Zugriff auf den Assistenten

Schritte

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

Wählen Sie einen Gruppentyp

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** aus.
2. Geben Sie einen Anzeigenamen für die Gruppe ein, den Sie später bei Bedarf aktualisieren können. Beispielsweise „Wartungsbenutzer“ oder „ILM-Administratoren“.
3. Geben Sie einen eindeutigen Namen für die Gruppe ein, den Sie später nicht mehr ändern können.
4. Wählen Sie **Weiter**.

Föderierte Gruppe

Schritte

1. Wählen Sie **Verbundgruppe** aus.
2. Geben Sie den Namen der Gruppe, die Sie importieren möchten, genau so ein, wie er in der konfigurierten Identitätsquelle angezeigt wird.
   - Verwenden Sie für Active Directory und Azure den sAMAccountName.
   - Verwenden Sie für OpenLDAP den CN (Common Name).
   - Verwenden Sie für ein anderes LDAP den entsprechenden eindeutigen Namen für den LDAP-Server.
3. Wählen Sie **Weiter**.

Gruppenberechtigungen verwalten

Schritte

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

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

2. Wählen Sie eine oder mehrere"Berechtigungen der Administratorgruppe" .

   Sie müssen jeder Gruppe mindestens eine Berechtigung zuweisen, da sich die Benutzer der Gruppe sonst nicht bei StorageGRID anmelden können.

3. Wenn Sie eine lokale Gruppe erstellen, wählen Sie **Weiter**. Wenn Sie eine föderierte Gruppe erstellen, wählen Sie **Gruppe erstellen** und **Fertig**.

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. Sehen"Benutzer verwalten" für Details.

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

Anzeigen und Bearbeiten von Administratorgruppen

Sie können Details zu vorhandenen Gruppen anzeigen, eine Gruppe ändern oder eine Gruppe duplizieren.

- Um grundlegende Informationen zu allen Gruppen anzuzeigen, sehen Sie sich die Tabelle auf der Seite „Gruppen“ an.
- 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
Gruppendetails anzeigen	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
Anzeigenamen bearbeiten (nur lokale Gruppen)	a. Aktivieren Sie das Kontrollkästchen für die Gruppe. b. Wählen Sie **Aktionen** > **Gruppennamen 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. Optional können Sie auswählen oder löschen"Berechtigungen der Administratorgruppe" . e. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Gruppennamen aus, um die Details anzuzeigen. b. Ändern Sie optional den Zugriffsmodus der Gruppe. c. Optional können Sie auswählen oder löschen"Berechtigungen der Administratorgruppe" . 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 zum Duplizieren von Gruppen ab.

Löschen einer Gruppe

Sie können eine Administratorgruppe löschen, wenn Sie die Gruppe aus dem System entfernen möchten, und alle mit der Gruppe verknüpften Berechtigungen entfernen. Durch das Löschen einer Administratorgruppe werden alle Benutzer aus der Gruppe entfernt, die Benutzer selbst werden 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 der Administratorgruppe

Beim Erstellen von Administratorbenutzergruppen wählen Sie eine oder mehrere Berechtigungen aus, um den Zugriff auf bestimmte Funktionen des Grid Managers zu steuern. Sie können dann jeden Benutzer einer oder mehreren dieser Administratorgruppen zuweisen, um festzulegen, welche Aufgaben der Benutzer ausführen kann.

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

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

- Sign in
- Dashboard anzeigen
- Anzeigen der Knotenseiten
- Aktuelle und gelöste Warnmeldungen anzeigen
- Das eigene Passwort ändern (nur lokale Benutzer)
- Zeigen Sie bestimmte Informationen auf den Konfigurations- und Wartungsseiten an

Interaktion zwischen Berechtigungen und Zugriffsmodus

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

In den folgenden Abschnitten werden die Berechtigungen beschrieben, die Sie beim Erstellen oder Bearbeiten einer Administratorgruppe zuweisen können. Für alle nicht ausdrücklich genannten Funktionen ist die Berechtigung **Root-Zugriff** erforderlich.

Root-Zugriff

Diese Berechtigung bietet Zugriff auf alle Grid-Verwaltungsfunktionen.

Ändern des Root-Passworts des Mandanten

Diese Berechtigung bietet Zugriff auf die Option **Root-Passwort ändern** auf der Seite „Mandanten“, sodass Sie steuern können, wer das Passwort für den lokalen Root-Benutzer des Mandanten ändern kann. Diese Berechtigung wird auch zum Migrieren von S3-Schlüsseln verwendet, wenn die Funktion zum Importieren von S3-Schlüsseln aktiviert ist. Benutzer ohne diese Berechtigung können die Option **Root-Passwort ändern** nicht sehen.

> Um Zugriff auf die Seite „Mandanten“ zu gewähren, die die Option „Root-Passwort ändern“ enthält, weisen Sie auch die Berechtigung „Mandantenkonten“ zu.

Konfiguration der Grid-Topologieseite

Diese Berechtigung bietet Zugriff auf die Konfigurationsregisterkarten auf der Seite **SUPPORT** > **Tools** > **Grid-Topologie**.

> Die Seite „Grid-Topologie“ ist veraltet und wird in einer zukünftigen Version entfernt.

ILM

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

- Regeln
- Richtlinien
- Richtlinien-Tags
- Speicherpools
- Lagerqualitäten
- Regionen
- Objektmetadatensuche

Benutzer müssen über die Berechtigungen **Andere Rasterkonfiguration** und **Rastertopologieseitenkonfiguration** verfügen, um Speicherklassen verwalten zu können.

Wartung

Benutzer müssen über die Berechtigung „Wartung“ verfügen, um diese Optionen verwenden zu können:

- **KONFIGURATION** > **Zugriffskontrolle**:
  - Grid-Passwörter
- **KONFIGURATION** > **Netzwerk**:
  - S3-Endpunktdomänennamen
- **WARTUNG** > **Aufgaben**:
  - Außerbetriebnahme
  - Erweiterung
  - Objektexistenzprüfung
  - Erholung
- **WARTUNG** > **System**:
  - Wiederherstellungspaket
  - Software-Update
- **SUPPORT** > **Tools**:
  - Protokolle

Benutzer ohne Wartungsberechtigung können die folgenden Seiten anzeigen, aber nicht bearbeiten:

- **WARTUNG** > **Netzwerk**:
  - DNS-Server
  - Netznetzwerk
  - NTP-Server
- **WARTUNG** > **System**:
  - Lizenz
- **KONFIGURATION** > **Netzwerk**:
  - S3-Endpunktdomänennamen
- **KONFIGURATION** > **Sicherheit**:

    - Zertifikate
- **KONFIGURATION** > **Überwachung**:
    - Audit- und Syslog-Server

Verwalten von Warnungen

Diese Berechtigung bietet Zugriff auf Optionen zum Verwalten von Warnungen. Benutzer müssen über diese Berechtigung verfügen, um Stummschaltungen, Warnbenachrichtigungen und Warnregeln zu verwalten.

Metrikabfrage

Diese Berechtigung bietet Zugriff auf:

- **SUPPORT** > **Tools** > **Metriken**-Seite
- Benutzerdefinierte Prometheus-Metrikabfragen mithilfe des Abschnitts **Metriken** der Grid Management API
- Grid Manager-Dashboardkarten mit Metriken

Objektmetadatensuche

Diese Berechtigung bietet Zugriff auf die Seite **ILM** > **Objektmetadatensuche**.

Andere Netzkonfiguration

Diese Berechtigung bietet Zugriff auf zusätzliche Rasterkonfigurationsoptionen.

> Um diese zusätzlichen Optionen anzuzeigen, müssen Benutzer auch über die Berechtigung **Konfiguration der Grid-Topologieseite** verfügen.

- **ILM**:
    - Lagerqualitäten
- **KONFIGURATION** > **System**:
- **SUPPORT** > **Sonstiges**:
    - Linkkosten

Speichergeräteadministrator

Diese Berechtigung bietet:

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

Mandantenkonten

Diese Berechtigung bietet die Möglichkeit:

- Greifen Sie auf die Seite „Mandanten“ zu, auf der Sie Mandantenkonten erstellen, bearbeiten und entfernen können.
- Vorhandene Richtlinien zur Verkehrsklassifizierung anzeigen

- Zeigen Sie Grid Manager-Dashboardkarten an, die Mieterdetails enthalten

Benutzer verwalten

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

Bevor Sie beginnen

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

Erstellen eines lokalen Benutzers

Sie können einen oder mehrere lokale Benutzer erstellen und jeden 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 föderierte Benutzer und Gruppen zu verwalten.

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

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

Zugriff auf den Assistenten

Schritte

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

Benutzeranmeldeinformationen eingeben

Schritte

1. Geben Sie den vollständigen Namen des Benutzers, einen eindeutigen Benutzernamen und ein Passwort 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. Optional können Sie den Benutzer einer oder mehreren Gruppen zuweisen, um die Berechtigungen des Benutzers festzulegen.

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

Wenn ein Benutzer mehreren Gruppen angehört, sind die Berechtigungen kumulativ. Sehen"Verwalten von Administratorgruppen" für Details.

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

Anzeigen und Bearbeiten lokaler Benutzer

Sie können Details zu vorhandenen lokalen und föderierten Benutzern anzeigen. Sie können einen lokalen Benutzer ändern, um den vollständigen Namen, das Kennwort oder die Gruppenmitgliedschaft des Benutzers zu ändern. Sie können einem Benutzer auch vorübergehend den Zugriff auf den Grid Manager und die Grid Management API verweigern.

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

- Um grundlegende Informationen zu allen lokalen und föderierten Benutzern anzuzeigen, sehen Sie sich die Tabelle auf der Seite „Benutzer“ an.
- Um alle Details für einen bestimmten Benutzer anzuzeigen, einen lokalen Benutzer zu bearbeiten oder das Kennwort eines lokalen Benutzers zu ändern, verwenden Sie das Menü **Aktionen** oder die Detailseite.

  Alle Änderungen werden angewendet, wenn sich der Benutzer das nächste Mal abmeldet und sich dann wieder beim Grid Manager anmeldet.

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

Aufgabe	Menü „Aktionen“	Detailseite
Benutzerdetails anzeigen	a. Aktivieren Sie das Kontrollkästchen für den Benutzer. b. Wählen Sie **Aktionen** > **Benutzerdetails anzeigen**.	Wählen Sie den Namen des Benutzers 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 Namen des Benutzers 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**, um zu verhindern, dass sich der Benutzer beim Grid Manager oder der Grid Management API anmeldet, oder wählen Sie **Nein**, um dem Benutzer die Anmeldung zu ermöglichen. e. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Namen des Benutzers aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte „Zugriff“ aus. c. Wählen Sie **Ja**, um zu verhindern, dass sich der Benutzer beim Grid Manager oder der Grid Management API anmeldet, oder wählen Sie **Nein**, um dem Benutzer die Anmeldung zu ermöglichen. 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 „Passwort“. d. Geben Sie ein neues Passwort ein. e. Wählen Sie **Passwort ändern**.	a. Wählen Sie den Namen des Benutzers aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte „Passwort“. 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 einem neuen Browser-Tab anzuzeigen. e. Wählen Sie **Gruppen bearbeiten**, um andere Gruppen auszuwählen. f. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Namen des Benutzers 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 einem neuen Browser-Tab anzuzeigen. d. Wählen Sie **Gruppen bearbeiten**, um andere 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 zum Duplizieren von Benutzern ab.

Löschen eines Benutzers

Sie können einen lokalen Benutzer löschen, um ihn 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**.

Verwenden Sie Single Sign-On (SSO).

Konfigurieren der einmaligen Anmeldung

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

So funktioniert Single Sign-On

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

Bevor Sie Single Sign-On (SSO) aktivieren, prüfen Sie, wie sich die Aktivierung von SSO auf die Anmelde- und Abmeldeprozesse von StorageGRID auswirkt.

Sign in, wenn SSO aktiviert ist

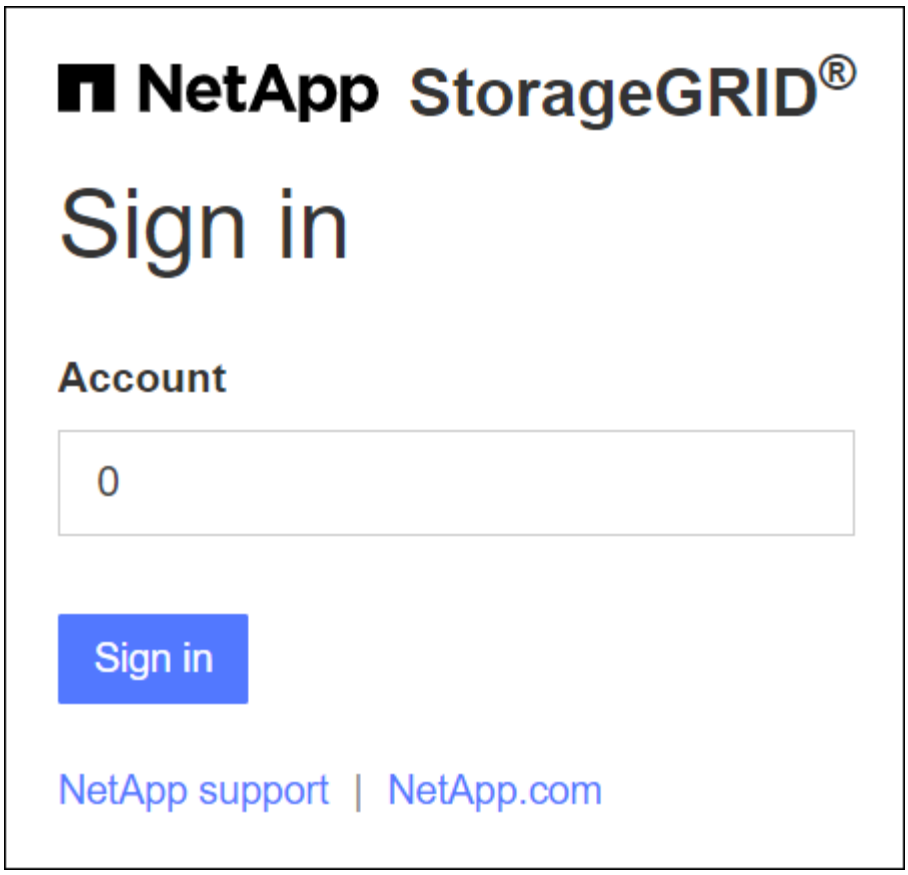
Wenn SSO aktiviert ist und Sie sich bei StorageGRID anmelden, werden Sie zur Validierung Ihrer Anmeldeinformationen auf die SSO-Seite Ihrer Organisation weitergeleitet.

Schritte

1. Geben Sie den vollqualifizierten Domänennamen oder die IP-Adresse eines beliebigen StorageGRID Admin-Knotens in einen Webbrowser ein.

   Die StorageGRID Sign in wird angezeigt.

   - Wenn Sie die URL zum ersten Mal in diesem Browser aufrufen, werden Sie zur Eingabe einer Konto-ID aufgefordert:

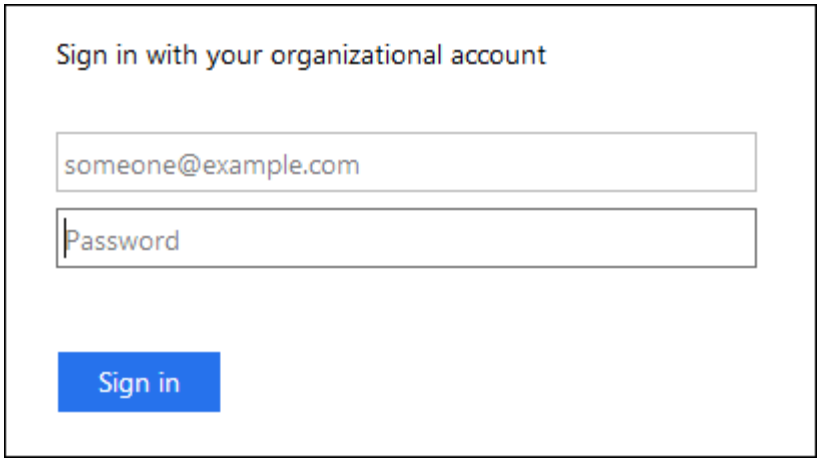


- Wenn Sie zuvor entweder auf den Grid Manager oder den Tenant Manager zugegriffen haben, werden Sie aufgefordert, ein aktuelles Konto auszuwählen oder eine Konto-ID einzugeben:

> Die StorageGRID Sign in wird nicht angezeigt, wenn Sie die vollständige URL für ein Mandantenkonto eingeben (d. h. einen vollqualifizierten Domänennamen oder eine IP-Adresse gefolgt von `/?accountId=20-digit-account-id`). Stattdessen werden Sie sofort auf die SSO-Anmeldeseite Ihrer Organisation weitergeleitet, wo SieMelden Sie sich mit Ihren SSO-Anmeldeinformationen 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 dieser 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 dieser in der Liste der letzten Konten angezeigt wird.
3. Wählen Sie * Sign in*

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



4. Sign in .

   Wenn Ihre SSO-Anmeldeinformationen korrekt sind:

   a. Der Identitätsanbieter (IdP) stellt StorageGRID eine Authentifizierungsantwort bereit.
   b. StorageGRID validiert die Authentifizierungsantwort.
   c. Wenn die Antwort gültig ist und Sie zu einer föderierten Gruppe mit StorageGRID Zugriffsberechtigungen gehören, werden Sie beim Grid Manager oder beim Tenant Manager angemeldet, je nachdem, welches Konto Sie ausgewählt haben.

   > Wenn auf das Dienstkonto nicht zugegriffen werden kann, können Sie sich trotzdem anmelden, solange Sie ein bestehender Benutzer sind, der zu einer föderierten Gruppe mit StorageGRID Zugriffsberechtigungen gehört.

5. Greifen Sie optional auf andere Admin-Knoten zu oder greifen Sie auf den Grid Manager oder den Tenant Manager zu, wenn Sie über die entsprechenden Berechtigungen verfügen.

   Sie müssen Ihre SSO-Anmeldeinformationen nicht erneut eingeben.

Abmelden, wenn SSO aktiviert ist

Wenn SSO für StorageGRID aktiviert ist, hängt das Geschehen beim Abmelden davon ab, bei was Sie angemeldet sind und von wo aus Sie sich abmelden.

Schritte

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

   Die StorageGRID Sign in wird angezeigt. Das Dropdown-Menü **Letzte Konten** wurde aktualisiert und enthält jetzt **Grid Manager** oder den Namen des Mandanten, sodass Sie in Zukunft schneller auf diese Benutzeroberflächen zugreifen können.

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

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

Anforderungen und Überlegungen zur einmaligen Anmeldung

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

Anforderungen an den Identitätsanbieter

StorageGRID unterstützt die folgenden SSO-Identitätsanbieter (IdP):

- Active Directory-Verbunddienst (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-Dienstes, den Sie für die Identitätsföderation verwenden, steuert, welche Art von SSO Sie implementieren können.

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

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 die "Update KB3201845" oder höher.

Zusätzliche 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 Benutzerprinzipalnamen verfügen, die nicht sAMAccountName als Präfix verwenden, können Anmeldeprobleme auftreten, wenn StorageGRID die Verbindung zum LDAP-Server verliert. Um Benutzern die Anmeldung zu ermöglichen, müssen Sie die Verbindung zum LDAP-Server wiederherstellen.

Serverzertifikatanforderungen

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

Wenn Sie dies noch nicht getan haben"ein benutzerdefiniertes Zertifikat für die Verwaltungsschnittstelle konfiguriert" , sollten Sie dies jetzt tun. Wenn Sie ein benutzerdefiniertes Serverzertifikat installieren, wird es für alle Admin-Knoten verwendet und Sie können es in allen StorageGRID -Vertrauensstellungen, Unternehmensanwendungen oder SP Verbindungen verwenden.

> Die Verwendung des Standardserverzertifikats eines Admin-Knotens in einer Vertrauensstellung der vertrauenden Partei, einer Unternehmensanwendung oder einer SP Verbindung wird nicht empfohlen. Wenn der Knoten ausfällt und Sie ihn wiederherstellen, wird ein neues Standardserverzertifikat generiert. Bevor Sie sich beim wiederhergestellten Knoten anmelden können, müssen Sie die Vertrauensstellung der vertrauenden Seite, die Unternehmensanwendung oder die SP Verbindung mit dem neuen Zertifikat aktualisieren.

Sie können auf das Serverzertifikat eines Admin-Knotens zugreifen, indem Sie sich bei der Befehlsshell des Knotens anmelden und zu `/var/local/mgmt-api` Verzeichnis. Ein benutzerdefiniertes Serverzertifikat heißt `custom-server.crt` . Das Standardserverzertifikat des Knotens heißt `server.crt` .

Portanforderungen

Single Sign-On (SSO) ist auf den eingeschränkten Grid Manager- oder Tenant Manager-Ports nicht verfügbar. Sie müssen den Standard-HTTPS-Port (443) verwenden, wenn Sie möchten, dass sich Benutzer per Single Sign-On authentifizieren. Sehen "Zugriffskontrolle an externer Firewall" .

Bestätigen, dass sich Verbundbenutzer anmelden können

Bevor Sie Single Sign-On (SSO) aktivieren, müssen Sie bestätigen, dass sich mindestens ein Verbundbenutzer beim Grid Manager und beim Tenant Manager für alle vorhandenen Tenant-Konten anmelden kann.

Bevor Sie beginnen

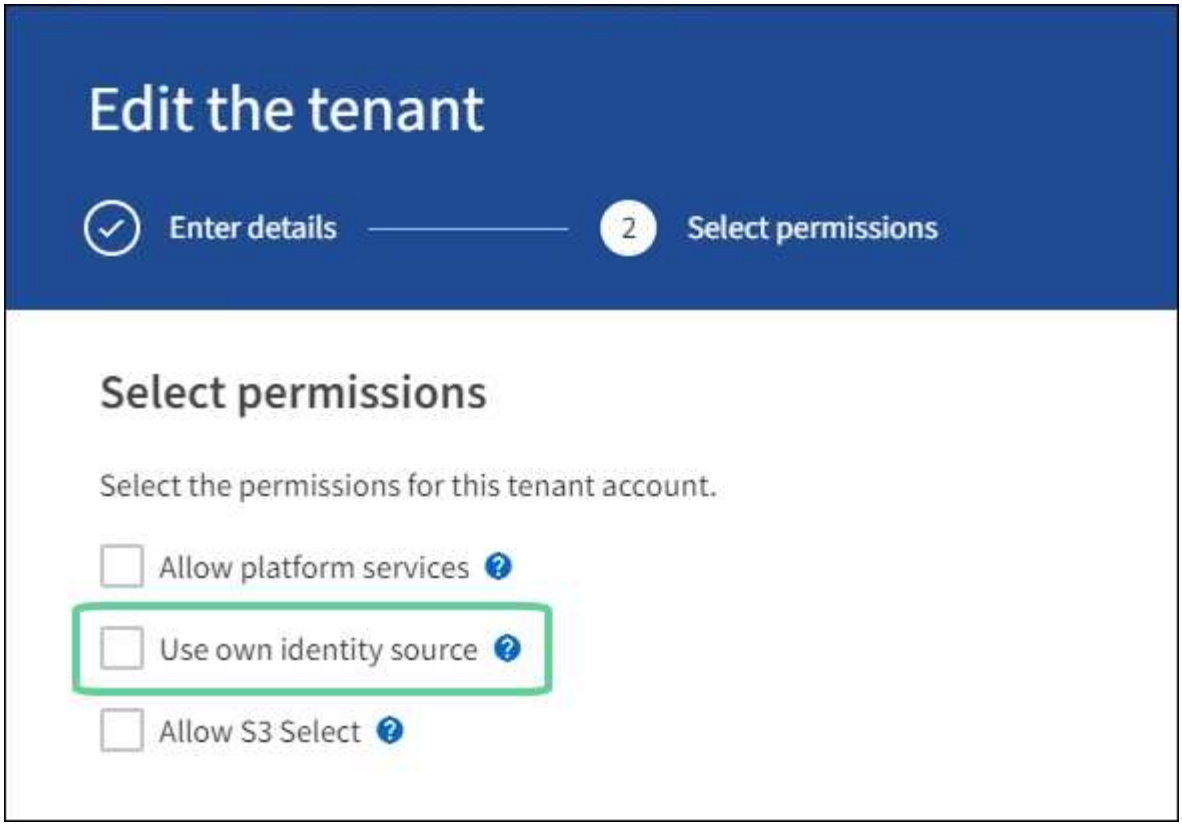
- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .
- Sie haben die Identitätsföderation bereits konfiguriert.

Schritte

1. Wenn bereits Mandantenkonten vorhanden sind, vergewissern Sie sich, dass keiner der Mandanten eine eigene Identitätsquelle verwendet.

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

   a. Sign in .
   b. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Identitätsföderation**.
   c. Vergewissern Sie sich, dass das Kontrollkästchen **Identitätsföderation aktivieren** nicht aktiviert ist.
   d. Wenn dies der Fall ist, bestätigen Sie, dass alle möglicherweise für dieses Mandantenkonto verwendeten Verbundgruppen nicht mehr benötigt werden, deaktivieren Sie das Kontrollkästchen und wählen Sie **Speichern**.
2. Bestätigen Sie, dass ein Verbundbenutzer auf den Grid Manager zugreifen kann:
   a. Wählen Sie im Grid Manager **KONFIGURATION** > **Zugriffskontrolle** > **Admin-Gruppen**.
   b. Stellen Sie sicher, dass mindestens eine Verbundgruppe aus der Active Directory-Identitätsquelle importiert wurde und dass ihr die Root-Zugriffsberechtigung zugewiesen wurde.
   c. Abmelden.
   d. Bestätigen Sie, dass Sie sich als Benutzer der Verbundgruppe erneut beim Grid Manager anmelden können.
3. Wenn vorhandene Mandantenkonten vorhanden sind, bestätigen Sie, dass sich ein Verbundbenutzer mit Root-Zugriffsberechtigung anmelden kann:
   a. Wählen Sie im Grid Manager **MIETER** aus.
   b. Wählen Sie das Mandantenkonto aus und wählen Sie **Aktionen** > **Bearbeiten**.
   c. Wählen Sie auf der Registerkarte „Details eingeben“ die Option „Weiter“ aus.
   d. Wenn das Kontrollkästchen **Eigene Identitätsquelle verwenden** aktiviert ist, deaktivieren Sie das Kontrollkästchen und wählen Sie **Speichern**.



Die Mandantenseite wird angezeigt.

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

b. Wählen Sie im Mandanten-Manager **ZUGRIFFSVERWALTUNG** > **Gruppen**.

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

d. Abmelden.

e. Bestätigen Sie, dass Sie sich als Benutzer der Verbundgruppe erneut beim Mandanten anmelden können.

Ähnliche Informationen

- "Anforderungen und Überlegungen zur einmaligen Anmeldung"
- "Verwalten von Administratorgruppen"
- "Verwenden eines Mandantenkontos"

Sandbox-Modus verwenden

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 in den Sandbox-Modus zurückkehren, wenn Sie die Konfiguration ändern oder erneut testen müssen.

Bevor Sie beginnen

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

- Sie haben die"Root-Zugriffsberechtigung" .
- Sie haben die Identitätsföderation für Ihr StorageGRID -System konfiguriert.
- Für den **LDAP-Diensttyp** der Identitätsföderation haben Sie je nach dem SSO-Identitätsanbieter, den Sie verwenden möchten, entweder Active Directory oder Azure ausgewählt.

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

Informationen zu diesem Vorgang

Wenn SSO aktiviert ist und ein Benutzer versucht, sich bei einem Admin-Knoten anzumelden, sendet StorageGRID eine Authentifizierungsanforderung an den SSO-Identitätsanbieter. Im Gegenzug sendet der SSO-Identitätsanbieter eine Authentifizierungsantwort zurück an StorageGRID, die angibt, ob die Authentifizierungsanforderung erfolgreich war. Für erfolgreiche Anfragen:

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

Damit StorageGRID (der Dienstanbieter) und der SSO-Identitätsanbieter 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-Knoten eine Vertrauensstellung der vertrauenden Seite (AD FS), eine Unternehmensanwendung (Azure) oder einen Dienstanbieter (PingFederate) zu erstellen. Abschließend müssen Sie zu StorageGRID zurückkehren, um SSO zu aktivieren.

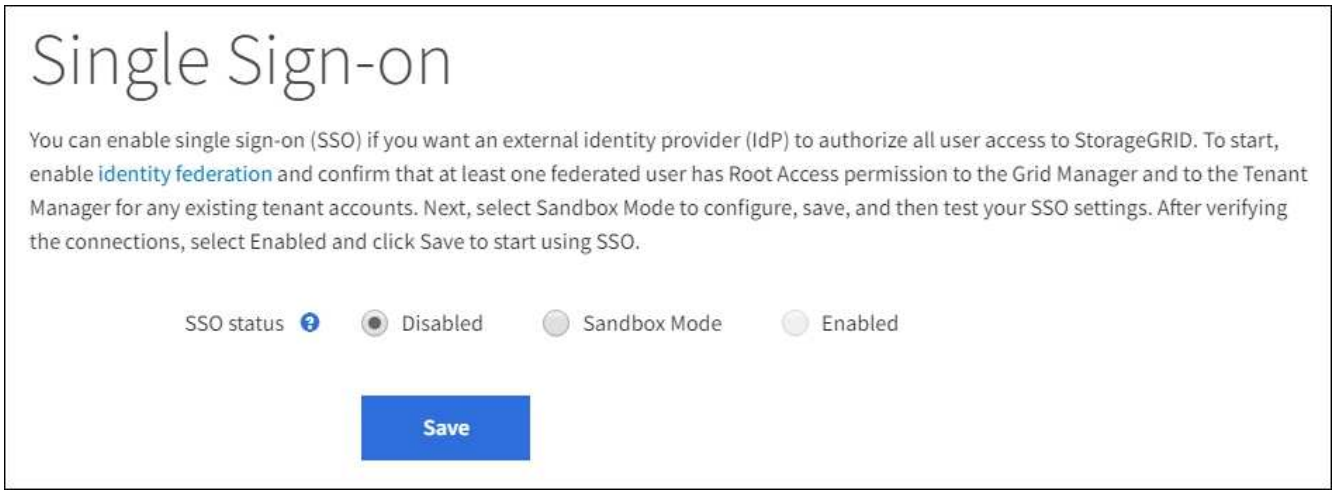
Der Sandbox-Modus erleichtert die Durchführung dieser Hin- und Her-Konfiguration und das Testen aller Ihrer Einstellungen, bevor Sie SSO aktivieren. Wenn Sie den Sandbox-Modus verwenden, können sich Benutzer nicht per SSO anmelden.

Zugriff auf den Sandbox-Modus

Schritte

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

   Die Seite „Single Sign-On“ wird mit der ausgewählten Option **Deaktiviert** angezeigt.



Wenn die SSO-Statusoptionen nicht angezeigt werden, bestätigen Sie, dass Sie den Identitätsanbieter als Verbundidentitätsquelle konfiguriert haben. Sehen "Anforderungen und Überlegungen zur einmaligen Anmeldung" .

2. Wählen Sie **Sandbox-Modus**.

   Der Abschnitt „Identitätsanbieter“ wird angezeigt.

Geben Sie die Details des Identitätsanbieters ein

Schritte

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

Active Directory

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

> Um den Namen des Verbunddienstes zu finden, gehen Sie zum Windows Server-Manager. Wählen Sie **Tools** > **AD FS-Verwaltung**. Wählen Sie im Aktionsmenü **Eigenschaften des Verbunddienstes bearbeiten** aus. Der Name des Verbunddienstes wird im zweiten Feld angezeigt.

b. Geben Sie an, welches TLS-Zertifikat zum Sichern der Verbindung verwendet wird, wenn der Identitätsanbieter als Antwort auf StorageGRID -Anfragen SSO-Konfigurationsinformationen sendet.

- **CA-Zertifikat des Betriebssystems verwenden**: 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.

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

> Wenn Sie das CA-Zertifikat ändern, sofort"Starten Sie den mgmt-api-Dienst auf den Admin-Knoten neu" und testen Sie, ob eine erfolgreiche einmalige Anmeldung beim Grid Manager erfolgt.

c. Geben Sie im Abschnitt „Relying Party“ die **Relying Party-Kennung** für StorageGRID an. Dieser Wert steuert den Namen, den Sie für jede Vertrauensstellung der vertrauenden Seite in AD FS verwenden.

- Wenn Ihr Grid beispielsweise nur einen Admin-Knoten hat und Sie nicht beabsichtigen, in Zukunft weitere Admin-Knoten hinzuzufügen, geben Sie `SG` oder `StorageGRID` .
- Wenn Ihr Raster mehr als einen Admin-Knoten enthält, fügen Sie die Zeichenfolge ein `[HOSTNAME]` im Bezeichner. Beispiel: `SG-[HOSTNAME]` . Dadurch wird eine Tabelle generiert, die die Kennung der vertrauenden Partei für jeden Admin-Knoten in Ihrem System basierend auf dem Hostnamen des Knotens anzeigt.

> Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID -System eine Vertrauensstellung der vertrauenden Partei erstellen. Durch die Einrichtung einer Vertrauensstellung der vertrauenden Partei für jeden Admin-Knoten wird sichergestellt, dass sich Benutzer sicher bei jedem Admin-Knoten an- und abmelden können.

d. Wählen Sie **Speichern**.

Auf der Schaltfläche **Speichern** wird für einige Sekunden ein grünes Häkchen angezeigt.

Azurblau

a. Geben Sie an, welches TLS-Zertifikat zum Sichern der Verbindung verwendet wird, wenn der Identitätsanbieter als Antwort auf StorageGRID -Anfragen SSO-Konfigurationsinformationen sendet.

   - **CA-Zertifikat des Betriebssystems verwenden**: 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.

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

   > Wenn Sie das CA-Zertifikat ändern, sofort"Starten Sie den mgmt-api-Dienst auf den Admin-Knoten neu" und testen Sie, ob eine erfolgreiche einmalige Anmeldung beim Grid Manager erfolgt.

b. Geben Sie im Abschnitt „Unternehmensanwendung“ den **Namen der Unternehmensanwendung** für StorageGRID an. Dieser Wert steuert den Namen, den Sie für jede Unternehmensanwendung in Azure AD verwenden.

   - Wenn Ihr Grid beispielsweise nur einen Admin-Knoten hat und Sie nicht beabsichtigen, in Zukunft weitere Admin-Knoten hinzuzufügen, geben Sie `SG` oder `StorageGRID`.
   - Wenn Ihr Raster mehr als einen Admin-Knoten enthält, fügen Sie die Zeichenfolge ein `[HOSTNAME]` im Bezeichner. Beispiel: `SG-[HOSTNAME]` . Dadurch wird eine Tabelle generiert, die basierend auf dem Hostnamen des Knotens einen Unternehmensanwendungsnamen für jeden Admin-Knoten in Ihrem System anzeigt.

   > Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID System eine Unternehmensanwendung erstellen. Durch die Bereitstellung einer Unternehmensanwendung für jeden Admin-Knoten wird sichergestellt, dass sich Benutzer sicher bei jedem Admin-Knoten anmelden und abmelden können.

c. Befolgen Sie die Schritte in"Erstellen von Unternehmensanwendungen in Azure AD" um für jeden in der Tabelle aufgeführten Admin-Knoten eine Unternehmensanwendung zu erstellen.

d. Kopieren Sie aus Azure AD die URL der Verbundmetadaten für jede Unternehmensanwendung. Fügen Sie diese URL dann in das entsprechende Feld **Federation metadata URL** in StorageGRID ein.

e. Nachdem Sie eine Föderationsmetadaten-URL für alle Admin-Knoten kopiert und eingefügt haben, wählen Sie **Speichern**.

   Auf der Schaltfläche **Speichern** wird für einige Sekunden ein grünes Häkchen angezeigt.

PingFederate

a. Geben Sie an, welches TLS-Zertifikat zum Sichern der Verbindung verwendet wird, wenn der Identitätsanbieter als Antwort auf StorageGRID -Anfragen SSO-Konfigurationsinformationen

sendet.

- **CA-Zertifikat des Betriebssystems verwenden**: 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.

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

> Wenn Sie das CA-Zertifikat ändern, sofort"Starten Sie den mgmt-api-Dienst auf den Admin-Knoten neu" und testen Sie, ob eine erfolgreiche einmalige Anmeldung beim Grid Manager erfolgt.

b. Geben Sie im Abschnitt „Service Provider (SP)“ die * SP Verbindungs-ID* für StorageGRID an. Dieser Wert steuert den Namen, den Sie für jede SP Verbindung in PingFederate verwenden.

- Wenn Ihr Grid beispielsweise nur einen Admin-Knoten hat und Sie nicht beabsichtigen, in Zukunft weitere Admin-Knoten hinzuzufügen, geben Sie `SG` oder `StorageGRID` .
- Wenn Ihr Raster mehr als einen Admin-Knoten enthält, fügen Sie die Zeichenfolge ein `[HOSTNAME]` im Bezeichner. Beispiel: `SG-[HOSTNAME]` . Dadurch wird eine Tabelle generiert, die die SP Verbindungs-ID für jeden Admin-Knoten in Ihrem System basierend auf dem Hostnamen des Knotens anzeigt.

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

c. Geben Sie die URL der Verbundmetadaten für jeden Admin-Knoten im Feld **URL der Verbundmetadaten** an.

Verwenden Sie das folgende Format:

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

d. Wählen Sie **Speichern**.

Auf der Schaltfläche **Speichern** wird für einige Sekunden ein grünes Häkchen angezeigt.

Wenn die Konfiguration gespeichert ist, wird die Bestätigungsmeldung für den Sandbox-Modus angezeigt. Dieser Hinweis bestätigt, dass der Sandbox-Modus jetzt aktiviert ist, und bietet eine Übersichtsanleitung.

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

Befolgen Sie diese Schritte, um Vertrauensstellungen der vertrauenden Seite (Active Directory) zu konfigurieren, Unternehmensanwendungen zu vervollständigen (Azure) oder SP Verbindungen zu konfigurieren (PingFederate).

Active Directory

Schritte

1. Gehen Sie zu Active Directory-Verbunddienste (AD FS).
2. Erstellen Sie eine oder mehrere Vertrauensstellungen der vertrauenden Seite für StorageGRID und verwenden Sie dabei die einzelnen Kennungen der vertrauenden Seite, die in der Tabelle auf der Seite „ StorageGRID Single Sign-on“ angezeigt werden.

   Sie müssen für jeden in der Tabelle angezeigten Admin-Knoten eine Vertrauensstellung erstellen.

   Anweisungen finden Sie unter"Erstellen von Vertrauensstellungen der vertrauenden Seite in AD FS" .

Azurblau

Schritte

1. Wählen Sie auf der Single Sign-On-Seite für den Admin-Knoten, bei dem Sie derzeit angemeldet sind, die Schaltfläche zum Herunterladen und Speichern der SAML-Metadaten aus.
2. Wiederholen Sie dann für alle anderen Admin-Knoten in Ihrem Raster diese Schritte:
   a. Sign in .
   b. Wählen Sie **KONFIGURATION** > **Zugriffskontrolle** > **Einmaliges Anmelden**.
   c. Laden Sie die SAML-Metadaten für diesen Knoten herunter und speichern Sie sie.
3. Gehen Sie zum Azure-Portal.
4. Befolgen Sie die Schritte in"Erstellen von Unternehmensanwendungen in Azure AD" um die SAML-Metadatendatei für jeden Admin-Knoten in die entsprechende Azure-Unternehmensanwendung hochzuladen.

PingFederate

Schritte

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

   Sie müssen für jeden in der Tabelle angezeigten Admin-Knoten eine SP Verbindung erstellen.

Testen Sie SSO-Verbindungen

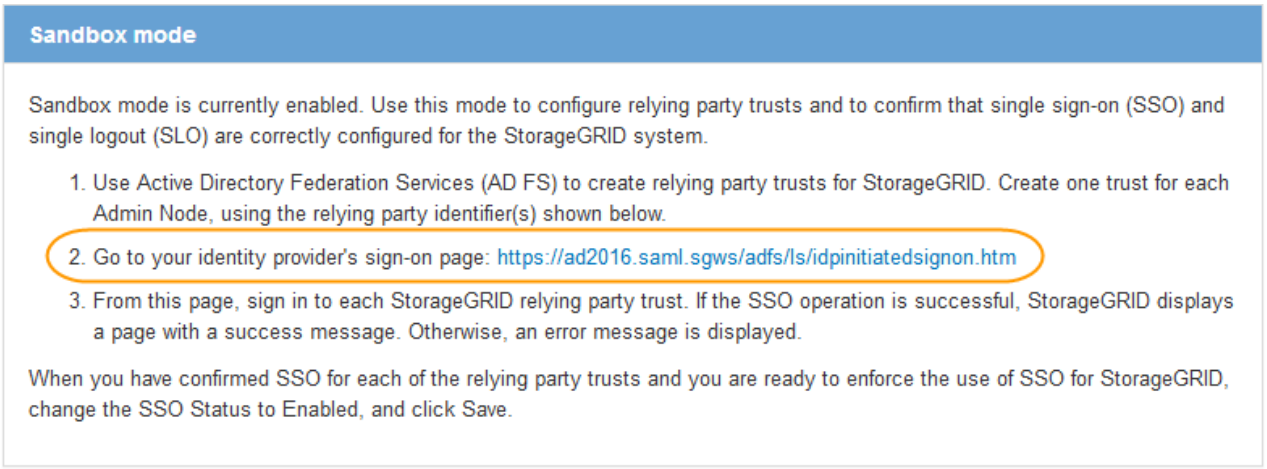
Bevor Sie die Verwendung von Single Sign-On für Ihr gesamtes StorageGRID System erzwingen, sollten Sie bestätigen, dass Single Sign-On und Single Logout für jeden Admin-Knoten richtig konfiguriert sind.

Active Directory

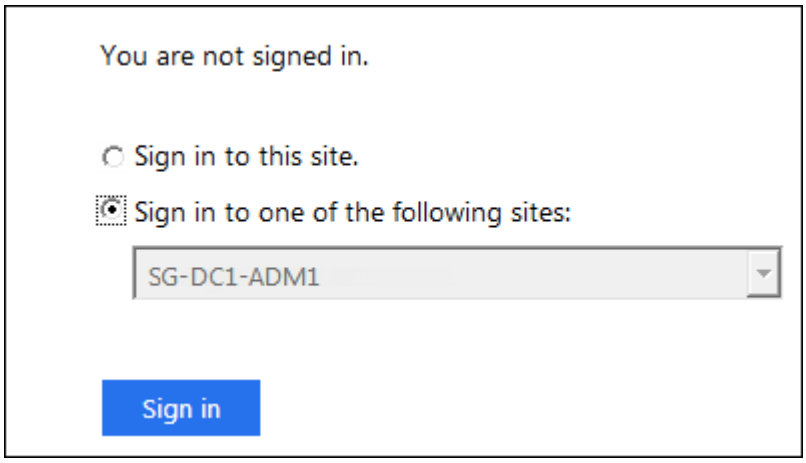
Schritte

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

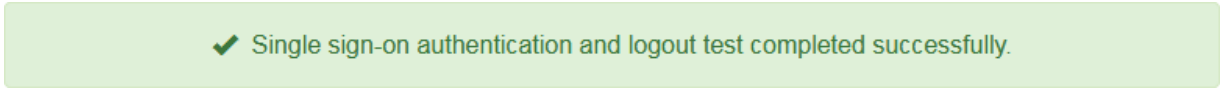
   Die URL wird aus dem Wert abgeleitet, den Sie in das Feld **Name des Verbunddienstes** eingegeben haben.

2. Wählen Sie den Link aus oder kopieren Sie die URL und fügen Sie sie in einen Browser ein, um auf die Anmeldeseite Ihres Identitätsanbieters zuzugreifen.
3. Um zu bestätigen, dass Sie sich mit SSO bei StorageGRID anmelden können, wählen Sie * Bei einer der folgenden Sites Sign in **, wählen Sie die Kennung der vertrauenden Partei für Ihren primären Admin-Knoten und wählen Sie * Sign in**.

4. Geben Sie Ihren föderierten Benutzernamen und Ihr Passwort ein.
   - Wenn die SSO-An- 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-Knoten in Ihrem Raster zu überprüfen.

Azurblau

Schritte

1. Wechseln Sie im Azure-Portal zur Seite „Einmaliges Anmelden“.
2. Wählen Sie **Diese Anwendung testen**.
3. Geben Sie die Anmeldeinformationen eines Verbundbenutzers ein.
   - Wenn die SSO-An- und Abmeldevorgänge erfolgreich sind, wird eine Erfolgsmeldung angezeigt.

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

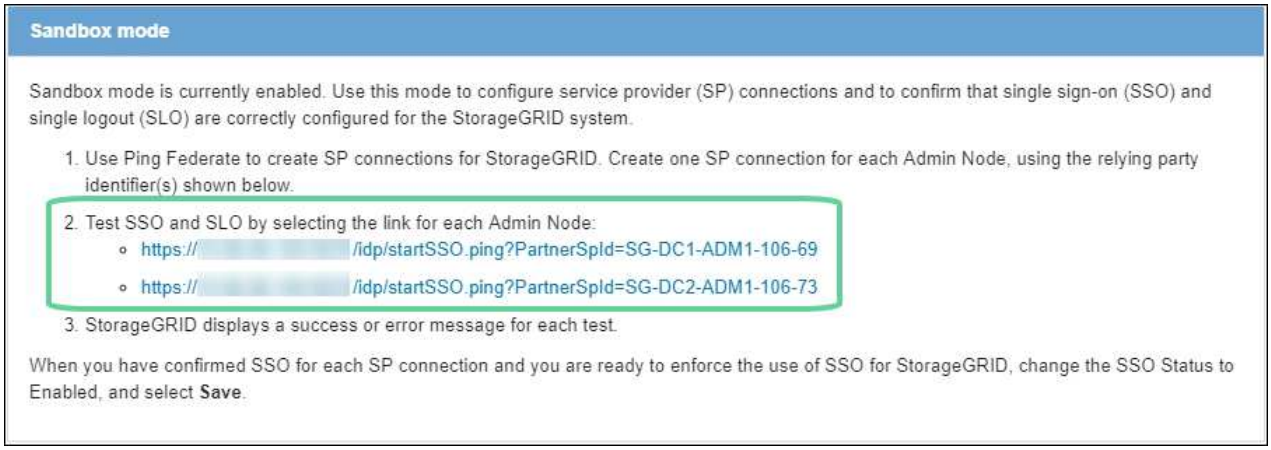
   - Wenn der SSO-Vorgang nicht erfolgreich ist, wird eine Fehlermeldung angezeigt. Beheben Sie das Problem, löschen Sie die Cookies des Browsers und versuchen Sie es erneut.
4. Wiederholen Sie diese Schritte, um die SSO-Verbindung für jeden Admin-Knoten in Ihrem Raster zu überprüfen.

PingFederate

Schritte

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

   Wählen und testen Sie jeweils einen Link.

2. Geben Sie die Anmeldeinformationen eines Verbundbenutzers ein.
   - Wenn die SSO-An- 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-Knoten in Ihrem Raster zu überprüfen.

   Wenn die Meldung „Seite abgelaufen“ angezeigt wird, wählen Sie in Ihrem Browser die Schaltfläche **Zurück** und senden Sie Ihre Anmeldeinformationen erneut.

Aktivieren der einmaligen Anmeldung

Wenn Sie bestätigt haben, dass Sie sich mit SSO bei jedem Admin-Knoten 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 Tenant Manager, die Grid Management API und die Tenant Management API zuzugreifen. Lokale Benutzer können nicht mehr auf StorageGRID zugreifen.

Schritte

1. Wählen Sie **KONFIGURATION** > **Zugriffskontrolle** > **Einmaliges Anmelden**.
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 vom selben Computer aus auf StorageGRID zugreifen, den Sie auch für den Zugriff auf Azure verwenden, stellen Sie sicher, dass der Azure-Portal-Benutzer auch ein autorisierter StorageGRID Benutzer ist (ein Benutzer in einer Verbundgruppe, die in StorageGRID importiert wurde) oder melden Sie sich vom Azure-Portal ab, bevor Sie versuchen, sich bei StorageGRID anzumelden.

Erstellen von Vertrauensstellungen der vertrauenden Seite in AD FS

Sie müssen Active Directory Federation Services (AD FS) verwenden, um für jeden Admin-Knoten in Ihrem System eine Vertrauensstellung der vertrauenden Seite zu erstellen. Sie können Vertrauensstellungen der vertrauenden Seite mithilfe von PowerShell-Befehlen erstellen, indem Sie SAML-Metadaten aus StorageGRID importieren oder die Daten manuell eingeben.

Bevor Sie beginnen

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

> Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID -System eine Vertrauensstellung der vertrauenden Partei erstellen. Durch die Einrichtung einer Vertrauensstellung der vertrauenden Partei für jeden Admin-Knoten wird sichergestellt, dass sich Benutzer sicher bei jedem Admin-Knoten an- und abmelden können.

- Sie haben Erfahrung mit der Erstellung von Vertrauensstellungen vertrauender Parteien in AD FS oder Zugriff auf die Microsoft AD FS-Dokumentation.
- Sie verwenden das AD FS-Verwaltungs-Snap-In und gehören zur Gruppe „Administratoren“.
- Wenn Sie die Vertrauensstellung der vertrauenden Seite manuell erstellen, verfügen Sie über das

benutzerdefinierte Zertifikat, das für die StorageGRID Verwaltungsschnittstelle hochgeladen wurde, oder Sie wissen, wie Sie sich über die Befehlsshell bei einem Admin-Knoten anmelden.

Informationen zu diesem Vorgang

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

Erstellen einer Vertrauensstellung der vertrauenden Seite mithilfe von Windows PowerShell

Sie können Windows PowerShell verwenden, um schnell eine oder mehrere Vertrauensstellungen der vertrauenden Seite zu erstellen.

Schritte

1. Wählen Sie im Windows-Startmenü mit der rechten Maustaste das PowerShell-Symbol aus und wählen Sie **Als Administrator ausführen**.
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 Relying Party Identifier für den Admin-Knoten genau so ein, wie sie auf der Single Sign-On-Seite angezeigt wird. Beispiel: `SG-DC1-ADM1` .
   - Für *`Admin_Node_FQDN`* , geben Sie den vollqualifizierten Domänennamen für denselben Admin-Knoten ein. (Bei Bedarf können Sie stattdessen die IP-Adresse des Knotens verwenden. Wenn Sie hier jedoch eine IP-Adresse eingeben, beachten Sie, dass Sie dieses Vertrauen der vertrauenden Partei aktualisieren oder neu erstellen müssen, wenn sich diese IP-Adresse jemals ändert.)
3. Wählen Sie im Windows Server Manager **Tools** > **AD FS-Verwaltung**.

   Das AD FS-Verwaltungstool wird angezeigt.
4. Wählen Sie **AD FS** > **Vertrauensstellungen der vertrauenden Seite**.

   Die Liste der Vertrauensstellungen der vertrauenden Seite wird angezeigt.
5. Fügen Sie der neu erstellten Vertrauensstellung der vertrauenden Seite eine Zugriffskontrollrichtlinie hinzu:
   a. Suchen Sie nach der Vertrauensstellung der vertrauenden Partei, die Sie gerade erstellt haben.
   b. Klicken Sie mit der rechten Maustaste auf die Vertrauensstellung und wählen Sie **Zugriffskontrollrichtlinie bearbeiten**.
   c. Wählen Sie eine Zugriffskontrollrichtlinie aus.
   d. Wählen Sie **Übernehmen** und dann **OK**
6. Fügen Sie dem neu erstellten Relying Party Trust eine Claim Issuance Policy hinzu:
   a. Suchen Sie nach der Vertrauensstellung der vertrauenden Partei, die Sie gerade erstellt haben.
   b. Klicken Sie mit der rechten Maustaste auf den Trust und wählen Sie **Richtlinie zur Anspruchsausstellung bearbeiten**.
   c. Wählen Sie **Regel hinzufügen**.
   d. Wählen Sie auf der Seite „Regelvorlage auswählen“ aus der Liste „LDAP-Attribute als Ansprüche senden“ aus und klicken Sie auf „Weiter“.

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

   Beispiel: **ObjectGUID zu Name-ID** oder **UPN zu Name-ID**.

f. Wählen Sie für den Attributspeicher **Active Directory** aus.

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

h. Wählen Sie in der Spalte „Ausgehender Anspruchstyp“ der Zuordnungstabelle aus der Dropdownliste „**Namens-ID**“ aus.

i. Wählen Sie **Fertig** und dann **OK**.

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

   a. Klicken Sie mit der rechten Maustaste auf die Vertrauensstellung der vertrauenden Seite, um ihre Eigenschaften zu öffnen.

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

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

8. Wiederholen Sie diese Schritte, um eine Vertrauensstellung der vertrauenden Partei für alle Admin-Knoten in Ihrem StorageGRID System zu konfigurieren.

9. Wenn Sie fertig sind, kehren Sie zu StorageGRID zurück und testen Sie alle Vertrauensstellungen der vertrauenden Parteien, um zu bestätigen, dass sie richtig konfiguriert sind. Sehen"Sandbox-Modus verwenden" Anweisungen hierzu finden Sie unter.

Erstellen einer Vertrauensstellung der vertrauenden Seite durch Importieren von Verbundmetadaten

Sie können die Werte für jede Vertrauensstellung der vertrauenden Partei importieren, indem Sie auf die SAML-Metadaten für jeden Admin-Knoten zugreifen.

Schritte

1. Wählen Sie im Windows Server-Manager **Tools** und dann **AD FS-Verwaltung** aus.
2. Wählen Sie unter „Aktionen“ die Option „Vertrauensstellung der vertrauenden Partei hinzufügen“ aus.
3. Wählen Sie auf der Willkommensseite **Claims aware** und dann **Start**.
4. Wählen Sie **Online oder in einem lokalen Netzwerk veröffentlichte Daten über die vertrauende Partei importieren**.
5. Geben Sie unter **Federation metadata address (host name or URL)** den Speicherort der SAML-Metadaten für diesen Admin-Knoten ein:

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

   Für *`Admin_Node_FQDN`* , geben Sie den vollqualifizierten Domänennamen für denselben Admin-Knoten ein. (Bei Bedarf können Sie stattdessen die IP-Adresse des Knotens verwenden. Wenn Sie hier jedoch eine IP-Adresse eingeben, beachten Sie, dass Sie dieses Vertrauen der vertrauenden Partei aktualisieren oder neu erstellen müssen, wenn sich diese IP-Adresse jemals ändert.)

6. Schließen Sie den Assistenten „Vertrauensstellung der vertrauenden Seite“ ab, speichern Sie die Vertrauensstellung der vertrauenden Seite und schließen Sie den Assistenten.

Verwenden Sie beim Eingeben des Anzeigenamens die Relying Party Identifier für den Admin-Knoten, genau so, wie sie auf der Single Sign-On-Seite im Grid Manager angezeigt wird. Beispiel: `SG-DC1-ADM1` .

7. Fügen Sie eine Anspruchsregel hinzu:
   a. Klicken Sie mit der rechten Maustaste auf den Trust und wählen Sie **Richtlinie zur Anspruchsausstellung bearbeiten**.
   b. Wählen Sie **Regel hinzufügen**:
   c. Wählen Sie auf der Seite „Regelvorlage auswählen“ aus der Liste „LDAP-Attribute als Ansprüche senden“ aus und klicken Sie auf „Weiter“.
   d. Geben Sie auf der Seite „Regel konfigurieren“ einen Anzeigenamen für diese Regel ein.

      Beispiel: **ObjectGUID zu Name-ID** oder **UPN zu Name-ID**.

   e. Wählen Sie für den Attributspeicher **Active Directory** aus.
   f. Geben Sie in der Spalte „LDAP-Attribut“ der Zuordnungstabelle **objectGUID** ein oder wählen Sie **User-Principal-Name** aus.
   g. Wählen Sie in der Spalte „Ausgehender Anspruchstyp“ der Zuordnungstabelle aus der Dropdownliste „**Namens-ID**“ aus.
   h. Wählen Sie **Fertig** und dann **OK**.
8. Bestätigen Sie, dass die Metadaten erfolgreich importiert wurden.
   a. Klicken Sie mit der rechten Maustaste auf die Vertrauensstellung der vertrauenden Seite, um ihre Eigenschaften zu öffnen.
   b. Bestätigen Sie, dass die Felder auf den Registerkarten **Endpunkte**, **Kennungen** und **Signatur** ausgefüllt sind.

      Wenn die Metadaten fehlen, bestätigen Sie, dass die Federation-Metadatenadresse korrekt ist, oder geben Sie die Werte manuell ein.
9. Wiederholen Sie diese Schritte, um eine Vertrauensstellung der vertrauenden Partei für alle Admin-Knoten in Ihrem StorageGRID System zu konfigurieren.
10. Wenn Sie fertig sind, kehren Sie zu StorageGRID zurück und testen Sie alle Vertrauensstellungen der vertrauenden Parteien, um zu bestätigen, dass sie richtig konfiguriert sind. Sehen"Sandbox-Modus verwenden" Anweisungen hierzu finden Sie unter.

Manuelles Erstellen einer Vertrauensstellung der vertrauenden Seite

Wenn Sie die Daten für die Vertrauensstellungen des vertrauenden Teils nicht importieren möchten, können Sie die Werte manuell eingeben.

Schritte

1. Wählen Sie im Windows Server-Manager **Tools** und dann **AD FS-Verwaltung** aus.
2. Wählen Sie unter „Aktionen“ die Option „Vertrauensstellung der vertrauenden Partei hinzufügen“ aus.
3. Wählen Sie auf der Willkommensseite **Claims aware** und dann **Start**.
4. Wählen Sie **Daten zur vertrauenden Partei manuell eingeben** und wählen Sie **Weiter**.
5. Schließen Sie den Assistenten „Relying Party Trust“ ab:

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

   Verwenden Sie aus Konsistenzgründen die Relying Party Identifier für den Admin-Knoten genau so, wie sie auf der Single Sign-On-Seite im Grid Manager angezeigt wird. Beispiel: `SG-DC1-ADM1` .

b. Überspringen Sie den Schritt zum Konfigurieren eines optionalen Token-Verschlüsselungszertifikats.

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

d. Geben Sie die SAML-Dienstendpunkt-URL für den Admin-Knoten ein:

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

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

e. Geben Sie auf der Seite „Kennungen konfigurieren“ die Kennung der vertrauenden Partei für denselben Admin-Knoten an:

   `Admin_Node_Identifier`

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

f. Überprüfen Sie die Einstellungen, speichern Sie die Vertrauensstellung der vertrauenden Seite und schließen Sie den Assistenten.

   Das Dialogfeld „Richtlinie zur Anspruchsausstellung bearbeiten“ wird angezeigt.

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

6. Um den Anspruchsregel-Assistenten zu starten, wählen Sie **Regel hinzufügen**:

   a. Wählen Sie auf der Seite „Regelvorlage auswählen“ aus der Liste „LDAP-Attribute als Ansprüche senden“ aus und klicken Sie auf „Weiter“.

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

      Beispiel: **ObjectGUID zu Name-ID** oder **UPN zu Name-ID**.

   c. Wählen Sie für den Attributspeicher **Active Directory** aus.

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

   e. Wählen Sie in der Spalte „Ausgehender Anspruchstyp“ der Zuordnungstabelle aus der Dropdownliste „**Namens-ID**“ aus.

   f. Wählen Sie **Fertig** und dann **OK**.

7. Klicken Sie mit der rechten Maustaste auf die Vertrauensstellung der vertrauenden Seite, um ihre Eigenschaften zu öffnen.

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

a. Wählen Sie **SAML hinzufügen**.

b. Wählen Sie **Endpunkttyp** > **SAML-Abmeldung**.

c. Wählen Sie **Bindung** > **Umleitung**.

d. Geben Sie im Feld **Vertrauenswürdige URL** die URL ein, die für die einmalige Abmeldung (SLO) von diesem Admin-Knoten verwendet wird:

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

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

a. Wählen Sie **OK**.

9. Geben Sie auf der Registerkarte **Signatur** das Signaturzertifikat für diese Vertrauensstellung der vertrauenden Seite an:

a. Fügen Sie das benutzerdefinierte Zertifikat hinzu:

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

> Verwenden des Standardzertifikats des Admin-Knotens(`server.crt`) wird nicht empfohlen. Wenn der Admin-Knoten ausfällt, wird das Standardzertifikat neu generiert, wenn Sie den Knoten wiederherstellen, und Sie müssen das Vertrauen der vertrauenden Seite aktualisieren.

b. Wählen Sie **Übernehmen** und dann **OK**.

Die Eigenschaften der vertrauenden Partei werden gespeichert und geschlossen.

10. Wiederholen Sie diese Schritte, um eine Vertrauensstellung der vertrauenden Partei für alle Admin-Knoten in Ihrem StorageGRID System zu konfigurieren.
11. Wenn Sie fertig sind, kehren Sie zu StorageGRID zurück und testen Sie alle Vertrauensstellungen der vertrauenden Parteien, um zu bestätigen, dass sie richtig konfiguriert sind. Sehen"Sandbox-Modus verwenden" Anweisungen hierzu finden Sie unter.

Erstellen von Unternehmensanwendungen in Azure AD

Sie verwenden Azure AD, um für jeden Admin-Knoten in Ihrem System eine Unternehmensanwendung zu erstellen.

Bevor Sie beginnen

- Sie haben mit der Konfiguration der einmaligen Anmeldung für StorageGRID begonnen und **Azure** als SSO-Typ ausgewählt.
- Der **Sandbox-Modus** ist auf der Single Sign-On-Seite im Grid Manager ausgewählt. Sehen "Sandbox-Modus verwenden" .

- Sie haben den **Namen der Unternehmensanwendung** für jeden Admin-Knoten in Ihrem System. Sie können diese Werte aus der Tabelle mit den Admin-Knotendetails auf der StorageGRID Single-Sign-On-Seite kopieren.

> Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID System eine Unternehmensanwendung erstellen. Durch die Bereitstellung einer Unternehmensanwendung für jeden Admin-Knoten wird sichergestellt, dass sich Benutzer sicher bei jedem Admin-Knoten anmelden und abmelden können.

- Sie haben Erfahrung mit der Erstellung von Unternehmensanwendungen in Azure Active Directory.
- Sie verfügen über ein Azure-Konto mit einem aktiven Abonnement.
- Sie haben eine der folgenden Rollen im Azure-Konto: Globaler Administrator, Cloud-Anwendungsadministrator, Anwendungsadministrator oder Besitzer des Dienstprinzipals.

Zugriff auf Azure AD

Schritte

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

Erstellen Sie Unternehmensanwendungen und speichern Sie die StorageGRID SSO-Konfiguration

Um die SSO-Konfiguration für Azure in StorageGRID zu speichern, müssen Sie mit Azure eine Unternehmensanwendung für jeden Admin-Knoten erstellen. Sie kopieren die URLs der Verbundmetadaten aus Azure und fügen sie in die entsprechenden Felder **URL der Verbundmetadaten** auf der StorageGRID Single-Sign-On-Seite ein.

Schritte

1. Wiederholen Sie die folgenden Schritte für jeden Admin-Knoten.
   a. Wählen Sie im Bereich „Azure Enterprise-Anwendungen“ **Neue Anwendung** aus.
   b. Wählen Sie **Eigene Anwendung erstellen**.
   c. Geben Sie als Namen den **Namen der Unternehmensanwendung** ein, den Sie aus der Tabelle mit den Admin-Knotendetails auf der StorageGRID Single-Sign-On-Seite kopiert haben.
   d. Lassen Sie das Optionsfeld **Alle anderen Anwendungen integrieren, die Sie nicht in der Galerie finden (Nicht-Galerie)** aktiviert.
   e. Wählen Sie **Erstellen**.
   f. Wählen Sie den Link **Erste Schritte** in **2. Setzen Sie das Feld „Single Sign-On einrichten“** ein oder wählen Sie den Link **Single Sign-On** im linken Rand aus.
   g. Wählen Sie das Feld **SAML** aus.
   h. Kopieren Sie die **App Federation Metadata Url**, die Sie unter **Schritt 3 SAML-Signaturzertifikat** finden.
   i. Gehen Sie zur StorageGRID Single Sign-On-Seite und fügen Sie die URL in das Feld **Federation metadata URL** ein, die dem von Ihnen verwendeten **Namen der Unternehmensanwendung** entspricht.
2. Nachdem Sie für jeden Admin-Knoten eine URL mit Verbundmetadaten eingefügt und alle anderen erforderlichen Änderungen an der SSO-Konfiguration vorgenommen haben, wählen Sie auf der

StorageGRID Single Sign-On-Seite **Speichern** aus.

Laden Sie SAML-Metadaten für jeden Admin-Knoten herunter

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

Schritte

1. Wiederholen Sie diese Schritte für jeden Admin-Knoten.
   a. Sign in bei StorageGRID an.
   b. Wählen Sie **KONFIGURATION** > **Zugriffskontrolle** > **Einmaliges Anmelden**.
   c. Wählen Sie die Schaltfläche aus, um die SAML-Metadaten für diesen Admin-Knoten herunterzuladen.
   d. Speichern Sie die Datei, die Sie in Azure AD hochladen.

Laden Sie SAML-Metadaten in jede Unternehmensanwendung hoch

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

Schritte

1. Kehren Sie zum Azure-Portal zurück.
2. Wiederholen Sie diese Schritte für jede Unternehmensanwendung:

   Möglicherweise müssen Sie die Seite „Unternehmensanwendungen“ aktualisieren, um die Anwendungen anzuzeigen, die Sie zuvor zur Liste hinzugefügt haben.

   a. Gehen Sie zur Eigenschaftenseite der Unternehmensanwendung.
   b. Setzen Sie **Zuweisung erforderlich** auf **Nein** (es sei denn, Sie möchten Zuweisungen separat konfigurieren).
   c. Gehen Sie zur Seite „Single Sign-On“.
   d. Schließen Sie die SAML-Konfiguration ab.
   e. Wählen Sie die Schaltfläche **Metadatendatei hochladen** und wählen Sie die SAML-Metadatendatei aus, die Sie für den entsprechenden Admin-Knoten heruntergeladen haben.
   f. Nachdem die Datei geladen wurde, wählen Sie **Speichern** und dann **X**, um den Bereich zu schließen. Sie werden zur Seite „Single Sign-On mit SAML einrichten“ zurückgeleitet.
3. Befolgen Sie die Schritte in"Sandbox-Modus verwenden" um jede Anwendung zu testen.

Erstellen Sie Service Provider (SP)-Verbindungen in PingFederate

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

Bevor Sie beginnen

- Sie haben Single Sign-On für StorageGRID konfiguriert und **Ping Federate** als SSO-Typ ausgewählt.
- Der **Sandbox-Modus** ist auf der Single Sign-On-Seite im Grid Manager ausgewählt. Sehen "Sandbox-Modus verwenden" .

- Sie haben die * SP Verbindungs-ID* für jeden Admin-Knoten in Ihrem System. Sie finden diese Werte in der Detailtabelle „Admin-Knoten“ auf der StorageGRID Single-Sign-On-Seite.
- Sie haben die **SAML-Metadaten** für jeden Admin-Knoten in Ihrem System heruntergeladen.
- Sie haben Erfahrung mit der Erstellung von SP Verbindungen im PingFederate Server.
- Sie haben diehttps://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html["Referenzhandbuch für Administratoren"^] für PingFederate Server. Die PingFederate-Dokumentation bietet detaillierte Schritt-für-Schritt-Anleitungen und Erklärungen.
- Sie haben die"Administratorberechtigung" für PingFederate Server.

Informationen zu diesem Vorgang

Diese Anweisungen fassen zusammen, 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. Ausführliche Anweisungen zu Ihrer Version finden Sie in der Dokumentation zum PingFederate-Server.

Erfüllen Sie die Voraussetzungen in PingFederate

Bevor Sie die SP Verbindungen erstellen können, die Sie für StorageGRID verwenden, müssen Sie die erforderlichen Aufgaben in PingFederate abschließen. Sie verwenden die Informationen aus diesen Voraussetzungen, wenn Sie die SP Verbindungen konfigurieren.

Datenspeicher erstellen

Erstellen Sie, falls noch nicht geschehen, einen Datenspeicher, um PingFederate mit dem AD FS-LDAP-Server zu verbinden. Verwenden Sie die Werte, die Sie verwendet haben,"Konfigurieren der Identitätsföderation" im StorageGRID.

- **Typ**: Verzeichnis (LDAP)
- **LDAP-Typ**: Active Directory
- **Name des binären Attributs**: Geben Sie **objectGUID** auf der Registerkarte „LDAP-Binärattribute“ genau wie angezeigt ein.

Erstellen Sie einen Validator für Kennwortanmeldeinformationen

Erstellen Sie einen Kennwort-Anmeldeinformationsvalidator, sofern Sie dies noch nicht getan haben.

- **Typ**: LDAP-Benutzername-Passwort-Anmeldeinformationsvalidator
- **Datenspeicher**: Wählen Sie den von Ihnen erstellten Datenspeicher aus.
- **Suchbasis**: Geben Sie Informationen aus LDAP ein (z. B. DC=saml,DC=sgws).
- **Suchfilter**: sAMAccountName=${username}
- **Umfang**: Teilbaum

IdP-Adapterinstanz erstellen

Erstellen Sie eine IdP-Adapterinstanz, falls Sie dies noch nicht getan haben.

Schritte

1. Gehen Sie zu **Authentifizierung** > **Integration** > **IdP-Adapter**.

2. Wählen Sie **Neue Instanz erstellen**.
3. Wählen Sie auf der Registerkarte „Typ“ **HTML-Formular-IdP-Adapter** aus.
4. Wählen Sie auf der Registerkarte „IdP-Adapter“ die Option „Neue Zeile zu ‚Credential Validators‘ hinzufügen“ aus.
5. Wählen Sie dieKennwort-Anmeldeinformationsvalidator Sie erstellt haben.
6. Wählen Sie auf der Registerkarte „Adapterattribute“ das Attribut „**Benutzername**“ für „**Pseudonym**“ aus.
7. Wählen Sie **Speichern**.

Signaturzertifikat erstellen oder importieren

Erstellen oder importieren Sie das Signaturzertifikat, sofern Sie dies noch nicht getan haben.

Schritte

1. Gehen Sie zu **Sicherheit** > **Signatur- und Entschlüsselungsschlüssel und -zertifikate**.
2. Erstellen oder importieren Sie das Signaturzertifikat.

Erstellen einer SP Verbindung in PingFederate

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

> Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID System eine SP Verbindung erstellen, damit sich Benutzer sicher bei jedem Knoten an- und abmelden können. Verwenden Sie diese Anweisungen, um die erste SP Verbindung herzustellen. Gehen Sie dann zuErstellen Sie zusätzliche SP Verbindungen um alle zusätzlichen Verbindungen herzustellen, 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 **Für diese Verbindung keine Vorlage verwenden**.
4. Wählen Sie **Browser-SSO-Profile** und **SAML 2.0** als Protokoll.

SP Metadaten importieren

Schritte

1. Wählen Sie auf der Registerkarte „Metadaten importieren“ die Option „Datei“ aus.
2. Wählen Sie die SAML-Metadatendatei aus, die Sie von der StorageGRID Single-Sign-On-Seite für den Admin-Knoten heruntergeladen haben.
3. Überprüfen Sie die Metadatenzusammenfassung und die auf der Registerkarte „Allgemeine Informationen“ bereitgestellten Informationen.

   Die Entitäts-ID des Partners und der Verbindungsname werden auf die StorageGRID SP Verbindungs-ID eingestellt. (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 des einmaligen Anmeldens im 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-initiiertes SSO*, * SP-initiales SLO*, * IdP-initiiertes SSO* und * IdP-initiiertes SLO* aus.
3. Wählen Sie **Weiter**.
4. Nehmen Sie auf der Registerkarte „Assertion Lifetime“ keine Änderungen vor.
5. Wählen Sie auf der Registerkarte „Assertion-Erstellung“ die Option „Assertion-Erstellung konfigurieren“ aus.
   a. Wählen Sie auf der Registerkarte „Identitätszuordnung“ **Standard** aus.
   b. Verwenden Sie auf der Registerkarte „Attributvertrag“ **SAML_SUBJECT** als Attributvertrag und das importierte, nicht angegebene Namensformat.
6. Wählen Sie zum Verlängern des Vertrags **Löschen**, um den `urn:oid` , das nicht verwendet wird.

Adapterinstanz zuordnen

Schritte

1. Wählen Sie auf der Registerkarte „Zuordnung der Authentifizierungsquelle“ die Option „Neue Adapterinstanz zuordnen“ aus.
2. Wählen Sie auf der Registerkarte Adapterinstanz die OptionAdapterinstanz Sie erstellt haben.
3. Wählen Sie auf der Registerkarte „Zuordnungsmethode“ die Option „Zusätzliche Attribute aus einem Datenspeicher abrufen“ aus.
4. Wählen Sie auf der Registerkarte „Attributquelle und Benutzersuche“ die Option „Attributquelle hinzufügen“ aus.
5. Geben Sie auf der Registerkarte Datenspeicher eine Beschreibung ein und wählen Sie dieDatenspeicher Sie haben hinzugefügt.
6. Gehen Sie auf der Registerkarte „LDAP-Verzeichnissuche“ wie folgt vor:
   - Geben Sie den **Basis-DN** ein, der genau mit dem Wert übereinstimmen sollte, den Sie in StorageGRID für den LDAP-Server eingegeben haben.
   - Wählen Sie als Suchbereich **Unterbaum** aus.
   - Suchen Sie für die Stammobjektklasse nach einem der folgenden Attribute und fügen Sie es hinzu: **objectGUID** oder **userPrincipalName**.
7. Wählen Sie auf der Registerkarte „LDAP-Binärattribut-Kodierungstypen“ **Base64** für das Attribut **objectGUID** aus.
8. Geben Sie auf der Registerkarte „LDAP-Filter“ **sAMAccountName=${username}** ein.
9. Wählen Sie auf der Registerkarte „Attribute Contract Fulfillment“ aus der Dropdown-Liste „Quelle“ die Option „LDAP (Attribut)“ und wählen Sie aus der Dropdown-Liste „Wert“ entweder „**objectGUID**“ oder „**userPrincipalName**“ aus.
10. Überprüfen und speichern Sie die Attributquelle.
11. Wählen Sie auf der Registerkarte „Failsave-Attributquelle“ die Option „SSO-Transaktion abbrechen“ aus.
12. Überprüfen Sie die Zusammenfassung und wählen Sie **Fertig**.

13. Wählen Sie **Fertig**.

Konfigurieren der Protokolleinstellungen

Schritte

1. Wählen Sie auf der Registerkarte * SP -Verbindung* > **Browser-SSO** > **Protokolleinstellungen** die Option **Protokolleinstellungen konfigurieren**.
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-Service-URLs die Standardwerte, die aus den StorageGRID SAML-Metadaten importiert wurden (**REDIRECT** für Binding und `/api/saml-logout` für die Endpunkt-URL.
4. Deaktivieren Sie auf der Registerkarte „Zulässige SAML-Bindungen“ die Optionen „**ARTIFACT**“ und „**SOAP**“. Nur **POST** und **REDIRECT** sind erforderlich.
5. Lassen Sie auf der Registerkarte „Signaturrichtlinie“ die Kontrollkästchen **Signatur von Authentifizierungsanforderungen erforderlich** und **Assertion immer signieren** aktiviert.
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 Browser-SSO-Einstellungen zu speichern.

Konfigurieren der Anmeldeinformationen

Schritte

1. Wählen Sie auf der Registerkarte „SP -Verbindung“ die Option „Anmeldeinformationen“ aus.
2. Wählen Sie auf der Registerkarte „Anmeldeinformationen“ die Option „Anmeldeinformationen konfigurieren“ aus.
3. Wählen Sie dieSignaturzertifikat Sie haben erstellt oder importiert.
4. Wählen Sie **Weiter**, um zu **Einstellungen für die Signaturüberprüfung verwalten** zu gelangen.
   a. Wählen Sie auf der Registerkarte „Vertrauensmodell“ die Option „Unverankert“ aus.
   b. Überprüfen Sie auf der Registerkarte „Signaturüberprüfungszertifikat“ die Informationen zum Signaturzertifikat, die aus den StorageGRID SAML-Metadaten importiert wurden.
5. Überprüfen 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 SP Verbindungen zu erstellen, die Sie für jeden Admin-Knoten in Ihrem Raster benötigen. Sie laden für jede Kopie neue Metadaten hoch.

> ⓘ Die SP Verbindungen für verschiedene Admin-Knoten verwenden identische Einstellungen, mit Ausnahme der Entitäts-ID, der Basis-URL, der Verbindungs-ID, des Verbindungsnamens, der Signaturüberprüfung und der SLO-Antwort-URL des Partners.

Schritte

1. Wählen Sie **Aktion** > **Kopieren**, um für jeden zusätzlichen Admin-Knoten eine Kopie der ursprünglichen 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 Metadatendatei aus, die dem Admin-Knoten entspricht:
   a. Wählen Sie **Aktion** > **Mit Metadaten aktualisieren**.
   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 > Assertionserstellung konfigurieren > Attributvertrag**.
   c. Löschen Sie den Eintrag für **urn:oid**.
   d. Wählen Sie **Speichern**.

Deaktivieren der einmaligen Anmeldung

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

Bevor Sie beginnen

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

Schritte

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

   Die Single Sign-On-Seite wird angezeigt.

2. Wählen Sie die Option **Deaktiviert**.
3. Wählen Sie **Speichern**.

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

4. Wählen Sie **OK**.

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

Deaktivieren und aktivieren Sie Single Sign-On für einen Admin-Knoten vorübergehend.

Wenn das Single Sign-On-System (SSO) ausfällt, können Sie sich möglicherweise nicht beim Grid Manager anmelden. In diesem Fall können Sie SSO für einen Admin-Knoten vorübergehend deaktivieren und wieder aktivieren. Um SSO zu deaktivieren und anschließend wieder zu aktivieren, müssen Sie auf die Befehlsshell des Knotens zugreifen.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Nachdem Sie SSO für einen Admin-Knoten deaktiviert haben, können Sie sich als lokaler Root-Benutzer beim Grid Manager anmelden. Um Ihr StorageGRID -System zu sichern, müssen Sie die Befehlsshell des Knotens verwenden, um SSO auf dem Admin-Knoten wieder zu aktivieren, sobald Sie sich abmelden.

> Das Deaktivieren von SSO für einen Admin-Knoten hat keine Auswirkungen auf die SSO-Einstellungen für andere Admin-Knoten im Raster. Das Kontrollkästchen **SSO aktivieren** auf der Single Sign-On-Seite im Grid Manager bleibt aktiviert und alle vorhandenen SSO-Einstellungen bleiben erhalten, 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 Passwort ein, das in der `Passwords.txt` Datei.
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

      Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Zu `#` .
2. Führen Sie den folgenden Befehl aus:`disable-saml`

   Eine Meldung weist darauf hin, dass der Befehl nur für diesen Admin-Knoten gilt.
3. Bestätigen Sie, dass Sie SSO deaktivieren möchten.

   Eine Meldung weist darauf hin, dass die einmalige Anmeldung auf dem Knoten deaktiviert ist.
4. Greifen Sie über einen Webbrowser auf den Grid Manager auf demselben Admin-Knoten zu.

   Die Anmeldeseite des Grid Managers wird jetzt angezeigt, da SSO deaktiviert wurde.
5. Sign in .
6. Wenn Sie SSO vorübergehend deaktiviert haben, weil Sie die SSO-Konfiguration korrigieren mussten:
   a. Wählen Sie **KONFIGURATION** > **Zugriffskontrolle** > **Einmaliges Anmelden**.
   b. Ändern Sie die falschen oder veralteten SSO-Einstellungen.
   c. Wählen Sie **Speichern**.

      Wenn Sie auf der Single Sign-On-Seite „Speichern“ auswählen, 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 aus, die Sie ausführen müssen.
b. Wählen Sie **Abmelden** und schließen Sie den Grid Manager.
c. Aktivieren Sie SSO auf dem Admin-Knoten erneut. Sie können einen der folgenden Schritte ausführen:

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

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

   Bestätigen Sie, dass Sie SSO aktivieren möchten.

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

   - Starten Sie den Grid-Knoten neu: `reboot`

8. Greifen Sie über einen Webbrowser vom selben Admin-Knoten aus auf den Grid Manager zu.
9. Vergewissern Sie sich, dass die StorageGRID Sign in angezeigt wird und dass Sie Ihre SSO-Anmeldeinformationen eingeben müssen, um auf den Grid Manager zuzugreifen.

Grid-Föderation verwenden

Was ist Grid-Föderation?

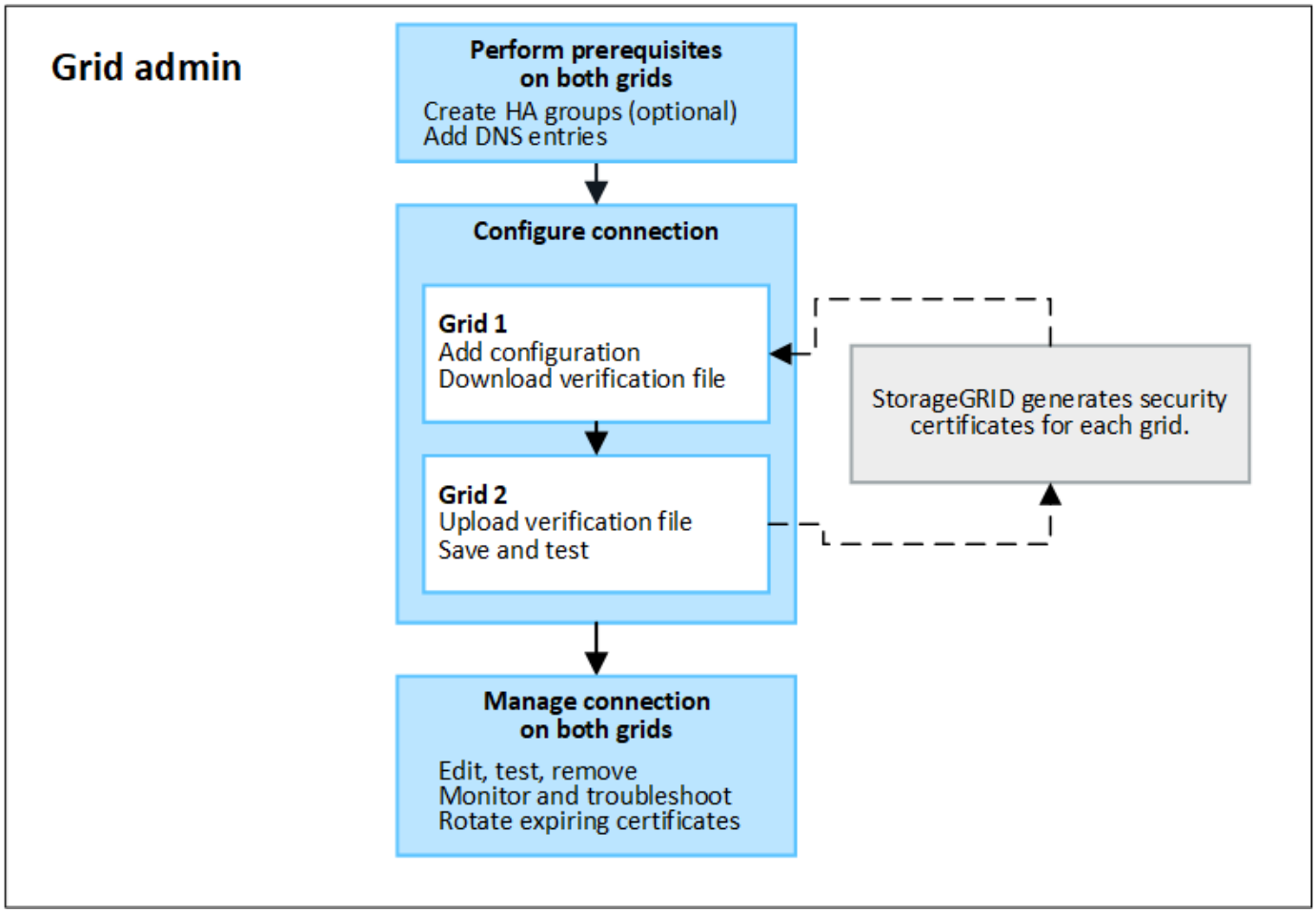
Sie können die Grid-Föderation verwenden, um Mandanten zu klonen und ihre Objekte zwischen zwei StorageGRID -Systemen zur Notfallwiederherstellung zu replizieren.

Was ist eine Grid-Föderation-Verbindung?

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

Workflow für die Grid-Föderation

Das Workflow-Diagramm fasst die Schritte zum Konfigurieren einer Grid-Föderation-Verbindung zwischen zwei Grids zusammen.



Überlegungen und Anforderungen für Grid-Föderation-Verbindungen

- Die für die Grid-Föderation verwendeten Grids müssen StorageGRID -Versionen ausführen, die entweder identisch sind oder sich höchstens in einer Hauptversion unterscheiden.

  Einzelheiten zu den Versionsanforderungen finden Sie im"Versionshinweise" .

- Ein Grid kann über eine oder mehrere Grid-Föderationsverbindungen zu anderen Grids verfügen. Jede Grid-Föderation-Verbindung ist unabhängig von allen anderen Verbindungen. Wenn beispielsweise Raster 1 eine Verbindung mit Raster 2 und eine zweite Verbindung mit Raster 3 hat, besteht keine implizite Verbindung zwischen Raster 2 und Raster 3.
- Grid-Föderation-Verbindungen sind bidirektional. Nachdem die Verbindung hergestellt wurde, können Sie die Verbindung von beiden Grids aus überwachen und verwalten.
- Mindestens eine Grid-Föderation-Verbindung muss vorhanden sein, bevor Sie"Kontoklon" oder"Cross-Grid-Replikation" .

Netzwerk- und IP-Adressanforderungen

- Grid-Föderationsverbindungen können im Grid-Netzwerk, Admin-Netzwerk oder Client-Netzwerk erfolgen.
- Eine Grid-Föderation-Verbindung verbindet ein Grid mit einem anderen Grid. Die Konfiguration für jedes Grid gibt einen Grid-Föderationsendpunkt auf dem anderen Grid an, der aus Admin-Knoten, Gateway-Knoten oder beidem besteht.
- Die beste Vorgehensweise besteht darin, eine Verbindung herzustellen"Hochverfügbarkeitsgruppen (HA)" von Gateway- und Admin-Knoten auf jedem Grid. Durch die Verwendung von HA-Gruppen wird

sichergestellt, dass Grid-Föderationsverbindungen online bleiben, wenn Knoten nicht verfügbar sind. Wenn die aktive Schnittstelle in einer der HA-Gruppen ausfällt, kann die Verbindung eine Backup-Schnittstelle verwenden.

- Das Erstellen einer Grid-Föderationsverbindung, die die IP-Adresse eines einzelnen Admin-Knotens oder Gateway-Knotens verwendet, wird nicht empfohlen. Wenn der Knoten nicht mehr verfügbar ist, ist auch die Grid-Föderationsverbindung nicht mehr verfügbar.
- "Cross-Grid-Replikation"von Objekten erfordert, dass die Speicherknoten in jedem Grid auf die konfigurierten Admin- und Gateway-Knoten im anderen Grid zugreifen können. Bestätigen Sie für jedes Grid, dass alle Speicherknoten über eine Route mit hoher Bandbreite zu den für die Verbindung verwendeten Admin-Knoten oder Gateway-Knoten verfügen.

Verwenden Sie FQDNs, um die Verbindung auszugleichen

Verwenden Sie für eine Produktionsumgebung vollqualifizierte Domänennamen (FQDNs), um jedes Grid in der Verbindung zu identifizieren. Erstellen Sie anschließend die entsprechenden DNS-Einträge wie folgt:

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

Wenn Sie mehrere DNS-Einträge verwenden, wird für die Anforderungen zur Verwendung der Verbindung wie folgt eine Lastverteilung vorgenommen:

- Bei DNS-Einträgen, die den VIP-Adressen mehrerer HA-Gruppen zugeordnet sind, wird die Last zwischen den aktiven Knoten in den HA-Gruppen ausgeglichen.
- Bei DNS-Einträgen, die den IP-Adressen mehrerer Admin-Knoten oder Gateway-Knoten zugeordnet sind, wird die Last zwischen den zugeordneten Knoten ausgeglichen.

Portanforderungen

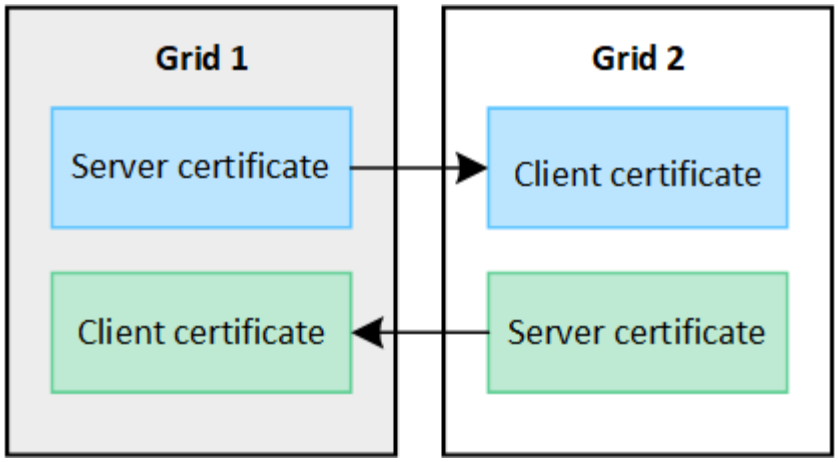
Beim Erstellen einer Grid-Föderation-Verbindung können Sie jede nicht verwendete Portnummer zwischen 23000 und 23999 angeben. Beide Grids in dieser Verbindung verwenden denselben Port.

Sie müssen sicherstellen, dass kein Knoten in einem der Grids diesen Port für andere Verbindungen verwendet.

Zertifikatsanforderungen

Wenn Sie eine Grid-Föderation-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 sich das Ablaufdatum dieser Zertifikate nähert, werden Sie durch die Warnung **Ablauf des Grid-Föderationszertifikats** daran erinnert, die Zertifikate zu rotieren. Dies können Sie mit dem Grid Manager tun.

> Wenn die Zertifikate an einem der Enden der Verbindung ablaufen, funktioniert die Verbindung nicht mehr. Die Datenreplikation wird ausgesetzt, bis die Zertifikate aktualisiert sind.

Mehr erfahren

- "Erstellen von Grid-Föderationsverbindungen"
- "Grid-Föderationsverbindungen verwalten"
- "Beheben von Grid-Föderationsfehlern"

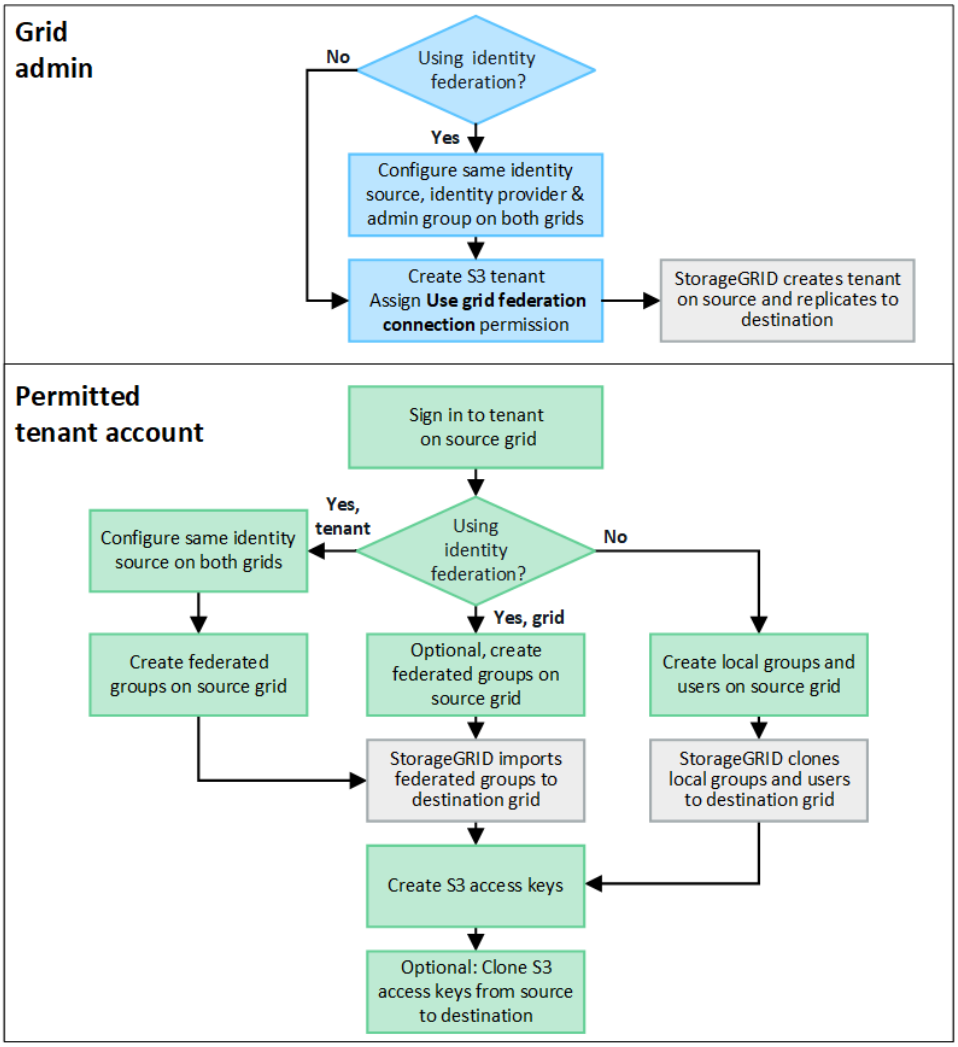
Was ist ein Kontoklon?

Beim Kontoklon handelt es sich um die automatische Replikation eines Mandantenkontos, von Mandantengruppen, Mandantenbenutzern und optional von S3-Zugriffsschlüsseln zwischen den StorageGRID Systemen in einem"Netzverbundanschluss" .

Kontoklon ist erforderlich für"Cross-Grid-Replikation" . Durch das Klonen von Kontoinformationen von 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 zum Klonen von Konten

Das Workflow-Diagramm zeigt die Schritte, die Grid-Administratoren und zugelassene Mandanten ausführen, um einen Kontoklon einzurichten. Diese Schritte werden ausgeführt, nachdem"Grid-Föderation-Verbindung ist konfiguriert" .



Grid-Admin-Workflow

Die Schritte, die Grid-Administratoren durchführen, hängen davon ab, ob die StorageGRID -Systeme im"Netzverbundanschluss" Verwenden Sie Single Sign-On (SSO) oder Identitätsföderation.

SSO für Kontoklon konfigurieren (optional)

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

Schritte

1. Konfigurieren Sie für beide Grids dieselbe Identitätsquelle. Sehen "Verwenden der Identitätsföderation" .
2. Konfigurieren Sie für beide Grids denselben SSO-Identitätsanbieter (IdP). Sehen "Konfigurieren der einmaligen Anmeldung" .
3. "Erstellen Sie die gleiche Administratorgruppe"auf beiden Grids durch Importieren derselben föderierten Gruppe.

   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 in beiden Rastern vorhanden ist, wird der Mandant nicht zum Ziel repliziert.

Konfigurieren Sie die Identitätsföderation auf Rasterebene für den Kontoklon (optional)

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

Schritte

1. Konfigurieren Sie für beide Grids dieselbe Identitätsquelle. Sehen "Verwenden der Identitätsföderation" .
2. Optional: Wenn eine Verbundgruppe über die anfängliche Root-Zugriffsberechtigung für die Quell- und Zielmandantenkonten verfügt,"Erstellen Sie dieselbe Administratorgruppe" auf beiden Grids durch Importieren derselben föderierten Gruppe.

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

3. Wenn Sie nicht möchten, dass eine föderierte Gruppe anfänglich über die Root-Zugriffsberechtigung für beide Konten verfügt, geben Sie ein Kennwort für den lokalen Root-Benutzer an.

Erstellen Sie ein zulässiges S3-Mandantenkonto

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

Schritte

1. Bestimmen Sie, welches Raster das Quellraster des Mandanten für Kontoklonvorgänge sein soll.

   Das Raster, in dem der Mandant ursprünglich erstellt wurde, wird als *Quellraster* des Mandanten bezeichnet. Das Raster, in dem der Mandant repliziert wird, wird als *Zielraster* des Mandanten bezeichnet.

2. Erstellen Sie in diesem Raster ein neues S3-Mandantenkonto oder bearbeiten Sie ein vorhandenes Konto.
3. Weisen Sie die Berechtigung **Grid-Föderationsverbindung verwenden** zu.
4. Wenn das Mandantenkonto seine eigenen Verbundbenutzer verwalten soll, weisen Sie die Berechtigung **Eigene Identitätsquelle verwenden** zu.

   Wenn diese Berechtigung zugewiesen ist, müssen sowohl die Quell- als auch die Zielmandantenkonten dieselbe Identitätsquelle konfigurieren, bevor Verbundgruppen erstellt werden. Dem Quellmandanten hinzugefügte föderierte Gruppen können nicht auf den Zielmandanten geklont werden, es sei denn, beide Raster verwenden dieselbe Identitätsquelle.

5. Wählen Sie eine bestimmte Grid-Föderation-Verbindung aus.
6. Speichern Sie den neuen oder geänderten Mandanten.

   Wenn ein neuer Mandant mit der Berechtigung **Grid-Föderationsverbindung verwenden** gespeichert wird, erstellt StorageGRID automatisch eine Replik dieses Mandanten auf dem anderen Grid, und zwar wie folgt:

   - Beide Mandantenkonten haben dieselbe Konto-ID, denselben Namen, dasselbe Speicherkontingent

und dieselben zugewiesenen 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-Zugriffsberechtigung für den Mandanten ausgewählt haben, wird dieser Benutzer auf den Zielmandanten geklont. Das Kennwort für diesen Benutzer wird jedoch nicht geklont.

Weitere Informationen finden Sie unter "Verwalten Sie zulässige Mandanten für die Grid-Föderation" .

Workflow für zulässige Mandantenkonten

Nachdem ein Mandant mit der Berechtigung **Grid-Föderationsverbindung verwenden** in das Ziel-Grid repliziert wurde, können berechtigte Mandantenkonten diese Schritte ausführen, um Mandantengruppen, Benutzer und S3-Zugriffsschlüssel zu klonen.

Schritte

1. Sign in beim Mandantenkonto im Quellraster des Mandanten an.
2. Konfigurieren Sie, sofern zulässig, die Identifizierungsföderation sowohl für die Quell- als auch für die Zielmandantenkonten.
3. Erstellen Sie Gruppen und Benutzer auf dem Quellmandanten.

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

4. Erstellen Sie S3-Zugriffsschlüssel.
5. Klonen Sie optional S3-Zugriffsschlüssel vom Quellmandanten auf den Zielmandanten.

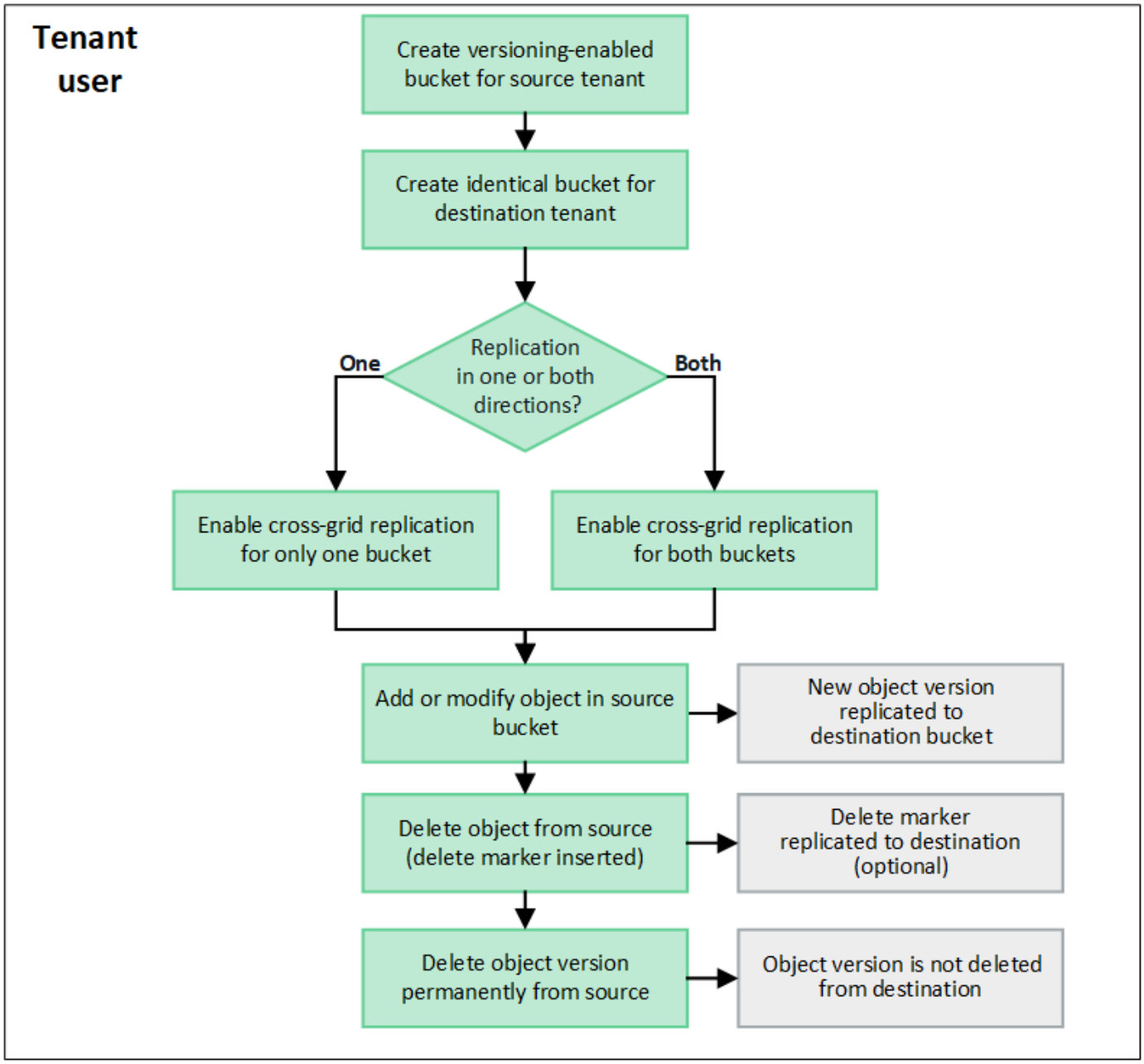
Weitere Informationen zum Workflow für zulässige Mandantenkonten und zum Klonen von Gruppen, Benutzern und S3-Zugriffsschlüsseln finden Sie unter"Mandantengruppen und Benutzer klonen" Und"Klonen Sie S3-Zugriffsschlüssel mithilfe der API" .

Was ist Cross-Grid-Replikation?

Cross-Grid-Replikation ist die automatische Replikation von Objekten zwischen ausgewählten S3-Buckets in zwei StorageGRID Systemen, die in einem"Netzverbundanschluss" . "Kontoklon" ist für die Cross-Grid-Replikation erforderlich.

Workflow für die Cross-Grid-Replikation

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



Voraussetzungen für die Cross-Grid-Replikation

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

- Muss den gleichen Namen haben, kann aber unterschiedliche Regionen haben
- Die Versionsverwaltung muss aktiviert sein
- S3 Object Lock muss deaktiviert sein
- Muss leer sein

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

Mehr erfahren

"Verwalten der Cross-Grid-Replikation"

So funktioniert die Cross-Grid-Replikation

Die Cross-Grid-Replikation kann so konfiguriert werden, dass sie in eine oder in beide Richtungen erfolgt.

Replikation in eine Richtung

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

Replikation in beide Richtungen

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

Was passiert, wenn Gegenstände verschluckt werden?

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

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

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

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

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

2. StorageGRID verwendet die aktiven ILM-Richtlinien jedes Grids, um die Objekte zu verwalten, genau wie jedes andere Objekt. Beispielsweise könnte Objekt A auf Grid 1 als zwei replizierte Kopien gespeichert und für immer aufbewahrt werden, während die Kopie von Objekt A, die auf Grid 2 repliziert wurde, mit 2+1-Löschcodierung gespeichert und nach drei Jahren gelöscht werden könnte.

Was passiert, wenn Objekte gelöscht werden?

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

- Der S3-Client stellt eine Löschanforderung.
- Ein Tenant Manager-Benutzer wählt die"Objekte im Bucket löschen" 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 eines Vorgangs zum Löschen von Objekten im Bucket, eines Ablaufs des Bucket-Lebenszyklus oder eines Ablaufs der ILM-Platzierung löscht, wird das replizierte Objekt in einer Grid-Föderationsverbindung nie aus dem anderen Grid gelöscht. Allerdings können Löschmarkierungen, die durch S3-Client-Löschvorgänge zum Quell-Bucket hinzugefügt wurden, optional in den Ziel-Bucket repliziert werden.

Um zu verstehen, was passiert, wenn ein S3-Client Objekte aus einem Bucket löscht, für den die Cross-Grid-Replikation aktiviert ist, sehen Sie sich an, wie S3-Clients Objekte aus Buckets löschen, für die die Versionierung aktiviert ist:

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

Wenn ein S3-Client ein Objekt aus einem Bucket löscht, für den die Cross-Grid-Replikation aktiviert ist, ermittelt StorageGRID wie folgt, ob die Löschanforderung an das Ziel repliziert werden soll:

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

In der Abbildung wurde **Löschmarkierungen replizieren** auf **Ja** gesetzt, als"Cross-Grid-Replikation wurde aktiviert" . Löschanforderungen für den Quell-Bucket, die eine Versions-ID enthalten, löschen keine Objekte aus dem Ziel-Bucket. Löschanforderungen für den Quell-Bucket, die keine Versions-ID enthalten, führen scheinbar zum Löschen von Objekten im Ziel-Bucket.

> Wenn Sie die Objektlöschungen zwischen den Grids synchron halten möchten, erstellen Sie entsprechende"S3-Lebenszykluskonfigurationen" für die Eimer auf beiden Gittern.

So werden verschlüsselte Objekte repliziert

Wenn Sie die Cross-Grid-Replikation zum Replizieren von Objekten zwischen Grids verwenden, können Sie einzelne Objekte verschlüsseln, die Standard-Bucket-Verschlüsselung verwenden oder eine Grid-weite Verschlüsselung konfigurieren. Sie können standardmäßige Bucket- oder Grid-weite Verschlüsselungseinstellungen hinzufügen, ändern oder entfernen, bevor oder nachdem Sie die Grid-übergreifende Replikation für einen Bucket aktivieren.

Um einzelne Objekte zu verschlüsseln, können Sie beim Hinzufügen der Objekte zum Quell-Bucket SSE (serverseitige Verschlüsselung mit von StorageGRID verwalteten Schlüsseln) verwenden. Verwenden Sie die `x-amz-server-side-encryption` Anforderungsheader und geben Sie `AES256` . Sehen "Verwenden Sie serverseitige Verschlüsselung" .

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

Um die Standardverschlüsselung für einen Bucket zu verwenden, verwenden Sie eine PutBucketEncryption-Anforderung und legen Sie die `SSEAlgorithm` Parameter auf `AES256` . Die Verschlüsselung auf Bucket-Ebene gilt für alle Objekte, die ohne die `x-amz-server-side-encryption` Anforderungsheader. Sehen "Operationen an Buckets" .

Um die Verschlüsselung auf Rasterebene 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 sind oder die ohne die `x-amz-server-side-encryption` Anforderungsheader. Sehen "Konfigurieren von Netzwerk- und Objektoptionen" .

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

Bei der Bestimmung, wie Quellobjekte verschlüsselt werden, wendet StorageGRID die folgenden Regeln an:

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

Bei der Bestimmung, wie replizierte Objekte verschlüsselt werden, wendet StorageGRID diese Regeln in

dieser Reihenfolge an:

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

PutObjectTagging und DeleteObjectTagging werden nicht unterstützt

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

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

So werden segmentierte Objekte repliziert

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

Vergleichen Sie Cross-Grid-Replikation und CloudMirror-Replikation

Wenn Sie mit der Grid-Föderation beginnen, überprüfen Sie die Ähnlichkeiten und Unterschiede zwischen"Cross-Grid-Replikation" und die"StorageGRID CloudMirror-Replikationsdienst" .

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

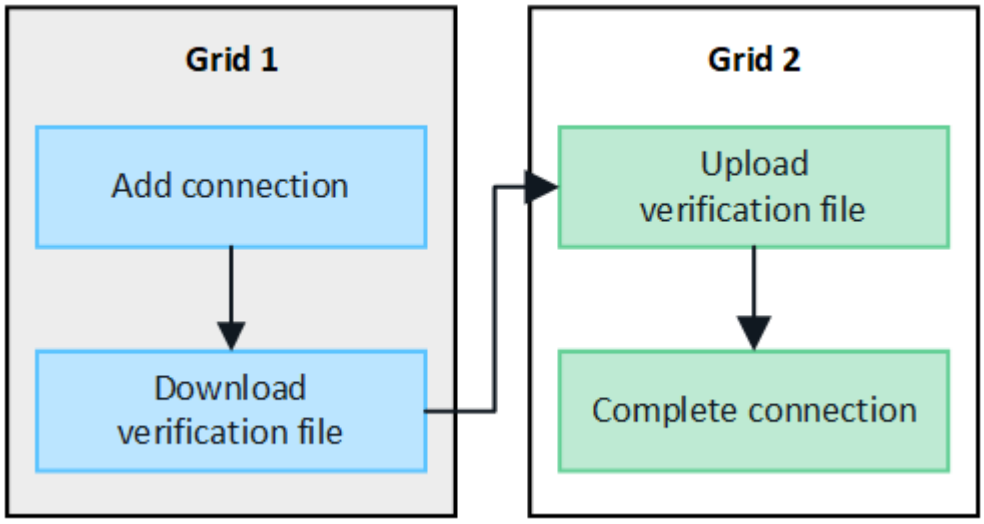
	Cross-Grid-Replikation	CloudMirror-Replikationsdienst
Wie ist es eingerichtet?	1. Konfigurieren Sie eine Grid-Föderationsverbindung zwischen zwei Grids. 2. Fügen Sie neue Mandantenkonten hinzu, die automatisch in das andere Raster geklont werden. 3. Fügen Sie neue Mandantengruppen und Benutzer hinzu, die ebenfalls geklont werden. 4. Erstellen Sie entsprechende Buckets auf jedem Grid und ermöglichen Sie die Cross-Grid-Replikation in eine oder beide Richtungen.	1. Ein Mandantenbenutzer konfiguriert die CloudMirror-Replikation, indem er mithilfe des Mandantenmanagers oder der S3-API einen CloudMirror-Endpunkt (IP-Adresse, Anmeldeinformationen usw.) definiert. 2. Jeder Bucket, der diesem Mandantenkonto gehört, kann so konfiguriert werden, dass er auf den CloudMirror-Endpunkt verweist.
Wer ist für die Einrichtung verantwortlich?	• Ein Grid-Administrator konfiguriert die Verbindung und die Mandanten. • Mandantenbenutzer konfigurieren die Gruppen, Benutzer, Schlüssel und Buckets.	Normalerweise ein Mieterbenutzer.
Was ist das Ziel?	Ein entsprechender und identischer S3-Bucket auf dem anderen StorageGRID -System in der Grid-Föderationsverbindung.	• Jede kompatible S3-Infrastruktur (einschließlich Amazon S3). • Google Cloud Platform (GCP)
Ist eine Objektversionierung erforderlich?	Ja, sowohl im Quell- als auch im Ziel-Bucket muss die Objektversionierung aktiviert sein.	Nein, die CloudMirror-Replikation unterstützt jede Kombination aus nicht versionierten und versionierten Buckets sowohl auf der Quelle als auch auf dem Ziel.
Was bewirkt, dass Objekte zum Ziel verschoben werden?	Objekte werden automatisch repliziert, wenn sie zu einem Bucket hinzugefügt werden, für den die Cross-Grid-Replikation aktiviert ist.	Objekte werden automatisch repliziert, wenn sie zu einem Bucket hinzugefügt werden, der mit einem CloudMirror-Endpunkt konfiguriert wurde. Objekte, die im Quell-Bucket vorhanden waren, bevor der Bucket mit dem CloudMirror-Endpunkt konfiguriert wurde, werden nicht repliziert, es sei denn, sie werden geändert.
Wie werden Objekte repliziert?	Bei der Cross-Grid-Replikation werden versionierte Objekte erstellt und die Versions-ID vom Quell-Bucket in den Ziel-Bucket repliziert. Dadurch kann die Versionsreihenfolge über beide Raster hinweg beibehalten werden.	Für die CloudMirror-Replikation sind keine Buckets mit aktivierter Versionierung erforderlich, daher kann CloudMirror nur die Reihenfolge für einen Schlüssel innerhalb einer Site aufrechterhalten. Es gibt keine Garantie dafür, dass die Reihenfolge bei Anfragen an ein Objekt an einem anderen Standort beibehalten wird.

	Cross-Grid-Replikation	CloudMirror-Replikationsdienst
Was passiert, wenn ein Objekt nicht repliziert werden kann?	Das Objekt wird zur Replikation in die Warteschlange gestellt und unterliegt den Speicherbeschränkungen für Metadaten.	Das Objekt wird zur Replikation in die Warteschlange gestellt, vorbehaltlich der Beschränkungen der Plattformdienste (siehe"Empfehlungen zur Nutzung von Plattformdiensten").
Werden die Systemmetadaten des Objekts repliziert?	Ja, wenn ein Objekt in das andere Raster repliziert wird, werden auch seine Systemmetadaten repliziert. Die Metadaten sind auf beiden Rastern identisch.	Nein, wenn ein Objekt in den externen Bucket repliziert wird, werden seine Systemmetadaten aktualisiert. Die Metadaten unterscheiden sich je nach Standort, abhängig vom Zeitpunkt der Aufnahme und dem Verhalten der unabhängigen S3-Infrastruktur.
Wie werden Objekte abgerufen?	Anwendungen können Objekte abrufen oder lesen, indem sie eine Anforderung an den Bucket in einem der Raster senden.	Anwendungen können Objekte abrufen oder lesen, indem sie eine Anfrage entweder an StorageGRID oder an das S3-Ziel senden. Angenommen, Sie verwenden die CloudMirror-Replikation, um Objekte in eine Partnerorganisation zu spiegeln. Der Partner kann seine eigenen Anwendungen verwenden, um Objekte direkt vom S3-Ziel zu lesen oder zu aktualisieren. Die Verwendung von StorageGRID ist nicht erforderlich.
Was passiert, wenn ein Objekt gelöscht wird?	• Löschanforderungen, die eine Versions-ID enthalten, werden nie in das Zielraster repliziert. • Löschanforderungen ohne Versions-ID fügen dem Quell-Bucket eine Löschmarkierung hinzu, die optional in das Zielraster repliziert werden kann. • Wenn die Cross-Grid-Replikation nur für eine Richtung konfiguriert ist, können Objekte im Ziel-Bucket gelöscht werden, ohne dass dies Auswirkungen auf die Quelle hat.	Die Ergebnisse variieren je nach Versionsstatus der Quell- und Ziel-Buckets (die nicht identisch sein müssen): • Wenn beide Buckets versioniert sind, wird bei einer Löschanforderung an beiden Stellen eine Löschmarkierung hinzugefügt. • Wenn nur der Quell-Bucket versioniert ist, fügt eine Löschanforderung der Quelle, aber nicht dem Ziel eine Löschmarkierung hinzu. • Wenn keiner der Buckets versioniert ist, löscht eine Löschanforderung das Objekt aus der Quelle, aber nicht aus dem Ziel. Ebenso können Objekte im Ziel-Bucket gelöscht werden, ohne dass dies Auswirkungen auf die Quelle hat.

Erstellen von Grid-Föderationsverbindungen

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

Wie in der Abbildung gezeigt, umfasst das Erstellen einer Grid-Föderationsverbindung Schritte auf beiden Grids. Sie fügen die Verbindung auf einem Raster hinzu und vervollständigen sie auf dem anderen Raster. Sie können von jedem Raster aus beginnen.



Bevor Sie beginnen

- Sie haben die"Überlegungen und Anforderungen" zum Konfigurieren von Grid-Föderation-Verbindungen.
- Wenn Sie für jedes Grid vollqualifizierte Domänennamen (FQDNs) anstelle von IP- oder VIP-Adressen verwenden möchten, wissen Sie, welche Namen Sie verwenden müssen, und Sie haben bestätigt, dass der DNS-Server für jedes Grid über die entsprechenden Einträge verfügt.
- Sie verwenden eine"unterstützter Webbrowser" .
- Sie verfügen über Root-Zugriffsberechtigung und die Bereitstellungspassphrase für beide Grids.

Verbindung hinzufügen

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

Schritte

1. Sign in .
2. Wählen Sie **KONFIGURATION** > **System** > **Grid-Föderation**.
3. Wählen Sie **Verbindung hinzufügen**.
4. Geben Sie Details für die Verbindung ein.

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

Feld	Beschreibung
FQDN oder IP für dieses Grid	Eine der folgenden Optionen: • Der FQDN des Grids, bei dem Sie derzeit angemeldet sind • Eine VIP-Adresse einer HA-Gruppe in diesem Grid • Eine IP-Adresse eines Admin-Knotens oder Gateway-Knotens in diesem Grid. Die IP kann sich in jedem Netzwerk befinden, das das Zielnetz erreichen kann.
Hafen	Der Port, den Sie für diese Verbindung verwenden möchten. Sie können jede nicht verwendete Portnummer zwischen 23000 und 23999 eingeben. Beide Grids verwenden in dieser Verbindung denselben Port. Sie müssen sicherstellen, dass kein Knoten in einem der Grids diesen Port für andere Verbindungen verwendet.
Zertifikat gültige Tage für dieses Raster	Die Anzahl der Tage, die die Sicherheitszertifikate für dieses Grid in der Verbindung gültig sein sollen. Der Standardwert beträgt 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.
Bereitstellungspassphrase für dieses Raster	Die Bereitstellungspassphrase für das Grid, bei dem Sie angemeldet sind.
FQDN oder IP für das andere Grid	Eine der folgenden Optionen: • Der FQDN des Grids, mit dem Sie sich verbinden möchten • Eine VIP-Adresse einer HA-Gruppe im anderen Grid • Eine IP-Adresse eines Admin-Knotens oder Gateway-Knotens im anderen Grid. Die IP kann sich in jedem Netzwerk befinden, das das Quellraster erreichen kann.

5. Wählen Sie **Speichern und fortfahren**.
6. Wählen Sie für den Schritt „Bestätigungsdatei herunterladen“ die Option „Bestätigungsdatei herunterladen“ aus.

   Nachdem die Verbindung im anderen Grid hergestellt wurde, können Sie die Bestätigungsdatei von keinem Grid mehr 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 übertragen werden.

8. Wählen Sie **Schließen**, um zur Grid-Föderationsseite zurückzukehren.
9. Bestätigen Sie, dass die neue Verbindung angezeigt wird und dass ihr **Verbindungsstatus Warten auf Verbindung** lautet.
10. Geben Sie die *connection-name*`.grid-federation` Datei an den Grid-Administrator für das andere Grid.

Vollständige Verbindung

Führen Sie diese Schritte auf dem StorageGRID -System aus, mit dem Sie eine Verbindung herstellen (dem anderen Grid).

Schritte

1. Sign in .
2. Wählen Sie **KONFIGURATION** > **System** > **Grid-Föderation**.
3. Wählen Sie **Bestätigungsdatei hochladen**, um auf die Upload-Seite zuzugreifen.
4. Wählen Sie **Verifizierungsdatei 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 zur Verbindung werden angezeigt.

5. Geben Sie optional eine andere Anzahl gültiger Tage für die Sicherheitszertifikate dieses Rasters ein. Der Eintrag **Gültigkeitstage des Zertifikats** entspricht standardmäßig dem Wert, den Sie im ersten Raster eingegeben haben, aber für jedes Raster können unterschiedliche Ablaufdaten verwendet werden.

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

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

6. Geben Sie die Bereitstellungspassphrase für das Grid ein, bei dem Sie derzeit angemeldet sind.
7. Wählen Sie **Speichern und testen**.

   Die Zertifikate werden generiert und die Verbindung getestet. Wenn die Verbindung gültig ist, wird eine Erfolgsmeldung angezeigt und die neue Verbindung wird auf der Grid-Föderationsseite aufgeführt. Der **Verbindungsstatus** lautet **Verbunden**.

   Wenn eine Fehlermeldung angezeigt wird, beheben Sie alle Probleme. Sehen "Beheben von Grid-Föderationsfehlern" .

8. Gehen Sie zur Grid-Föderationsseite im ersten Grid und aktualisieren Sie den Browser. Bestätigen Sie, dass der **Verbindungsstatus** jetzt **Verbunden** ist.
9. Nachdem die Verbindung hergestellt wurde, löschen Sie alle Kopien der Verifizierungsdatei sicher.

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

Nach Abschluss

- Überprüfen Sie die Überlegungen für"Verwaltung zugelassener Mieter" .

- "Erstellen Sie ein oder mehrere neue Mandantenkonten", weisen Sie die Berechtigung **Grid-Föderationsverbindung verwenden** zu und wählen Sie die neue Verbindung aus.
- "Verwalten der Verbindung"nach Bedarf. Sie können Verbindungswerte bearbeiten, eine Verbindung testen, Verbindungszertifikate rotieren oder eine Verbindung entfernen.
- "Überwachen Sie die Verbindung"als Teil Ihrer normalen StorageGRID Überwachungsaktivitäten.
- "Beheben Sie Verbindungsprobleme", einschließlich der Behebung aller Warnungen und Fehler im Zusammenhang mit dem Klonen von Konten und der Cross-Grid-Replikation.

Grid-Föderationsverbindungen verwalten

Die Verwaltung von Grid-Föderationsverbindungen zwischen StorageGRID -Systemen umfasst das Bearbeiten von Verbindungsdetails, das Rotieren der Zertifikate, das Entfernen von Mandantenberechtigungen und das Entfernen nicht verwendeter Verbindungen.

Bevor Sie beginnen

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

Bearbeiten einer Grid-Föderation-Verbindung

Sie können eine Grid-Föderationsverbindung bearbeiten, indem Sie sich beim primären Admin-Knoten auf einem der Grids in 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 für Kontoklon- oder Cross-Grid-Replikationsanforderungen weiterhin die vorhandenen Verbindungseinstellungen verwendet. Alle Änderungen, die Sie am ersten Raster vornehmen, werden lokal gespeichert, aber erst verwendet, wenn sie in das zweite Raster hochgeladen, gespeichert und getestet wurden.

Beginnen Sie mit der Bearbeitung der Verbindung

Schritte

1. Sign in .
2. Wählen Sie **NODES** und bestätigen Sie, dass alle anderen Admin-Knoten in Ihrem System online sind.

> ⓘ Wenn Sie eine Grid-Föderationsverbindung bearbeiten, versucht StorageGRID , eine „Kandidatenkonfigurationsdatei“ auf allen Admin-Knoten im ersten Grid zu speichern. Wenn diese Datei nicht auf allen Admin-Knoten gespeichert werden kann, wird eine Warnmeldung angezeigt, wenn Sie **Speichern und testen** auswählen.

3. Wählen Sie **KONFIGURATION** > **System** > **Grid-Föderation**.
4. Bearbeiten Sie die Verbindungsdetails mithilfe des Menüs **Aktionen** auf der Grid-Föderationsseite oder der Detailseite für eine bestimmte Verbindung. Sehen"Erstellen von Grid-Föderationsverbindungen" für was eingegeben werden soll.

Menü „Aktionen“

a. Wählen Sie das Optionsfeld für die Verbindung aus.
b. Wählen Sie **Aktionen** > **Bearbeiten**.
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 Bereitstellungspassphrase für das Grid ein, bei dem Sie angemeldet sind.
6. Wählen Sie **Speichern und fortfahren**.

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

7. Wählen Sie **Bestätigungsdatei herunterladen**.

   Um diese Datei zu einem späteren Zeitpunkt herunterzuladen, gehen Sie auf die Detailseite der Verbindung.

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

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

9. Wählen Sie **Schließen**, um zur Grid-Föderationsseite zurückzukehren.
10. Bestätigen Sie, dass der **Verbindungsstatus Bearbeitung ausstehend** ist.

    Wenn der Verbindungsstatus beim Beginn der Bearbeitung der Verbindung nicht „**Verbunden**“ war, ändert er sich nicht in „**Bearbeitung ausstehend**“.

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

Beenden Sie die Bearbeitung der Verbindung

Schließen Sie die Bearbeitung der Verbindung ab, indem Sie die Bestätigungsdatei in das andere Raster hochladen.

Schritte

1. Sign in .
2. Wählen Sie **KONFIGURATION** > **System** > **Grid-Föderation**.
3. Wählen Sie **Bestätigungsdatei hochladen**, um auf die Upload-Seite zuzugreifen.
4. Wählen Sie **Verifizierungsdatei hochladen**. Navigieren Sie dann zu der Datei, die aus dem ersten Raster heruntergeladen wurde, und wählen Sie sie aus.

5. Geben Sie die Bereitstellungspassphrase für das Grid ein, bei dem Sie derzeit angemeldet sind.
6. Wählen Sie **Speichern und testen**.

   Wenn die Verbindung mit den bearbeiteten Werten hergestellt werden kann, erscheint eine Erfolgsmeldung. Andernfalls erscheint eine Fehlermeldung. Überprüfen Sie die Nachricht und beheben Sie etwaige Probleme.

7. Schließen Sie den Assistenten, um zur Grid-Föderationsseite zurückzukehren.
8. Bestätigen Sie, dass der **Verbindungsstatus Verbunden** ist.
9. Gehen Sie zur Grid-Föderationsseite im ersten Grid und aktualisieren Sie den Browser. Bestätigen Sie, dass der **Verbindungsstatus** jetzt **Verbunden** ist.
10. Nachdem die Verbindung hergestellt wurde, löschen Sie alle Kopien der Verifizierungsdatei sicher.

Testen Sie eine Grid-Föderation-Verbindung

Schritte

1. Sign in .
2. Wählen Sie **KONFIGURATION** > **System** > **Grid-Föderation**.
3. Testen Sie die Verbindung mithilfe des Menüs **Aktionen** auf der Grid-Föderationsseite oder der Detailseite für eine bestimmte Verbindung.

   Menü „Aktionen“

   a. Wählen Sie das Optionsfeld für die Verbindung aus.

   b. Wählen Sie **Aktionen** > **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 verbunden und kommunizieren normal.
Fehler	Die Verbindung befindet sich in einem Fehlerzustand. Beispielsweise ist ein Zertifikat abgelaufen oder ein Konfigurationswert ist nicht mehr gültig.
Ausstehende Bearbeitung	Sie haben die Verbindung in diesem Raster bearbeitet, aber die Verbindung verwendet immer noch die vorhandene Konfiguration. Um die Bearbeitung abzuschließen, laden Sie die neue Verifizierungsdatei in das andere Raster hoch.

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

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

Verbindungszertifikate rotieren

Jede Grid-Föderation-Verbindung verwendet vier automatisch generierte SSL-Zertifikate, um die Verbindung zu sichern. Wenn sich das Ablaufdatum der beiden Zertifikate für jedes Grid nähert, werden Sie durch die Warnung **Ablauf des Grid-Föderationszertifikats** daran erinnert, die Zertifikate zu rotieren.

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

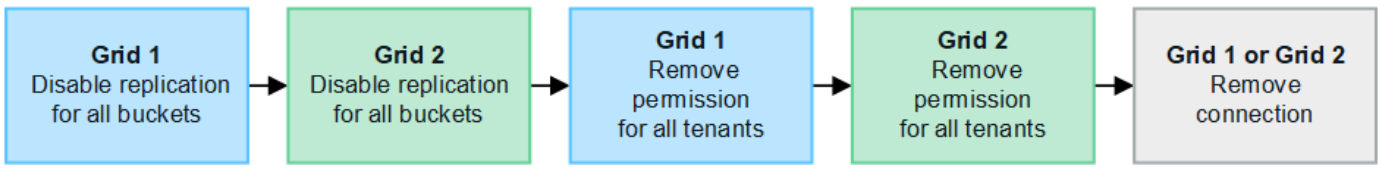
Schritte

1. Sign in .
2. Wählen Sie **KONFIGURATION** > **System** > **Grid-Föderation**.
3. Wählen Sie auf einer der Registerkarten der Grid-Föderationsseite den Verbindungsnamen aus, um dessen Details anzuzeigen.
4. Wählen Sie die Registerkarte **Zertifikate**.
5. Wählen Sie **Zertifikate rotieren**.
6. Geben Sie an, wie viele Tage die neuen Zertifikate gültig sein sollen.
7. Geben Sie die Bereitstellungspassphrase für das Grid ein, bei dem Sie angemeldet sind.
8. Wählen Sie **Zertifikate rotieren**.
9. Wiederholen Sie diese Schritte bei Bedarf auf dem anderen Raster in der Verbindung.

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

Entfernen Sie eine Grid-Föderation-Verbindung

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



Beachten Sie vor dem Entfernen einer Verbindung Folgendes:

- Durch das Entfernen einer Verbindung werden keine Elemente gelöscht, die bereits zwischen Rastern kopiert wurden. Beispielsweise werden Mandantenbenutzer, -gruppen und -objekte, die in beiden Rastern vorhanden sind, aus keinem der Raster 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, schlägt die Replikation aller Objekte, deren Replikation aussteht (aufgenommen, aber noch nicht in das andere Grid repliziert), dauerhaft fehl.

Deaktivieren Sie die Replikation für alle Mandanten-Buckets

Schritte

1. Melden Sie sich von einem der beiden Raster aus vom primären Admin-Knoten aus beim Grid Manager an.
2. Wählen Sie **KONFIGURATION** > **System** > **Grid-Föderation**.
3. Wählen Sie den Verbindungsnamen aus, um dessen Details anzuzeigen.
4. Stellen Sie auf der Registerkarte **Zulässige Mandanten** fest, ob die Verbindung von Mandanten verwendet wird.
5. Wenn Mieter aufgeführt sind, weisen Sie alle Mieter an,"Deaktivieren Sie die Cross-Grid-Replikation" für alle ihre Buckets auf beiden Grids in der Verbindung.

> Sie können die Berechtigung **Grid-Föderationsverbindung verwenden** nicht entfernen, wenn für Mandanten-Buckets die Cross-Grid-Replikation aktiviert ist. Jedes Mandantenkonto muss die Cross-Grid-Replikation für seine Buckets auf beiden Grids deaktivieren.

Entfernen Sie die Berechtigung für jeden Mandanten

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

Schritte

1. Wählen Sie **KONFIGURATION** > **System** > **Grid-Föderation**.
2. Wählen Sie den Verbindungsnamen aus, um dessen Details anzuzeigen.
3. Entfernen Sie für jeden Mandanten auf der Registerkarte **Zulässige Mandanten** die Berechtigung **Grid-Föderationsverbindung verwenden**. Sehen "Zulässige Mandanten verwalten" .
4. Wiederholen Sie diese Schritte für die zulässigen Mieter im anderen Raster.

Verbindung entfernen

Schritte

1. Wenn in keinem der Grids ein Mandant die Verbindung nutzt, wählen Sie **Entfernen**.
2. Überprüfen Sie die Bestätigungsnachricht und wählen Sie **Entfernen**.
   - Wenn die Verbindung getrennt werden kann, wird eine Erfolgsmeldung angezeigt. Die Grid-Föderation-Verbindung wird nun aus beiden Grids entfernt.
   - Wenn die Verbindung nicht entfernt werden kann (z. B. weil sie noch verwendet wird oder ein Verbindungsfehler vorliegt), wird eine Fehlermeldung angezeigt. Sie können einen der folgenden Schritte ausführen:

- Beheben Sie den Fehler (empfohlen). Sehen "Beheben von Grid-Föderationsfehlern" .
- Trennen Sie die Verbindung mit Gewalt. Siehe den nächsten Abschnitt.

Entfernen Sie eine Grid-Föderation-Verbindung mit Gewalt

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

Durch das erzwungene Entfernen wird lediglich die Verbindung aus dem lokalen Netz gelöscht. Um die Verbindung vollständig zu entfernen, führen Sie auf beiden Gittern die gleichen Schritte aus.

Schritte

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

   Es erscheint eine Erfolgsmeldung. Diese Grid-Föderation-Verbindung kann nicht mehr genutzt werden. Allerdings ist für Mandanten-Buckets möglicherweise noch immer die Cross-Grid-Replikation aktiviert und einige Objektkopien wurden möglicherweise bereits zwischen den Grids in der Verbindung repliziert.

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

Verwalten der zulässigen Mandanten für die Grid-Föderation

Sie können S3-Mandantenkonten die Verwendung einer Grid-Föderationsverbindung zwischen zwei StorageGRID Systemen erlauben. Wenn Mietern die Nutzung einer Verbindung gestattet wird, sind spezielle Schritte erforderlich, um Mieterdetails zu bearbeiten oder die Berechtigung eines Mieters zur Nutzung der Verbindung dauerhaft zu entfernen.

Bevor Sie beginnen

- Sie sind beim Grid Manager auf einem der beiden Grids mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" für das Raster, bei dem Sie angemeldet sind.
- Du hast"eine Grid-Föderation-Verbindung erstellt" zwischen zwei Gittern.
- Sie haben die Workflows für"Kontoklon" Und"Cross-Grid-Replikation" .
- Bei Bedarf haben Sie bereits Single Sign-On (SSO) oder die Identifizierungsföderation für beide Grids in der Verbindung konfiguriert. Sehen "Was ist ein Kontoklon?" .

Erstellen eines zulässigen Mandanten

Wenn Sie einem neuen oder bestehenden Mandantenkonto die Verwendung einer Grid-Föderationsverbindung für Kontoklone und Cross-Grid-Replikation erlauben möchten, folgen Sie den allgemeinen Anweisungen zum"Erstellen Sie einen neuen S3-Mandanten" oder"Bearbeiten eines Mieterkontos" und beachten Sie Folgendes:

- Sie können den Mandanten aus jedem Raster in der Verbindung erstellen. Das Raster, in dem ein Mandant erstellt wird, ist das *Quellraster des Mandanten*.

- Der Status der Verbindung muss **Verbunden** sein.
- Wenn der Mandant erstellt oder bearbeitet wird, um die Berechtigung **Grid-Föderationsverbindung verwenden** zu aktivieren, und dann im ersten Grid gespeichert wird, wird ein identischer Mandant automatisch in das andere Grid repliziert. Das Raster, in dem der Mandant repliziert wird, ist das *Zielraster des Mandanten*.
- Die Mandanten in beiden Grids verfügen über dieselbe 20-stellige Konto-ID, denselben Namen, dieselbe Beschreibung, dasselbe Kontingent und dieselben Berechtigungen. Optional können Sie das Feld **Beschreibung** verwenden, um zu ermitteln, welcher der Quellmandant und welcher der Zielmandant ist. Beispielsweise wird diese Beschreibung für einen in Grid 1 erstellten Mandanten auch für den in Grid 2 replizierten Mandanten angezeigt: „Dieser Mandant wurde in Grid 1 erstellt.“
- Aus Sicherheitsgründen wird das Passwort für einen lokalen Root-Benutzer nicht in das Ziel-Grid kopiert.

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

- Nachdem der neue oder bearbeitete Mandant in beiden Rastern verfügbar ist, können Mandantenbenutzer die folgenden Vorgänge ausführen:
  - Erstellen Sie aus dem Quellraster des Mandanten Gruppen und lokale Benutzer, die automatisch in das Zielraster des Mandanten geklont werden. Sehen "Mandantengruppen und Benutzer klonen" .
  - Erstellen Sie neue S3-Zugriffsschlüssel, die optional in das Zielraster des Mandanten geklont werden können. Sehen "Klonen Sie S3-Zugriffsschlüssel mithilfe der API" .
  - Erstellen Sie identische Buckets auf beiden Grids in der Verbindung und aktivieren Sie die Cross-Grid-Replikation in eine oder beide Richtungen. Sehen "Verwalten der Cross-Grid-Replikation" .

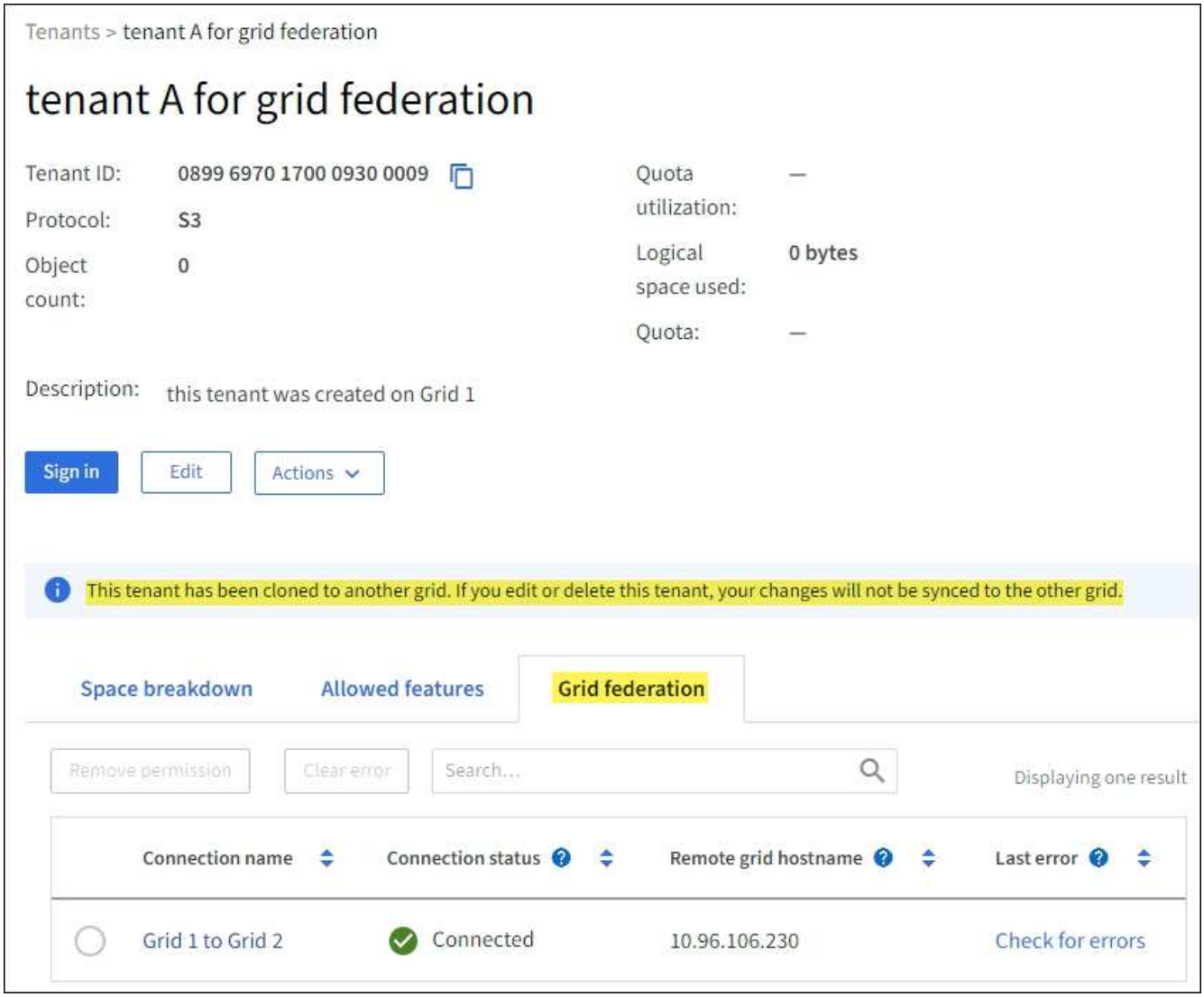
Anzeigen eines zulässigen Mandanten

Sie können Details zu einem Mandanten anzeigen, der eine Grid-Föderation-Verbindung verwenden darf.

Schritte

1. Wählen Sie **MIETER** aus.
2. Wählen Sie auf der Seite „Mandanten“ den Namen des Mandanten aus, um die Seite mit den Mieterdetails anzuzeigen.

   Wenn dies das Quellraster für den Mandanten ist (d. h., wenn der Mandant auf diesem Raster erstellt wurde), wird ein Banner angezeigt, das Sie daran erinnert, dass der Mandant in ein anderes 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-Föderation** aus, um"Überwachen Sie die Grid-Föderation-Verbindung" .

Bearbeiten eines zulässigen Mandanten

Wenn Sie einen Mandanten bearbeiten müssen, der über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, folgen Sie den allgemeinen Anweisungen für"Bearbeiten eines Mieterkontos" und beachten Sie Folgendes:

- Wenn ein Mandant über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, können Sie Mandantendetails von jedem Grid in der Verbindung aus bearbeiten. Von Ihnen vorgenommene Änderungen werden jedoch nicht in das andere Raster kopiert. Wenn Sie die Mieterdetails zwischen den Rastern synchron halten möchten, müssen Sie in beiden Rastern dieselben Änderungen vornehmen.
- Sie können die Berechtigung **Grid-Föderationsverbindung verwenden** nicht löschen, wenn Sie einen Mandanten bearbeiten.
- Sie können keine andere Grid-Föderation-Verbindung auswählen, wenn Sie einen Mandanten bearbeiten.

Löschen eines zulässigen Mandanten

Wenn Sie einen Mandanten entfernen müssen, der über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, folgen Sie den allgemeinen Anweisungen für"Löschen eines Mieterkontos" und beachten

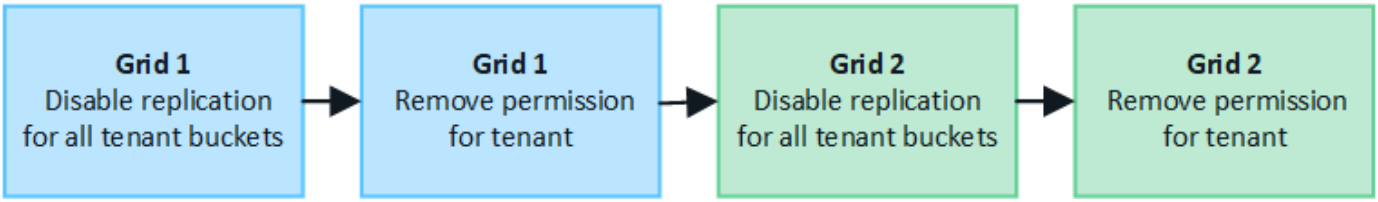
Sie Folgendes:

- 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 entweder den ursprünglichen oder den geklonten Mandanten entfernen, kann das Konto nicht mehr für die netzübergreifende Replikation verwendet werden.
- Wenn Sie den ursprünglichen Mandanten im Quellraster entfernen, bleiben alle Mandantengruppen, Benutzer oder Schlüssel, die in das Zielraster geklont wurden, davon unberührt. Sie können den geklonten Mandanten entweder löschen oder ihm erlauben, seine eigenen Gruppen, Benutzer, Zugriffsschlüssel und Buckets zu 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-Föderationsverbindung, bevor Sie den Mandanten aus diesem Grid löschen.

Entfernen Sie die Berechtigung „Grid-Föderationsverbindung verwenden“.

Um zu verhindern, dass ein Mandant eine Grid-Föderationsverbindung verwendet, müssen Sie die Berechtigung **Grid-Föderationsverbindung verwenden** entfernen.



Bevor Sie einem Mandanten die Berechtigung zur Verwendung einer Grid-Föderation-Verbindung entziehen, beachten Sie Folgendes:

- Sie können die Berechtigung **Grid-Föderationsverbindung verwenden** nicht entfernen, wenn für einen der Buckets des Mandanten die Cross-Grid-Replikation aktiviert ist. Das Mandantenkonto muss zuerst die Cross-Grid-Replikation für alle seine Buckets deaktivieren.
- Durch das Entfernen der Berechtigung **Grid-Föderationsverbindung verwenden** werden keine Elemente gelöscht, die bereits zwischen Grids repliziert wurden. Beispielsweise werden alle Mandantenbenutzer, -gruppen und -objekte, die in beiden Rastern vorhanden sind, nicht aus einem der Raster gelöscht, wenn die Berechtigung des Mandanten entfernt wird. Wenn Sie diese Elemente löschen möchten, müssen Sie sie manuell aus beiden Rastern löschen.
- Wenn Sie diese Berechtigung mit derselben Grid-Föderationsverbindung erneut aktivieren möchten, löschen Sie zuerst diesen Mandanten im Ziel-Grid. Andernfalls führt die erneute Aktivierung dieser Berechtigung zu einem Fehler.

> Durch erneutes Aktivieren der Berechtigung **Grid-Föderationsverbindung verwenden** wird das lokale Grid zum Quell-Grid und das Klonen in das Remote-Grid ausgelöst, das durch die ausgewählte Grid-Föderationsverbindung angegeben wird. Wenn das Mandantenkonto bereits im Remote-Raster vorhanden ist, führt das Klonen zu einem Konfliktfehler.

Bevor Sie beginnen

- Sie verwenden eine"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" für beide Gitter.

Deaktivieren der Replikation für Mandanten-Buckets

Deaktivieren Sie als ersten Schritt die Cross-Grid-Replikation für alle Mandanten-Buckets.

Schritte

1. Melden Sie sich von einem der beiden Raster aus vom primären Admin-Knoten aus beim Grid Manager an.
2. Wählen Sie **KONFIGURATION** > **System** > **Grid-Föderation**.
3. Wählen Sie den Verbindungsnamen aus, um dessen Details anzuzeigen.
4. Stellen Sie auf der Registerkarte **Zulässige Mandanten** fest, ob der Mandant die Verbindung verwendet.
5. Wenn der Mieter aufgeführt ist, weisen Sie ihn an,"Deaktivieren Sie die Cross-Grid-Replikation" für alle ihre Buckets auf beiden Grids in der Verbindung.

> Sie können die Berechtigung **Grid-Föderationsverbindung verwenden** nicht entfernen, wenn für Mandanten-Buckets die Cross-Grid-Replikation aktiviert ist. Der Mandant muss die Cross-Grid-Replikation für seine Buckets auf beiden Grids deaktivieren.

Berechtigung für Mandanten entfernen

Nachdem die Cross-Grid-Replikation für Mandanten-Buckets deaktiviert wurde, können Sie dem Mandanten die Berechtigung zur Verwendung der Grid-Föderationsverbindung entziehen.

Schritte

1. Sign in .
2. Entfernen Sie die Berechtigung von der Grid-Föderationsseite oder der Mandantenseite.

Grid-Föderationsseite

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

Mieterseite

a. Wählen Sie **MIETER** aus.
b. Wählen Sie den Namen des Mieters aus, um die Detailseite anzuzeigen.
c. Wählen Sie auf der Registerkarte **Grid-Föderation** 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, werden Sie zur Detailseite zurückgeleitet und es wird eine Erfolgsmeldung angezeigt. Dieser Mieter kann die Grid-Föderation-Verbindung nicht mehr nutzen.

◦ Wenn für einen oder mehrere Mandanten-Buckets noch immer die Cross-Grid-Replikation aktiviert ist, wird ein Fehler angezeigt.

Sie können einen der folgenden Schritte ausführen:

- (Empfohlen.) Sign in und deaktivieren Sie die Replikation für jeden Bucket des Mandanten. Sehen "Verwalten der Cross-Grid-Replikation" . Wiederholen Sie dann die Schritte, um die Berechtigung **Netzverbindung verwenden** zu entfernen.
- Entfernen Sie die Berechtigung mit Gewalt. Siehe den nächsten Abschnitt.

4. Gehen Sie zum anderen Raster und wiederholen Sie diese Schritte, um die Berechtigung für denselben Mandanten im anderen Raster zu entfernen.

Entfernen Sie die Berechtigung mit Gewalt

Bei Bedarf können Sie die Aufhebung der Berechtigung eines Mandanten zur Verwendung einer Grid-Föderationsverbindung erzwingen, auch wenn für Mandanten-Buckets die Grid-übergreifende Replikation aktiviert ist.

Bevor Sie einem Mieter die Erlaubnis mit Gewalt entziehen, beachten Sie die allgemeinen Überlegungen fürEntfernen der Berechtigung sowie diese zusätzlichen Überlegungen:

- Wenn Sie die Berechtigung **Grid-Föderationsverbindung verwenden** zwangsweise entfernen, werden alle Objekte, deren Replikation in das andere Grid aussteht (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 Grid entfernen.
- Alle Objekte, die in den Quell-Bucket aufgenommen werden, nachdem Sie die Berechtigung **Grid-Föderationsverbindung verwenden** entfernt haben, werden nie in den Ziel-Bucket repliziert.

Schritte

1. Sign in .
2. Wählen Sie **KONFIGURATION** > **System** > **Grid-Föderation**.
3. Wählen Sie den Verbindungsnamen aus, um die Detailseite anzuzeigen.
4. Wählen Sie auf der Registerkarte **Zulässige Mieter** das Optionsfeld für den Mieter aus.
5. Wählen Sie **Berechtigung entfernen**.
6. Überprüfen Sie die Warnungen im Bestätigungsdialogfeld und wählen Sie **Entfernen erzwingen**.

   Es erscheint eine Erfolgsmeldung. Dieser Mieter kann die Grid-Föderation-Verbindung nicht mehr nutzen.

7. Gehen Sie bei Bedarf zum anderen Raster und wiederholen Sie diese Schritte, um die Berechtigung für dasselbe Mandantenkonto im anderen Raster zwangsweise zu entfernen. Sie sollten diese Schritte beispielsweise auf dem anderen Raster wiederholen, um zu verhindern, dass Objekte im Prozess den Ziel-Bucket erreichen.

Beheben von Grid-Föderationsfehlern

Möglicherweise müssen Sie Warnungen und Fehler im Zusammenhang mit Grid-Föderationsverbindungen, Kontoklonen und Grid-übergreifender Replikation beheben.

Warnungen und Fehler bei der Grid-Föderation-Verbindung

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

Nachdem Sie Änderungen zur Behebung eines Verbindungsproblems vorgenommen haben, testen Sie die Verbindung, um sicherzustellen, dass der Verbindungsstatus wieder auf **Verbunden** zurückkehrt. Anweisungen hierzu finden Sie unter"Grid-Föderationsverbindungen verwalten" .

Warnung bei Verbindungsfehlern im Grid-Verbund

Ausgabe

Die Warnung **Fehler bei der Grid-Föderationsverbindung** wurde ausgelöst.

Details

Diese Warnung weist darauf hin, dass die Grid-Föderationsverbindung zwischen den Grids nicht funktioniert.

Empfohlene Maßnahmen

1. Überprüfen Sie die Einstellungen auf der Seite „Grid Federation“ für beide Grids. Bestätigen Sie, dass alle Werte korrekt sind. Sehen "Grid-Föderationsverbindungen verwalten" .
2. Überprüfen Sie die für die Verbindung verwendeten Zertifikate. Stellen Sie sicher, dass keine Warnungen für abgelaufene Grid-Föderation-Zertifikate vorliegen und dass die Details für jedes Zertifikat gültig sind. Die Anweisungen zum Rotieren von Verbindungszertifikaten finden Sie in"Grid-Föderationsverbindungen verwalten" .
3. Bestätigen Sie, dass alle Admin- und Gateway-Knoten in beiden Grids online und verfügbar sind. Beheben Sie alle Warnungen, die diese Knoten möglicherweise betreffen, und versuchen Sie es erneut.
4. Wenn Sie einen vollqualifizierten Domänennamen (FQDN) für das lokale oder Remote-Grid angegeben haben, bestätigen Sie, dass der DNS-Server online und verfügbar ist. Sehen"Was ist Grid-Föderation?" für Netzwerk-, IP-Adress- und DNS-Anforderungen.

Ablaufwarnung für Grid-Föderation-Zertifikat

Ausgabe

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

Details

Diese Warnung weist darauf hin, dass ein oder mehrere Grid-Föderationszertifikate bald ablaufen.

Empfohlene Maßnahmen

Die Anweisungen zum Rotieren von Verbindungszertifikaten finden Sie in"Grid-Föderationsverbindungen verwalten" .

Fehler beim Bearbeiten einer Grid-Föderation-Verbindung

Ausgabe

Beim Bearbeiten einer Grid-Föderation-Verbindung wird die folgende Warnmeldung angezeigt, wenn Sie **Speichern und testen** auswählen: „Fehler beim Erstellen einer Kandidatenkonfigurationsdatei auf einem oder mehreren Knoten.“

Details

Wenn Sie eine Grid-Föderationsverbindung bearbeiten, versucht StorageGRID , eine „Kandidatenkonfigurationsdatei“ auf allen Admin-Knoten im ersten Grid zu speichern. Eine Warnmeldung wird

angezeigt, wenn diese Datei nicht auf allen Admin-Knoten gespeichert werden kann, beispielsweise weil ein Admin-Knoten offline ist.

Empfohlene Maßnahmen

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

Fehler beim Klonen des Kontos

Anmeldung bei einem geklonten Mandantenkonto nicht möglich

Ausgabe

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

Details

Aus Sicherheitsgründen wird das von Ihnen für den lokalen Root-Benutzer des Mandanten festgelegte Kennwort nicht geklont, wenn ein Mandantenkonto vom Quellraster des Mandanten in das Zielraster des Mandanten geklont wird. Wenn ein Mandant lokale Benutzer in seinem Quellraster erstellt, werden die Kennwörter der lokalen Benutzer ebenfalls nicht in das Zielraster geklont.

Empfohlene Maßnahmen

Bevor sich der Root-Benutzer beim Ziel-Grid des Mandanten anmelden kann, muss ein Grid-Administrator zunächst"Ändern Sie das Passwort für den lokalen Root-Benutzer" auf dem Zielraster.

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

Mandant ohne Klon erstellt

Ausgabe

Sie sehen die Meldung „Mandant ohne Klon erstellt“, nachdem Sie einen neuen Mandanten mit der Berechtigung **Grid-Föderationsverbindung verwenden** erstellt haben.

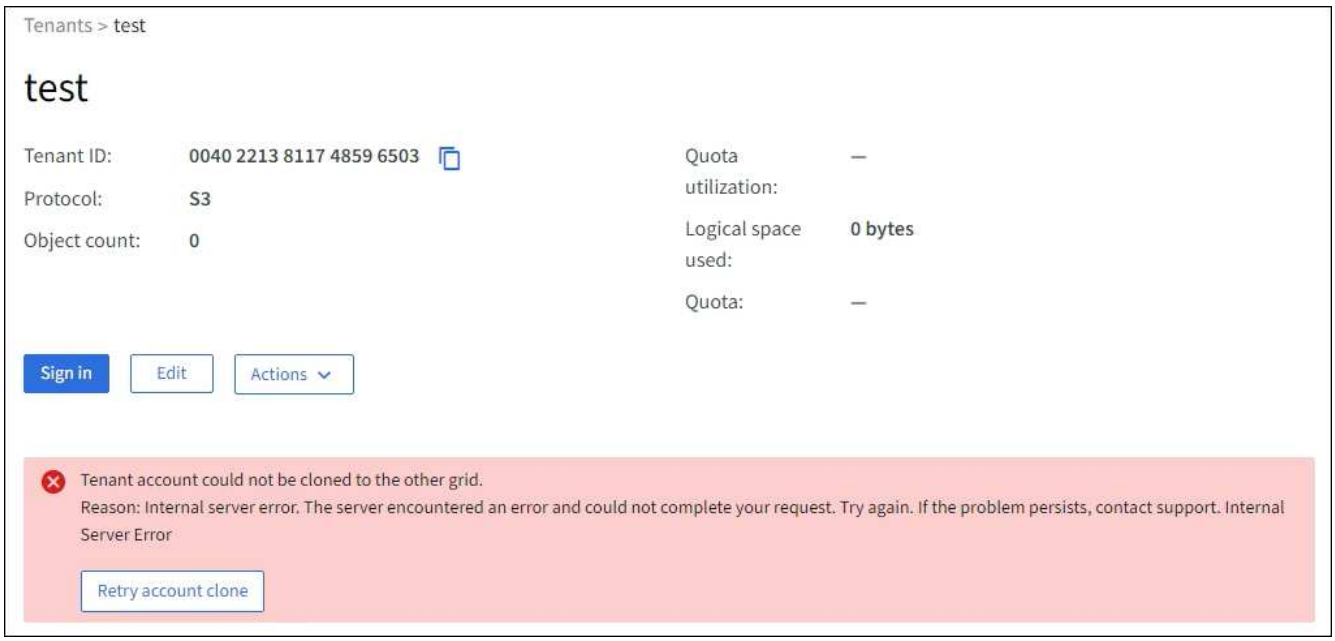
Details

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 sonstigen Probleme, die möglicherweise die Funktionsfähigkeit der Verbindung verhindern. Sehen Warnungen und Fehler bei der Grid-Föderation-Verbindung .
2. Folgen Sie den Anweisungen, um eine Grid-Föderation-Verbindung zu testen in"Grid-Föderationsverbindungen verwalten" um zu bestätigen, dass das Problem behoben wurde.
3. Wählen Sie im Quellraster des Mandanten **MIETER** aus.
4. Suchen Sie das Mandantenkonto, dessen Klonen fehlgeschlagen ist.

5. Wählen Sie den Mandantennamen aus, um die Detailseite anzuzeigen.
6. Wählen Sie **Kontoklon erneut versuchen**.



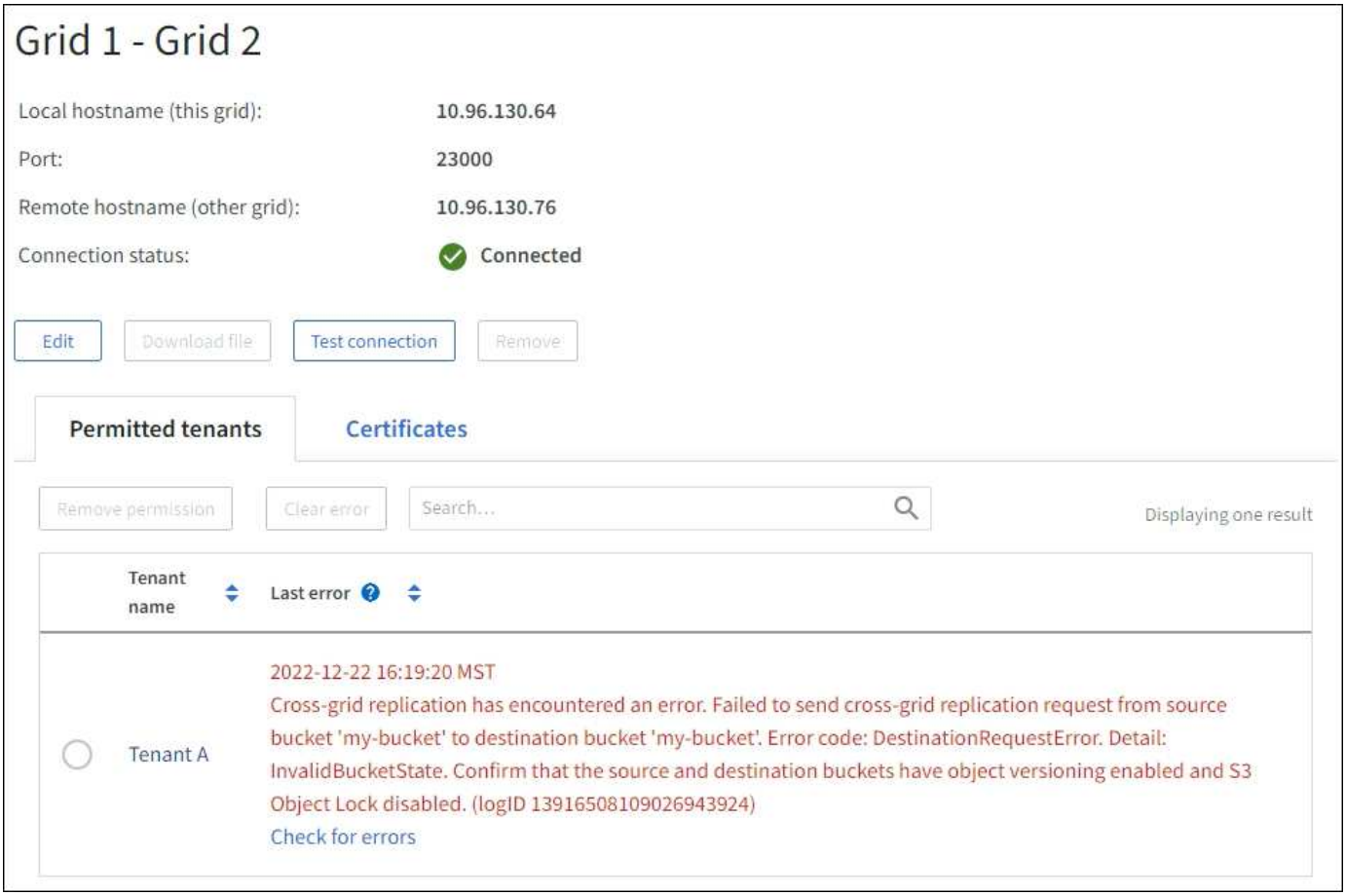
Wenn der Fehler behoben wurde, wird das Mandantenkonto nun in das andere Grid geklont.

Warnungen und Fehler bei der Grid-übergreifenden Replikation

Letzter angezeigter Fehler für Verbindung oder Mandant

Ausgabe

Wann"Anzeigen einer Grid-Föderation-Verbindung" (oder wenn"Verwaltung der zugelassenen Mieter" für eine Verbindung), bemerken Sie einen Fehler in der Spalte **Letzter Fehler** auf der Seite mit den Verbindungsdetails. Beispiel:



Details

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

- Die Quellobjektversion wurde nicht gefunden.
- Der Quell-Bucket wurde nicht gefunden.
- Der Ziel-Bucket wurde gelöscht.
- Der Ziel-Bucket wurde von einem anderen Konto neu erstellt.
- Die Versionsverwaltung des Ziel-Buckets ist ausgesetzt.
- Der Ziel-Bucket wurde vom selben Konto neu erstellt, ist jetzt aber nicht mehr versioniert.

Empfohlene Maßnahmen

Wenn in der Spalte **Letzter Fehler** eine Fehlermeldung angezeigt wird, gehen Sie folgendermaßen vor:

1. Überprüfen Sie den Nachrichtentext.
2. Führen Sie alle empfohlenen Aktionen aus. Wenn beispielsweise die Versionierung für den Ziel-Bucket für die Cross-Grid-Replikation ausgesetzt wurde, aktivieren Sie die Versionierung für diesen Bucket erneut.
3. Wählen Sie die Verbindung oder das Mandantenkonto aus der Tabelle aus.
4. Wählen Sie **Fehler löschen**.
5. Wählen Sie **Ja**, um die Nachricht zu löschen und den Systemstatus zu aktualisieren.

6. Warten Sie 5–6 Minuten und nehmen Sie dann einen neuen Gegenstand in den Eimer. Vergewissern Sie sich, dass die Fehlermeldung nicht erneut angezeigt wird.

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

   Nachdem Sie den Fehler behoben haben, wird möglicherweise ein neuer **Letzter Fehler** angezeigt, wenn Objekte in einem anderen Bucket aufgenommen werden, der ebenfalls einen Fehler aufweist.

7. Um festzustellen, ob Objekte aufgrund des Bucket-Fehlers nicht repliziert werden konnten, siehe"Identifizieren und wiederholen Sie fehlgeschlagene Replikationsvorgänge" .

Dauerhafter Fehleralarm bei Cross-Grid-Replikation

Ausgabe

Die Warnung **Dauerhafter Fehler bei der Cross-Grid-Replikation** wurde ausgelöst.

Details

Diese Warnung weist darauf hin, dass Mandantenobjekte aus einem Grund, für dessen Lösung ein Benutzereingriff erforderlich ist, nicht zwischen den Buckets auf zwei Grids repliziert werden können. Diese Warnung wird normalerweise durch eine Änderung am Quell- oder Ziel-Bucket verursacht.

Empfohlene Maßnahmen

1. Sign in , in dem die Warnung ausgelöst wurde.
2. Gehen Sie zu **KONFIGURATION** > **System** > **Grid-Föderation** und suchen Sie den in der Warnung aufgeführten Verbindungsnamen.
3. Sehen Sie sich auf der Registerkarte „Zulässige Mandanten“ die Spalte „Letzter Fehler“ an, um festzustellen, welche Mandantenkonten Fehler aufweisen.
4. Weitere Informationen zum Fehler finden Sie in den Anweisungen in"Überwachen von Grid-Föderation-Verbindungen" um die Cross-Grid-Replikationsmetriken zu überprüfen.
5. Für jedes betroffene Mandantenkonto:
   a. Die Anweisungen finden Sie in"Überwachen Sie die Mieteraktivität" um zu bestätigen, dass der Mandant sein Kontingent im Zielgrid für die Grid-übergreifende Replikation nicht überschritten hat.
   b. Erhöhen Sie bei Bedarf das Kontingent des Mandanten im Zielraster, um das Speichern neuer Objekte zu ermöglichen.
6. Melden Sie sich für jeden betroffenen Mandanten in beiden Rastern beim Mandanten-Manager an, damit Sie die Bucket-Liste vergleichen können.
7. Bestätigen Sie für jeden Bucket, für den die Cross-Grid-Replikation aktiviert ist, Folgendes:
   - Für denselben Mandanten gibt es im anderen Raster einen entsprechenden Bucket (der genaue Name muss verwendet werden).
   - Für beide Buckets ist die Objektversionierung aktiviert (die Versionierung kann in keinem der Grids ausgesetzt werden).
   - Bei beiden Buckets ist die S3-Objektsperre deaktiviert.
   - Keiner der Buckets befindet sich im Status **Objekte werden gelöscht: schreibgeschützt**.
8. Um zu bestätigen, dass das Problem behoben wurde, lesen Sie die Anweisungen in"Überwachen von Grid-Föderation-Verbindungen" um die Metriken der Cross-Grid-Replikation zu überprüfen, oder führen Sie

diese Schritte aus:

a. Gehen Sie zurück zur Grid-Föderationsseite.

b. Wählen Sie den betroffenen Mandanten aus und wählen Sie in der Spalte **Letzter Fehler** die Option **Fehler löschen**.

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

d. Warten Sie 5–6 Minuten und nehmen Sie dann einen neuen Gegenstand in den Eimer. Vergewissern Sie sich, dass die Fehlermeldung nicht erneut angezeigt wird.

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

> Nach der Lösung des Alarms kann es bis zu einem Tag dauern, bis dieser gelöscht wird.

a. Gehe zu"Identifizieren und wiederholen Sie fehlgeschlagene Replikationsvorgänge" um alle Objekte zu identifizieren oder Markierungen zu löschen, die nicht in das andere Raster repliziert werden konnten, und um die Replikation bei Bedarf erneut zu versuchen.

Warnung: Gridübergreifende Replikationsressource nicht verfügbar

Ausgabe

Die Warnung **Gridübergreifende Replikationsressource nicht verfügbar** wurde ausgelöst.

Details

Diese Warnung weist darauf hin, dass Grid-übergreifende Replikationsanforderungen ausstehen, weil eine Ressource nicht verfügbar ist. Beispielsweise könnte ein Netzwerkfehler vorliegen.

Empfohlene Maßnahmen

1. Überwachen Sie die Warnung, um zu sehen, ob sich das Problem von selbst löst.
2. Wenn das Problem weiterhin besteht, ermitteln Sie, ob für eines der Grids eine Warnung „Fehler bei der Grid-Föderationsverbindung“ für dieselbe Verbindung oder eine Warnung „Kommunikation mit Knoten nicht möglich“ für einen Knoten vorliegt. Diese Warnung kann möglicherweise behoben werden, wenn Sie diese Warnungen beheben.
3. Weitere Informationen zum Fehler finden Sie in den Anweisungen in"Überwachen von Grid-Föderation-Verbindungen" um die Cross-Grid-Replikationsmetriken zu überprüfen.
4. Wenn Sie die Warnung nicht beheben können, wenden Sie sich an den technischen Support.

Die Cross-Grid-Replikation wird nach der Lösung des Problems wie gewohnt fortgesetzt.

Identifizieren und wiederholen Sie fehlgeschlagene Replikationsvorgänge

Nachdem Sie die Warnung „Dauerhafter Fehler bei der gitterübergreifenden Replikation“ behoben haben, sollten Sie feststellen, ob bei der Replikation von Objekten oder Löschmarkierungen in das andere Gitter ein Fehler aufgetreten ist. Sie können diese Objekte dann erneut aufnehmen oder die Grid Management-API verwenden, um die Replikation erneut zu versuchen.

Die Warnung **Dauerhafter Fehler bei der gitterübergreifenden Replikation** weist darauf hin, dass

Mandantenobjekte aus einem Grund, für dessen Lösung ein Benutzereingriff erforderlich ist, nicht zwischen den Buckets auf zwei Gittern repliziert werden können. Diese Warnung wird normalerweise durch eine Änderung am Quell- oder Ziel-Bucket verursacht. Weitere Informationen finden Sie unter "Beheben von Grid-Föderationsfehlern" .

Ermitteln Sie, ob bei der Replikation von Objekten Fehler aufgetreten sind.

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

Sie können die"Audit-Erklärtool" um die Ergebnisse in ein leichter lesbares Format zu übersetzen.

Bevor Sie beginnen

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

Schritte

1. Melden Sie sich beim primären Admin-Knoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

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

2. Durchsuchen Sie das Audit.log nach CGRR-Nachrichten und formatieren Sie die Ergebnisse mit dem Audit-Explain-Tool.

   Dieser Befehl sucht beispielsweise nach allen CGRR-Nachrichten der letzten 30 Minuten und verwendet das Tool „Audit-Explain“.

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

   Die Ergebnisse des Befehls sehen wie in diesem Beispiel aus, das Einträge für sechs CGRR-Nachrichten enthält. Im Beispiel gaben alle Cross-Grid-Replikationsanforderungen einen allgemeinen Fehler zurück, da das Objekt nicht repliziert werden konnte. Die ersten drei Fehler betreffen Vorgänge zum Replizieren von Objekten und die letzten drei Fehler betreffen Vorgänge zum Replizieren von Löschmarkierungen.

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

Jeder Eintrag enthält die folgenden Informationen:

Feld	Beschreibung
CGRR Cross-Grid-Replikationsanforderung	Der Name der Anfrage
Mieter	Die Konto-ID des Mieters
Verbindung	Die ID der Grid-Föderation-Verbindung
Betrieb	Der Typ des Replikationsvorgangs, der versucht wurde: • 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 Cross-Grid-Replikation fehlgeschlagen ist, lautet der Fehler „Allgemeiner Fehler“.

Wiederholen Sie fehlgeschlagene Replikationen

Nachdem Sie eine Liste der Objekte und Löschmarkierungen erstellt haben, die nicht in den Ziel-Bucket repliziert wurden, und die zugrunde liegenden Probleme behoben haben, 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 und dann **API-Dokumentation** aus.
2. Wählen Sie **Zur privaten API-Dokumentation gehen**.

   Die als „Privat“ gekennzeichneten StorageGRID -API-Endpunkte können ohne vorherige Ankündigung geändert werden. Private StorageGRID Endpunkte ignorieren auch die API-Version der Anfrage.

3. Wählen Sie im Abschnitt **cross-grid-replication-advanced** den folgenden Endpunkt aus:

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

4. Wählen Sie **Ausprobieren**.
5. Ersetzen Sie im Textfeld **body** den Beispieleintrag für **versionID** durch eine Versions-ID aus dem Audit-Log, die einer fehlgeschlagenen Cross-Grid-Replikationsanforderung entspricht.

   Achten Sie darauf, die doppelten Anführungszeichen um die Zeichenfolge beizubehalten.

6. Wählen Sie **Ausführen**.
7. Bestätigen Sie, dass der Serverantwortcode **204** lautet. Dies bedeutet, dass das Objekt oder die Löschmarkierung für die Cross-Grid-Replikation in das andere Grid als ausstehend markiert wurde.

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

Überwachen von Replikationswiederholungen

Sie sollten die Wiederholungsvorgänge der Replikation überwachen, um sicherzustellen, dass sie abgeschlossen werden.

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

Sie können Wiederholungsvorgänge auf zwei Arten überwachen:

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

Netz	Replikationsstatus
Quelle	• **ABGESCHLOSSEN**: Die Replikation war erfolgreich. • **AUSSTEHEND**: Das Objekt wurde noch nicht repliziert. • **FEHLER**: Die Replikation ist mit einem dauerhaften Fehler fehlgeschlagen. Der Fehler muss von einem Benutzer behoben werden.
Ziel	**REPLICA**: 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 **Ausprobieren**.
3. Geben Sie im Abschnitt „Parameter“ die Versions-ID ein, die Sie in der `cross-grid-replication-retry-failed` Anfrage.
4. Wählen Sie **Ausführen**.
5. Bestätigen Sie, dass der Serverantwortcode **200** ist.
6. Überprüfen Sie den Replikationsstatus. Dieser kann einer der folgenden sein:
   - **AUSSTEHEND**: Das Objekt wurde noch nicht repliziert.
   - **ABGESCHLOSSEN**: Die Replikation war erfolgreich.
   - **FEHLGESCHLAGEN**: Die Replikation ist mit einem dauerhaften Fehler fehlgeschlagen. Der Fehler muss von einem Benutzer behoben werden.

Verwalten der Sicherheit

Verwalten der Sicherheit

Sie können im Grid Manager verschiedene Sicherheitseinstellungen konfigurieren, um Ihr StorageGRID -System zu sichern.

Verwalten der Verschlüsselung

StorageGRID bietet mehrere Optionen zum Verschlüsseln von Daten. Du solltest"Überprüfen Sie die verfügbaren Verschlüsselungsmethoden" um festzustellen, welche Ihren Datenschutzanforderungen entsprechen.

Zertifikate verwalten

Du kannst"Konfigurieren und Verwalten der Serverzertifikate" Wird für HTTP-Verbindungen oder die Client-Zertifikate verwendet, um eine Client- oder Benutzeridentität gegenüber dem Server zu authentifizieren.

Konfigurieren von Schlüsselverwaltungsservern

Mit einem"Schlüsselverwaltungsserver" ermöglicht Ihnen den Schutz von StorageGRID -Daten, selbst wenn ein Gerät aus dem Rechenzentrum entfernt wird. Nachdem die Appliance-Volumes verschlüsselt wurden, können Sie auf keine Daten auf der Appliance zugreifen, es sei denn, der Knoten kann mit dem KMS kommunizieren.

> Um die Verschlüsselungsschlüsselverwaltung zu verwenden, müssen Sie während der Installation die Einstellung **Knotenverschlüsselung** für jede Appliance aktivieren, bevor die Appliance zum Grid hinzugefügt wird.

Proxy-Einstellungen verwalten

Wenn Sie S3-Plattformdienste oder Cloud Storage Pools verwenden, können Sie eine"Speicherproxyserver" zwischen Speicherknoten und den externen S3-Endpunkten. Wenn Sie AutoSupport -Pakete über HTTPS oder HTTP senden, können Sie eine"Admin-Proxyserver" zwischen Admin-Knoten und technischem Support.

Kontrollieren Sie Firewalls

Um die Sicherheit Ihres Systems zu erhöhen, können Sie den Zugriff auf StorageGRID Admin-Knoten steuern, indem Sie bestimmte Ports öffnen oder schließen."externe Firewall" . Sie können den Netzwerkzugriff auf jeden Knoten auch steuern, indem Sie seine"interne Firewall" . Sie können den Zugriff auf alle Ports verhindern, mit Ausnahme derjenigen, die für Ihre Bereitstellung erforderlich sind.

Überprüfen Sie die Verschlüsselungsmethoden von StorageGRID

StorageGRID bietet mehrere Optionen zum Verschlüsseln von Daten. Sie sollten die verfügbaren Methoden überprüfen, um festzustellen, welche Methoden Ihren Datenschutzanforderungen entsprechen.

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

Verschlüsselungsoption	So funktioniert es	Gilt für:
Schlüsselverwaltungsserver (KMS) im Grid Manager	Du"Konfigurieren eines Schlüsselverwaltungsservers" für die StorageGRID -Site und "Aktivieren Sie die Knotenverschlüsselung für die Appliance" . Anschließend stellt ein Appliance-Knoten eine Verbindung zum KMS her, um einen Schlüsselverschlüsselungsschlüssel (KEK) anzufordern. Dieser Schlüssel verschlüsselt und entschlüsselt den Datenverschlüsselungsschlüssel (DEK) auf jedem Volume.	Appliance-Knoten, bei denen während der Installation die **Knotenverschlüsselung** aktiviert wurde. Alle Daten auf dem Gerät sind vor physischem Verlust oder Entfernung aus dem Rechenzentrum geschützt. **Hinweis**: Die Verwaltung von Verschlüsselungsschlüsseln mit einem KMS wird nur für Speicherknoten und Service-Appliances unterstützt.
Seite „Laufwerkverschlüsselung“ im StorageGRID Appliance Installer	Wenn die Appliance Laufwerke enthält, die Hardwareverschlüsselung unterstützen, können Sie während der Installation eine Laufwerkspassphrase festlegen. Wenn Sie eine Laufwerkspassphrase festlegen, ist es für niemanden möglich, gültige Daten von Laufwerken wiederherzustellen, die aus dem System entfernt wurden, es sei denn, er kennt die Passphrase. Gehen Sie vor Beginn der Installation zu **Hardware konfigurieren** > **Laufwerkverschlüsselung**, um eine Laufwerkspassphrase festzulegen, die für alle von StorageGRID verwalteten, selbstverschlüsselnden Laufwerke in einem Knoten gilt.	Geräte, die selbstverschlüsselnde Laufwerke enthalten. Alle Daten auf den gesicherten Laufwerken sind vor physischem Verlust oder Entfernung aus dem Rechenzentrum geschützt. Die Laufwerkverschlüsselung gilt nicht für von SANtricity verwaltete Laufwerke. Wenn Sie über ein Speichergerät mit selbstverschlüsselnden Laufwerken und SANtricity Controllern verfügen, können Sie die Laufwerkssicherheit in SANtricity aktivieren.
Laufwerkssicherheit im SANtricity System Manager	Wenn die Funktion „Laufwerksicherheit“ für Ihr StorageGRID Gerät aktiviert ist, können Sie "SANtricity Systemmanager" um den Sicherheitsschlüssel zu erstellen und zu verwalten. Der Schlüssel wird benötigt, um auf die Daten auf den gesicherten Laufwerken zuzugreifen.	Speichergeräte mit Laufwerken mit vollständiger Festplattenverschlüsselung (FDE) oder selbstverschlüsselnden Laufwerken. Alle Daten auf den gesicherten Laufwerken sind vor physischem Verlust oder Entfernung aus dem Rechenzentrum geschützt. Kann nicht mit einigen Speichergeräten oder Servicegeräten verwendet werden.

Verschlüsselungsoption	So funktioniert es	Gilt für:
Gespeicherte Objektverschlüsselung	Sie aktivieren die"Gespeicherte Objektverschlüsselung" Option im Grid Manager. Wenn diese Option aktiviert ist, werden alle neuen Objekte, die nicht auf Bucket- oder Objektebene verschlüsselt sind, während der Aufnahme verschlüsselt.	Neu aufgenommene S3-Objektdaten. Vorhandene gespeicherte Objekte werden nicht verschlüsselt. Objektmetadaten und andere sensible Daten werden nicht verschlüsselt.
S3-Bucket-Verschlüsselung	Sie stellen eine PutBucketEncryption-Anforderung, um die Verschlüsselung für den Bucket zu aktivieren. Alle neuen Objekte, die nicht auf Objektebene verschlüsselt sind, werden während 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 an Buckets"
Serverseitige Verschlüsselung (SSE) für S3-Objekte	Sie stellen eine S3-Anforderung zum Speichern eines Objekts und schließen die `x-amz-server-side-encryption` Anforderungsheader.	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. "Verwenden Sie serverseitige Verschlüsselung"
Serverseitige Verschlüsselung von S3-Objekten mit vom Kunden bereitgestellten Schlüsseln (SSE-C)	Sie stellen eine S3-Anforderung zum Speichern eines Objekts und fügen drei Anforderungsheader ein. • `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 verwaltet. "Verwenden Sie serverseitige Verschlüsselung"

Verschlüsselungsoption	So funktioniert es	Gilt für:
Externe Volume- oder Datenspeicherverschlüsselung	Sie verwenden eine Verschlüsselungsmethode außerhalb von StorageGRID , um ein ganzes Volume oder einen ganzen Datenspeicher zu verschlüsseln, sofern Ihre Bereitstellungsplattform dies unterstützt.	Alle Objektdaten, Metadaten und Systemkonfigurationsdaten, vorausgesetzt, jedes Volume oder jeder Datenspeicher ist verschlüsselt. Eine externe Verschlüsselungsmethode bietet eine strengere Kontrolle über Verschlüsselungsalgorithmen und Schlüssel. Kann mit den anderen aufgeführten Methoden kombiniert werden.
Objektverschlüsselung außerhalb von StorageGRID	Sie verwenden eine Verschlüsselungsmethode außerhalb von StorageGRID , um Objektdaten und Metadaten zu verschlüsseln, bevor sie in StorageGRID aufgenommen werden.	Nur Objektdaten und Metadaten (Systemkonfigurationsdaten werden nicht verschlüsselt). Eine externe Verschlüsselungsmethode bietet eine strengere Kontrolle über Verschlüsselungsalgorithmen und Schlüssel. Kann mit den anderen aufgeführten Methoden kombiniert werden. "Amazon Simple Storage Service – Benutzerhandbuch: Schützen von Daten durch clientseitige Verschlüsselung"

Verwenden Sie mehrere Verschlüsselungsmethoden

Je nach Bedarf können Sie mehrere Verschlüsselungsmethoden gleichzeitig verwenden. Beispiel:

- Sie können ein KMS zum Schutz von Appliance-Knoten verwenden und außerdem die Laufwerkssicherheitsfunktion im SANtricity System Manager nutzen, um Daten auf den selbstverschlüsselnden Laufwerken in denselben Appliances „doppelt zu verschlüsseln“.
- Sie können ein KMS verwenden, um Daten auf Appliance-Knoten zu sichern, und außerdem die Option „Gespeicherte Objektverschlüsselung“ verwenden, um alle Objekte bei der Aufnahme zu verschlüsseln.

Wenn nur ein kleiner Teil Ihrer Objekte verschlüsselt werden muss, sollten Sie stattdessen die Steuerung der Verschlüsselung auf Bucket- oder Einzelobjektebene in Betracht ziehen. Das Aktivieren mehrerer Verschlüsselungsebenen geht mit zusätzlichen Leistungseinbußen einher.

Zertifikate verwalten

Sicherheitszertifikate verwalten

Sicherheitszertifikate sind kleine Datendateien, die zum Erstellen sicherer,

vertrauenswürdiger Verbindungen zwischen StorageGRID Komponenten sowie 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 gegenüber seinen Clients zu authentifizieren und einen sicheren Kommunikationspfad für Daten bereitzustellen. Sowohl der Server als auch der Client verfügen über eine Kopie des Zertifikats.
- **Client-Zertifikate** authentifizieren die Identität eines Clients oder Benutzers gegenüber dem Server und bieten eine sicherere Authentifizierung als Passwörter allein. Client-Zertifikate 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 auf seiner Kopie des Zertifikats vergleicht. Wenn die Signaturen übereinstimmen, startet der Client eine Sitzung mit dem Server unter Verwendung desselben öffentlichen Schlüssels.

StorageGRID fungiert als Server für einige Verbindungen (z. B. den Load Balancer-Endpunkt) 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 verwendet, um den internen StorageGRID -Verkehr zu sichern. Eine externe Zertifizierungsstelle (CA) kann benutzerdefinierte Zertifikate ausstellen, die vollständig mit den Informationssicherheitsrichtlinien Ihres Unternehmens konform sind. Obwohl Sie das Grid-CA-Zertifikat für eine Nicht-Produktionsumgebung verwenden können, besteht die bewährte Vorgehensweise für eine Produktionsumgebung darin, benutzerdefinierte Zertifikate zu verwenden, die von einer externen Zertifizierungsstelle signiert wurden. Ungesicherte Verbindungen ohne Zertifikat werden ebenfalls unterstützt, aber nicht empfohlen.

- Benutzerdefinierte CA-Zertifikate entfernen die internen Zertifikate nicht. Die benutzerdefinierten Zertifikate sollten jedoch diejenigen sein, die zum Überprüfen von Serververbindungen angegeben sind.
- Alle benutzerdefinierten Zertifikate müssen die"Richtlinien zur Systemhärtung für Serverzertifikate" .
- StorageGRID unterstützt die Bündelung von Zertifikaten einer Zertifizierungsstelle in einer einzigen Datei (bekannt als CA-Zertifikatspaket).

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

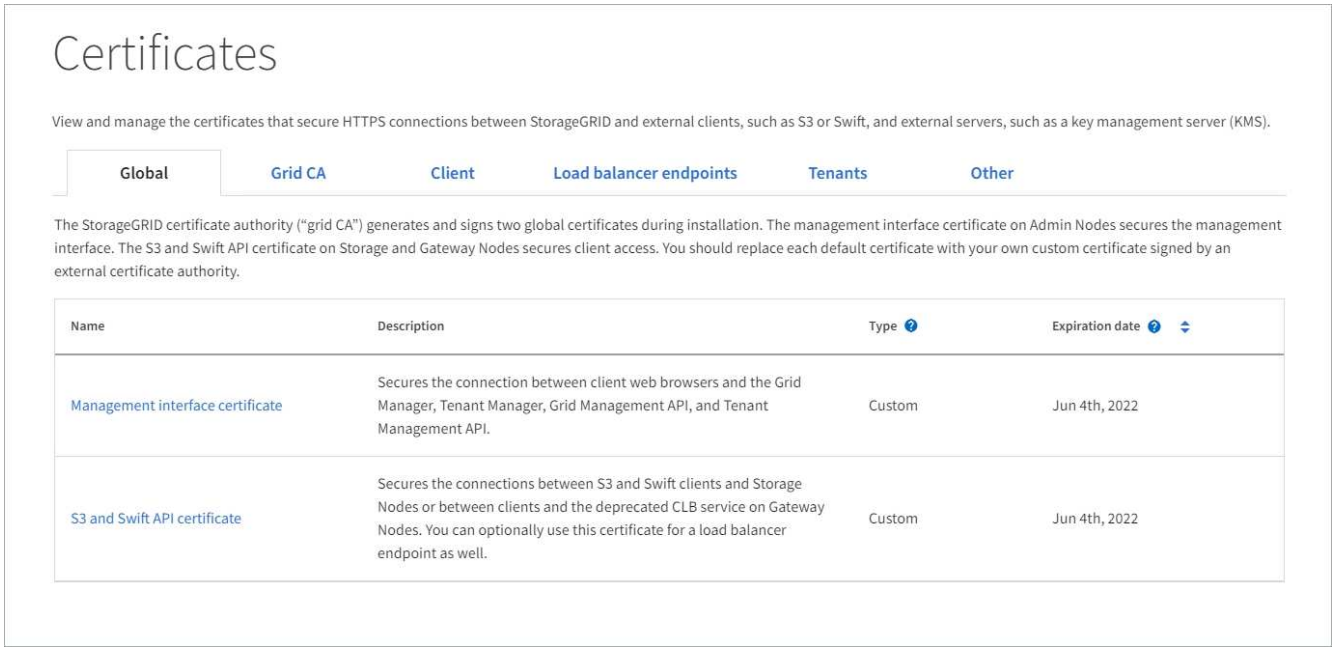
Varianten der Server- und Client-Zertifikattypen werden auf verschiedene Weise implementiert. Sie sollten alle für Ihre spezifische StorageGRID Konfiguration erforderlichen Zertifikate bereithalten, bevor Sie das System konfigurieren.

Zugriff auf Sicherheitszertifikate

Sie können an einem einzigen Ort auf Informationen zu allen StorageGRID -Zertifikaten zugreifen, zusammen mit Links zum Konfigurations-Workflow für jedes Zertifikat.

Schritte

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



2. Wählen Sie auf der Seite „Zertifikate“ eine Registerkarte aus, um Informationen zu den einzelnen Zertifikatskategorien zu erhalten und auf die Zertifikatseinstellungen zuzugreifen. Sie können auf eine Registerkarte zugreifen, wenn Sie über die"entsprechende Erlaubnis" .

   - **Global**: Sichert den StorageGRID Zugriff von Webbrowsern und externen API-Clients.
   - **Grid CA**: Sichert den internen StorageGRID Verkehr.
   - **Client**: Sichert Verbindungen zwischen externen Clients und der StorageGRID Prometheus-Datenbank.
   - **Load Balancer-Endpunkte**: Sichert Verbindungen zwischen S3-Clients und dem StorageGRID Load Balancer.
   - **Mandanten**: Sichert Verbindungen zu Identitätsföderationsservern oder von Plattformdienst-Endpunkten zu S3-Speicherressourcen.
   - **Sonstiges**: Sichert StorageGRID Verbindungen, die bestimmte Zertifikate erfordern.

     Jede Registerkarte wird unten mit Links zu weiteren Zertifikatsdetails beschrieben.

Allgemein

Die globalen Zertifikate sichern den StorageGRID Zugriff von Webbrowsern und externen S3-API-Clients. Während der Installation werden zunächst zwei globale Zertifikate von der StorageGRID Zertifizierungsstelle generiert. Die bewährte Vorgehensweise für eine Produktionsumgebung besteht darin, benutzerdefinierte Zertifikate zu verwenden, die von einer externen Zertifizierungsstelle signiert wurden.

- Management-Schnittstellenzertifikat: Sichert Client-Webbrowser-Verbindungen zu StorageGRID Verwaltungsschnittstellen.
- S3-API-Zertifikat: Sichert Client-API-Verbindungen zu Speicherknoten, Admin-Knoten und Gateway-Knoten, die von S3-Clientanwendungen zum Hoch- und Herunterladen von Objektdaten verwendet werden.

Zu den installierten globalen Zertifikaten gehören:

- **Name**: Zertifikatsname mit Link zur Verwaltung des Zertifikats.
- **Beschreibung**
- **Typ**: Benutzerdefiniert oder Standard. + Sie sollten für eine verbesserte Grid-Sicherheit immer ein benutzerdefiniertes Zertifikat verwenden.
- **Ablaufdatum**: Bei Verwendung des Standardzertifikats wird kein Ablaufdatum angezeigt.

Du kannst:

- Ersetzen Sie die Standardzertifikate durch benutzerdefinierte Zertifikate, die von einer externen Zertifizierungsstelle signiert wurden, um die Grid-Sicherheit zu verbessern:
  - "Ersetzen Sie das standardmäßige, von StorageGRID generierte Management-Schnittstellenzertifikat"Wird für Grid Manager- und Tenant Manager-Verbindungen verwendet.
  - "Ersetzen des S3-API-Zertifikats"Wird für Verbindungen zu Speicherknoten und Lastenausgleichsendpunkten (optional) verwendet.
- "Wiederherstellen des Standardzertifikats der Verwaltungsschnittstelle" .
- "Wiederherstellen des Standard-S3-API-Zertifikats" .
- "Verwenden Sie ein Skript, um ein neues selbstsigniertes Management-Schnittstellenzertifikat zu generieren" .
- Kopieren oder herunterladen Sie die"Management-Schnittstellenzertifikat" oder"S3-API-Zertifikat" .

Grid CA

DerGrid-CA-Zertifikat , das von der StorageGRID Zertifizierungsstelle während der StorageGRID Installation generiert wird, sichert den gesamten internen StorageGRID Verkehr.

Zu den Zertifikatsinformationen gehören das Ablaufdatum des Zertifikats und der Zertifikatsinhalt.

Du kannst"Kopieren oder laden Sie das Grid CA-Zertifikat herunter" , aber Sie können es nicht ändern.

Kunde

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

Die Zertifikatstabelle enthält eine Zeile für jedes konfigurierte Client-Zertifikat und gibt an, ob das Zertifikat für den Zugriff auf die Prometheus-Datenbank verwendet werden kann, sowie das Ablaufdatum des Zertifikats.

Du kannst:

- "Laden Sie ein neues Client-Zertifikat hoch oder generieren Sie ein neues."
- Wählen Sie einen Zertifikatsnamen aus, um die Zertifikatsdetails anzuzeigen. Dort können Sie:
  - "Ändern Sie den Namen des Client-Zertifikats."
  - "Legen Sie die Prometheus-Zugriffsberechtigung fest."
  - "Laden Sie das Client-Zertifikat hoch und ersetzen Sie es."
  - "Kopieren oder laden Sie das Client-Zertifikat herunter."
  - "Entfernen Sie das Client-Zertifikat."
- Wählen Sie **Aktionen**, um schnell"bearbeiten" ,"befestigen" , oder"entfernen" ein Client-Zertifikat. Sie können bis zu 10 Client-Zertifikate auswählen und diese gleichzeitig über **Aktionen** > **Entfernen** entfernen.

Load Balancer-Endpunkte

Load Balancer-EndpunktzertifikateSichern Sie die Verbindungen zwischen S3-Clients und dem StorageGRID Load Balancer-Dienst auf Gateway-Knoten und Admin-Knoten.

Die Load Balancer-Endpunkttabelle enthält eine Zeile für jeden konfigurierten Load Balancer-Endpunkt und gibt an, ob für den Endpunkt das globale S3-API-Zertifikat oder ein benutzerdefiniertes Load Balancer-Endpunktzertifikat verwendet wird. Außerdem wird das Ablaufdatum jedes Zertifikats angezeigt.

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

Du kannst:

- "Einen Load Balancer-Endpunkt anzeigen", einschließlich der Zertifikatsdetails.
- "Geben Sie ein Load Balancer-Endpunktzertifikat für FabricPool an."
- "Verwenden Sie das globale S3-API-Zertifikat"anstatt ein neues Load Balancer-Endpunktzertifikat zu generieren.

Mieter

Mieter könnenIdentity Federation Server-Zertifikate oderPlattformdienst-Endpunktzertifikate um ihre Verbindungen mit StorageGRID zu sichern.

Die Mandantentabelle enthält für jeden Mandanten eine Zeile und gibt an, ob jeder Mandant die Berechtigung hat, seine eigene Identitätsquelle oder Plattformdienste zu verwenden.

Du kannst:

- "Wählen Sie einen Mandantennamen aus, um sich beim Mandantenmanager anzumelden"
- "Wählen Sie einen Mandantennamen aus, um die Details zur Mandantenidentitätsföderation anzuzeigen."
- "Wählen Sie einen Mandantennamen aus, um Details zu den Mandantenplattformdiensten

anzuzeigen"

- "Geben Sie während der Endpunkterstellung ein Plattformdienstendpunktzertifikat an"

Sonstige

StorageGRID verwendet für bestimmte Zwecke andere Sicherheitszertifikate. Diese Zertifikate werden nach ihrem Funktionsnamen aufgelistet. Weitere Sicherheitszertifikate sind:

- Cloud Storage Pool-Zertifikate
- Zertifikate für E-Mail-Benachrichtigungen
- Externe Syslog-Server-Zertifikate
- Netzverbund-Anschlusszertifikate
- Identitätsverbundzertifikate
- Schlüsselverwaltungsserver-Zertifikate (KMS)
- Single Sign-On-Zertifikate

Die Informationen geben den Zertifikatstyp an, den eine Funktion verwendet, sowie gegebenenfalls die Ablaufdaten des Server- und Client-Zertifikats. Wenn Sie einen Funktionsnamen auswählen, wird eine Browserregisterkarte geöffnet, in der Sie die Zertifikatsdetails anzeigen und bearbeiten können.

> Informationen zu anderen Zertifikaten können Sie nur einsehen und abrufen, wenn Sie über die Berechtigung"entsprechende Erlaubnis" .

Du kannst:

- "Geben Sie ein Cloud Storage Pool-Zertifikat für S3, C2S S3 oder Azure an"
- "Geben Sie ein Zertifikat für E-Mail-Benachrichtigungen an"
- "Verwenden Sie ein Zertifikat für einen externen Syslog-Server"
- "Rotieren von Grid-Föderation-Verbindungszertifikaten"
- "Anzeigen und Bearbeiten eines Identitätsverbundzertifikats"
- "Hochladen von KMS-Server- und Client-Zertifikaten (Key Management Server)"
- "Manuelles Angeben eines SSO-Zertifikats für eine Vertrauensstellung der vertrauenden Seite"

Details zum Sicherheitszertifikat

Nachfolgend wird jeder Typ von Sicherheitszertifikat beschrieben, mit Links zu den Implementierungsanweisungen.

Management-Schnittstellenzertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server	Authentifiziert die Verbindung zwischen Client-Webbrowsern und der StorageGRID Verwaltungsschnittstelle, sodass Benutzer ohne Sicherheitswarnungen auf den Grid Manager und den Tenant Manager zugreifen können. Dieses Zertifikat authentifiziert auch Grid Management API- und Tenant Management API-Verbindungen. Sie können das während der Installation erstellte Standardzertifikat verwenden oder ein benutzerdefiniertes Zertifikat hochladen.	**KONFIGURATION** > **Sicherheit** > **Zertifikate**, wählen Sie die Registerkarte **Global** und dann **Management-Schnittstellenzertifikat**	"Konfigurieren von Management-Schnittstellenzertifikaten"

S3-API-Zertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server	Authentifiziert sichere S3-Clientverbindungen zu einem Speicherknoten und zu Load Balancer-Endpunkten (optional).	**KONFIGURATION** > **Sicherheit** > **Zertifikate**, wählen Sie die Registerkarte **Global** und dann **S3-API-Zertifikat**	"Konfigurieren von S3-API-Zertifikaten"

Grid-CA-Zertifikat

Siehe dieBeschreibung des Standard-Grid-CA-Zertifikats .

Administrator-Client-Zertifikat

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

Load Balancer-Endpunktzertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server	Authentifiziert die Verbindung zwischen S3-Clients und dem StorageGRID Load Balancer-Dienst auf Gateway-Knoten und Admin-Knoten. Sie können ein Load Balancer-Zertifikat hochladen oder generieren, wenn Sie einen Load Balancer-Endpunkt konfigurieren. Clientanwendungen verwenden das Load Balancer-Zertifikat beim Herstellen einer Verbindung mit StorageGRID , um Objektdaten zu speichern und abzurufen. Sie können auch eine benutzerdefinierte Version des globalenS3-API-Zertifikat Zertifikat zur Authentifizierung von Verbindungen mit dem Load Balancer-Dienst. Wenn das globale Zertifikat zum Authentifizieren von Load Balancer-Verbindungen verwendet wird, müssen Sie nicht für jeden Load Balancer-Endpunkt ein separates Zertifikat hochladen oder generieren. **Hinweis:** Das für die Load Balancer-Authentifizierung verwendete Zertifikat ist das am häufigsten verwendete Zertifikat während des normalen StorageGRID -Betriebs.	**KONFIGURATION** > **Netzwerk** > **Load Balancer-Endpunkte**	• "Konfigurieren von Load Balancer-Endpunkten" • "Erstellen Sie einen Load Balancer-Endpunkt für FabricPool"

Cloud Storage Pool-Endpunktzertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server	Authentifiziert die Verbindung von einem StorageGRID Cloud Storage Pool zu einem externen Speicherort, wie z. B. S3 Glacier oder Microsoft Azure Blob Storage. Für jeden Cloud-Anbietertyp ist ein anderes Zertifikat erforderlich.	**ILM** > **Speicherpools**	"Erstellen Sie einen Cloud-Speicherpool"

Zertifikat für E-Mail-Benachrichtigungen

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server und Client	Authentifiziert die Verbindung zwischen einem SMTP-E-Mail-Server und StorageGRID , die für Warnbenachrichtigungen verwendet wird. • Wenn für die Kommunikation mit dem SMTP-Server Transport Layer Security (TLS) erforderlich ist, müssen Sie das CA-Zertifikat des E-Mail-Servers angeben. • Geben Sie nur dann ein Client-Zertifikat an, wenn der SMTP-E-Mail-Server Client-Zertifikate zur Authentifizierung erfordert.	**WARNUNGEN** > **E-Mail-Einrichtung**	"E-Mail-Benachrichtigungen für Warnmeldungen einrichten"

Externes Syslog-Server-Zertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server	Authentifiziert die TLS- oder RELP/TLS-Verbindung zwischen einem externen Syslog-Server, der Ereignisse in StorageGRID protokolliert. **Hinweis:** Für TCP-, RELP/TCP- und UDP-Verbindungen zu einem externen Syslog-Server ist kein externes Syslog-Serverzertifikat erforderlich.	**KONFIGURATION** > **Überwachung** > **Audit- und Syslog-Server**	"Verwenden Sie einen externen Syslog-Server"

Grid-Föderation-Verbindungszertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server und Client	Authentifizieren und verschlüsseln Sie Informationen, die zwischen dem aktuellen StorageGRID -System und einem anderen Grid in einer Grid-Föderationsverbindung gesendet werden.	**KONFIGURATION** > **System** > **Grid-Föderation**	• "Erstellen von Grid-Föderationsverbindungen" • "Verbindungszertifikate rotieren"

Identitätsverbundzertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server	Authentifiziert die Verbindung zwischen StorageGRID und einem externen Identitätsanbieter wie Active Directory, OpenLDAP oder Oracle Directory Server. Wird für die Identitätsföderation verwendet, wodurch Administratorgruppen und Benutzer von einem externen System verwaltet werden können.	**KONFIGURATION** > **Zugriffskontrolle** > **Identitätsföderation**	"Verwenden der Identitätsföderation"

Schlüsselverwaltungsserver-Zertifikat (KMS)

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server und Client	Authentifiziert die Verbindung zwischen StorageGRID und einem externen Schlüsselverwaltungsserver (KMS), der Verschlüsselungsschlüssel für StorageGRID Appliance-Knoten bereitstellt.	**KONFIGURATION** > **Sicherheit** > **Schlüsselverwaltungsserver**	"Schlüsselverwaltungsserver (KMS) hinzufügen"

Plattformdienste-Endpunktzertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server	Authentifiziert die Verbindung vom StorageGRID -Plattformdienst zu einer S3-Speicherressource.	**Mandantenmanager** > **SPEICHER (S3)** > **Plattformdienst-Endpunkte**	"Plattformdienst-Endpunkt erstellen" "Plattformdienst-Endpunkt bearbeiten"

Single Sign-On (SSO)-Zertifikat

Zertifikatstyp	Beschreibung	Navigationsstandort	Details
Server	Authentifiziert die Verbindung zwischen Identitätsföderationsdiensten wie Active Directory Federation Services (AD FS) und StorageGRID , die für Single Sign-On (SSO)-Anfragen verwendet werden.	**KONFIGURATION** > **Zugriffskontrolle** > **Single Sign-On**	"Konfigurieren der einmaligen Anmeldung"

Zertifikatbeispiele

Beispiel 1: Load Balancer-Dienst

In diesem Beispiel fungiert StorageGRID als Server.

1. Sie konfigurieren einen Load Balancer-Endpunkt und laden ein Serverzertifikat in StorageGRID hoch oder generieren es.
2. Sie konfigurieren eine S3-Client-Verbindung zum Load Balancer-Endpunkt und laden dasselbe Zertifikat auf den Client hoch.
3. Wenn der Client Daten speichern oder abrufen möchte, stellt er über HTTPS eine Verbindung zum Load Balancer-Endpunkt her.

4. StorageGRID antwortet mit dem Serverzertifikat, das einen öffentlichen Schlüssel enthält, und mit einer Signatur, die auf dem privaten Schlüssel basiert.
5. Der Client überprüft dieses Zertifikat, indem er die Serversignatur mit der Signatur auf 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 Schlüsselverwaltungsserver (KMS)

In diesem Beispiel fungiert StorageGRID als Client.

1. Mithilfe externer Key Management Server-Software konfigurieren Sie StorageGRID als KMS-Client und erhalten ein von einer Zertifizierungsstelle signiertes Serverzertifikat, ein öffentliches Client-Zertifikat und den privaten Schlüssel für das Client-Zertifikat.
2. Mithilfe des Grid Managers konfigurieren Sie einen KMS-Server und laden die Server- und Client-Zertifikate sowie den privaten Client-Schlüssel hoch.
3. Wenn ein StorageGRID Knoten einen Verschlüsselungsschlüssel benötigt, sendet er eine Anfrage an den KMS-Server, die Daten aus dem Zertifikat und eine auf dem privaten Schlüssel basierende Signatur enthält.
4. Der KMS-Server validiert die Zertifikatssignatur und entscheidet, dass er StorageGRID vertrauen kann.
5. Der KMS-Server antwortet über die validierte Verbindung.

Unterstützte Serverzertifikattypen

Das StorageGRID -System unterstützt benutzerdefinierte Zertifikate, die mit RSA oder ECDSA (Elliptic Curve Digital Signature Algorithm) verschlüsselt sind.

> Der Verschlüsselungstyp für die Sicherheitsrichtlinie muss mit dem Serverzertifikatstyp übereinstimmen. Beispielsweise erfordern RSA-Chiffren RSA-Zertifikate und ECDSA-Chiffren ECDSA-Zertifikate. Sehen "Sicherheitszertifikate verwalten" . Wenn Sie eine benutzerdefinierte Sicherheitsrichtlinie konfigurieren, die nicht mit dem Serverzertifikat kompatibel ist, können Sie"vorübergehend zur Standardsicherheitsrichtlinie zurückkehren" .

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

Konfigurieren von Management-Schnittstellenzertifikaten

Sie können das Standardzertifikat der Verwaltungsschnittstelle durch ein einzelnes benutzerdefiniertes Zertifikat ersetzen, das Benutzern den Zugriff auf den Grid Manager und den Tenant Manager ermöglicht, ohne dass Sicherheitswarnungen angezeigt werden. Sie können auch zum Standardzertifikat der Verwaltungsschnittstelle zurückkehren oder ein neues generieren.

Informationen zu diesem Vorgang

Standardmäßig wird jedem Admin-Knoten ein von der Grid-CA signiertes Zertifikat ausgestellt. Diese von der Zertifizierungsstelle signierten Zertifikate können durch ein einzelnes gemeinsames benutzerdefiniertes Verwaltungsschnittstellenzertifikat und den entsprechenden privaten Schlüssel ersetzt werden.

Da für alle Admin-Knoten ein einziges benutzerdefiniertes Verwaltungsschnittstellenzertifikat verwendet wird, müssen Sie das Zertifikat als Platzhalter- oder Multidomänenzertifikat angeben, wenn Clients den Hostnamen beim Herstellen einer Verbindung mit dem Grid Manager und Tenant Manager überprüfen müssen. Definieren Sie das benutzerdefinierte Zertifikat so, dass es mit allen Admin-Knoten im Raster übereinstimmt.

Sie müssen die Konfiguration auf dem Server abschließen. Je nach der von Ihnen verwendeten Stammzertifizierungsstelle (CA) müssen Benutzer möglicherweise auch das Grid-CA-Zertifikat in dem Webbrowser installieren, den sie für den Zugriff auf den Grid Manager und den Tenant Manager verwenden.

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

Wenn Sie auf den Grid Manager oder Tenant Manager über einen Domänennamen statt einer IP-Adresse zugreifen, zeigt der Browser einen Zertifikatsfehler ohne Umgehungsoption an, wenn einer der folgenden Fälle eintritt:

- Ihr benutzerdefiniertes Verwaltungsschnittstellenzertifikat läuft ab.
- Duvon einem benutzerdefinierten Verwaltungsschnittstellenzertifikat auf das Standardserverzertifikat zurücksetzen .

Hinzufügen eines benutzerdefinierten Verwaltungsschnittstellenzertifikats

Um ein benutzerdefiniertes Verwaltungsschnittstellenzertifikat hinzuzufügen, können Sie Ihr eigenes Zertifikat bereitstellen oder mithilfe des Grid Managers eines generieren.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global** die Option **Management-Schnittstellenzertifikat** aus.
3. Wählen Sie **Benutzerdefiniertes Zertifikat verwenden**.
4. Laden Sie das Zertifikat hoch oder generieren Sie es.

Zertifikat hochladen

Laden Sie die erforderlichen Serverzertifikatsdateien hoch.

a. Wählen Sie **Zertifikat hochladen**.

b. Laden Sie die erforderlichen Serverzertifikatsdateien hoch:

- **Serverzertifikat**: Die benutzerdefinierte Serverzertifikatsdatei (PEM-codiert).
- **Privater Zertifikatsschlüssel**: Die benutzerdefinierte private Schlüsseldatei des Serverzertifikats(`.key`).

> Private EC-Schlüssel müssen mindestens 224 Bit lang sein. Private RSA-Schlüssel müssen mindestens 2048 Bit lang sein.

- **CA-Paket**: Eine einzelne optionale Datei, die die Zertifikate jeder zwischengeschalteten ausstellenden Zertifizierungsstelle (CA) enthält. Die Datei sollte alle PEM-codierten CA-Zertifikatsdateien enthalten, die in der Reihenfolge der Zertifikatskette aneinandergereiht sind.

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

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

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

  Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Zertifikat PEM kopieren** oder **CA-Paket PEM kopieren**, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.

d. Wählen Sie **Speichern**. + Das benutzerdefinierte Verwaltungsschnittstellenzertifikat wird für alle nachfolgenden neuen Verbindungen zum Grid Manager, Tenant Manager, Grid Manager API oder Tenant Manager API verwendet.

Zertifikat generieren

Generieren Sie die Serverzertifikatsdateien.

> Die bewährte Vorgehensweise für eine Produktionsumgebung besteht darin, ein benutzerdefiniertes Verwaltungsschnittstellenzertifikat zu verwenden, das von einer externen Zertifizierungsstelle signiert wurde.

a. Wählen Sie **Zertifikat generieren**.

b. Geben Sie die Zertifikatsinformationen an:

Feld	Beschreibung
Domänenname	Ein oder mehrere vollqualifizierte Domänennamen, die in das Zertifikat aufgenommen werden sollen. Verwenden Sie ein * als Platzhalter, um mehrere Domänennamen darzustellen.

Feld	Beschreibung
IP	Eine oder mehrere IP-Adressen, die in das Zertifikat aufgenommen werden sollen.
Betreff (optional)	X.509-Betreff oder Distinguished Name (DN) des Zertifikatsinhabers. Wenn in dieses Feld kein Wert eingegeben wird, verwendet das generierte Zertifikat den ersten Domänennamen oder die erste IP-Adresse als allgemeinen Namen (CN) des Betreffs.
Gültigkeitstage	Anzahl der Tage nach der Erstellung, bis zu der das Zertifikat abläuft.
Hinzufügen von Schlüsselverwendungserweiterungen	Wenn ausgewählt (Standard und empfohlen), werden dem generierten Zertifikat Schlüsselverwendung und erweiterte Schlüsselverwendungserweiterungen hinzugefügt. Diese Erweiterungen definieren den Zweck des im Zertifikat enthaltenen Schlüssels. **Hinweis**: Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, Sie haben Verbindungsprobleme mit älteren Clients, wenn die Zertifikate diese Erweiterungen enthalten.

c. Wählen Sie **Generieren**.

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

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

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

   Beispiel: `storagegrid_certificate.pem`

   - Wählen Sie **Zertifikat PEM kopieren**, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.

e. Wählen Sie **Speichern**. + Das benutzerdefinierte Verwaltungsschnittstellenzertifikat wird für alle nachfolgenden neuen Verbindungen zum Grid Manager, Tenant Manager, Grid Manager API oder Tenant Manager API verwendet.

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

   Warten Sie nach dem Hochladen oder Generieren eines neuen Zertifikats bis zu einem Tag, bis alle zugehörigen Warnungen zum Ablauf des Zertifikats gelöscht werden.

6. Nachdem Sie ein benutzerdefiniertes Management-Schnittstellenzertifikat hinzugefügt haben, werden auf der Seite „Management-Schnittstellenzertifikat“ detaillierte Zertifikatsinformationen zu den verwendeten Zertifikaten angezeigt. + Sie können das Zertifikat PEM nach Bedarf herunterladen oder kopieren.

Wiederherstellen des Standardzertifikats der Verwaltungsschnittstelle

Sie können für Grid Manager- und Tenant Manager-Verbindungen wieder das Standardzertifikat der Verwaltungsschnittstelle verwenden.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global** die Option **Management-Schnittstellenzertifikat** aus.
3. Wählen Sie **Standardzertifikat verwenden**.

   Wenn Sie das Standardzertifikat der Verwaltungsschnittstelle wiederherstellen, werden die von Ihnen konfigurierten benutzerdefinierten Serverzertifikatdateien gelöscht und können nicht vom System wiederhergestellt werden. Für alle nachfolgenden neuen Clientverbindungen wird das Standardzertifikat der Verwaltungsschnittstelle verwendet.

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

Verwenden Sie ein Skript, um ein neues selbstsigniertes Management-Schnittstellenzertifikat zu generieren

Wenn eine strenge Hostnamenvalidierung erforderlich ist, können Sie ein Skript zum Generieren des Verwaltungsschnittstellenzertifikats verwenden.

Bevor Sie beginnen

- Du hast"spezifische Zugriffsberechtigungen" .
- Sie haben die `Passwords.txt` Datei.

Informationen zu diesem Vorgang

Die bewährte Vorgehensweise für eine Produktionsumgebung besteht darin, ein von einer externen Zertifizierungsstelle signiertes Zertifikat zu verwenden.

Schritte

1. Besorgen Sie sich den vollqualifizierten Domänennamen (FQDN) jedes Admin-Knotens.
2. Melden Sie sich beim primären Admin-Knoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
   b. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.
   c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
   d. Geben Sie das Passwort ein, das in der `Passwords.txt` Datei.

   Wenn Sie als Root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Zu `#` .
3. Konfigurieren Sie StorageGRID mit einem neuen selbstsignierten Zertifikat.

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

   - Für `--domains` , verwenden Sie Platzhalter, um die vollqualifizierten Domänennamen aller Admin-Knoten darzustellen. Zum Beispiel, `*.ui.storagegrid.example.com` verwendet das Platzhalterzeichen * zur Darstellung `admin1.ui.storagegrid.example.com` Und `admin2.ui.storagegrid.example.com` .
   - Satz `--type` Zu `management` um das Management-Schnittstellenzertifikat zu konfigurieren, das von

Grid Manager und Tenant Manager verwendet wird.

- Standardmäßig sind generierte Zertifikate ein Jahr (365 Tage) gültig und müssen vor ihrem Ablauf neu erstellt werden. Sie können die `--days` Argument, um die Standardgültigkeitsdauer zu überschreiben.

> Die Gültigkeitsdauer eines Zertifikats beginnt, wenn `make-certificate` wird ausgeführt. Sie müssen sicherstellen, dass der Verwaltungsclient mit derselben Zeitquelle wie StorageGRID synchronisiert ist. Andernfalls kann es sein, dass der Client das Zertifikat ablehnt.

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

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

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

   Schließen Sie die Tags BEGIN und END in Ihre Auswahl ein.

5. Melden Sie sich von der Befehlsshell 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-Schnittstellenzertifikat** aus.
7. Konfigurieren Sie Ihren Verwaltungsclient so, dass er das von Ihnen kopierte öffentliche Zertifikat verwendet. Fügen Sie die Tags BEGIN und END ein.

Laden Sie das Management-Interface-Zertifikat herunter oder kopieren Sie es

Sie können den Inhalt des Management-Schnittstellenzertifikats zur Verwendung an anderer Stelle speichern oder kopieren.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global** die Option **Management-Schnittstellenzertifikat** aus.
3. Wählen Sie die Registerkarte **Server** oder **CA-Paket** und laden Sie anschließend das Zertifikat herunter oder kopieren Sie es.

Zertifikatsdatei oder CA-Paket herunterladen

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

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

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

b. Geben Sie den Namen der Zertifikatsdatei und den Download-Speicherort 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 anderer Stelle einzufügen. Wenn Sie ein optionales CA-Paket verwenden, wird jedes Zertifikat im Paket auf einer eigenen Unterregisterkarte angezeigt.

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

   Wenn Sie ein CA-Paket kopieren, werden alle Zertifikate in den sekundären Registerkarten des CA-Pakets zusammen kopiert.

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-API-Zertifikaten

Sie können das Serverzertifikat ersetzen oder wiederherstellen, das für S3-Clientverbindungen zu Speicherknoten oder Load Balancer-Endpunkten verwendet wird. Das benutzerdefinierte Ersatzserverzertifikat ist spezifisch für Ihre Organisation.

Swift-Details wurden aus dieser Version der Dokumentationssite entfernt. Sehen "StorageGRID 11.8: Konfigurieren von S3- und Swift-API-Zertifikaten" .

Informationen zu diesem Vorgang

Standardmäßig wird jedem Speicherknoten ein von der Grid-CA signiertes X.509-Serverzertifikat ausgestellt. Diese von einer Zertifizierungsstelle signierten Zertifikate können durch ein einzelnes gemeinsames benutzerdefiniertes Serverzertifikat und den entsprechenden privaten Schlüssel ersetzt werden.

Für alle Speicherknoten wird ein einzelnes benutzerdefiniertes Serverzertifikat verwendet. Sie müssen das Zertifikat daher als Platzhalter- oder Multidomänenzertifikat angeben, wenn Clients beim Herstellen einer Verbindung mit dem Speicherendpunkt den Hostnamen überprüfen müssen. Definieren Sie das benutzerdefinierte Zertifikat so, dass es mit allen Speicherknoten im Raster übereinstimmt.

Nachdem Sie die Konfiguration auf dem Server abgeschlossen haben, müssen Sie je nach der von Ihnen verwendeten Stammzertifizierungsstelle (CA) möglicherweise auch das Grid-CA-Zertifikat im S3-API-Client

installieren, den Sie für den Zugriff auf das System verwenden.

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

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

Fügen Sie ein benutzerdefiniertes S3-API-Zertifikat hinzu

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate**.
2. Wählen Sie auf der Registerkarte **Global S3-API-Zertifikat** aus.
3. Wählen Sie **Benutzerdefiniertes Zertifikat verwenden**.
4. Laden Sie das Zertifikat hoch oder generieren Sie es.

Zertifikat hochladen

Laden Sie die erforderlichen Serverzertifikatsdateien hoch.

a. Wählen Sie **Zertifikat hochladen**.

b. Laden Sie die erforderlichen Serverzertifikatsdateien hoch:

- **Serverzertifikat**: Die benutzerdefinierte Serverzertifikatsdatei (PEM-codiert).
- **Privater Zertifikatsschlüssel**: Die benutzerdefinierte private Schlüsseldatei des Serverzertifikats(`.key`).

> Private EC-Schlüssel müssen mindestens 224 Bit lang sein. Private RSA-Schlüssel müssen mindestens 2048 Bit lang sein.

- **CA-Paket**: Eine einzelne optionale Datei, die die Zertifikate aller ausstellenden Zwischenzertifizierungsstellen enthält. Die Datei sollte alle PEM-codierten CA-Zertifikatsdateien enthalten, die in der Reihenfolge der Zertifikatskette aneinandergereiht sind.

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

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

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

  Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Zertifikat PEM kopieren** oder **CA-Paket PEM kopieren**, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.

d. Wählen Sie **Speichern**.

  Das benutzerdefinierte Serverzertifikat wird für nachfolgende neue S3-Clientverbindungen verwendet.

Zertifikat generieren

Generieren Sie die Serverzertifikatsdateien.

a. Wählen Sie **Zertifikat generieren**.

b. Geben Sie die Zertifikatsinformationen an:

Feld	Beschreibung
Domänenname	Ein oder mehrere vollqualifizierte Domänennamen, die in das Zertifikat aufgenommen werden sollen. Verwenden Sie ein * als Platzhalter, um mehrere Domänennamen darzustellen.
IP	Eine oder mehrere IP-Adressen, die in das Zertifikat aufgenommen werden sollen.

Feld	Beschreibung
Betreff (optional)	X.509-Betreff oder Distinguished Name (DN) des Zertifikatsinhabers. Wenn in dieses Feld kein Wert eingegeben wird, verwendet das generierte Zertifikat den ersten Domänennamen oder die erste IP-Adresse als allgemeinen Namen (CN) des Betreffs.
Gültigkeitstage	Anzahl der Tage nach der Erstellung, bis zu der das Zertifikat abläuft.
Hinzufügen von Schlüsselverwendungserweiterungen	Wenn ausgewählt (Standard und empfohlen), werden dem generierten Zertifikat Schlüsselverwendung und erweiterte Schlüsselverwendungserweiterungen hinzugefügt. Diese Erweiterungen definieren den Zweck des im Zertifikat enthaltenen Schlüssels. **Hinweis**: Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, Sie haben Verbindungsprobleme mit älteren Clients, wenn die Zertifikate diese Erweiterungen enthalten.

c. Wählen Sie **Generieren**.

d. Wählen Sie **Zertifikatdetails** aus, um die Metadaten und PEM für das generierte benutzerdefinierte S3-API-Zertifikat anzuzeigen.

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

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

     Beispiel: `storagegrid_certificate.pem`

   - Wählen Sie **Zertifikat PEM kopieren**, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.

e. Wählen Sie **Speichern**.

   Das benutzerdefinierte Serverzertifikat wird für nachfolgende neue S3-Clientverbindungen verwendet.

5. Wählen Sie eine Registerkarte aus, um Metadaten für das Standard StorageGRID Serverzertifikat, ein hochgeladenes, von einer Zertifizierungsstelle signiertes Zertifikat oder ein generiertes benutzerdefiniertes Zertifikat anzuzeigen.

   Warten Sie nach dem Hochladen oder Generieren eines neuen Zertifikats bis zu einem Tag, bis alle zugehörigen Warnungen zum Ablauf des Zertifikats gelöscht werden.

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

7. Nachdem Sie ein benutzerdefiniertes S3-API-Zertifikat hinzugefügt haben, werden auf der S3-API-Zertifikatseite detaillierte Zertifikatsinformationen für das verwendete benutzerdefinierte S3-API-Zertifikat angezeigt. + Sie können das Zertifikat PEM nach Bedarf herunterladen oder kopieren.

Wiederherstellen des Standard-S3-API-Zertifikats

Sie können für S3-Clientverbindungen zu Speicherknoten wieder das standardmäßige S3-API-Zertifikat verwenden. Sie können das Standard-S3-API-Zertifikat jedoch nicht für einen Load Balancer-Endpunkt verwenden.

Schritte

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

   Wenn Sie die Standardversion des globalen S3-API-Zertifikats wiederherstellen, werden die von Ihnen konfigurierten benutzerdefinierten Serverzertifikatsdateien gelöscht und können nicht vom System wiederhergestellt werden. Das standardmäßige S3-API-Zertifikat wird für nachfolgende neue S3-Clientverbindungen zu Speicherknoten verwendet.

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

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

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

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

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

Schritte

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

Zertifikatsdatei oder CA-Paket herunterladen

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

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

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

b. Geben Sie den Namen der Zertifikatsdatei und den Download-Speicherort 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 anderer Stelle einzufügen. Wenn Sie ein optionales CA-Paket verwenden, wird jedes Zertifikat im Paket auf einer eigenen Unterregisterkarte angezeigt.

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

   Wenn Sie ein CA-Paket kopieren, werden alle Zertifikate in den sekundären Registerkarten des CA-Pakets zusammen kopiert.

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

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

   Beispiel: `storagegrid_certificate.pem`

Ähnliche Informationen

- "Verwenden Sie die S3 REST-API"
- "Konfigurieren von S3-Endpunktdomänennamen"

Kopieren Sie das Grid CA-Zertifikat

StorageGRID verwendet eine interne Zertifizierungsstelle (CA), um den internen Datenverkehr zu sichern. Dieses Zertifikat ändert sich nicht, wenn Sie eigene Zertifikate hochladen.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Wenn ein benutzerdefiniertes Serverzertifikat konfiguriert wurde, sollten Clientanwendungen den Server mithilfe des benutzerdefinierten Serverzertifikats überprüfen. Sie sollten das CA-Zertifikat nicht vom StorageGRID -System kopieren.

Schritte

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

Zertifikatsdatei herunterladen

Laden Sie das Zertifikat herunter `.pem` Datei.

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

   Beispiel: `storagegrid_certificate.pem`

Kopie des Zertifikats PEM

Kopieren Sie den Zertifikatstext, um ihn an anderer Stelle einzufügen.

a. Wählen Sie **Zertifikat PEM kopieren**.
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 eine strenge Hostnamenvalidierung durchführen und die Deaktivierung der strengen Hostnamenvalidierung nicht unterstützen, wie z. B. ONTAP Clients, die FabricPool verwenden, können Sie beim Konfigurieren des Load Balancer-Endpunkts ein Serverzertifikat generieren oder hochladen.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

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

Die folgenden Schritte bieten allgemeine Richtlinien für S3-Clients, die FabricPool verwenden. Ausführlichere Informationen und Vorgehensweisen finden Sie unter"Konfigurieren von StorageGRID für FabricPool" .

Schritte

1. Konfigurieren Sie optional eine Hochverfügbarkeitsgruppe (HA) für die Verwendung durch FabricPool .
2. Erstellen Sie einen S3-Load Balancer-Endpunkt für die Verwendung durch FabricPool .

Wenn Sie einen HTTPS-Load Balancer-Endpunkt erstellen, werden Sie aufgefordert, Ihr Serverzertifikat, Ihren privaten Zertifikatsschlüssel und das optionale CA-Paket hochzuladen.

3. Hängen Sie StorageGRID als Cloud-Ebene in ONTAP an.

   Geben Sie den Endpunktport des Lastenausgleichs und den vollqualifizierten Domänennamen an, der im von Ihnen hochgeladenen CA-Zertifikat verwendet wird. Geben Sie dann das CA-Zertifikat an.

> ⓘ Wenn das StorageGRID -Zertifikat von einer Zwischenzertifizierungsstelle ausgestellt wurde, müssen Sie das Zwischenzertifizierungsstellenzertifikat angeben. Wenn das StorageGRID -Zertifikat direkt von der Root-CA ausgestellt wurde, müssen Sie das Root-CA-Zertifikat angeben.

Konfigurieren von Clientzertifikaten

Client-Zertifikate ermöglichen autorisierten externen Clients den Zugriff auf die StorageGRID Prometheus-Datenbank und bieten externen Tools eine sichere Möglichkeit, StorageGRID zu überwachen.

Wenn Sie über ein externes Überwachungstool auf StorageGRID zugreifen müssen, müssen Sie mithilfe des Grid Managers ein Client-Zertifikat hochladen oder generieren und die Zertifikatsinformationen in das externe Tool kopieren.

Sehen"Sicherheitszertifikate verwalten" Und"Konfigurieren benutzerdefinierter Serverzertifikate" .

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

> ⓘ Wenn Sie einen Schlüsselverwaltungsserver (KMS) zum Schutz der Daten auf speziell konfigurierten Appliance-Knoten verwenden, lesen Sie die spezifischen Informationen zu"Hochladen eines KMS-Client-Zertifikats" .

Bevor Sie beginnen

- Sie verfügen über Root-Zugriffsberechtigung.
- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- So konfigurieren Sie ein Client-Zertifikat:
  - Sie haben die IP-Adresse oder den Domänennamen des Admin-Knotens.
  - Wenn Sie das Zertifikat der StorageGRID -Verwaltungsschnittstelle konfiguriert haben, verfügen Sie über die Zertifizierungsstelle, das Client-Zertifikat und den privaten Schlüssel, die zum Konfigurieren des Zertifikats der Verwaltungsschnittstelle verwendet werden.
  - Um Ihr eigenes Zertifikat hochzuladen, steht Ihnen der private Schlüssel für das Zertifikat auf Ihrem lokalen Computer zur Verfügung.
  - Der private Schlüssel muss zum Zeitpunkt seiner Erstellung gespeichert oder aufgezeichnet worden sein. Wenn Sie nicht über den ursprünglichen privaten Schlüssel verfügen, müssen Sie einen neuen erstellen.

- So bearbeiten Sie ein Client-Zertifikat:
  - Sie haben die IP-Adresse oder den Domänennamen des Admin-Knotens.
  - Um Ihr eigenes Zertifikat oder ein neues Zertifikat hochzuladen, stehen Ihnen der private Schlüssel, das Client-Zertifikat und die CA (sofern verwendet) auf Ihrem lokalen Computer zur Verfügung.

Client-Zertifikate hinzufügen

Um das Client-Zertifikat hinzuzufügen, verwenden Sie eines der folgenden Verfahren:

- Management-Schnittstellenzertifikat bereits konfiguriert
- Von der Zertifizierungsstelle ausgestelltes Client-Zertifikat
- Generiertes Zertifikat vom Grid Manager

Management-Schnittstellenzertifikat bereits konfiguriert

Verwenden Sie dieses Verfahren, um ein Client-Zertifikat hinzuzufügen, wenn bereits ein Management-Schnittstellenzertifikat mit einer vom Kunden bereitgestellten Zertifizierungsstelle, einem Client-Zertifikat und einem privaten Schlüssel konfiguriert ist.

Schritte

1. Wählen Sie im Grid Manager **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Client**.
2. Wählen Sie **Hinzufügen**.
3. Geben Sie einen Zertifikatsnamen ein.
4. Um mit Ihrem externen Überwachungstool auf Prometheus-Metriken zuzugreifen, wählen Sie **Prometheus zulassen**.
5. Wählen Sie **Weiter**.
6. Laden Sie für den Schritt **Zertifikate anhängen** das Verwaltungsschnittstellenzertifikat hoch.
   a. Wählen Sie **Zertifikat hochladen**.
   b. Wählen Sie **Durchsuchen** und wählen Sie die Zertifikatsdatei der Verwaltungsschnittstelle aus(`.pem`).
      - Wählen Sie **Client-Zertifikatdetails** aus, um die Zertifikatmetadaten und das Zertifikat-PEM anzuzeigen.
      - Wählen Sie **Zertifikat PEM kopieren**, um den Zertifikatsinhalt zum Einfügen an anderer 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. Konfigurieren eines externen Überwachungstools, wie Grafana.

Von der Zertifizierungsstelle ausgestelltes Client-Zertifikat

Verwenden Sie dieses Verfahren, um ein Administrator-Client-Zertifikat hinzuzufügen, wenn kein Management-Schnittstellenzertifikat konfiguriert wurde und Sie ein Client-Zertifikat für Prometheus hinzufügen möchten, das ein von einer Zertifizierungsstelle ausgestelltes Client-Zertifikat und einen privaten Schlüssel verwendet.

Schritte

1. Führen Sie die Schritte aus, um"Konfigurieren eines Management-Schnittstellenzertifikats" .
2. Wählen Sie im Grid Manager **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Client**.
3. Wählen Sie **Hinzufügen**.
4. Geben Sie einen Zertifikatsnamen ein.
5. Um mit Ihrem externen Überwachungstool auf Prometheus-Metriken zuzugreifen, wählen Sie **Prometheus zulassen**.
6. Wählen Sie **Weiter**.
7. Laden Sie für den Schritt **Zertifikate anhängen** das Client-Zertifikat, den privaten Schlüssel und die CA-Bundle-Dateien hoch:
   a. Wählen Sie **Zertifikat hochladen**.
   b. Wählen Sie **Durchsuchen** und wählen Sie das Client-Zertifikat, den privaten Schlüssel und die CA-Bundle-Dateien aus(`.pem`).
      - Wählen Sie **Client-Zertifikatdetails** aus, um die Zertifikatmetadaten und das Zertifikat-PEM anzuzeigen.
      - Wählen Sie **Zertifikat PEM kopieren**, um den Zertifikatsinhalt zum Einfügen an anderer 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. Konfigurieren eines externen Überwachungstools, wie Grafana.

Generiertes Zertifikat vom Grid Manager

Verwenden Sie dieses Verfahren, um ein Administrator-Client-Zertifikat hinzuzufügen, wenn kein Management-Schnittstellenzertifikat konfiguriert wurde und Sie ein Client-Zertifikat für Prometheus hinzufügen möchten, das die Funktion zum Generieren von Zertifikaten in Grid Manager verwendet.

Schritte

1. Wählen Sie im Grid Manager **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Client**.
2. Wählen Sie **Hinzufügen**.
3. Geben Sie einen Zertifikatsnamen ein.
4. Um mit Ihrem externen Überwachungstool auf Prometheus-Metriken zuzugreifen, wählen Sie **Prometheus zulassen**.
5. Wählen Sie **Weiter**.
6. Wählen Sie für den Schritt **Zertifikate anhängen** die Option **Zertifikat generieren** aus.
7. Geben Sie die Zertifikatsinformationen an:
   - **Betreff** (optional): X.509-Betreff oder Distinguished Name (DN) des Zertifikatsinhabers.
   - **Gültigkeitstage**: Die Anzahl der Tage, die das generierte Zertifikat gültig ist, beginnend mit dem Zeitpunkt der Generierung.
   - **Schlüsselverwendungserweiterungen hinzufügen**: Wenn ausgewählt (Standard und empfohlen), werden dem generierten Zertifikat Schlüsselverwendungs- und erweiterte

Schlüsselverwendungserweiterungen hinzugefügt.

Diese Erweiterungen definieren den Zweck des im Zertifikat enthaltenen Schlüssels.

> Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, Sie haben Verbindungsprobleme mit älteren Clients, wenn die Zertifikate diese Erweiterungen enthalten.

8. Wählen Sie **Generieren**.
9. Wählen Sie **Client-Zertifikatdetails**, um die Zertifikatmetadaten und das Zertifikat-PEM anzuzeigen.

> Nachdem Sie das Dialogfeld geschlossen haben, können Sie den privaten Schlüssel des Zertifikats nicht mehr anzeigen. Kopieren oder laden Sie den Schlüssel an einen sicheren Ort herunter.

   - Wählen Sie **Zertifikat PEM kopieren**, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.
   - Wählen Sie **Zertifikat herunterladen**, um die Zertifikatsdatei zu speichern.

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

     Beispiel: `storagegrid_certificate.pem`

   - Wählen Sie **Privaten Schlüssel kopieren**, um den privaten Schlüssel des Zertifikats zum Einfügen an anderer Stelle zu kopieren.
   - Wählen Sie **Privaten Schlüssel herunterladen**, um den privaten Schlüssel als Datei zu speichern.

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

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

    Das neue Zertifikat wird auf der Registerkarte „Client“ angezeigt.

11. Wählen Sie im Grid Manager **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Global**.
12. Wählen Sie **Management Interface-Zertifikat**.
13. Wählen Sie **Benutzerdefiniertes Zertifikat verwenden**.
14. Laden Sie die Dateien certificate.pem und private_key.pem von derClient-Zertifikatdetails Schritt. Es ist nicht erforderlich, ein CA-Paket hochzuladen.
    a. Wählen Sie **Zertifikat hochladen** und dann **Weiter**.
    b. Laden Sie jede Zertifikatsdatei hoch(`.pem`).
    c. Wählen Sie **Speichern**, um das Zertifikat im Grid Manager zu speichern.

       Das neue Zertifikat wird auf der Zertifikatsseite der Verwaltungsschnittstelle angezeigt.

15. Konfigurieren eines externen Überwachungstools, wie Grafana.

Konfigurieren Sie ein externes Überwachungstool

Schritte

1. Konfigurieren Sie die folgenden Einstellungen in Ihrem externen Überwachungstool, 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 Domänennamen oder die IP-Adresse für den Admin-Knoten ein. Geben Sie HTTPS und Port 9091 an.

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

   c. Aktivieren Sie **TLS-Client-Authentifizierung** und **Mit CA-Zertifikat**.
   d. Kopieren und fügen Sie unter TLS/SSL-Authentifizierungsdetails Folgendes ein:
      - Das CA-Zertifikat der Verwaltungsschnittstelle an **CA Cert**
      - Das Client-Zertifikat an **Client Cert**
      - Der private Schlüssel zum **Client-Schlüssel**
   e. **Servername**: Geben Sie den Domänennamen des Admin-Knotens ein.

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

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

   Sie können jetzt mit Ihrem externen Überwachungstool auf die Prometheus-Metriken von StorageGRID zugreifen.

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

Client-Zertifikate bearbeiten

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

Schritte

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

   Ablaufdaten der Zertifikate und Zugriffsberechtigungen für Prometheus sind in der Tabelle aufgeführt. Läuft ein Zertifikat bald ab oder ist es bereits abgelaufen, erscheint in der Tabelle eine Meldung und es wird ein Alarm ausgelöst.

2. Wählen Sie das Zertifikat aus, das Sie bearbeiten möchten.
3. Wählen Sie **Bearbeiten** und dann **Name und Berechtigung bearbeiten**
4. Geben Sie einen Zertifikatsnamen ein.
5. Um mit Ihrem externen Überwachungstool auf Prometheus-Metriken 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.

Neues Client-Zertifikat anhängen

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

Schritte

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

   Ablaufdaten der Zertifikate und Zugriffsberechtigungen für Prometheus sind in der Tabelle aufgeführt. Läuft ein Zertifikat bald ab oder ist es bereits abgelaufen, erscheint in der Tabelle eine Meldung und es wird ein Alarm ausgelöst.

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

Zertifikat hochladen

Kopieren Sie den Zertifikatstext, um ihn an anderer Stelle einzufügen.

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

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

   Wählen Sie **Client-Zertifikatdetails** aus, um die Zertifikatmetadaten und das Zertifikat-PEM anzuzeigen.

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

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

   Beispiel: `storagegrid_certificate.pem`

   - Wählen Sie **Zertifikat PEM kopieren**, um den Zertifikatsinhalt zum Einfügen an anderer 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 generieren

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

a. Wählen Sie **Zertifikat generieren**.

b. Geben Sie die Zertifikatsinformationen an:

   - **Betreff** (optional): X.509-Betreff oder Distinguished Name (DN) des Zertifikatsinhabers.
   - **Gültigkeitstage**: Die Anzahl der Tage, die das generierte Zertifikat gültig ist, beginnend mit dem Zeitpunkt der Generierung.
   - **Schlüsselverwendungserweiterungen hinzufügen**: Wenn ausgewählt (Standard und empfohlen), werden dem generierten Zertifikat Schlüsselverwendungs- und erweiterte Schlüsselverwendungserweiterungen hinzugefügt.

     Diese Erweiterungen definieren den Zweck des im Zertifikat enthaltenen Schlüssels.

     Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, Sie haben Verbindungsprobleme mit älteren Clients, wenn die Zertifikate diese Erweiterungen enthalten.

c. Wählen Sie **Generieren**.

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

   Nachdem Sie das Dialogfeld geschlossen haben, können Sie den privaten Schlüssel des Zertifikats nicht mehr anzeigen. Kopieren oder laden Sie den Schlüssel an einen sicheren Ort herunter.

- Wählen Sie **Zertifikat PEM kopieren**, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.
- Wählen Sie **Zertifikat herunterladen**, um die Zertifikatsdatei zu speichern.

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

  Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Privaten Schlüssel kopieren**, um den privaten Schlüssel des Zertifikats zum Einfügen an anderer Stelle zu kopieren.
- Wählen Sie **Privaten Schlüssel herunterladen**, um den privaten Schlüssel als Datei zu speichern.

  Geben Sie den Dateinamen des privaten Schlüssels und den Download-Speicherort 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 Client-Zertifikaten

Sie können ein Client-Zertifikat zur Verwendung an anderer Stelle herunterladen oder kopieren.

Schritte

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

Zertifikatsdatei herunterladen

Laden Sie das Zertifikat herunter `.pem` Datei.

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

   Beispiel: `storagegrid_certificate.pem`

Zertifikat kopieren

Kopieren Sie den Zertifikatstext, um ihn an anderer Stelle einzufügen.

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

   Beispiel: `storagegrid_certificate.pem`

Client-Zertifikate entfernen

Wenn Sie ein Administrator-Client-Zertifikat nicht mehr benötigen, können Sie es entfernen.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Zertifikate** und dann die Registerkarte **Client**.
2. Wählen Sie das Zertifikat aus, das Sie entfernen möchten.
3. Wählen Sie **Löschen** und bestätigen Sie anschließend.

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

Nachdem ein Zertifikat entfernt wurde, müssen Clients, die das Zertifikat verwendet haben, ein neues Client-Zertifikat angeben, um auf die StorageGRID Prometheus-Datenbank zugreifen zu können.

Konfigurieren der Sicherheitseinstellungen

Verwalten der TLS- und SSH-Richtlinie

Die TLS- und SSH-Richtlinie bestimmt, welche Protokolle und Chiffren zum Herstellen sicherer TLS-Verbindungen mit Clientanwendungen und sicherer SSH-Verbindungen zu internen StorageGRID Diensten verwendet werden.

Die Sicherheitsrichtlinie steuert, wie TLS und SSH übertragene Daten verschlüsseln. Verwenden Sie im Allgemeinen die moderne Kompatibilitätsrichtlinie (Standard), es sei denn, Ihr System muss Common Criteria-kompatibel 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 beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .

Wählen Sie eine Sicherheitsrichtlinie

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Sicherheitseinstellungen**.

   Auf der Registerkarte **TLS- und SSH-Richtlinien** werden die verfügbaren Richtlinien angezeigt. Die aktuell aktive Richtlinie wird durch ein grünes Häkchen auf der Richtlinienkachel gekennzeichnet.

2. Sehen Sie sich die Kacheln an, um mehr über die verfügbaren Richtlinien zu erfahren.

Politik	Beschreibung
Moderne Kompatibilität (Standard)	Verwenden Sie die Standardrichtlinie, wenn Sie eine starke Verschlüsselung benötigen und keine besonderen Anforderungen haben. Diese Richtlinie ist mit den meisten TLS- und SSH-Clients kompatibel.
Legacy-Kompatibilität	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 streng	Verwenden Sie diese Richtlinie, wenn Sie eine Common Criteria-Zertifizierung benötigen und das NetApp Cryptographic Security Module 3.0.8 für externe Clientverbindungen zu Load Balancer-Endpunkten, Tenant Manager und Grid Manager verwenden müssen. Die Verwendung dieser Richtlinie kann die Leistung beeinträchtigen. **Hinweis**: Nachdem Sie diese Richtlinie ausgewählt haben, müssen alle Knoten"rollierend neu gestartet" um das NetApp Cryptographic Security Module zu aktivieren. Verwenden Sie **Wartung** > **Rollierender Neustart**, um Neustarts zu initiieren und zu überwachen.
Brauch	Erstellen Sie eine benutzerdefinierte Richtlinie, wenn Sie Ihre eigenen Chiffren anwenden müssen.

3. Um Details zu den Chiffren, Protokollen und Algorithmen jeder Richtlinie anzuzeigen, wählen Sie **Details anzeigen**.
4. Um die aktuelle Richtlinie zu ändern, wählen Sie **Richtlinie verwenden**.

   Auf der Richtlinienkachel wird neben **Aktuelle Richtlinie** ein grünes Häkchen angezeigt.

Erstellen einer benutzerdefinierten 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 die Zwischenablage kopieren** und dann **Abbrechen**.

3. Wählen Sie auf der Kachel **Benutzerdefinierte Richtlinie** die Option **Konfigurieren und verwenden** aus.
4. Fügen Sie das kopierte JSON ein und nehmen Sie die erforderlichen Änderungen vor.
5. Wählen Sie **Richtlinie verwenden**.

   Auf der Kachel „Benutzerdefinierte Richtlinie“ wird neben **Aktuelle Richtlinie** ein grünes Häkchen angezeigt.

6. Wählen Sie optional **Konfiguration bearbeiten** aus, um weitere Änderungen an der neuen benutzerdefinierten Richtlinie vorzunehmen.

Vorübergehend zur Standardsicherheitsrichtlinie zurückkehren

Wenn Sie eine benutzerdefinierte Sicherheitsrichtlinie konfiguriert haben, können Sie sich möglicherweise nicht beim Grid Manager anmelden, wenn die konfigurierte TLS-Richtlinie nicht mit der"konfiguriertes Serverzertifikat" .

Sie können vorübergehend zur Standardsicherheitsrichtlinie zurückkehren.

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

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

2. Führen Sie den folgenden Befehl aus:

   ```
   restore-default-cipher-configurations
   ```

3. Greifen Sie über einen Webbrowser auf den Grid Manager auf demselben Admin-Knoten zu.
4. Befolgen Sie die Schritte inWählen Sie eine Sicherheitsrichtlinie um die Richtlinie erneut zu konfigurieren.

Konfigurieren der Netzwerk- und Objektsicherheit

Sie können die Netzwerk- und Objektsicherheit so konfigurieren, dass gespeicherte Objekte verschlüsselt werden, bestimmte S3-Anfragen verhindert werden oder Clientverbindungen zu Speicherknoten HTTP statt HTTPS verwenden.

Gespeicherte Objektverschlüsselung

Die Verschlüsselung gespeicherter Objekte ermöglicht die Verschlüsselung aller Objektdaten, wenn diese über S3 aufgenommen werden. Standardmäßig werden gespeicherte Objekte nicht verschlüsselt, Sie können die Objekte jedoch mit dem Verschlüsselungsalgorithmus AES-128 oder AES-256 verschlüsseln. Wenn Sie die Einstellung aktivieren, werden alle neu aufgenommenen Objekte verschlüsselt, es werden jedoch keine Änderungen an vorhandenen gespeicherten Objekten vorgenommen. Wenn Sie die Verschlüsselung deaktivieren, bleiben aktuell verschlüsselte Objekte verschlüsselt, neu aufgenommene Objekte werden jedoch nicht verschlüsselt.

Die Einstellung „Gespeicherte Objektverschlüsselung“ gilt nur für S3-Objekte, die nicht durch Verschlüsselung auf Bucket- oder Objektebene verschlüsselt wurden.

Weitere Informationen zu den Verschlüsselungsmethoden von StorageGRID finden Sie unter"Überprüfen Sie die Verschlüsselungsmethoden von StorageGRID" .

Client-Änderungen verhindern

„Client-Änderungen verhindern“ ist eine systemweite Einstellung. Wenn die Option **Client-Änderung verhindern** ausgewählt ist, werden die folgenden Anfragen abgelehnt.

S3 REST API

- DeleteBucket-Anfragen
- Alle Anfragen zum Ändern der Daten eines vorhandenen Objekts, benutzerdefinierter Metadaten oder S3-Objekt-Tagging

Aktivieren Sie HTTP für Storage Node-Verbindungen

Standardmäßig verwenden Clientanwendungen das HTTPS-Netzwerkprotokoll für alle direkten Verbindungen zu Speicherknoten. Sie können HTTP für diese Verbindungen optional aktivieren, beispielsweise beim Testen eines Nicht-Produktionsrasters.

Verwenden Sie HTTP für Speicherknotenverbindungen nur, wenn S3-Clients HTTP-Verbindungen direkt zu Speicherknoten 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"Konfigurieren Sie jeden Load Balancer-Endpunkt" um entweder HTTP oder HTTPS zu verwenden).

Sehen"Zusammenfassung: IP-Adressen und Ports für Clientverbindungen" um zu erfahren, welche Ports S3-Clients verwenden, wenn sie über HTTP oder HTTPS eine Verbindung zu Speicherknoten herstellen.

Ausführung wählen

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie verfügen über Root-Zugriffsberechtigung.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Sicherheitseinstellungen**.
2. Wählen Sie die Registerkarte **Netzwerk und Objekte**.
3. Verwenden Sie für die Verschlüsselung gespeicherter Objekte die Einstellung **Keine** (Standard), wenn Sie keine Verschlüsselung gespeicherter Objekte wünschen, oder wählen Sie **AES-128** oder **AES-256**, um gespeicherte Objekte zu verschlüsseln.
4. Wählen Sie optional **Client-Änderung verhindern** aus, wenn Sie verhindern möchten, dass S3-Clients bestimmte Anfragen stellen.

> Wenn Sie diese Einstellung ändern, dauert es etwa eine Minute, bis die neue Einstellung übernommen wird. Der konfigurierte Wert wird aus Leistungs- und Skalierungsgründen zwischengespeichert.

5. Wählen Sie optional **HTTP für Speicherknotenverbindungen aktivieren** aus, wenn Clients eine direkte Verbindung zu Speicherknoten herstellen und Sie HTTP-Verbindungen verwenden möchten.

> Seien Sie vorsichtig, wenn Sie HTTP für ein Produktionsraster aktivieren, da Anfragen unverschlüsselt gesendet werden.

6. Wählen Sie **Speichern**.

Ändern der Schnittstellensicherheitseinstellungen

Über die Sicherheitseinstellungen der Schnittstelle können Sie steuern, ob Benutzer abgemeldet werden, wenn sie länger als die angegebene Zeit inaktiv sind, und ob in den API-Fehlerantworten ein Stacktrace enthalten sein soll.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Du hast"Root-Zugriffsberechtigung" .

Informationen zu diesem Vorgang

Die Seite **Sicherheitseinstellungen** enthält die Einstellungen **Browser-Inaktivitäts-Timeout** und **Management-API-Stack-Trace**.

Browser-Inaktivitäts-Timeout

Gibt an, wie lange der Browser eines Benutzers inaktiv sein kann, bevor der Benutzer abgemeldet wird. Der Standardwert beträgt 15 Minuten.

Das Timeout für Browserinaktivität wird auch durch Folgendes gesteuert:

- Ein separater, nicht konfigurierbarer StorageGRID Timer, der zur Systemsicherheit enthalten ist. Das Authentifizierungstoken jedes Benutzers läuft 16 Stunden nach der Anmeldung des Benutzers ab. Wenn die Authentifizierung eines Benutzers abläuft, wird dieser Benutzer automatisch abgemeldet, auch wenn das Inaktivitätstimeout 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 Identitätsanbieter, vorausgesetzt, Single Sign-On (SSO) ist für StorageGRID aktiviert.

  Wenn SSO aktiviert ist und es beim Browser eines Benutzers zu einer Zeitüberschreitung kommt, muss der Benutzer seine SSO-Anmeldeinformationen erneut eingeben, um wieder auf StorageGRID

zugreifen zu können. Sehen "Konfigurieren der einmaligen Anmeldung" .

Stapelüberwachung der Verwaltungs-API

Steuert, ob in den Fehlerantworten der Grid Manager- und Tenant Manager-API ein Stacktrace zurückgegeben wird.

Diese Option ist standardmäßig deaktiviert, Sie möchten diese Funktion jedoch möglicherweise für eine Testumgebung aktivieren. Im Allgemeinen sollten Sie den Stacktrace in Produktionsumgebungen deaktiviert lassen, um zu vermeiden, dass beim Auftreten von API-Fehlern interne Softwaredetails preisgegeben werden.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Sicherheitseinstellungen**.
2. Wählen Sie die Registerkarte **Schnittstelle**.
3. So ändern Sie die Einstellung für das Inaktivitäts-Timeout des Browsers:
   a. Erweitern Sie das Akkordeon.
   b. Um die Zeitüberschreitungsdauer zu ändern, geben Sie einen Wert zwischen 60 Sekunden und 7 Tagen an. Das Standard-Timeout beträgt 15 Minuten.
   c. Um diese Funktion zu deaktivieren, deaktivieren Sie das Kontrollkästchen.
   d. Wählen Sie **Speichern**.

      Die neue Einstellung wirkt sich nicht auf Benutzer aus, die derzeit angemeldet sind. Benutzer müssen sich erneut anmelden oder ihren Browser aktualisieren, damit die neue Timeout-Einstellung wirksam wird.

4. So ändern Sie die Einstellung für den Management-API-Stack-Trace:
   a. Erweitern Sie das Akkordeon.
   b. Aktivieren Sie das Kontrollkästchen, um in den Fehlerantworten der Grid Manager- und Tenant Manager-API einen Stacktrace zurückzugeben.

      Lassen Sie den Stacktrace in Produktionsumgebungen deaktiviert, um zu vermeiden, dass beim Auftreten von API-Fehlern interne Softwaredetails preisgegeben werden.

   c. Wählen Sie **Speichern**.

Konfigurieren von Schlüsselverwaltungsservern

Was ist ein Schlüsselverwaltungsserver (KMS)?

Ein Schlüsselverwaltungsserver (KMS) ist ein externes Drittanbietersystem, das mithilfe des Key Management Interoperability Protocol (KMIP) Verschlüsselungsschlüssel für StorageGRID Appliance-Knoten am zugehörigen StorageGRID Standort bereitstellt.

StorageGRID unterstützt nur bestimmte Schlüsselverwaltungsserver. Eine Liste der unterstützten Produkte und Versionen finden Sie im "NetApp Interoperability Matrix Tool (IMT)" .

Sie können einen oder mehrere Schlüsselverwaltungsserver verwenden, um die Knotenverschlüsselungsschlüssel für alle StorageGRID Appliance-Knoten zu verwalten, bei denen während der Installation die Einstellung **Knotenverschlüsselung** aktiviert wurde. Durch die Verwendung von

Schlüsselverwaltungsservern mit diesen Appliance-Knoten können Sie Ihre Daten schützen, selbst wenn eine Appliance aus dem Rechenzentrum entfernt wird. Nachdem die Appliance-Volumes verschlüsselt wurden, können Sie auf keine Daten auf der Appliance zugreifen, es sei denn, der Knoten kann mit dem KMS kommunizieren.

> StorageGRID erstellt oder verwaltet die externen Schlüssel, die zum Verschlüsseln und Entschlüsseln von Appliance-Knoten verwendet werden, nicht. Wenn Sie zum Schutz von StorageGRID -Daten einen externen Schlüsselverwaltungsserver verwenden möchten, müssen Sie wissen, wie dieser Server eingerichtet wird und wie die Verschlüsselungsschlüssel verwaltet werden. Die Durchführung wichtiger Verwaltungsaufgaben geht über den Rahmen dieser Anweisungen hinaus. Wenn Sie Hilfe benötigen, lesen Sie die Dokumentation zu Ihrem Schlüsselverwaltungsserver oder wenden Sie sich an den technischen Support.

KMS- und Appliance-Konfiguration

Bevor Sie einen Schlüsselverwaltungsserver (KMS) zum Sichern von StorageGRID -Daten auf Appliance-Knoten verwenden können, müssen Sie zwei Konfigurationsaufgaben ausführen: Einrichten eines oder mehrerer KMS-Server und Aktivieren der Knotenverschlüsselung für die Appliance-Knoten. Wenn diese beiden Konfigurationsaufgaben abgeschlossen sind, erfolgt der Schlüsselverwaltungsprozess automatisch.

Das Flussdiagramm zeigt die allgemeinen Schritte zur Verwendung eines KMS zum Sichern von StorageGRID -Daten auf Appliance-Knoten.

Das Flussdiagramm zeigt, dass die KMS-Einrichtung und die Einrichtung der Appliance parallel erfolgen. Sie können die Schlüsselverwaltungsserver jedoch je nach Ihren Anforderungen vor oder nach der Aktivierung der Knotenverschlüsselung für neue Appliance-Knoten einrichten.

Einrichten des Schlüsselverwaltungsservers (KMS)

Das Einrichten eines Schlüsselverwaltungsservers umfasst die folgenden allgemeinen 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"
Besorgen Sie sich die erforderlichen Informationen für den StorageGRID -Client auf dem KMS.	"Konfigurieren Sie StorageGRID als Client im KMS"
Fügen Sie das KMS zum Grid Manager hinzu, weisen Sie es einer einzelnen Site oder einer Standardgruppe von Sites zu, laden Sie die erforderlichen Zertifikate hoch und speichern Sie die KMS-Konfiguration.	"Hinzufügen eines Schlüsselverwaltungsservers (KMS)"

Einrichten der Appliance

Das Einrichten eines Appliance-Knotens für die KMS-Verwendung umfasst die folgenden allgemeinen Schritte.

1. Verwenden Sie während der Hardwarekonfigurationsphase der Appliance-Installation das StorageGRID Appliance Installer, um die Einstellung **Knotenverschlüsselung** für die Appliance zu aktivieren.

   > Sie können die Einstellung **Knotenverschlüsselung** nicht aktivieren, nachdem eine Appliance zum Grid hinzugefügt wurde, und Sie können die externe Schlüsselverwaltung nicht für Appliances verwenden, bei denen die Knotenverschlüsselung nicht aktiviert ist.

2. Führen Sie das StorageGRID Appliance-Installationsprogramm aus. Während der Installation wird jedem Appliance-Volume wie folgt ein zufälliger Datenverschlüsselungsschlüssel (DEK) zugewiesen:
   - Die DEKs werden zum Verschlüsseln der Daten auf jedem Volume verwendet. Diese Schlüssel werden mithilfe der Linux Unified Key Setup (LUKS)-Festplattenverschlüsselung im Betriebssystem der Appliance generiert und können nicht geändert werden.
   - Jeder einzelne DEK wird durch einen Master-Key-Verschlüsselungsschlüssel (KEK) verschlüsselt. Der anfängliche KEK ist ein temporärer Schlüssel, der die DEKs verschlüsselt, bis das Gerät eine Verbindung zum KMS herstellen kann.
3. Fügen Sie den Appliance-Knoten zu StorageGRID hinzu.

Sehen "Knotenverschlüsselung aktivieren" für Details.

Schlüsselverwaltungs-Verschlüsselungsprozess (erfolgt automatisch)

Die Schlüsselverwaltungsverschlüsselung umfasst die folgenden Schritte auf hoher Ebene, die automatisch ausgeführt werden.

1. Wenn Sie eine Appliance mit aktivierter Knotenverschlüsselung im Grid installieren, ermittelt StorageGRID , ob für die Site, die den neuen Knoten enthält, eine KMS-Konfiguration vorhanden ist.
   - Wenn für die Site bereits ein KMS konfiguriert wurde, erhält die Appliance die KMS-Konfiguration.
   - Wenn für die Site noch kein KMS konfiguriert wurde, werden die Daten auf der Appliance weiterhin durch den temporären KEK verschlüsselt, bis Sie für die Site ein KMS 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. Das KMS sendet einen Verschlüsselungsschlüssel an das Gerät. Der neue Schlüssel vom KMS ersetzt den temporären KEK und wird nun zum Verschlüsseln und Entschlüsseln der DEKs für die Appliance-Volumes verwendet.

   > Alle Daten, die vorhanden sind, bevor der verschlüsselte Appliance-Knoten eine Verbindung zum konfigurierten KMS herstellt, werden mit einem temporären Schlüssel verschlüsselt. Allerdings sollten die Appliance-Volumes erst dann als vor der Entfernung aus dem Rechenzentrum geschützt betrachtet werden, wenn der temporäre Schlüssel durch den KMS-Verschlüsselungsschlüssel ersetzt wurde.

4. Wenn das Gerät eingeschaltet oder neu gestartet wird, stellt es erneut eine Verbindung zum KMS her, um den Schlüssel anzufordern. Der im flüchtigen Speicher gespeicherte Schlüssel übersteht einen Stromausfall oder Neustart nicht.

Überlegungen und Anforderungen zur Verwendung eines Schlüsselverwaltungsservers

Bevor Sie einen externen Schlüsselverwaltungsserver (KMS) konfigurieren, müssen Sie die Überlegungen und Anforderungen verstehen.

Welche Version von KMIP wird unterstützt?

StorageGRID unterstützt KMIP Version 1.4.

"Key Management Interoperability Protocol-Spezifikation Version 1.4"

Welche Netzwerkaspekte sind zu berücksichtigen?

Die Netzwerk-Firewall-Einstellungen müssen jedem Appliance-Knoten die Kommunikation über den für die KMIP-Kommunikation (Key Management Interoperability Protocol) verwendeten Port ermöglichen. Der Standard-KMIP-Port ist 5696.

Sie müssen sicherstellen, dass jeder Appliance-Knoten, der Knotenverschlüsselung verwendet, Netzwerkzugriff auf den KMS oder KMS-Cluster hat, den Sie für die Site konfiguriert haben.

Welche TLS-Versionen werden unterstützt?

Die Kommunikation zwischen den Appliance-Knoten und dem konfigurierten KMS erfolgt über sichere TLS-Verbindungen. StorageGRID kann entweder das TLS 1.2- oder das TLS 1.3-Protokoll unterstützen, wenn es KMIP-Verbindungen zu einem KMS oder KMS-Cluster herstellt, je nachdem, was das KMS unterstützt und welche"TLS- und SSH-Richtlinie" Sie verwenden.

StorageGRID handelt beim Herstellen der Verbindung das Protokoll und die Verschlüsselung (TLS 1.2) oder die Verschlüsselungssuite (TLS 1.3) mit dem KMS aus. Um zu sehen, welche Protokollversionen und Chiffren/Chiffrensammlungen verfügbar sind, lesen Sie die `tlsOutbound` Abschnitt der aktiven TLS- und SSH-Richtlinie des Grids (**KONFIGURATION** > **Sicherheit Sicherheitseinstellungen**).

Welche Geräte werden unterstützt?

Sie können einen Schlüsselverwaltungsserver (KMS) verwenden, um Verschlüsselungsschlüssel für jedes StorageGRID Gerät in Ihrem Grid zu verwalten, bei dem die Einstellung **Knotenverschlüsselung** aktiviert ist. Diese Einstellung kann nur während der Hardwarekonfigurationsphase der Geräteinstallation mit dem StorageGRID Appliance Installer aktiviert werden.

> Sie können die Knotenverschlüsselung nicht aktivieren, nachdem ein Gerät zum Grid hinzugefügt wurde, und Sie können die externe Schlüsselverwaltung nicht für Geräte verwenden, bei denen die Knotenverschlüsselung nicht aktiviert ist.

Sie können das konfigurierte KMS für StorageGRID -Geräte und Geräteknoten verwenden.

Sie können den konfigurierten KMS nicht für softwarebasierte (nicht-Appliance-)Knoten verwenden, einschließlich der folgenden:

- Als virtuelle Maschinen (VMs) bereitgestellte Knoten
- In Container-Engines auf Linux-Hosts bereitgestellte Knoten

Auf diesen anderen Plattformen bereitgestellte Knoten können die Verschlüsselung außerhalb von StorageGRID auf Datenspeicher- oder Festplattenebene verwenden.

Wann sollte ich Schlüsselverwaltungsserver konfigurieren?

Bei einer Neuinstallation sollten Sie normalerweise einen oder mehrere Schlüsselverwaltungsserver im Grid Manager einrichten, bevor Sie Mandanten erstellen. Diese Reihenfolge stellt sicher, dass die Knoten geschützt sind, bevor Objektdaten auf ihnen gespeichert werden.

Sie können die Schlüsselverwaltungsserver im Grid Manager vor oder nach der Installation der Appliance-Knoten konfigurieren.

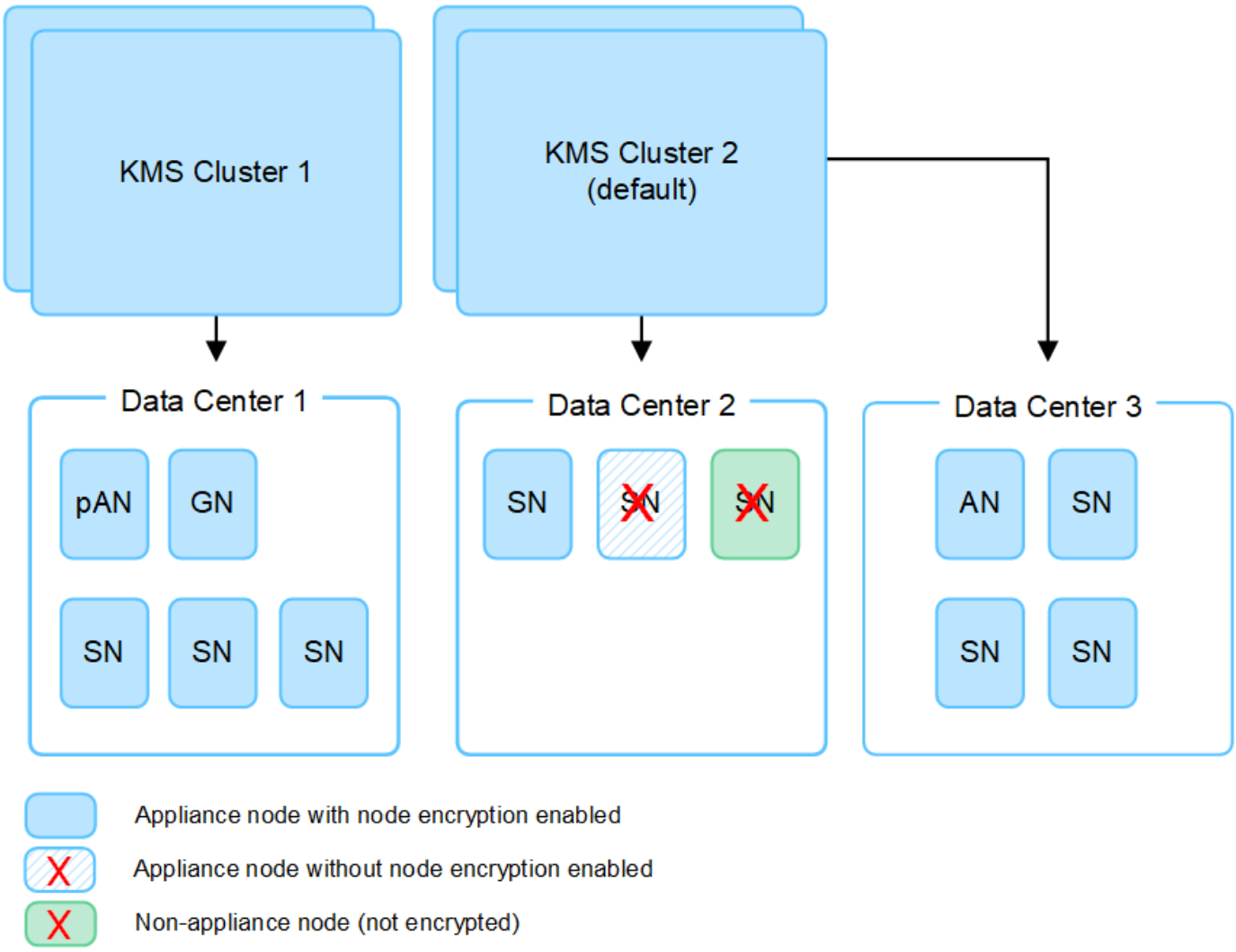
Wie viele Schlüsselverwaltungsserver benötige ich?

Sie können einen oder mehrere externe Schlüsselverwaltungsserver konfigurieren, um den Appliance-Knoten in Ihrem StorageGRID System Verschlüsselungsschlüssel bereitzustellen. Jeder KMS stellt den StorageGRID Appliance-Knoten an einem einzelnen Standort oder einer Gruppe von Standorten einen einzelnen Verschlüsselungsschlüssel bereit.

StorageGRID unterstützt die Verwendung von KMS-Clustern. Jeder KMS-Cluster enthält mehrere replizierte Schlüsselverwaltungsserver, die Konfigurationseinstellungen und Verschlüsselungsschlüssel gemeinsam nutzen. Die Verwendung von KMS-Clustern für die Schlüsselverwaltung wird empfohlen, da dadurch die Failover-Funktionen einer Hochverfügbarkeitskonfiguration verbessert werden.

Nehmen wir beispielsweise an, Ihr StorageGRID -System verfügt über drei Rechenzentrumsstandorte. Sie können einen KMS-Cluster so konfigurieren, dass er allen Appliance-Knoten im Rechenzentrum 1 einen Schlüssel bereitstellt, und einen zweiten KMS-Cluster, der allen Appliance-Knoten an allen anderen Standorten einen Schlüssel bereitstellt. Wenn Sie den zweiten KMS-Cluster hinzufügen, können Sie ein Standard-KMS für Data Center 2 und Data Center 3 konfigurieren.

Beachten Sie, dass Sie keinen KMS für Nicht-Appliance-Knoten oder für Appliance-Knoten verwenden können, bei denen die Einstellung **Knotenverschlüsselung** während der Installation nicht aktiviert wurde.



Was passiert, wenn ein Schlüssel rotiert wird?

Als bewährte Sicherheitsmaßnahme sollten Sie regelmäßig"Rotieren Sie den Verschlüsselungsschlüssel" wird von jedem konfigurierten KMS verwendet.

Wenn die neue Schlüsselversion verfügbar ist:

- Es wird automatisch an die verschlüsselten Appliance-Knoten an dem oder den mit dem KMS verbundenen Standorten verteilt. Die Verteilung sollte innerhalb einer Stunde nach der Schlüsselrotation erfolgen.
- Wenn der verschlüsselte Appliance-Knoten offline ist, wenn die neue Schlüsselversion verteilt wird, erhält der Knoten den neuen Schlüssel, sobald er neu gestartet wird.
- Wenn die neue Schlüsselversion aus irgendeinem Grund nicht zum Verschlüsseln von Appliance-Volumes verwendet werden kann, wird für den Appliance-Knoten die Warnung **Rotation des KMS-Verschlüsselungsschlüssels fehlgeschlagen** ausgelöst. Möglicherweise müssen Sie sich an den technischen Support wenden, um Hilfe bei der Lösung dieser Warnung zu erhalten.

Kann ich einen Appliance-Knoten nach der Verschlüsselung wiederverwenden?

Wenn Sie ein verschlüsseltes Gerät in einem anderen StorageGRID -System installieren müssen, müssen Sie zuerst den Grid-Knoten außer Betrieb nehmen, um Objektdaten auf einen anderen Knoten zu verschieben.

Anschließend können Sie den StorageGRID Appliance Installer verwenden, um "Löschen Sie die KMS-Konfiguration" . Durch das Löschen der KMS-Konfiguration wird die Einstellung **Knotenverschlüsselung** deaktiviert und die Verknüpfung zwischen dem Appliance-Knoten und der KMS-Konfiguration für die StorageGRID -Site entfernt.

> Ohne Zugriff auf den KMS-Verschlüsselungsschlüssel sind alle auf dem Gerät verbleibenden Daten nicht mehr zugänglich und dauerhaft gesperrt.

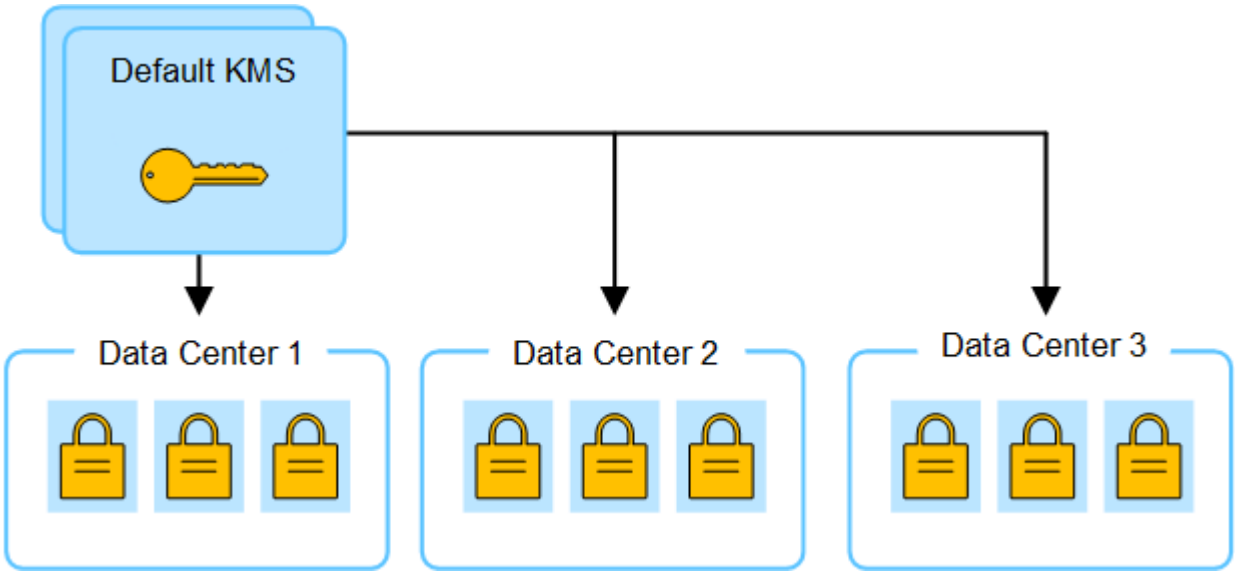
Überlegungen zum Ändern des KMS für eine Site

Jeder Schlüsselverwaltungsserver (KMS) oder KMS-Cluster stellt allen Appliance-Knoten an einem einzelnen Standort oder einer Gruppe von Standorten einen Verschlüsselungsschlüssel bereit. Wenn Sie ändern müssen, welches KMS für eine Site verwendet wird, müssen Sie möglicherweise den Verschlüsselungsschlüssel von einem KMS in ein anderes kopieren.

Wenn Sie das für eine Site verwendete KMS ändern, müssen Sie sicherstellen, dass die zuvor verschlüsselten Appliance-Knoten an dieser Site 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 in das neue KMS kopieren. Sie müssen sicherstellen, dass das KMS über den richtigen Schlüssel zum Entschlüsseln der verschlüsselten Appliance-Knoten am Standort verfügt.

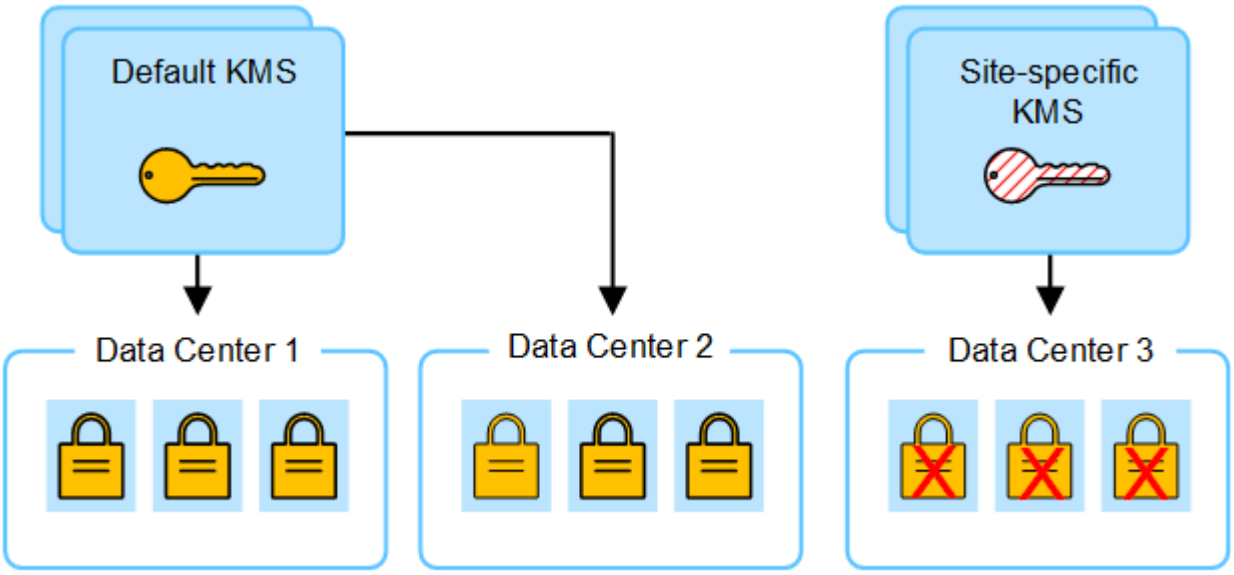
Beispiel:

1. Sie konfigurieren zunächst ein Standard-KMS, das für alle Sites gilt, die nicht über ein dediziertes KMS verfügen.
2. Wenn das KMS gespeichert ist, stellen alle Appliance-Knoten, bei denen die Einstellung **Knotenverschlüsselung** aktiviert ist, eine Verbindung zum KMS her und fordern den Verschlüsselungsschlüssel an. Dieser Schlüssel wird zum Verschlüsseln der Appliance-Knoten an allen Standorten verwendet. Derselbe Schlüssel muss auch zum Entschlüsseln dieser Geräte verwendet werden.

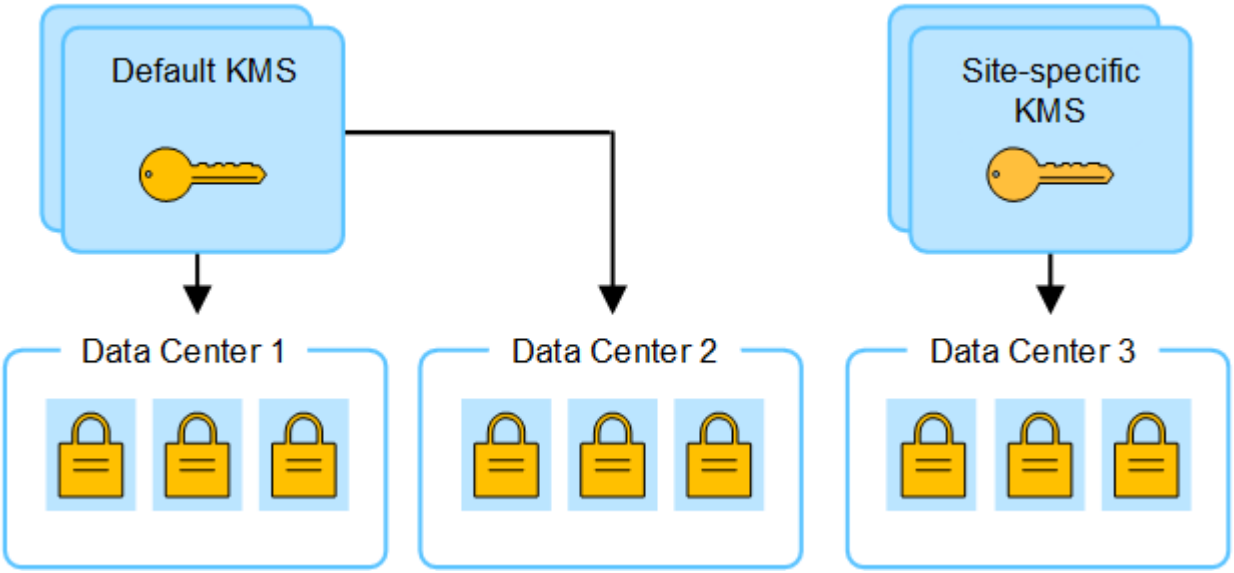


3. Sie entscheiden sich, für einen Standort (Rechenzentrum 3 in der Abbildung) ein standortspezifisches KMS hinzuzufügen. Da die Appliance-Knoten jedoch bereits verschlüsselt sind, tritt ein Validierungsfehler auf, wenn Sie versuchen, die Konfiguration für das standortspezifische KMS zu speichern. Der Fehler tritt

auf, weil das standortspezifische KMS nicht über den richtigen Schlüssel zum Entschlüsseln der Knoten an diesem Standort verfügt.



4. Um das Problem zu beheben, kopieren Sie die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS in das neue KMS. (Technisch gesehen kopieren Sie den Originalschlüssel in einen neuen Schlüssel mit demselben Alias. Der Originalschlüssel wird zu einer früheren Version des neuen Schlüssels.) Das standortspezifische KMS verfügt jetzt über den richtigen Schlüssel zum Entschlüsseln der Appliance-Knoten im Rechenzentrum 3, sodass es in StorageGRID gespeichert werden kann.



Anwendungsfälle zum Ändern des für eine Site verwendeten KMS

Die Tabelle fasst die erforderlichen Schritte für die gängigsten Fälle zum Ändern des KMS für eine Site zusammen.

Anwendungsfall zum Ändern des KMS einer Site	Erforderliche Schritte
Sie haben einen oder mehrere standortspezifische KMS-Einträge und möchten einen davon als Standard-KMS verwenden.	Bearbeiten Sie das standortspezifische KMS. Wählen Sie im Feld **Verwaltet Schlüssel für** die Option **Sites, die nicht von einem anderen KMS verwaltet werden (Standard-KMS)** aus. Das standortspezifische KMS wird jetzt als Standard-KMS verwendet. Dies gilt für alle Sites, die nicht über ein dediziertes KMS verfügen. "Bearbeiten eines Schlüsselverwaltungsservers (KMS)"
Sie haben ein Standard-KMS und fügen in einer Erweiterung eine neue Site hinzu. Sie möchten für die neue Site nicht das Standard-KMS verwenden.	1. Wenn die Appliance-Knoten am neuen Standort bereits vom Standard-KMS verschlüsselt wurden, verwenden Sie die KMS-Software, um die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS auf ein neues KMS zu kopieren. 2. Fügen Sie mithilfe des Grid Managers das neue KMS hinzu und wählen Sie die Site aus. "Hinzufügen eines Schlüsselverwaltungsservers (KMS)"
Sie möchten, dass das KMS für eine Site einen anderen Server verwendet.	1. Wenn die Appliance-Knoten am Standort bereits vom vorhandenen KMS verschlüsselt wurden, verwenden Sie die KMS-Software, um die aktuelle Version des Verschlüsselungsschlüssels vom vorhandenen KMS auf das neue KMS zu kopieren. 2. Bearbeiten Sie mithilfe des Grid Managers die vorhandene KMS-Konfiguration und geben Sie den neuen Hostnamen oder die neue IP-Adresse ein. "Hinzufügen eines Schlüsselverwaltungsservers (KMS)"

Konfigurieren Sie StorageGRID als Client im KMS

Sie müssen StorageGRID als Client für jeden externen Schlüsselverwaltungsserver oder KMS-Cluster konfigurieren, bevor Sie das KMS zu StorageGRID hinzufügen können.

Diese Anweisungen gelten für Thales CipherTrust Manager und Hashicorp Vault. Eine Liste der unterstützten Produkte und Versionen finden Sie im "NetApp Interoperability Matrix Tool (IMT)" .

Schritte

1. Erstellen Sie mit der KMS-Software einen StorageGRID Client für jedes KMS oder jeden KMS-Cluster, den Sie verwenden möchten.

   Jedes KMS verwaltet einen einzelnen Verschlüsselungsschlüssel für die StorageGRID -Geräteknoten an einem einzelnen Standort oder einer Gruppe von Standorten.

2. Erstellen Sie einen Schlüssel mit einer der folgenden beiden Methoden:
   - Verwenden Sie die Schlüsselverwaltungsseite Ihres KMS-Produkts. Erstellen Sie für jeden KMS oder KMS-Cluster einen AES-Verschlüsselungsschlüssel.

     Der Verschlüsselungsschlüssel muss mindestens 2.048 Bit lang sein und exportierbar sein.

- Lassen Sie den Schlüssel von StorageGRID erstellen. Sie werden beim Testen und Speichern danach aufgefordert"Hochladen von Client-Zertifikaten" .

3. Notieren Sie die folgenden Informationen für jeden KMS oder KMS-Cluster.

   Sie benötigen diese Informationen, wenn Sie das KMS zu StorageGRID hinzufügen:

   - Hostname oder IP-Adresse für jeden Server.
   - Vom KMS verwendeter KMIP-Port.
   - Schlüsselalias für den Verschlüsselungsschlüssel im KMS.

4. Besorgen Sie sich für jeden KMS oder KMS-Cluster ein von einer Zertifizierungsstelle (CA) signiertes Serverzertifikat oder ein Zertifikatspaket, das alle PEM-codierten CA-Zertifikatsdateien enthält, die in der Reihenfolge der Zertifikatskette aneinandergereiht sind.

   Das Serverzertifikat ermöglicht dem externen KMS, sich gegenüber StorageGRID zu authentifizieren.

   - Das Zertifikat muss das Base-64-codierte X.509-Format von Privacy Enhanced Mail (PEM) verwenden.
   - Das Feld „Subject Alternative Name“ (SAN) in jedem Serverzertifikat muss den vollqualifizierten 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 in das Feld **Hostname** eingeben.

   - Das Serverzertifikat muss mit dem von der KMIP-Schnittstelle des KMS verwendeten Zertifikat übereinstimmen, das normalerweise Port 5696 verwendet.

5. Besorgen Sie sich das öffentliche Client-Zertifikat, das vom externen KMS an StorageGRID ausgestellt wurde, und den privaten Schlüssel für das Client-Zertifikat.

   Das Client-Zertifikat ermöglicht StorageGRID , sich gegenüber dem KMS zu authentifizieren.

Hinzufügen eines Schlüsselverwaltungsservers (KMS)

Sie verwenden den StorageGRID Key Management Server-Assistenten, um jeden KMS oder KMS-Cluster hinzuzufügen.

Bevor Sie beginnen

- Sie haben die"Überlegungen und Anforderungen zur Verwendung eines Schlüsselverwaltungsservers" .
- Du hast"StorageGRID als Client im KMS konfiguriert" , und Sie verfügen über die erforderlichen Informationen für jeden KMS oder KMS-Cluster.
- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .

Informationen zu diesem Vorgang

Konfigurieren Sie nach Möglichkeit alle standortspezifischen Schlüsselverwaltungsserver, bevor Sie ein Standard-KMS konfigurieren, das für alle Standorte gilt, die nicht von einem anderen KMS verwaltet werden. Wenn Sie zuerst das Standard-KMS erstellen, werden alle knotenverschlüsselten Appliances im Grid durch das Standard-KMS verschlüsselt. Wenn Sie später ein standortspezifisches KMS erstellen möchten, müssen Sie zunächst die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS in das neue KMS kopieren. Sehen"Überlegungen zum Ändern des KMS für eine Site" für Details.

Schritt 1: KMS-Details

In Schritt 1 (KMS-Details) des Assistenten „Schlüsselverwaltungsserver hinzufügen“ geben Sie Details zum KMS oder KMS-Cluster an.

Schritte

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

   Die Seite „Schlüsselverwaltungsserver“ wird mit der ausgewählten Registerkarte „Konfigurationsdetails“ angezeigt.

2. Wählen Sie **Erstellen**.

   Schritt 1 (KMS-Details) des Assistenten „Schlüsselverwaltungsserver hinzufügen“ wird angezeigt.

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

Feld	Beschreibung
KMS-Name	Ein beschreibender Name, der Ihnen bei der Identifizierung dieses KMS hilft. Muss zwischen 1 und 64 Zeichen lang sein.
Schlüsselname	Der genaue Schlüsselalias für den StorageGRID -Client im KMS. Muss zwischen 1 und 255 Zeichen lang sein. **Hinweis**: Wenn Sie mit Ihrem KMS-Produkt keinen Schlüssel erstellt haben, werden Sie aufgefordert, den Schlüssel von StorageGRID erstellen zu lassen.
Verwaltet Schlüssel für	Die StorageGRID -Site, die mit diesem KMS verknüpft wird. Wenn möglich, sollten Sie alle standortspezifischen Schlüsselverwaltungsserver konfigurieren, bevor Sie ein Standard-KMS konfigurieren, das für alle Standorte gilt, die nicht von einem anderen KMS verwaltet werden. • Wählen Sie einen Standort aus, wenn dieses KMS die Verschlüsselungsschlüssel für die Appliance-Knoten an einem bestimmten Standort verwalten soll. • Wählen Sie **Sites, die nicht von einem anderen KMS verwaltet werden (Standard-KMS)** aus, um ein Standard-KMS zu konfigurieren, das für alle Sites gilt, die nicht über ein dediziertes KMS verfügen, sowie 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 vom Standard-KMS verschlüsselt wurde, Sie dem neuen KMS jedoch nicht die aktuelle Version des ursprünglichen Verschlüsselungsschlüssels bereitgestellt haben.

Feld	Beschreibung
Hafen	Der Port, den der KMS-Server für die KMIP-Kommunikation (Key Management Interoperability Protocol) verwendet. Der Standardwert ist 5696, der KMIP-Standardport.
Hostname	Der vollqualifizierte 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 in einem KMS-Cluster herstellen.

4. Wenn Sie einen KMS-Cluster konfigurieren, wählen Sie **Weiteren Hostnamen hinzufügen** aus, um für jeden Server im Cluster einen Hostnamen hinzuzufügen.
5. Wählen Sie **Weiter**.

Schritt 2: Server-Zertifikat hochladen

In Schritt 2 (Serverzertifikat hochladen) des Assistenten „Schlüsselverwaltungsserver hinzufügen“ laden Sie das Serverzertifikat (oder Zertifikatspaket) für den KMS hoch. Das Serverzertifikat ermöglicht dem externen KMS, sich gegenüber StorageGRID zu authentifizieren.

Schritte

1. Navigieren Sie in **Schritt 2 (Serverzertifikat hochladen)** zum Speicherort des gespeicherten Serverzertifikats oder Zertifikatspakets.
2. Laden Sie die Zertifikatsdatei hoch.

   Die Metadaten des Serverzertifikats werden angezeigt.

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

3. Wählen Sie **Weiter**.

Schritt 3: Client-Zertifikate hochladen

In Schritt 3 (Client-Zertifikate hochladen) des Assistenten „Schlüsselverwaltungsserver hinzufügen“ laden Sie das Client-Zertifikat und den privaten Schlüssel des Client-Zertifikats hoch. Das Client-Zertifikat ermöglicht StorageGRID , sich gegenüber dem KMS zu authentifizieren.

Schritte

1. Navigieren Sie in **Schritt 3 (Client-Zertifikate hochladen)** zum Speicherort des Client-Zertifikats.
2. Laden Sie die Client-Zertifikatdatei hoch.

   Die Metadaten des Client-Zertifikats werden angezeigt.

3. Navigieren Sie zum Speicherort des privaten Schlüssels für das Client-Zertifikat.
4. Laden Sie die private Schlüsseldatei hoch.
5. Wählen Sie **Testen und speichern**.

Wenn kein Schlüssel vorhanden ist, werden Sie aufgefordert, StorageGRID einen erstellen zu lassen.

Die Verbindungen zwischen dem Schlüsselverwaltungsserver und den Appliance-Knoten werden getestet. Wenn alle Verbindungen gültig sind und der richtige Schlüssel auf dem KMS gefunden wird, wird der neue Schlüsselverwaltungsserver der Tabelle auf der Seite „Schlüsselverwaltungsserver“ hinzugefügt.

> Unmittelbar nachdem Sie einen KMS hinzugefügt haben, wird der Zertifikatsstatus auf der Seite „Schlüsselverwaltungsserver“ als „Unbekannt“ angezeigt. Es kann bis zu 30 Minuten dauern, bis StorageGRID den tatsächlichen Status jedes Zertifikats abruft. Sie müssen Ihren Webbrowser aktualisieren, um den aktuellen Status anzuzeigen.

6. Wenn beim Auswählen von **Testen und speichern** eine Fehlermeldung angezeigt wird, überprüfen Sie die Nachrichtendetails und wählen Sie dann **OK**.

   Beispielsweise erhalten Sie möglicherweise den Fehler „422: Unprocessable Entity“, wenn ein Verbindungstest fehlgeschlagen ist.

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

   > Durch Auswahl von **Speichern erzwingen** wird die KMS-Konfiguration gespeichert, die externe Verbindung von jedem Gerät zu diesem KMS wird jedoch nicht getestet. Wenn ein Problem mit der Konfiguration vorliegt, können Sie Appliance-Knoten, bei denen die Knotenverschlüsselung am betroffenen Standort aktiviert ist, möglicherweise nicht neu starten. Bis zur Lösung der Probleme verlieren Sie möglicherweise den Zugriff auf Ihre Daten.

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, aber die Verbindung zum KMS wird nicht getestet.

Verwalten eines KMS

Die Verwaltung eines Schlüsselverwaltungsservers (KMS) umfasst das Anzeigen oder Bearbeiten von Details, das Verwalten von Zertifikaten, das Anzeigen verschlüsselter Knoten und das Entfernen eines KMS, wenn dieser nicht mehr benötigt wird.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"erforderliche Zugriffsberechtigung" .

KMS-Details anzeigen

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

Schritte

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

   Die Seite „Schlüsselverwaltungsserver“ wird angezeigt und zeigt die folgenden Informationen:

- Auf der Registerkarte „Konfigurationsdetails“ werden alle konfigurierten Schlüsselverwaltungsserver aufgelistet.
- Auf der Registerkarte „Verschlüsselte Knoten“ werden alle Knoten aufgelistet, bei denen die Knotenverschlüsselung aktiviert ist.

2. Um die Details für ein bestimmtes KMS anzuzeigen und Vorgänge auf diesem KMS auszuführen, wählen Sie den Namen des KMS aus. Auf der Detailseite für das KMS sind die folgenden Informationen aufgeführt:

Feld	Beschreibung
Verwaltet Schlüssel für	Die mit dem KMS verknüpfte StorageGRID -Site. In diesem Feld wird der Name einer bestimmten StorageGRID Site oder **Sites angezeigt, die nicht von einem anderen KMS verwaltet werden (Standard-KMS).**
Hostname	Der vollqualifizierte Domänenname oder die IP-Adresse des KMS. Wenn ein Cluster aus zwei Schlüsselverwaltungsservern vorhanden ist, werden die vollqualifizierten Domänennamen oder IP-Adressen beider Server aufgelistet. Wenn in einem Cluster mehr als zwei Schlüsselverwaltungsserver vorhanden sind, wird der vollqualifizierte Domänenname oder die IP-Adresse des ersten KMS zusammen mit der Anzahl der zusätzlichen Schlüsselverwaltungsserver im Cluster aufgelistet. Zum Beispiel: `10.10.10.10 and 10.10.10.11` oder `10.10.10.10 and 2 others`. Um alle Hostnamen in einem Cluster anzuzeigen, wählen Sie ein KMS aus und wählen Sie **Bearbeiten** oder **Aktionen** > **Bearbeiten**.

3. Wählen Sie auf der KMS-Detailseite eine Registerkarte aus, um die folgenden Informationen anzuzeigen:

Tab	Feld	Beschreibung
Wichtige Informationen	Schlüsselname	Der Schlüsselalias für den StorageGRID -Client im KMS.
Schlüssel-UID	Die eindeutige Kennung der neuesten Version des Schlüssels.	Zuletzt geändert
Datum und Uhrzeit der neuesten Version des Schlüssels.	Serverzertifikat	Metadaten

Tab	Feld	Beschreibung
Die Metadaten für das Zertifikat, wie Seriennummer, Ablaufdatum und -uhrzeit sowie das Zertifikat-PEM.	Zertifikat PEM	Der Inhalt der PEM-Datei (Privacy Enhanced Mail) für das Zertifikat.
Client-Zertifikat	Metadaten	Die Metadaten für das Zertifikat, wie Seriennummer, Ablaufdatum und -uhrzeit sowie das Zertifikat-PEM.

4. Wählen Sie so oft wie es die Sicherheitspraktiken Ihres Unternehmens erfordern **Schlüssel rotieren** oder verwenden Sie die KMS-Software, um eine neue Version des Schlüssels zu erstellen.

   Wenn die Schlüsselrotation erfolgreich war, werden die Felder „Schlüssel-UID“ und „Zuletzt geändert“ aktualisiert.

> Wenn Sie den Verschlüsselungsschlüssel mithilfe der KMS-Software rotieren, rotieren Sie ihn von der zuletzt verwendeten Version des Schlüssels zu einer neuen Version desselben Schlüssels. Wechseln Sie nicht zu einem völlig anderen Schlüssel.
>
> Versuchen Sie niemals, einen Schlüssel zu rotieren, indem Sie den Schlüsselnamen (Alias) für das KMS ändern. StorageGRID erfordert, dass alle zuvor verwendeten Schlüsselversionen (sowie alle zukünftigen) vom KMS mit demselben Schlüsselalias aus zugänglich sind. Wenn Sie den Schlüsselalias für ein konfiguriertes KMS ändern, kann StorageGRID Ihre Daten möglicherweise nicht entschlüsseln.

Zertifikate verwalten

Beheben Sie umgehend alle Probleme mit Server- oder Clientzertifikaten. Ersetzen Sie Zertifikate nach Möglichkeit vor ihrem Ablauf.

> Sie müssen alle Zertifikatsprobleme so schnell wie möglich beheben, um den Datenzugriff aufrechtzuerhalten.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Schlüsselverwaltungsserver**.
2. Sehen Sie sich in der Tabelle den Wert für den Zertifikatsablauf für jeden KMS an.
3. Wenn das Ablaufdatum des Zertifikats für einen KMS unbekannt ist, warten Sie bis zu 30 Minuten und aktualisieren Sie dann Ihren Webbrowser.
4. Wenn in der Spalte „Zertifikatablauf“ angegeben ist, dass ein Zertifikat abgelaufen ist oder bald abläuft, wählen Sie das KMS aus, um zur KMS-Detailseite zu gelangen.
   a. Wählen Sie **Serverzertifikat** aus und überprüfen Sie den Wert für das Feld „Läuft ab am“.
   b. Um das Zertifikat zu ersetzen, wählen Sie **Zertifikat bearbeiten**, um ein neues Zertifikat hochzuladen.
   c. Wiederholen Sie diese Teilschritte und wählen Sie **Client-Zertifikat** anstelle von Server-Zertifikat.
5. Wenn die Warnungen **Ablauf des KMS-CA-Zertifikats**, **Ablauf des KMS-Client-Zertifikats** und **Ablauf des KMS-Server-Zertifikats** ausgelöst werden, notieren Sie sich die Beschreibung der einzelnen

Warnungen und führen Sie die empfohlenen Aktionen aus.

Es kann bis zu 30 Minuten dauern, bis StorageGRID Aktualisierungen zum Ablauf des Zertifikats erhält. Aktualisieren Sie Ihren Webbrowser, um die aktuellen Werte anzuzeigen.

> Wenn Sie den Status „Serverzertifikatstatus unbekannt“ erhalten, stellen Sie sicher, dass Ihr KMS den Erhalt eines Serverzertifikats ohne Clientzertifikat zulässt.

Verschlüsselte Knoten anzeigen

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

Schritte

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

   Die Seite „Schlüsselverwaltungsserver“ 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 Appliance-Knoten in Ihrem StorageGRID -System aufgelistet, für die die Einstellung **Knotenverschlüsselung** aktiviert ist.

3. Überprüfen Sie die Informationen in der Tabelle für jeden Appliance-Knoten.

Spalte	Beschreibung
Knotenname	Der Name des Appliance-Knotens.
Knotentyp	Der Knotentyp: Speicher, Admin oder Gateway.
Website	Der Name der StorageGRID -Site, an der der Knoten 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 Schlüsselverwaltungsservers (KMS)"
Schlüssel-UID	Die eindeutige ID des Verschlüsselungsschlüssels, der zum Verschlüsseln und Entschlüsseln von Daten auf dem Appliance-Knoten verwendet wird. Um eine vollständige Schlüssel-UID anzuzeigen, wählen Sie den Text aus. Ein Bindestrich (--) zeigt an, dass die Schlüssel-UID unbekannt ist, möglicherweise aufgrund eines Verbindungsproblems zwischen dem Appliance-Knoten und dem KMS.

Spalte	Beschreibung
Status	Der Status der Verbindung zwischen dem KMS und dem Appliance-Knoten. Wenn der Knoten verbunden ist, wird der Zeitstempel alle 30 Minuten aktualisiert. Es kann mehrere Minuten dauern, bis der Verbindungsstatus nach Änderungen der KMS-Konfiguration aktualisiert wird. **Hinweis:** Aktualisieren Sie Ihren Webbrowser, um die neuen Werte anzuzeigen.

4. Wenn in der Spalte „Status“ ein KMS-Problem angezeigt wird, beheben Sie das Problem umgehend.

   Während des normalen KMS-Betriebs lautet der Status **Mit KMS verbunden**. Wenn ein Knoten vom Netz getrennt wird, wird der Verbindungsstatus des Knotens angezeigt (Administrativ deaktiviert oder Unbekannt).

   Andere Statusmeldungen entsprechen StorageGRID -Warnungen mit denselben Namen:

   - KMS-Konfiguration konnte nicht geladen werden
   - KMS-Konnektivitätsfehler
   - Name des KMS-Verschlüsselungsschlüssels nicht gefunden
   - Fehler bei der Rotation des KMS-Verschlüsselungsschlüssels
   - KMS-Schlüssel konnte ein Appliance-Volume nicht entschlüsseln
   - KMS ist nicht konfiguriert

   Führen Sie die empfohlenen Aktionen für diese Warnungen aus.

> ⚠ Sie müssen alle Probleme sofort beheben, um sicherzustellen, dass Ihre Daten vollständig geschützt sind.

Bearbeiten eines KMS

Möglicherweise müssen Sie die Konfiguration eines Schlüsselverwaltungsservers bearbeiten, beispielsweise wenn ein Zertifikat bald abläuft.

Bevor Sie beginnen

- Wenn Sie die für ein KMS ausgewählte Site aktualisieren möchten, haben Sie die"Überlegungen zum Ändern des KMS für eine Site" .
- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .

Schritte

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

   Die Seite „Schlüsselverwaltungsserver“ wird angezeigt und zeigt alle konfigurierten Schlüsselverwaltungsserver.

2. Wählen Sie das KMS aus, das Sie bearbeiten möchten, und wählen Sie **Aktionen** > **Bearbeiten**.

   Sie können ein 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 „Schlüsselverwaltungsserver bearbeiten“.

Feld	Beschreibung
KMS-Name	Ein beschreibender Name, der Ihnen bei der Identifizierung dieses KMS hilft. Muss zwischen 1 und 64 Zeichen lang sein.
Schlüsselname	Der genaue Schlüsselalias für den StorageGRID -Client im KMS. Muss zwischen 1 und 255 Zeichen lang sein. Nur in seltenen Fällen müssen Sie den Schlüsselnamen bearbeiten. Beispielsweise müssen Sie den Schlüsselnamen bearbeiten, wenn der Alias im KMS umbenannt wird oder wenn alle Versionen des vorherigen Schlüssels in den Versionsverlauf des neuen Alias kopiert wurden.
Verwaltet Schlüssel für	Wenn Sie ein standortspezifisches KMS bearbeiten und noch kein Standard-KMS haben, wählen Sie optional **Standorte, die nicht von einem anderen KMS verwaltet werden (Standard-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 Standorte, die in einer Erweiterung hinzugefügt werden. **Hinweis:** Wenn Sie ein standortspezifisches KMS bearbeiten, können Sie keine andere Site auswählen. Wenn Sie das Standard-KMS bearbeiten, können Sie keine bestimmte Site auswählen.
Hafen	Der Port, den der KMS-Server für die KMIP-Kommunikation (Key Management Interoperability Protocol) verwendet. Der Standardwert ist 5696, der KMIP-Standardport.
Hostname	Der vollqualifizierte 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 in einem KMS-Cluster herstellen.

4. Wenn Sie einen KMS-Cluster konfigurieren, wählen Sie **Weiteren Hostnamen hinzufügen** aus, um für jeden Server im Cluster einen Hostnamen hinzuzufügen.
5. Wählen Sie **Weiter**.

   Schritt 2 (Serverzertifikat hochladen) des Assistenten „Schlüsselverwaltungsserver bearbeiten“ wird angezeigt.

6. Wenn Sie das Serverzertifikat ersetzen müssen, wählen Sie **Durchsuchen** und laden Sie die neue Datei hoch.
7. Wählen Sie **Weiter**.

   Schritt 3 (Client-Zertifikate hochladen) des Assistenten „Schlüsselverwaltungsserver bearbeiten“ wird

angezeigt.

8. Wenn Sie das Client-Zertifikat und den privaten Schlüssel des Client-Zertifikats ersetzen müssen, wählen Sie **Durchsuchen** und laden Sie die neuen Dateien hoch.
9. Wählen Sie **Testen und speichern**.

   Die Verbindungen zwischen dem Schlüsselverwaltungsserver und allen knotenverschlüsselten Appliance-Knoten an den betroffenen Standorten werden getestet. Wenn alle Knotenverbindungen gültig sind und der richtige Schlüssel auf dem KMS gefunden wird, wird der Schlüsselverwaltungsserver der Tabelle auf der Seite „Schlüsselverwaltungsserver“ hinzugefügt.

10. Wenn eine Fehlermeldung angezeigt wird, überprüfen Sie die Nachrichtendetails und wählen Sie **OK**.

    Beispielsweise erhalten Sie möglicherweise den Fehler „422: Unprocessable Entity“, wenn die Site, die Sie für dieses KMS ausgewählt haben, 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**.

    > Durch Auswahl von **Speichern erzwingen** wird die KMS-Konfiguration gespeichert, die externe Verbindung von jedem Gerät zu diesem KMS wird jedoch nicht getestet. Wenn ein Problem mit der Konfiguration vorliegt, können Sie Appliance-Knoten, bei denen die Knotenverschlüsselung am betroffenen Standort aktiviert ist, möglicherweise nicht neu starten. Bis zur Lösung der Probleme verlieren Sie möglicherweise den Zugriff auf Ihre Daten.

    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 Schlüsselverwaltungsservers (KMS)

In manchen Fällen möchten Sie möglicherweise einen Schlüsselverwaltungsserver entfernen. Beispielsweise möchten Sie möglicherweise ein standortspezifisches KMS entfernen, wenn Sie die Site außer Betrieb genommen haben.

Bevor Sie beginnen

- Sie haben die"Überlegungen und Anforderungen zur Verwendung eines Schlüsselverwaltungsservers" .
- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .

Informationen zu diesem Vorgang

Sie können einen KMS in folgenden Fällen entfernen:

- Sie können ein standortspezifisches KMS entfernen, wenn der Standort außer Betrieb genommen wurde oder wenn der Standort keine Appliance-Knoten mit aktivierter Knotenverschlüsselung enthält.
- Sie können das Standard-KMS entfernen, wenn für jeden Standort mit Appliance-Knoten und aktivierter Knotenverschlüsselung bereits ein standortspezifischer KMS vorhanden ist.

Schritte

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

   Die Seite „Schlüsselverwaltungsserver“ wird angezeigt und zeigt alle konfigurierten Schlüsselverwaltungsserver.

2. Wählen Sie das KMS aus, das Sie entfernen möchten, und wählen Sie **Aktionen** > **Entfernen**.

   Sie können ein 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 eine Site, die keinen Appliance-Knoten mit aktivierter Knotenverschlüsselung hat.
   - Sie entfernen das Standard-KMS, aber für jede Site ist bereits ein standortspezifisches KMS mit Knotenverschlüsselung vorhanden.
4. Wählen Sie **Ja**.

   Die KMS-Konfiguration wird entfernt.

Proxy-Einstellungen verwalten

Konfigurieren des Speicherproxys

Wenn Sie Plattformdienste oder Cloud-Speicherpools verwenden, können Sie einen nicht transparenten Proxy zwischen Speicherknoten und den externen S3-Endpunkten konfigurieren. Beispielsweise benötigen Sie möglicherweise einen nicht transparenten Proxy, um das Senden von Nachrichten der Plattformdienste an externe Endpunkte, beispielsweise einen Endpunkt im Internet, zu ermöglichen.

Konfigurierte Speicherproxyeinstellungen gelten nicht für Endpunkte der Kafka-Plattformdienste.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Sie können die Einstellungen für einen einzelnen Speicherproxy konfigurieren.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Proxy-Einstellungen**.
2. Aktivieren Sie auf der Registerkarte **Speicher** das Kontrollkästchen **Speicherproxy aktivieren**.
3. Wählen Sie das Protokoll für den Speicherproxy aus.
4. Geben Sie den Hostnamen oder die IP-Adresse des Proxyservers ein.
5. Geben Sie optional den Port ein, der für die Verbindung mit dem Proxyserver verwendet wird.

   Lassen Sie dieses Feld leer, um den Standardport für das Protokoll zu verwenden: 80 für HTTP oder 1080 für SOCKS5.

6. Wählen Sie **Speichern**.

   Nachdem der Speicherproxy gespeichert wurde, können neue Endpunkte für Plattformdienste oder Cloud-Speicherpools konfiguriert und getestet werden.

   Es kann bis zu 10 Minuten dauern, bis Proxy-Änderungen wirksam werden.

7. Überprüfen Sie die Einstellungen Ihres Proxyservers, um sicherzustellen, dass plattformdienstbezogene Nachrichten von StorageGRID nicht blockiert werden.
8. Wenn Sie einen Speicherproxy deaktivieren müssen, deaktivieren Sie das Kontrollkästchen und wählen Sie **Speichern**.

Konfigurieren der Administratorproxyeinstellungen

Wenn Sie AutoSupport Pakete über HTTP oder HTTPS senden, können Sie einen nicht transparenten Proxyserver zwischen Admin-Knoten und technischem Support (AutoSupport) konfigurieren.

Weitere Informationen zu AutoSupport finden Sie unter"Konfigurieren Sie AutoSupport" .

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

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

Schritte

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

   Die Seite „Proxy-Einstellungen“ wird angezeigt. Standardmäßig ist im Registerkartenmenü „Speicher“ ausgewählt.

2. Wählen Sie die Registerkarte **Admin**.
3. Aktivieren Sie das Kontrollkästchen **Admin-Proxy aktivieren**.
4. Geben Sie den Hostnamen oder die IP-Adresse des Proxyservers ein.
5. Geben Sie den Port ein, der für die Verbindung mit dem Proxyserver verwendet wird.
6. Geben Sie optional einen Benutzernamen und ein Kennwort für den Proxyserver ein.

   Lassen Sie diese Felder leer, wenn Ihr Proxyserver weder einen Benutzernamen noch ein Passwort erfordert.

7. Wähle eine der folgenden:

   - Wenn Sie die Verbindung zum Admin-Proxy sichern möchten, wählen Sie **Proxy-Zertifikat überprüfen**. Laden Sie ein CA-Paket hoch, um die Authentizität der vom Admin-Proxyserver bereitgestellten SSL-Zertifikate zu überprüfen.

AutoSupport on Demand, E-Series AutoSupport über StorageGRID und die Update-Pfadbestimmung auf der StorageGRID -Upgrade-Seite funktionieren nicht, wenn ein Proxy-Zertifikat verifiziert wird.

Nachdem Sie das CA-Paket hochgeladen haben, werden dessen Metadaten angezeigt.

- Wenn Sie bei der Kommunikation mit dem Admin-Proxyserver keine Zertifikate validieren möchten, wählen Sie **Proxy-Zertifikat nicht überprüfen**.

8. Wählen Sie **Speichern**.

   Nachdem der Admin-Proxy gespeichert wurde, wird der Proxy-Server zwischen Admin-Knoten und technischem Support konfiguriert.

   Es kann bis zu 10 Minuten dauern, bis Proxy-Änderungen wirksam werden.

9. Wenn Sie den Admin-Proxy deaktivieren müssen, deaktivieren Sie das Kontrollkästchen **Admin-Proxy aktivieren** und wählen Sie dann **Speichern**.

Kontrollieren Sie Firewalls

Zugriffskontrolle an externer Firewall

Sie können bestimmte Ports an der externen Firewall öffnen oder schließen.

Sie können den Zugriff auf die Benutzeroberflächen und APIs auf StorageGRID Admin-Knoten steuern, indem Sie bestimmte Ports an der externen Firewall öffnen oder schließen. Beispielsweise möchten Sie möglicherweise verhindern, dass Mandanten über die Firewall eine Verbindung zum Grid Manager herstellen können, und zusätzlich andere Methoden zur Kontrolle des Systemzugriffs verwenden.

Wenn Sie die interne Firewall von StorageGRID konfigurieren möchten, lesen Sie"Konfigurieren der internen Firewall" .

Hafen	Beschreibung	Wenn der Port offen ist …
443	Standard-HTTPS-Port für Admin-Knoten	Webbrowser und Management-API-Clients können auf den Grid Manager, die Grid Management API, den Tenant Manager und die Tenant Management API zugreifen. **Hinweis:** Port 443 wird auch für einen Teil des internen Datenverkehrs verwendet.
8443	Eingeschränkter Grid Manager-Port auf Admin-Knoten	• Webbrowser und Management-API-Clients können über HTTPS auf den Grid Manager und die Grid Management API zugreifen. • Webbrowser und Management-API-Clients können nicht auf den Tenant Manager oder die Tenant Management API zugreifen. • Anfragen nach internen Inhalten werden abgelehnt.

Hafen	Beschreibung	Wenn der Port offen ist …
9443	Eingeschränkter Tenant Manager-Port auf Admin-Knoten	• Webbrowser und Management-API-Clients können über HTTPS auf den Tenant Manager und die Tenant Management API zugreifen. • Webbrowser und Management-API-Clients können nicht auf den Grid Manager oder die Grid Management API zugreifen. • Anfragen nach internen Inhalten werden abgelehnt.

Single Sign-On (SSO) ist auf den eingeschränkten Grid Manager- oder Tenant Manager-Ports nicht verfügbar. Sie müssen den Standard-HTTPS-Port (443) verwenden, wenn Sie möchten, dass sich Benutzer per Single Sign-On authentifizieren.

Ähnliche Informationen

- "Sign in"
- "Mieterkonto erstellen"
- "Externe Kommunikation"

Verwalten Sie interne Firewall-Kontrollen

StorageGRID umfasst auf jedem Knoten eine interne Firewall, die die Sicherheit Ihres Grids erhöht, indem sie Ihnen die Kontrolle des Netzwerkzugriffs auf den Knoten ermöglicht. Verwenden Sie die Firewall, um den Netzwerkzugriff auf allen Ports zu verhindern, mit Ausnahme der Ports, die für Ihre spezielle Grid-Bereitstellung erforderlich sind. Die Konfigurationsänderungen, die Sie auf der Firewall-Steuerungsseite vornehmen, werden auf jedem Knoten bereitgestellt.

Verwenden Sie die drei Registerkarten auf der Firewall-Steuerungsseite, um den für Ihr Grid erforderlichen Zugriff anzupassen.

- **Liste privilegierter Adressen**: Verwenden Sie diese Registerkarte, um ausgewählten Zugriff auf geschlossene Ports zuzulassen. Sie können IP-Adressen oder Subnetze in CIDR-Notation hinzufügen, die über die Registerkarte „Externen Zugriff verwalten“ auf geschlossene Ports zugreifen können.
- **Externen Zugriff verwalten**: Verwenden Sie diese Registerkarte, um standardmäßig geöffnete Ports zu schließen oder zuvor geschlossene Ports erneut zu öffnen.
- **Nicht vertrauenswürdiges Client-Netzwerk**: Verwenden Sie diese Registerkarte, um anzugeben, ob ein Knoten eingehendem Datenverkehr aus dem Client-Netzwerk vertraut.

  Die Einstellungen auf dieser Registerkarte überschreiben die Einstellungen auf der Registerkarte „Externen Zugriff verwalten“.

  - Ein Knoten mit einem nicht vertrauenswürdigen Client-Netzwerk akzeptiert nur Verbindungen über die auf diesem Knoten konfigurierten Endpunktports des Lastenausgleichs (globale, Knotenschnittstellen- und Knotentyp-gebundene Endpunkte).
  - Die Endpunktports des Lastenausgleichs sind die einzigen offenen Ports in nicht vertrauenswürdigen Clientnetzwerken, unabhängig von den Einstellungen auf der Registerkarte „Externe Netzwerke

verwalten“.

- Wenn sie vertrauenswürdig sind, sind alle unter der Registerkarte „Externen Zugriff verwalten“ geöffneten Ports 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 unbedingt die Einstellungen auf allen Registerkarten, um sicherzustellen, dass sich Ihr Netzwerk wie erwartet verhält.

Informationen zum Konfigurieren interner Firewall-Steuerelemente finden Sie unter"Konfigurieren der Firewall-Steuerelemente" .

Weitere Informationen zu externen Firewalls und Netzwerksicherheit finden Sie unter"Zugriffskontrolle an externer Firewall" .

Registerkarten „Liste privilegierter Adressen“ und „Externen Zugriff verwalten“

Auf der Registerkarte „Liste privilegierter 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 Nicht-Grid-Knoten standardmäßig zugreifen können). Diese beiden Registerkarten können häufig zusammen verwendet werden, um den genauen Netzwerkzugriff anzupassen, den Sie für Ihr Grid zulassen müssen.

> 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 Host mit gehärteter Sicherheit) für die Netzwerkadministration verwenden. Sie können diese allgemeinen Schritte verwenden:

1. Verwenden Sie die Registerkarte „Liste privilegierter 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 über einen blockierten Port verbunden sind (einschließlich Ihnen), verlieren den Zugriff auf Grid Manager, sofern ihre IP-Adresse nicht zur Liste der privilegierten Adressen hinzugefügt wurde.

Nachdem Sie Ihre Konfiguration gespeichert haben, werden alle externen Ports auf dem Admin-Knoten in Ihrem Grid für alle Hosts außer dem Jump-Host blockiert. Anschließend können Sie den Jump-Host verwenden, um Wartungsaufgaben an Ihrem Grid sicherer durchzuführen.

Beispiel 2: Sperren sensibler Ports

Angenommen, Sie möchten sensible Ports und den Dienst auf diesem Port sperren (z. B. SSH auf Port 22). Sie können die folgenden allgemeinen Schritte ausführen:

1. Verwenden Sie die Registerkarte „Liste privilegierter Adressen“, um nur den Hosts Zugriff zu gewähren, die Zugriff auf den Dienst benötigen.
2. Verwenden Sie die Registerkarte „Externen Zugriff verwalten“, um alle Ports zu blockieren.

Fügen Sie die privilegierte IP-Adresse hinzu, bevor Sie den Zugriff auf Ports blockieren, die für den Zugriff auf Grid Manager und Tenant Manager zugewiesen sind (voreingestellte Ports sind 443 und 8443). Alle Benutzer, die derzeit über einen blockierten Port verbunden sind (einschließlich Ihnen), verlieren den Zugriff auf Grid Manager, sofern ihre IP-Adresse nicht zur Liste der privilegierten Adressen hinzugefügt wurde.

Nachdem Sie Ihre Konfiguration gespeichert haben, stehen Port 22 und der SSH-Dienst den Hosts auf der Liste privilegierter Adressen zur Verfügung. Allen anderen Hosts wird der Zugriff auf den Dienst verweigert, unabhängig davon, von welcher Schnittstelle die Anforderung kommt.

Beispiel 3: Zugriff auf nicht verwendete Dienste deaktivieren

Auf Netzwerkebene können Sie einige Dienste deaktivieren, die Sie nicht verwenden möchten. Um beispielsweise den HTTP S3-Client-Verkehr zu blockieren, verwenden Sie den Schalter auf der Registerkarte „Externen Zugriff verwalten“, um Port 18084 zu blockieren.

Registerkarte „Nicht vertrauenswürdige Clientnetzwerke“

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

Standardmäßig ist das Client-Netzwerk auf jedem Grid-Knoten *vertrauenswürdig*. Das heißt, StorageGRID vertraut standardmäßig eingehenden Verbindungen zu jedem Grid-Knoten auf allen"verfügbare externe Ports" .

Sie können die Gefahr feindlicher Angriffe auf Ihr StorageGRID -System verringern, indem Sie festlegen, dass das Client-Netzwerk auf jedem Knoten *nicht vertrauenswürdig* ist. Wenn das Client-Netzwerk eines Knotens nicht vertrauenswürdig ist, akzeptiert der Knoten eingehende Verbindungen nur auf Ports, die explizit als Endpunkte des Lastenausgleichs konfiguriert sind. Sehen"Konfigurieren von Load Balancer-Endpunkten" Und"Konfigurieren der Firewall-Steuerelemente" .

Beispiel 1: Gateway-Knoten akzeptiert nur HTTPS S3-Anfragen

Angenommen, Sie möchten, dass ein Gateway-Knoten den gesamten eingehenden Datenverkehr im Client-Netzwerk mit Ausnahme von HTTPS S3-Anfragen ablehnt. Sie würden diese allgemeinen Schritte ausführen:

1. Aus dem"Load Balancer-Endpunkte" Konfigurieren Sie auf der Seite einen Load Balancer-Endpunkt für S3 über HTTPS auf Port 443.
2. Wählen Sie auf der Firewall-Steuerungsseite „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 gelöscht, mit Ausnahme von HTTPS-S3-Anfragen auf Port 443 und ICMP-Echo-(Ping-)Anfragen.

Beispiel 2: Storage Node sendet S3-Plattformdienstanfragen

Angenommen, Sie möchten ausgehenden S3-Plattformdienstdatenverkehr von einem Speicherknoten aktivieren, aber alle eingehenden Verbindungen zu diesem Speicherknoten im Clientnetzwerk verhindern. Sie würden diesen allgemeinen Schritt ausführen:

- Geben Sie auf der Registerkarte „Nicht vertrauenswürdige Clientnetzwerke“ der Firewall-Steuerungsseite an, dass das Clientnetzwerk auf dem Speicherknoten nicht vertrauenswürdig ist.

Nachdem Sie Ihre Konfiguration gespeichert haben, akzeptiert der Speicherknoten keinen eingehenden Datenverkehr mehr im Client-Netzwerk, lässt jedoch weiterhin ausgehende Anfragen an konfigurierte Plattformdienstziele zu.

Beispiel 3: Beschränkung des Zugriffs auf Grid Manager auf ein Subnetz

Angenommen, Sie möchten dem Grid Manager nur Zugriff auf ein bestimmtes Subnetz gewähren. Sie würden die folgenden Schritte ausführen:

1. Verbinden Sie das Client-Netzwerk Ihrer Admin-Knoten mit dem Subnetz.
2. Verwenden Sie die Registerkarte „Nicht vertrauenswürdiges Client-Netzwerk“, um das Client-Netzwerk als nicht vertrauenswürdig zu konfigurieren.
3. Wenn Sie einen Lastenausgleichsendpunkt für die Verwaltungsschnittstelle erstellen, geben Sie den Port ein und wählen Sie die Verwaltungsschnittstelle aus, auf die der Port zugreifen soll.
4. Wählen Sie **Ja** für nicht vertrauenswürdiges Clientnetzwerk.
5. Verwenden Sie die Registerkarte „Externen Zugriff verwalten“, um alle externen Ports zu blockieren (mit oder ohne privilegierte IP-Adressen, die für Hosts außerhalb dieses Subnetzes festgelegt sind).

Nachdem Sie Ihre Konfiguration gespeichert haben, können nur Hosts im von Ihnen angegebenen Subnetz auf den Grid Manager zugreifen. Alle anderen Hosts sind blockiert.

Konfigurieren der internen Firewall

Sie können die StorageGRID -Firewall so konfigurieren, dass der Netzwerkzugriff auf bestimmte Ports Ihrer StorageGRID Knoten gesteuert wird.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .
- Sie haben die Informationen in"Verwalten von Firewall-Steuerelementen" Und"Netzwerkrichtlinien" .
- Wenn Sie möchten, dass ein Admin-Knoten oder Gateway-Knoten eingehenden Datenverkehr nur an explizit konfigurierten Endpunkten akzeptiert, haben Sie die Load Balancer-Endpunkte definiert.

> ⓘ Beim Ändern der Konfiguration des Client-Netzwerks können vorhandene Client-Verbindungen fehlschlagen, wenn die Endpunkte des Lastenausgleichs nicht konfiguriert wurden.

Informationen zu diesem Vorgang

StorageGRID enthält auf jedem Knoten eine interne Firewall, die es Ihnen ermöglicht, einige der Ports auf den Knoten Ihres Grids zu öffnen oder zu schließen. Sie können die Firewall-Steuerungsregisterkarten verwenden, um Ports zu öffnen oder zu schließen, die im Grid-Netzwerk, Admin-Netzwerk und Client-Netzwerk standardmäßig geöffnet sind. Sie können auch eine Liste privilegierter IP-Adressen erstellen, die auf geschlossene Grid-Ports zugreifen können. Wenn Sie ein Client-Netzwerk verwenden, können Sie angeben, ob ein Knoten eingehendem Datenverkehr aus dem Client-Netzwerk vertraut, und Sie können den Zugriff auf bestimmte Ports im Client-Netzwerk konfigurieren.

Die Sicherheit Ihres Grids wird erhöht, indem Sie die Anzahl der für IP-Adressen außerhalb Ihres Grids geöffneten Ports auf die unbedingt erforderlichen beschränken. Sie verwenden die Einstellungen auf jeder der drei Firewall-Steuerungsregisterkarten, um sicherzustellen, dass nur die benötigten Ports geöffnet sind.

Weitere Informationen zur Verwendung von Firewall-Steuerelementen, einschließlich Beispielen, finden Sie unter"Verwalten von Firewall-Steuerelementen" .

Weitere Informationen zu externen Firewalls und Netzwerksicherheit finden Sie unter"Zugriffskontrolle an externer Firewall" .

Zugriff auf Firewall-Steuerelemente

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Firewall-Steuerung**.

   Die drei Registerkarten auf dieser Seite werden beschrieben in"Verwalten von Firewall-Steuerelementen" .

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, schränken Ihre Möglichkeiten auf den anderen Registerkarten nicht ein. Allerdings können Konfigurationsänderungen, die Sie auf einer Registerkarte vornehmen, das Verhalten der auf anderen Registerkarten konfigurierten Ports ändern.

Liste privilegierter Adressen

Über die Registerkarte „Liste privilegierter Adressen“ können Sie Hosts Zugriff auf Ports gewähren, die standardmäßig oder durch Einstellungen auf der Registerkarte „Externen Zugriff verwalten“ geschlossen sind.

Privilegierte IP-Adressen und Subnetze haben standardmäßig keinen internen Grid-Zugriff. Darüber hinaus sind Lastenausgleichsendpunkte und zusätzliche Ports, die auf der Registerkarte „Liste privilegierter Adressen“ geöffnet sind, auch dann zugänglich, wenn sie auf der Registerkarte „Externen Zugriff verwalten“ blockiert sind.

> Einstellungen auf der Registerkarte „Liste privilegierter Adressen“ können Einstellungen auf der Registerkarte „Nicht vertrauenswürdiges Clientnetzwerk“ nicht überschreiben.

Schritte

1. Geben Sie auf der Registerkarte „Liste privilegierter Adressen“ die Adresse oder das IP-Subnetz ein, dem Sie Zugriff auf geschlossene Ports gewähren möchten.
2. Wählen Sie optional **Weitere IP-Adresse oder Subnetz in CIDR-Notation hinzufügen** aus, um weitere privilegierte Clients hinzuzufügen.

   > Fügen Sie der privilegierten Liste so wenige Adressen wie möglich hinzu.

3. Wählen Sie optional **Privilegierten IP-Adressen den Zugriff auf interne StorageGRID -Ports erlauben**. Sehen "Interne StorageGRID Ports" .

   > Diese Option entfernt einige Schutzmaßnahmen für interne Dienste. Lassen Sie es nach Möglichkeit deaktiviert.

4. Wählen Sie **Speichern**.

Verwalten des externen Zugriffs

Wenn ein Port auf der Registerkarte „Externen Zugriff verwalten“ geschlossen ist, kann von keiner Nicht-Grid-IP-Adresse auf den Port zugegriffen werden, es sei denn, Sie fügen die IP-Adresse zur Liste der privilegierten

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 Einstellungen auf der Registerkarte „Nicht vertrauenswürdiges Clientnetzwerk“ nicht überschreiben. Wenn beispielsweise ein Knoten nicht vertrauenswürdig ist, wird Port SSH/22 im Client-Netzwerk blockiert, auch wenn er auf der Registerkarte „Externen Zugriff verwalten“ geöffnet ist. Einstellungen auf der Registerkarte „Nicht vertrauenswürdiges Client-Netzwerk“ überschreiben geschlossene Ports (wie 443, 8443, 9443) im Client-Netzwerk.

Schritte

1. Wählen Sie **Externen Zugriff verwalten**. Die Registerkarte zeigt eine Tabelle mit allen externen Ports (Ports, die standardmäßig für Nicht-Grid-Knoten zugänglich sind) für die Knoten in Ihrem Grid an.
2. Konfigurieren Sie die Ports, die Sie öffnen und schließen möchten, mithilfe der folgenden Optionen:
   - Verwenden Sie den Schalter 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 über einen blockierten Port verbunden sind (einschließlich Ihnen), den Zugriff auf Grid Manager, sofern ihre IP-Adresse nicht zur Liste der privilegierten Adressen hinzugefügt wurde.

   > Verwenden Sie die Bildlaufleiste auf der rechten Seite der Tabelle, um sicherzustellen, dass Sie alle verfügbaren Ports angezeigt haben. Verwenden Sie das Suchfeld, um die Einstellungen für einen beliebigen externen Port zu finden, indem Sie eine Portnummer eingeben. Sie können eine teilweise Portnummer eingeben. Wenn Sie beispielsweise eine **2** eingeben, werden alle Ports angezeigt, die die Zeichenfolge „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 eingehenden Datenverkehr nur auf den als Lastenausgleichsendpunkte konfigurierten Ports und optional auf zusätzlichen Ports, die Sie auf dieser Registerkarte auswählen. Sie können diese Registerkarte auch verwenden, um die Standardeinstellung für neue Knoten festzulegen, die in einer Erweiterung hinzugefügt werden.

> Vorhandene Clientverbindungen können fehlschlagen, wenn keine Load Balancer-Endpunkte konfiguriert wurden.

Die Konfigurationsänderungen, die Sie auf der Registerkarte **Nicht vertrauenswürdiges Clientnetzwerk** 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 dem Raster in einem Erweiterungsvorgang neue Knoten hinzugefügt werden.

- **Vertrauenswürdig** (Standard): Wenn ein Knoten in einer Erweiterung hinzugefügt wird, wird seinem Client-Netzwerk vertraut.
- **Nicht vertrauenswürdig**: Wenn in einer Erweiterung ein Knoten 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 Auswirkungen auf die vorhandenen Knoten in Ihrem StorageGRID System.

3. Verwenden Sie die folgenden Optionen, um die Knoten auszuwählen, die Clientverbindungen nur auf explizit konfigurierten Load Balancer-Endpunkten oder zusätzlichen ausgewählten Ports zulassen sollen:
   - Wählen Sie **Angezeigten Knoten nicht vertrauenswürdig machen** aus, um alle in der Tabelle angezeigten Knoten zur Liste „Nicht vertrauenswürdiges Clientnetzwerk“ hinzuzufügen.
   - Wählen Sie **Angezeigten Knoten vertrauen** aus, um alle in der Tabelle angezeigten Knoten aus der Liste „Nicht vertrauenswürdiges Clientnetzwerk“ zu entfernen.
   - Verwenden Sie den Schalter neben jedem Knoten, um das Client-Netzwerk für den ausgewählten Knoten als vertrauenswürdig oder nicht vertrauenswürdig festzulegen.

     Sie können beispielsweise **Angezeigten Knoten nicht vertrauen** auswählen, um alle Knoten zur Liste „Nicht vertrauenswürdige Clientnetzwerke“ hinzuzufügen, und dann den Umschalter neben einem einzelnen Knoten verwenden, um diesen einzelnen Knoten zur Liste „Vertrauenswürdige Clientnetzwerke“ 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 einen beliebigen Knoten zu finden, indem Sie den Knotennamen eingeben. Sie können einen Teilnamen eingeben. Wenn Sie beispielsweise **GW** eingeben, werden alle Knoten angezeigt, deren Name die Zeichenfolge „GW“ enthält.

4. Wählen Sie **Speichern**.

   Die neuen Firewall-Einstellungen werden sofort angewendet und durchgesetzt. Vorhandene Clientverbindungen können fehlschlagen, wenn keine Load Balancer-Endpunkte konfiguriert wurden.

Mandanten verwalten

Was sind Mieterkonten?

Mit einem Mandantenkonto können Sie die REST-API des Simple Storage Service (S3) verwenden, um Objekte in einem StorageGRID -System zu speichern und abzurufen.

> Swift-Details wurden aus dieser Version der Dokumentationssite entfernt. Sehen "StorageGRID 11.8: Mandanten verwalten" .

Als Grid-Administrator erstellen und verwalten Sie die Mandantenkonten, die S3-Clients zum Speichern und

Abrufen von Objekten verwenden.

Jedes Mandantenkonto verfügt über föderierte oder lokale Gruppen, Benutzer, S3-Buckets und Objekte.

Mandantenkonten können verwendet werden, um gespeicherte Objekte nach verschiedenen Entitäten zu trennen. Beispielsweise können mehrere Mandantenkonten für einen der folgenden Anwendungsfälle verwendet werden:

- **Anwendungsfall für Unternehmen:** Wenn Sie ein StorageGRID -System in einer Unternehmensanwendung verwalten, möchten Sie den Objektspeicher des Grids möglicherweise nach den verschiedenen Abteilungen in Ihrer Organisation trennen. In diesem Fall könnten Sie Mandantenkonten für die Marketingabteilung, die Kundensupportabteilung, die Personalabteilung usw. erstellen.

  > Wenn Sie das S3-Clientprotokoll verwenden, können Sie S3-Buckets und Bucket-Richtlinien verwenden, um Objekte zwischen den Abteilungen in einem Unternehmen zu trennen. Sie müssen keine Mieterkonten verwenden. Siehe Anweisungen zur Implementierung"S3-Buckets und Bucket-Richtlinien" für weitere Informationen.

- **Anwendungsfall für Dienstanbieter:** Wenn Sie ein StorageGRID -System als Dienstanbieter verwalten, können Sie den Objektspeicher des Grids nach den verschiedenen Entitäten trennen, die den Speicher in Ihrem Grid mieten. In diesem Fall würden Sie Mandantenkonten für Unternehmen A, Unternehmen B, Unternehmen C usw. erstellen.

Weitere Informationen finden Sie unter "Verwenden eines Mandantenkontos" .

Wie erstelle ich ein Mieterkonto?

Verwenden Sie den Grid-Manager, um ein Mandantenkonto zu erstellen. Wenn Sie ein Mandantenkonto erstellen, geben Sie die folgenden Informationen an:

- Grundlegende Informationen, einschließlich Mandantenname, Clienttyp (S3) und optionalem Speicherkontingent.
- Berechtigungen für das Mandantenkonto, z. B. ob das Mandantenkonto S3-Plattformdienste verwenden, seine eigene Identitätsquelle konfigurieren, S3 Select verwenden oder eine Grid-Föderationsverbindung verwenden kann.
- Der anfängliche Root-Zugriff für den Mandanten, basierend darauf, ob das StorageGRID -System lokale Gruppen und Benutzer, Identitätsföderation oder Single Sign-On (SSO) verwendet.

Darüber hinaus können Sie die S3-Objektsperreinstellung für das StorageGRID -System aktivieren, wenn S3-Mandantenkonten gesetzliche Anforderungen erfüllen müssen. Wenn S3 Object Lock aktiviert ist, können alle S3-Mandantenkonten konforme Buckets erstellen und verwalten.

Wofür wird Tenant Manager verwendet?

Nachdem Sie das Mandantenkonto erstellt haben, können sich Mandantenbenutzer beim Mandantenmanager anmelden, um beispielsweise die folgenden Aufgaben auszuführen:

- Identitätsföderation einrichten (es sei denn, die Identitätsquelle wird mit dem Grid geteilt)
- Verwalten von Gruppen und Benutzern
- Verwenden Sie die Grid-Föderation für Kontoklone und Cross-Grid-Replikation
- S3-Zugriffsschlüssel verwalten

- Erstellen und Verwalten von S3-Buckets
- Verwenden Sie S3-Plattformdienste
- Verwenden Sie S3 Select
- Überwachen der Speichernutzung

Während S3-Tenant-Benutzer mit dem Tenant Manager S3-Zugriffsschlüssel und Buckets erstellen und verwalten können, müssen sie zum Aufnehmen und Verwalten von Objekten eine S3-Clientanwendung verwenden. Sehen"Verwenden Sie die S3 REST-API" für Details.

Erstellen Sie ein Mieterkonto

Sie müssen mindestens ein Mandantenkonto erstellen, um den Zugriff auf den Speicher in Ihrem StorageGRID System zu steuern.

Die Schritte zum Erstellen eines Mandantenkontos variieren je nachdem, ob"Identitätsföderation" Und"Einmaliges Anmelden" konfiguriert sind und ob das Grid Manager-Konto, das Sie zum Erstellen des Mandantenkontos verwenden, zu einer Administratorgruppe mit Root-Zugriffsberechtigung gehört.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriff oder Mandantenkontenberechtigung" .
- Wenn das Mandantenkonto die für den Grid Manager konfigurierte Identitätsquelle verwendet und Sie einer föderierten Gruppe Root-Zugriffsberechtigungen für das Mandantenkonto erteilen möchten, haben Sie diese föderierte Gruppe in den Grid Manager importiert. Sie müssen dieser Administratorgruppe keine Grid Manager-Berechtigungen zuweisen. Sehen "Verwalten von Administratorgruppen" .
- Wenn Sie einem S3-Mandanten das Klonen von Kontodaten und das Replizieren von Bucket-Objekten in ein anderes Grid mithilfe einer Grid-Föderationsverbindung erlauben möchten:
  - Du hast"die Grid-Föderation-Verbindung konfiguriert" .
  - Der Status der Verbindung ist **Verbunden**.
  - Sie verfügen über Root-Zugriffsberechtigung.
  - Sie haben die Überlegungen für"Verwaltung der zulässigen Mandanten für die Grid-Föderation" .
  - Wenn das Mandantenkonto die für Grid Manager konfigurierte Identitätsquelle verwendet, haben Sie in beiden Grids dieselbe föderierte Gruppe in Grid Manager 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 in beiden Rastern vorhanden ist, wird der Mandant nicht zum Ziel repliziert.

Zugriff auf den Assistenten

Schritte

1. Wählen Sie **MIETER** aus.
2. Wählen Sie **Erstellen**.

Details eingeben

Schritte

1. Geben Sie die Details zum Mieter ein.

Feld	Beschreibung
Name	Ein Name für das Mandantenkonto. Mandantennamen müssen nicht eindeutig sein. Beim Anlegen des Mandantenkontos erhält dieses eine eindeutige, 20-stellige Konto-ID.
Beschreibung (optional)	Eine Beschreibung zur Identifizierung des Mieters. Wenn Sie einen Mandanten erstellen, der eine Grid-Föderation-Verbindung verwendet, können Sie dieses Feld optional verwenden, um zu ermitteln, welcher der Quellmandant und welcher der Zielmandant ist. Beispielsweise wird diese Beschreibung für einen in Grid 1 erstellten Mandanten auch für den in Grid 2 replizierten Mandanten angezeigt: „Dieser Mandant wurde in Grid 1 erstellt.“
Client-Typ	Der Typ des Clientprotokolls, das dieser Mandant verwenden wird, entweder **S3** oder **Swift**. **Hinweis**: Die Unterstützung für Swift-Clientanwendungen ist veraltet und wird in einer zukünftigen Version entfernt.
Speicherkontingent (optional)	Wenn Sie möchten, dass dieser Mandant über ein Speicherkontingent verfügt, geben Sie einen numerischen Wert für das Kontingent und die Einheiten ein.

2. Wählen Sie **Weiter**.

Berechtigungen auswählen

Schritte

1. Wählen Sie optional die grundlegenden Berechtigungen aus, die dieser Mandant haben soll.

> Für einige dieser Berechtigungen gelten zusätzliche Anforderungen. Um Einzelheiten zu erfahren, wählen Sie das Hilfesymbol für jede Berechtigung aus.

Erlaubnis	Falls ausgewählt…
Plattformdienste zulassen	Der Mieter kann S3-Plattformdienste wie CloudMirror verwenden. Sehen "Plattformdienste für S3-Mandantenkonten verwalten" .
Eigene Identitätsquelle verwenden	Der Mandant kann seine eigene Identitätsquelle für föderierte Gruppen und Benutzer konfigurieren und verwalten. Diese Option ist deaktiviert, wenn Sie"konfiguriertes SSO" für Ihr StorageGRID System.

Erlaubnis	Falls ausgewählt…
S3-Auswahl zulassen	Der Mandant kann S3 SelectObjectContent-API-Anfragen stellen, um Objektdaten zu filtern und abzurufen. Sehen "Verwalten von S3 Select für Mandantenkonten" . **Wichtig**: SelectObjectContent-Anfragen können die Leistung des Load Balancers für alle S3-Clients und alle Mandanten verringern. Aktivieren Sie diese Funktion nur bei Bedarf und nur für vertrauenswürdige Mandanten.

2. Wählen Sie optional die erweiterten Berechtigungen aus, die dieser Mandant haben soll.

Erlaubnis	Falls ausgewählt…
Grid-Föderation-Verbindung	Der Mieter kann eine Grid-Föderation-Verbindung nutzen, die: • Bewirkt, dass dieser Mandant und alle dem Konto hinzugefügten Mandantengruppen und Benutzer von diesem Raster (dem *Quellraster*) in das andere Raster in der ausgewählten Verbindung (das *Zielraster*) geklont werden. • Ermöglicht diesem Mandanten, die Cross-Grid-Replikation zwischen entsprechenden Buckets auf jedem Grid zu konfigurieren. Sehen "Verwalten der zulässigen Mandanten für die Grid-Föderation" .
S3-Objektsperre	Erlauben Sie dem Mandanten, bestimmte Funktionen von S3 Object Lock zu verwenden: • **Maximale Aufbewahrungsdauer festlegen** definiert, wie lange neue Objekte, die diesem Bucket hinzugefügt werden, ab dem Zeitpunkt ihrer Aufnahme aufbewahrt werden sollen. • **Compliance-Modus zulassen** verhindert, dass Benutzer während der Aufbewahrungsfrist geschützte Objektversionen überschreiben oder löschen.

3. Wählen Sie **Weiter**.

Definieren Sie den Root-Zugriff und erstellen Sie einen Mandanten

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 dies
Wenn die Identitätsföderation nicht aktiviert ist	Geben Sie das Kennwort an, das bei der Anmeldung beim Mandanten als lokaler Root-Benutzer verwendet werden soll.

Option	Tun Sie dies
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 bei der Anmeldung beim Mandanten als lokaler Root-Benutzer verwendet werden soll.
Wenn sowohl die Identitätsföderation als auch Single Sign-On (SSO) aktiviert sind	Wählen Sie eine vorhandene Verbundgruppe aus, um Root-Zugriffsberechtigungen für den Mandanten zu erhalten. Es können sich keine lokalen Benutzer anmelden.

2. Wählen Sie **Mandanten erstellen**.

   Es wird eine Erfolgsmeldung angezeigt und der neue Mandant wird auf der Seite „Mandanten“ aufgeführt. Informationen zum Anzeigen von Mandantendetails und Überwachen der Mandantenaktivität finden Sie unter"Überwachen Sie die Mieteraktivität" .

   Das Anwenden von Mandanteneinstellungen im gesamten Grid kann je nach Netzwerkkonnektivität, Knotenstatus und Cassandra-Vorgängen 15 Minuten oder länger dauern.

3. Wenn Sie für den Mandanten die Berechtigung **Grid-Föderationsverbindung verwenden** ausgewählt haben:

   a. Bestätigen Sie, dass ein identischer Mandant in das andere Grid in der Verbindung repliziert wurde. Die Mandanten in beiden Grids verfügen über dieselbe 20-stellige Konto-ID, denselben Namen, dieselbe Beschreibung, dasselbe Kontingent und dieselben Berechtigungen.

      Wenn die Fehlermeldung „Mandant ohne Klon erstellt“ angezeigt wird, lesen Sie die Anweisungen in"Beheben von Grid-Föderationsfehlern" .

   b. Wenn Sie beim Definieren des Root-Zugriffs ein lokales Root-Benutzerkennwort angegeben haben,"Ändern Sie das Passwort für den lokalen Root-Benutzer" für den replizierten Mandanten.

      Ein lokaler Root-Benutzer kann sich erst beim Tenant Manager im Zielraster anmelden, wenn das Kennwort geändert wurde.

Beim Mandanten Sign in (optional)

Bei Bedarf können Sie sich jetzt beim neuen Mandanten anmelden, um die Konfiguration abzuschließen, oder Sie können sich später beim Mandanten anmelden. Die Anmeldeschritte hängen davon ab, ob Sie über den Standardport (443) oder einen eingeschränkten Port beim Grid Manager angemeldet sind. Sehen "Zugriffskontrolle an externer Firewall" .

Jetzt Sign in

Wenn Sie verwenden…	Machen Sie Folgendes…
Port 443 und Sie legen ein Passwort für den lokalen Root-Benutzer fest	1. Wählen Sie * Als Root Sign in *. Wenn Sie sich anmelden, werden Links zum Konfigurieren von Buckets, Identitätsföderation, Gruppen und Benutzern angezeigt. 2. Wählen Sie die Links aus, um das Mandantenkonto zu konfigurieren. Jeder Link öffnet die entsprechende Seite im Mandantenmanager. Um die Seite zu vervollständigen, sehen Sie sich die"Anleitung zur Nutzung von Mieterkonten" .
Port 443 und Sie haben kein Passwort für den lokalen Root-Benutzer festgelegt	Wählen Sie * Sign in* aus und geben Sie die Anmeldeinformationen für einen Benutzer in der Verbundgruppe mit Root-Zugriff ein.
Ein eingeschränkter Port	1. Wählen Sie **Fertig** 2. Wählen Sie in der Mandantentabelle **Eingeschränkt** aus, um mehr über den Zugriff auf dieses Mandantenkonto zu erfahren. Die URL für den Tenant Manager hat dieses Format: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ `*FQDN_or_Admin_Node_IP*`ist ein vollqualifizierter Domänenname oder die IP-Adresse eines Admin-Knotens ◦ `*port*`ist der Tenant-Only-Port ◦ `*20-digit-account-id*`ist die eindeutige Konto-ID des Mandanten

Später Sign in

Wenn Sie verwenden…	Machen Sie eines davon …
Port 443	• Wählen Sie im Grid Manager **MIETER** und rechts neben dem Mandantennamen * Sign in* aus. • Geben Sie die URL des Mandanten in einen Webbrowser ein: `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ `*FQDN_or_Admin_Node_IP*`ist ein vollqualifizierter Domänenname oder die IP-Adresse eines Admin-Knotens ◦ `*20-digit-account-id*`ist die eindeutige Konto-ID des Mandanten

Wenn Sie verwenden…	Machen Sie eines davon …
Ein eingeschränkter Port	• Wählen Sie im Grid Manager **MIETER** und dann **Eingeschränkt** aus. • Geben Sie die URL des Mandanten in einen Webbrowser ein: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ `FQDN_or_Admin_Node_IP`ist ein vollqualifizierter Domänenname oder die IP-Adresse eines Admin-Knotens ◦ `port`ist der eingeschränkte Port nur für Mandanten ◦ `20-digit-account-id`ist die eindeutige Konto-ID des Mandanten

Konfigurieren des Mandanten

Befolgen Sie die Anweisungen in"Verwenden eines Mandantenkontos" zur Verwaltung von Mandantengruppen und Benutzern, S3-Zugriffsschlüsseln, Buckets, Plattformdiensten sowie Kontoklonen und Cross-Grid-Replikation.

Mieterkonto bearbeiten

Sie können ein Mandantenkonto bearbeiten, um den Anzeigenamen, das Speicherkontingent oder die Mandantenberechtigungen zu ändern.

Wenn ein Mandant über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, können Sie Mandantendetails von jedem Grid in der Verbindung aus bearbeiten. Änderungen, die Sie in der Verbindung an einem Raster vornehmen, werden jedoch nicht in das andere Raster kopiert. Wenn Sie die Mieterdetails zwischen den Rastern genau synchron halten möchten, nehmen Sie in beiden Rastern die gleichen Änderungen vor. Sehen "Verwalten Sie die zulässigen Mandanten für die Grid-Föderation-Verbindung" .

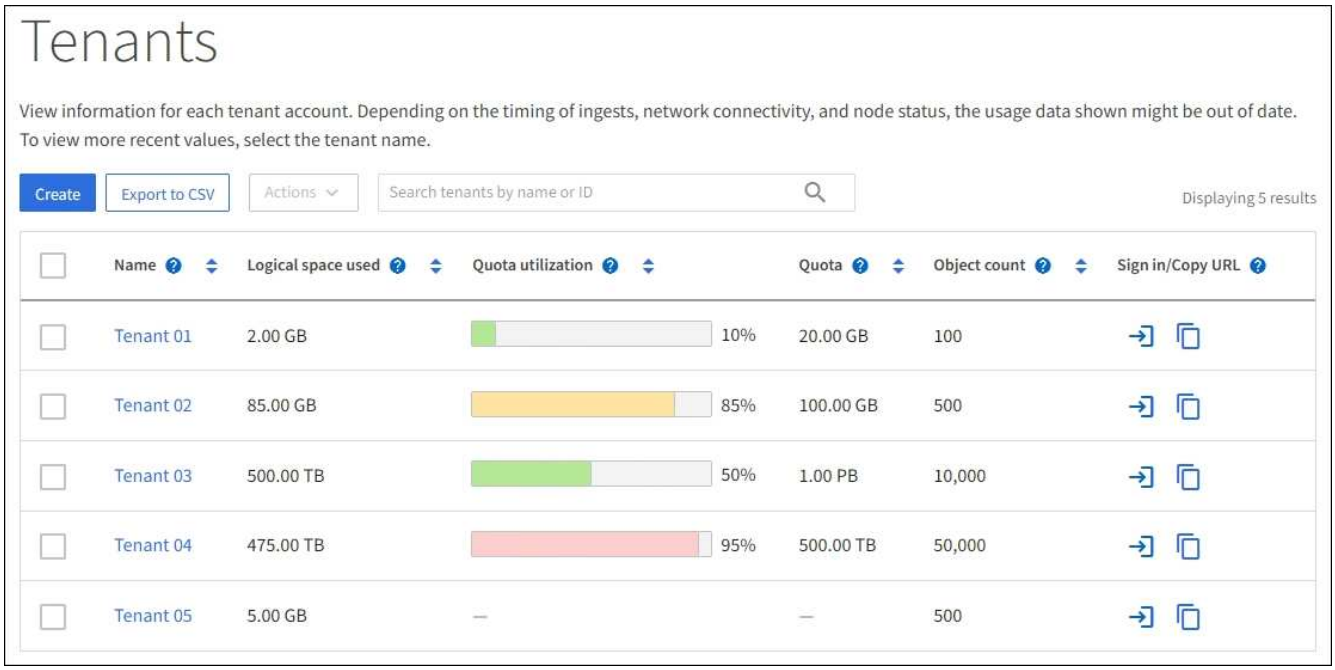
Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriff oder Mandantenkontenberechtigung" .

Das Anwenden von Mandanteneinstellungen im gesamten Grid kann je nach Netzwerkkonnektivität, Knotenstatus und Cassandra-Vorgängen 15 Minuten oder länger dauern.

Schritte

1. Wählen Sie **MIETER** aus.



2. Suchen Sie das Mandantenkonto, das Sie bearbeiten möchten.

   Verwenden Sie das Suchfeld, um nach einem Mieter anhand seines Namens oder seiner Mieter-ID zu suchen.

3. Wählen Sie den Mandanten aus. Sie können einen der folgenden Schritte ausführen:
   - Aktivieren Sie das Kontrollkästchen für den Mandanten und wählen Sie **Aktionen** > **Bearbeiten**.
   - Wählen Sie den Mandantennamen aus, um die Detailseite anzuzeigen, und wählen Sie **Bearbeiten**.
4. Ändern Sie optional die Werte für diese Felder:
   - **Name**
   - **Beschreibung**
   - **Speicherkontingent**
5. Wählen Sie **Weiter**.
6. Aktivieren oder deaktivieren Sie die Berechtigungen für das Mandantenkonto.
   - Wenn Sie **Plattformdienste** für einen Mandanten deaktivieren, der sie bereits verwendet, funktionieren die Dienste, die er für seine S3-Buckets konfiguriert hat, nicht mehr. Es wird keine Fehlermeldung an den Mieter gesendet. Wenn der Mandant beispielsweise die CloudMirror-Replikation für einen S3-Bucket konfiguriert hat, kann er zwar weiterhin Objekte im Bucket speichern, es werden jedoch keine Kopien dieser Objekte mehr im externen S3-Bucket erstellt, den er als Endpunkt konfiguriert hat. Sehen "Plattformdienste für S3-Mandantenkonten verwalten" .
   - Ändern Sie die Einstellung **Eigene Identitätsquelle verwenden**, um festzulegen, ob das Mandantenkonto seine eigene Identitätsquelle oder die für den Grid Manager konfigurierte Identitätsquelle verwendet.

     Wenn **Eigene Identitätsquelle verwenden** lautet:

     - Deaktiviert und ausgewählt: Der Mandant hat seine eigene Identitätsquelle bereits 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.

◦ Aktivieren oder deaktivieren Sie die Berechtigung **S3 Select zulassen** nach Bedarf. Sehen "Verwalten von S3 Select für Mandantenkonten" .

◦ So entfernen Sie die Berechtigung **Grid-Föderationsverbindung verwenden**:

i. Wählen Sie die Registerkarte **Grid-Föderation**.

ii. Wählen Sie **Berechtigung entfernen**.

◦ So fügen Sie die Berechtigung **Grid-Föderationsverbindung verwenden** hinzu:

i. Wählen Sie die Registerkarte **Grid-Föderation**.

ii. Aktivieren Sie das Kontrollkästchen **Grid-Föderationsverbindung verwenden**.

iii. Wählen Sie optional **Vorhandene lokale Benutzer und Gruppen klonen** aus, um sie in das Remote-Raster zu klonen. Wenn Sie möchten, können Sie den laufenden Klonvorgang anhalten oder den Klonvorgang wiederholen, wenn das Klonen einiger lokaler Benutzer oder Gruppen nach Abschluss des letzten Klonvorgangs fehlgeschlagen ist.

◦ So legen Sie eine maximale Aufbewahrungsdauer fest oder aktivieren den Compliance-Modus:

> ⓘ Bevor Sie diese Einstellungen verwenden können, muss die S3-Objektsperre im Raster aktiviert sein.

i. Wählen Sie die Registerkarte **S3-Objektsperre**.

ii. Geben Sie für **Maximale Aufbewahrungsdauer festlegen** einen Wert ein und wählen Sie den Zeitraum aus dem Pulldown-Menü aus.

iii. Aktivieren Sie das Kontrollkästchen für **Compliance-Modus zulassen**.

Ändern Sie das Kennwort für den lokalen Root-Benutzer des Mandanten

Möglicherweise müssen Sie das Kennwort für den lokalen Root-Benutzer eines Mandanten ändern, wenn der Root-Benutzer vom Konto ausgeschlossen ist.

Bevor Sie beginnen

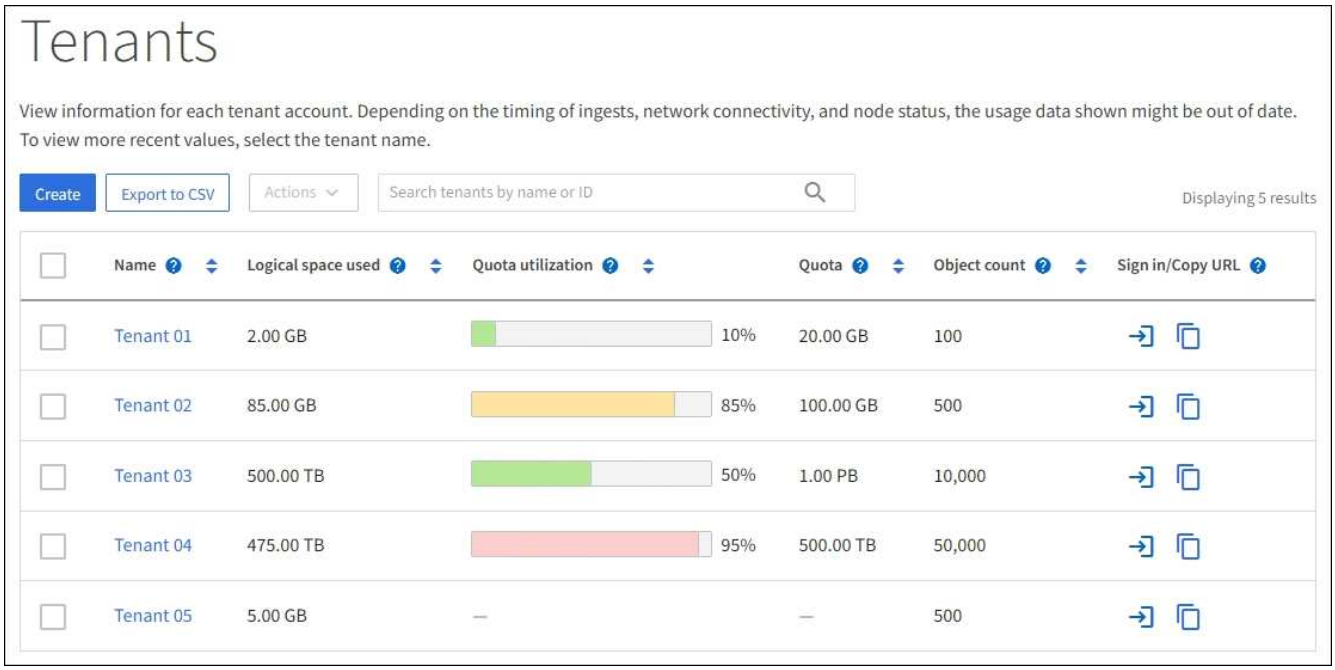
- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .

Informationen zu diesem Vorgang

Wenn Single Sign-On (SSO) für Ihr StorageGRID System aktiviert ist, kann sich der lokale Root-Benutzer nicht beim Mandantenkonto anmelden. Um Root-Benutzeraufgaben ausführen zu können, müssen Benutzer einer föderierten Gruppe angehören, die über die Root-Zugriffsberechtigung für den Mandanten verfügt.

Schritte

1. Wählen Sie **MIETER** aus.



2. Wählen Sie das Mandantenkonto aus. Sie können einen der folgenden Schritte ausführen:
   - Aktivieren Sie das Kontrollkästchen für den Mandanten und wählen Sie **Aktionen** > **Root-Passwort ändern**.
   - Wählen Sie den Namen des Mandanten aus, um die Detailseite anzuzeigen, und wählen Sie **Aktionen** > **Root-Passwort ändern**.
3. Geben Sie das neue Passwort für das Mieterkonto ein.
4. Wählen Sie **Speichern**.

Mieterkonto löschen

Sie können ein Mieterkonto löschen, wenn Sie dem Mieter den Zugriff auf das System dauerhaft entziehen möchten.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .
- Sie haben alle mit dem Mandantenkonto verknüpften S3-Buckets und -Objekte entfernt.
- Wenn der Mieter eine Grid-Föderation-Verbindung verwenden darf, haben Sie die Überlegungen für"Löschen eines Mandanten mit der Berechtigung „Grid-Föderationsverbindung verwenden“" .

Schritte

1. Wählen Sie **MIETER** aus.
2. Suchen Sie das oder die Mandantenkonten, die Sie löschen möchten.

   Verwenden Sie das Suchfeld, um nach einem Mieter anhand seines Namens oder seiner Mieter-ID zu suchen.

3. Um mehrere Mandanten zu löschen, aktivieren Sie die Kontrollkästchen und wählen Sie **Aktionen** > **Löschen**.

4. Um einen einzelnen Mandanten zu löschen, führen Sie einen der folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen und wählen Sie **Aktionen** > **Löschen**.
   - Wählen Sie den Mandantennamen aus, um die Detailseite anzuzeigen, und wählen Sie dann **Aktionen** > **Löschen**.
5. Wählen Sie **Ja**.

Plattformdienste verwalten

Was sind Plattformdienste?

Zu den Plattformdiensten gehören CloudMirror-Replikation, Ereignisbenachrichtigungen und der Suchintegrationsdienst.

Wenn Sie Plattformdienste für S3-Mandantenkonten aktivieren, müssen Sie Ihr Grid so konfigurieren, dass Mandanten auf die externen Ressourcen zugreifen können, die zur Verwendung dieser Dienste erforderlich sind.

CloudMirror-Replikation

Der StorageGRID CloudMirror-Replikationsdienst wird verwendet, um bestimmte Objekte aus einem StorageGRID Bucket an ein angegebenes externes Ziel zu spiegeln.

Sie können beispielsweise die CloudMirror-Replikation verwenden, um bestimmte Kundendatensätze in Amazon S3 zu spiegeln und dann AWS-Dienste nutzen, um Analysen Ihrer Daten durchzuführen.

> Die CloudMirror-Replikation weist einige wichtige Ähnlichkeiten und Unterschiede zur Cross-Grid-Replikationsfunktion auf. Weitere Informationen finden Sie unter"Vergleichen Sie Cross-Grid-Replikation und CloudMirror-Replikation" .

> Die CloudMirror-Replikation wird nicht unterstützt, wenn im Quell-Bucket S3 Object Lock aktiviert ist.

Benachrichtigungen

Bucket-spezifische Ereignisbenachrichtigungen werden verwendet, um Benachrichtigungen über bestimmte an Objekten ausgeführte Aktionen an einen angegebenen externen Kafka-Cluster oder Amazon Simple Notification Service zu senden.

Sie können beispielsweise Warnmeldungen konfigurieren, die an Administratoren gesendet werden, wenn ein Objekt zu einem Bucket hinzugefügt wird, wobei die Objekte Protokolldateien darstellen, die mit einem kritischen Systemereignis verknüpft sind.

> Obwohl die Ereignisbenachrichtigung für einen Bucket mit aktivierter S3-Objektsperre konfiguriert werden kann, werden die S3-Objektsperre-Metadaten (einschließlich „Aufbewahrungsdatum“ und „Legal Hold“-Status) der Objekte nicht in die Benachrichtigungsnachrichten aufgenommen.

Suchintegrationsdienst

Der Suchintegrationsdienst wird verwendet, um S3-Objektmetadaten an einen angegebenen Elasticsearch-Index zu senden, wo die Metadaten mithilfe des externen Dienstes gesucht oder analysiert werden können.

Sie können Ihre Buckets beispielsweise so konfigurieren, dass S3-Objektmetadaten an einen Remote-Elasticsearch-Dienst gesendet werden. Anschließend können Sie Elasticsearch verwenden, um Bucket-übergreifende Suchen durchzuführen und anspruchsvolle Analysen der in Ihren Objektmetadaten vorhandenen Muster durchzuführen.

> Obwohl die Elasticsearch-Integration für einen Bucket mit aktivierter S3 Object Lock konfiguriert werden kann, werden die S3 Object Lock-Metadaten (einschließlich „Retain Until Date“ und „Legal Hold“-Status) der Objekte nicht in die Benachrichtigungsnachrichten aufgenommen.

Plattformdienste geben Mietern die Möglichkeit, externe Speicherressourcen, Benachrichtigungsdienste sowie Such- oder Analysedienste mit ihren Daten zu verwenden. Da sich der Zielspeicherort für Plattformdienste normalerweise außerhalb Ihrer StorageGRID -Bereitstellung befindet, müssen Sie entscheiden, ob Sie Mandanten die Nutzung dieser Dienste gestatten möchten. In diesem Fall müssen Sie die Verwendung von Plattformdiensten aktivieren, wenn Sie Mandantenkonten erstellen oder bearbeiten. Sie müssen Ihr Netzwerk außerdem so konfigurieren, dass die von den Mandanten generierten Plattformdienstnachrichten ihre Ziele erreichen können.

Empfehlungen zur Nutzung von Plattformdiensten

Beachten Sie vor der Verwendung von Plattformdiensten die folgenden Empfehlungen:

- Wenn für einen S3-Bucket im StorageGRID -System sowohl die Versionierung als auch die CloudMirror-Replikation aktiviert ist, sollten Sie auch die S3-Bucket-Versionierung für den Zielendpunkt aktivieren. Dadurch kann die CloudMirror-Replikation ähnliche Objektversionen auf dem Endpunkt generieren.
- Sie sollten nicht mehr als 100 aktive Mandanten mit S3-Anfragen verwenden, die CloudMirror-Replikation, Benachrichtigungen und Suchintegration erfordern. Mehr als 100 aktive Mandanten können zu einer langsameren Leistung des S3-Clients führen.
- Anfragen an einen Endpunkt, die nicht abgeschlossen werden können, werden auf maximal 500.000 Anfragen in die Warteschlange gestellt. Dieses Limit wird gleichmäßig unter den aktiven Mietern aufgeteilt. Damit neu hinzukommende Mieter nicht ungerechterweise benachteiligt werden, ist es neuen Mietern gestattet, diese Grenze von 500.000 vorübergehend zu überschreiten.

Ähnliche Informationen

- "Plattformdienste verwalten"
- "Konfigurieren der Speicherproxyeinstellungen"
- "StorageGRID überwachen"

Netzwerk und Ports für Plattformdienste

Wenn Sie einem S3-Mandanten die Verwendung von Plattformdiensten gestatten, müssen Sie die Vernetzung für das Grid konfigurieren, um sicherzustellen, dass Nachrichten der Plattformdienste an ihre Ziele übermittelt werden können.

Sie können Plattformdienste für ein S3-Mandantenkonto aktivieren, wenn Sie das Mandantenkonto erstellen oder aktualisieren. Wenn Plattformdienste aktiviert sind, kann der Mandant Endpunkte erstellen, die als Ziel für CloudMirror-Replikation, Ereignisbenachrichtigungen oder Suchintegrationsnachrichten aus seinen S3-Buckets dienen. Diese Plattformdienstnachrichten werden von Speicherknoten, die den ADC-Dienst ausführen, an die Zielendpunkte gesendet.

Beispielsweise können Mandanten die folgenden Arten von Zielendpunkten konfigurieren:

- Ein lokal gehosteter Elasticsearch-Cluster
- Eine lokale Anwendung, die den Empfang von Amazon Simple Notification Service-Nachrichten unterstützt
- Ein lokal gehosteter Kafka-Cluster
- Ein lokal gehosteter S3-Bucket auf derselben oder einer anderen Instanz von StorageGRID
- Ein externer Endpunkt, z. B. ein Endpunkt auf Amazon Web Services.

Um sicherzustellen, dass Nachrichten der Plattformdienste zugestellt werden können, müssen Sie das Netzwerk oder die Netzwerke konfigurieren, die die ADC-Speicherknoten enthalten. Sie müssen sicherstellen, dass die folgenden Ports zum Senden von Plattformdienstnachrichten an die Zielendpunkte verwendet werden können.

Standardmäßig werden Nachrichten der Plattformdienste über die folgenden Ports gesendet:

- **80**: Für Endpunkt-URIs, die mit http beginnen (die meisten Endpunkte)
- **443**: Für Endpunkt-URIs, die mit https beginnen (die meisten Endpunkte)
- **9092**: Für Endpunkt-URIs, die mit http oder https beginnen (nur Kafka-Endpunkte)

Mandanten können beim Erstellen oder Bearbeiten eines Endpunkts einen anderen Port angeben.

> Wenn eine StorageGRID Bereitstellung als Ziel für die CloudMirror-Replikation verwendet wird, werden Replikationsnachrichten möglicherweise auf einem anderen Port als 80 oder 443 empfangen. Stellen Sie sicher, dass der von der StorageGRID Zielbereitstellung für S3 verwendete Port im Endpunkt angegeben ist.

Wenn Sie einen nicht-transparenten Proxy-Server verwenden, müssen Sie außerdem"Konfigurieren der Speicherproxyeinstellungen" um das Senden von Nachrichten an externe Endpunkte zu ermöglichen, beispielsweise an einen Endpunkt im Internet.

Ähnliche Informationen

"Verwenden eines Mandantenkontos"

Pro Site-Zustellung von Plattformdienstnachrichten

Alle Vorgänge der Plattformdienste werden pro Site durchgeführt.

Das heißt, wenn ein Mandant einen Client verwendet, um einen S3-API-Erstellungsvorgang für ein Objekt auszuführen, indem er eine Verbindung zu einem Gateway-Knoten am Rechenzentrumsstandort 1 herstellt, wird die Benachrichtigung über diese Aktion ausgelöst und vom Rechenzentrumsstandort 1 gesendet.

Wenn der Client anschließend einen S3-API-Löschvorgang für dasselbe Objekt vom Rechenzentrumsstandort 2 aus durchführt, wird die Benachrichtigung über die Löschaktion ausgelöst und vom Rechenzentrumsstandort 2 gesendet.

Stellen Sie sicher, dass das Netzwerk an jedem Standort so konfiguriert ist, dass Nachrichten der Plattformdienste an ihre Ziele übermittelt werden können.

Fehlerbehebung bei Plattformdiensten

Die in Plattformdiensten verwendeten Endpunkte werden von Mandantenbenutzern im

Mandanten-Manager erstellt und verwaltet. Wenn ein Mandant jedoch Probleme bei der Konfiguration oder Verwendung von Plattformdiensten hat, können Sie möglicherweise den Grid-Manager zur Lösung des Problems verwenden.

Probleme mit neuen Endpunkten

Bevor ein Mandant Plattformdienste nutzen kann, muss er mithilfe des Mandanten-Managers einen oder mehrere Endpunkte erstellen. Jeder Endpunkt stellt ein externes Ziel für einen Plattformdienst dar, beispielsweise einen StorageGRID S3-Bucket, einen Amazon Web Services-Bucket, ein Amazon Simple Notification Service-Thema, ein Kafka-Thema oder einen lokal oder auf AWS gehosteten Elasticsearch-Cluster. Jeder Endpunkt enthält sowohl den Standort der externen Ressource als auch die für den Zugriff auf diese Ressource erforderlichen Anmeldeinformationen.

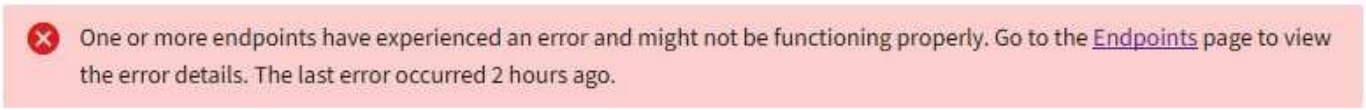
Wenn ein Mandant einen Endpunkt erstellt, überprüft das StorageGRID -System, ob der Endpunkt vorhanden ist und mit den angegebenen Anmeldeinformationen erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Knoten an jedem Standort validiert.

Wenn die Endpunktvalidierung fehlschlägt, wird in einer Fehlermeldung der Grund für das Fehlschlagen der Endpunktvalidierung erläutert. Der Mandantenbenutzer sollte das Problem beheben und dann erneut versuchen, den Endpunkt zu erstellen.

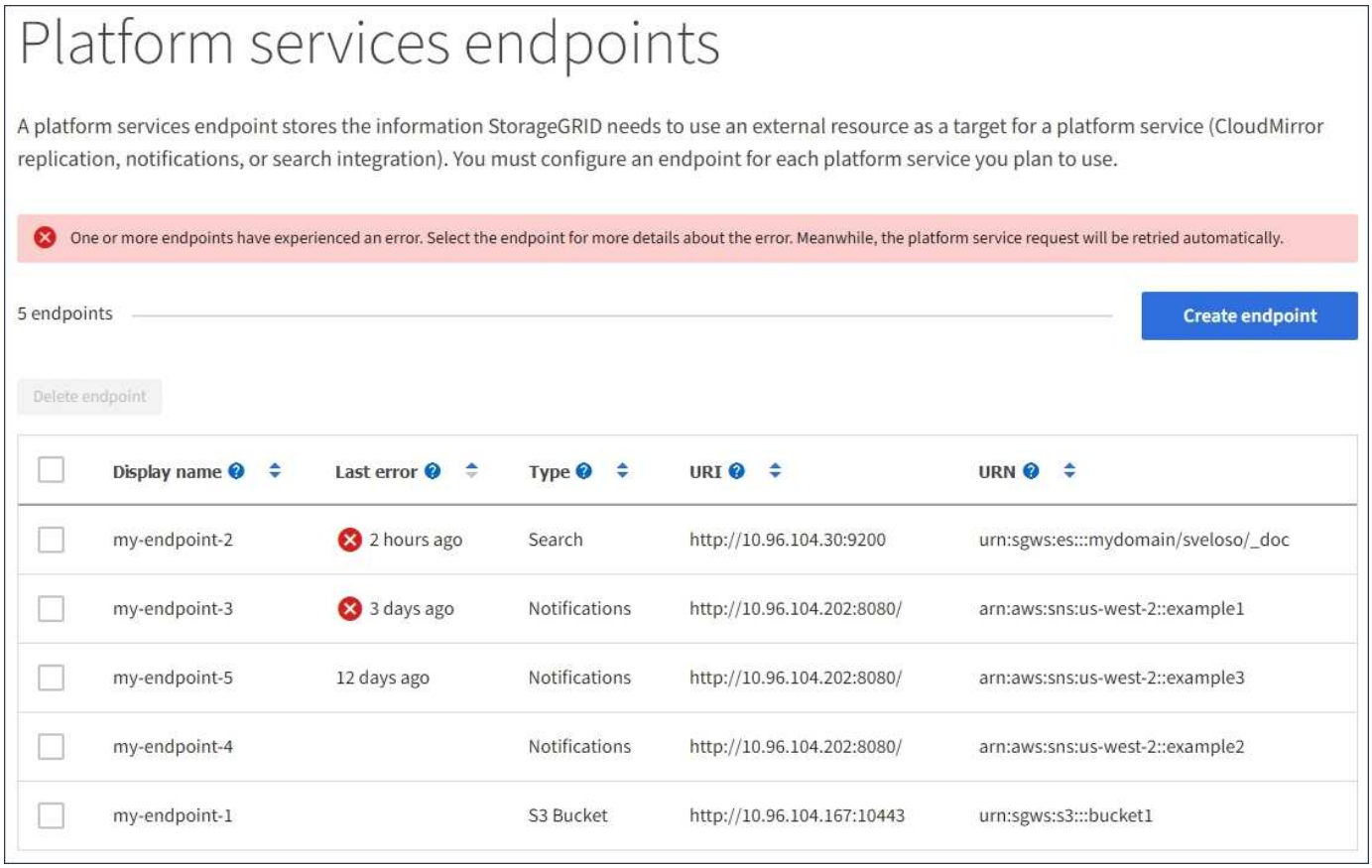
> ⓘ Die Endpunkterstellung schlägt fehl, wenn die Plattformdienste für das Mandantenkonto nicht aktiviert sind.

Probleme mit vorhandenen Endpunkten

Wenn beim Versuch von StorageGRID , einen vorhandenen Endpunkt zu erreichen, ein Fehler auftritt, wird auf dem Dashboard im Tenant Manager eine Meldung angezeigt.



Mandantenbenutzer können auf der Seite „Endpunkte“ die neueste Fehlermeldung für jeden Endpunkt überprüfen und feststellen, wie lange der Fehler her ist. In der Spalte **Letzter Fehler** wird für jeden Endpunkt die aktuellste Fehlermeldung angezeigt und angegeben, wie lange der Fehler her ist. Fehler, die Folgendes beinhalten: Symbol ist innerhalb der letzten 7 Tage aufgetreten.



Einige Fehlermeldungen in der Spalte **Letzter Fehler** enthalten möglicherweise eine Protokoll-ID in Klammern. Ein Grid-Administrator oder der technische Support kann anhand dieser ID detailliertere Informationen zum Fehler im bycast.log finden.

Probleme im Zusammenhang mit Proxyservern

Wenn Sie eine"Speicherproxy" zwischen Speicherknoten und Plattformdienst-Endpunkten können Fehler auftreten, wenn Ihr Proxydienst keine Nachrichten von StorageGRID zulässt. Um diese Probleme zu beheben, überprüfen Sie die Einstellungen Ihres Proxyservers, um sicherzustellen, dass plattformdienstbezogene Nachrichten nicht blockiert werden.

Feststellen, ob ein Fehler aufgetreten ist

Wenn innerhalb der letzten 7 Tage Endpunktfehler aufgetreten sind, wird im Dashboard im Tenant Manager eine Warnmeldung angezeigt. Weitere Einzelheiten zum Fehler finden Sie auf der Seite „Endpunkte“.

Clientvorgänge schlagen fehl

Einige Probleme mit Plattformdiensten können dazu führen, dass Clientvorgänge im S3-Bucket fehlschlagen. Beispielsweise schlagen S3-Clientvorgänge fehl, wenn der interne Dienst „Replicated State Machine“ (RSM) angehalten wird oder wenn zu viele Nachrichten der Plattformdienste zur Zustellung in der Warteschlange stehen.

So überprüfen Sie den Status der Dienste:

1. Wählen Sie **SUPPORT** > **Tools** > **Gittertopologie**.
2. Wählen Sie ***site*** > ***Storage Node*** > **SSM** > **Services**.

Behebbare und nicht behebbare Endpunktfehler

Nachdem Endpunkte erstellt wurden, können aus verschiedenen Gründen Fehler bei Plattform-Serviceanforderungen auftreten. Einige Fehler können durch Benutzereingriff behoben werden. Behebbare Fehler können beispielsweise aus folgenden Gründen auftreten:

- Die Anmeldeinformationen des Benutzers wurden gelöscht oder sind abgelaufen.
- Der Ziel-Bucket existiert nicht.
- Die Benachrichtigung kann nicht zugestellt werden.

Wenn StorageGRID auf einen behebbaren Fehler stößt, wird die Plattform-Serviceanforderung so lange wiederholt, bis sie erfolgreich ist.

Andere Fehler sind nicht behebbar. Beispielsweise tritt ein nicht behebbarer Fehler auf, wenn der Endpunkt gelöscht wird.

Wenn StorageGRID auf einen nicht behebbaren Endpunktfehler stößt:

- Gehen Sie im Grid Manager zu **Support** > **Tools** > **Metriken** > **Grafana** > **Übersicht über Plattformdienste**, um Fehlerdetails anzuzeigen.
- Gehen Sie im Tenant Manager zu **STORAGE (S3)** > **Platform Services Endpoints**, um die Fehlerdetails anzuzeigen.
- Überprüfen Sie die `/var/local/log/bycast-err.log` für zugehörige Fehler. Speicherknoten mit dem ADC-Dienst enthalten diese Protokolldatei.

Nachrichten der Plattformdienste können nicht zugestellt werden

Wenn beim Ziel ein Problem auftritt, das die Annahme von Plattformdienstnachrichten verhindert, ist der Clientvorgang für den Bucket zwar erfolgreich, die Plattformdienstnachricht wird jedoch nicht zugestellt. Dieser Fehler kann beispielsweise auftreten, wenn die Anmeldeinformationen am Ziel aktualisiert werden, sodass StorageGRID sich nicht mehr beim Zieldienst authentifizieren kann.

Suchen Sie nach zugehörigen Warnungen.

Geringere Leistung bei Plattformdienstanfragen

Die StorageGRID Software drosselt möglicherweise eingehende S3-Anfragen für einen Bucket, wenn die Rate, mit der die Anfragen gesendet werden, die Rate überschreitet, mit der der Zielendpunkt die Anfragen empfangen kann. Eine Drosselung tritt nur auf, wenn ein Rückstand an Anfragen besteht, die darauf warten, an den Zielendpunkt gesendet zu werden.

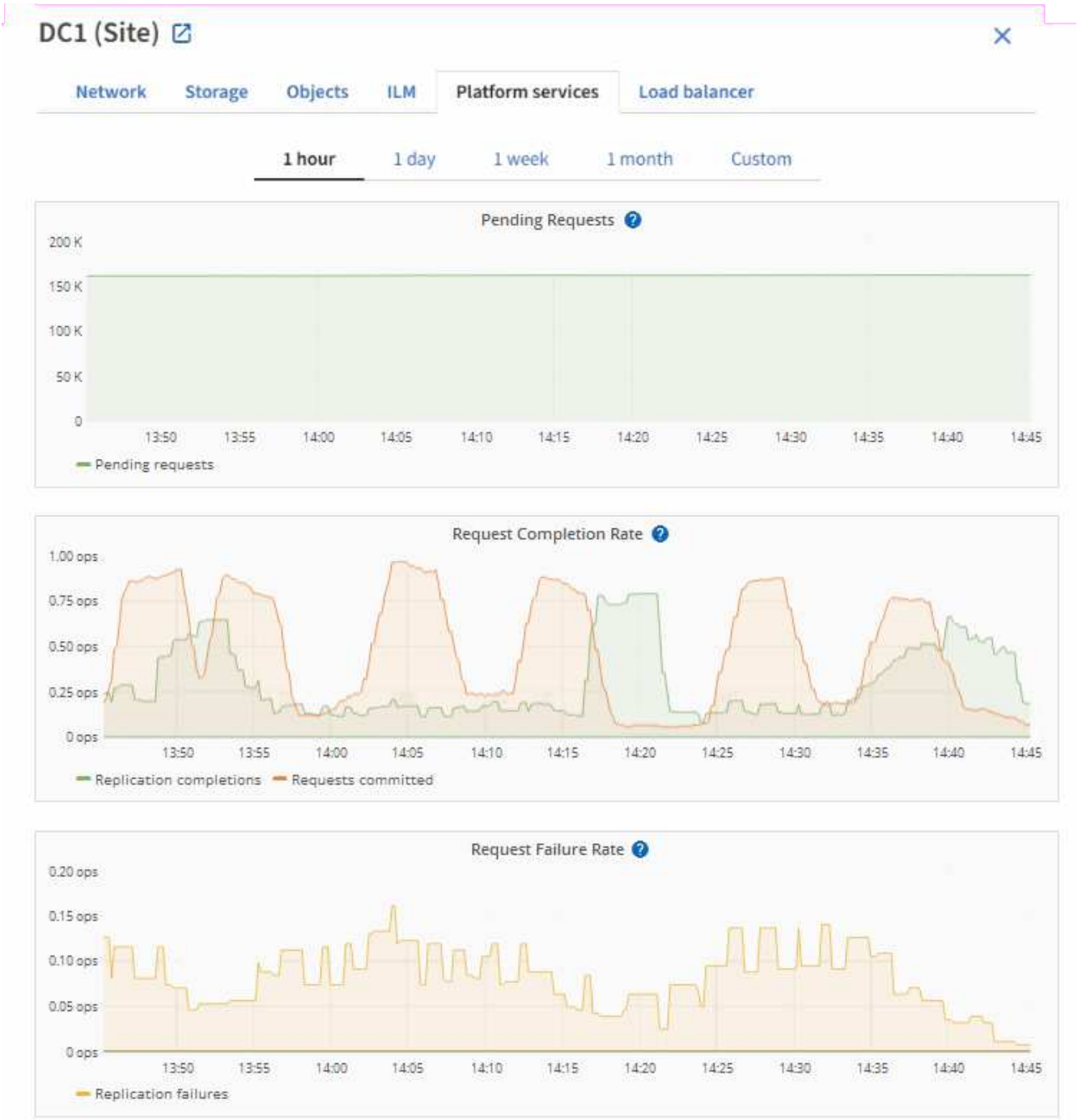
Der einzige sichtbare Effekt besteht darin, dass die Ausführung eingehender S3-Anfragen länger dauert. Wenn Sie eine deutlich langsamere Leistung feststellen, sollten Sie die Aufnahmerate reduzieren oder einen Endpunkt mit höherer Kapazität verwenden. Wenn der Rückstand an Anfragen weiter wächst, schlagen Client-S3-Operationen (wie etwa PUT-Anfragen) letztendlich fehl.

Bei CloudMirror-Anfragen ist die Leistung des Zielendpunkts wahrscheinlicher beeinträchtigt, da diese Anfragen in der Regel mehr Datenübertragungen beinhalten als Anfragen zur Suchintegration oder Ereignisbenachrichtigung.

Plattformdienstanforderungen schlagen fehl

So zeigen Sie die Anforderungsfehlerrate für Plattformdienste an:

1. Wählen Sie **NODES**.
2. Wählen Sie ***site*** > **Plattformdienste**.
3. Sehen Sie sich das Diagramm zur Anforderungsfehlerrate an.



Warnung: Nicht verfügbare Plattformdienste

Die Warnung **Plattformdienste nicht verfügbar** weist darauf hin, dass an einem Standort keine Plattformdienstvorgänge ausgeführt werden können, da zu wenige Speicherknoten mit dem RSM-Dienst ausgeführt werden oder verfügbar sind.

Der RSM-Dienst stellt sicher, dass Plattformdienstanforderungen an ihre jeweiligen Endpunkte gesendet werden.

Um diese Warnung zu beheben, ermitteln Sie, welche Speicherknoten am Standort den RSM-Dienst enthalten. (Der RSM-Dienst ist auf Speicherknoten vorhanden, die auch den ADC-Dienst enthalten.) Stellen Sie dann sicher, dass die einfache Mehrheit dieser Speicherknoten ausgeführt wird und verfügbar ist.

> Wenn an einem Standort mehr als ein Speicherknoten ausfällt, der den RSM-Dienst enthält, gehen alle ausstehenden Plattformdienstanforderungen für diesen Standort verloren.

Zusätzliche Anleitung zur Fehlerbehebung für Plattformdienst-Endpunkte

Weitere Informationen finden Sie unter**Verwenden Sie ein Mandantenkonto › Beheben Sie Probleme mit Plattformdienst-Endpunkten** .

Ähnliche Informationen

"Fehlerbehebung beim StorageGRID -System"

Verwalten von S3 Select für Mandantenkonten

Sie können bestimmten S3-Mandanten erlauben, S3 Select zu verwenden, um SelectObjectContent-Anfragen für einzelne Objekte auszugeben.

S3 Select bietet eine effiziente Möglichkeit, große Datenmengen zu durchsuchen, ohne dass für die Suche eine Datenbank und zugehörige Ressourcen bereitgestellt werden müssen. Außerdem werden die Kosten und die Latenz beim Abrufen von Daten reduziert.

Was ist S3 Select?

Mit S3 Select können S3-Clients SelectObjectContent-Anfragen verwenden, um nur die benötigten Daten aus einem Objekt zu filtern und abzurufen. Die StorageGRID -Implementierung von S3 Select umfasst eine Teilmenge der Befehle und Funktionen von S3 Select.

Überlegungen und Anforderungen zur Verwendung von S3 Select

Anforderungen an die Netzverwaltung

Der Grid-Administrator muss den Mandanten die S3 Select-Berechtigung erteilen. Wählen Sie **S3 Select zulassen**, wenn"Erstellen eines Mandanten" oder"Bearbeiten eines Mandanten" .

Anforderungen an das Objektformat

Das abzufragende Objekt muss eines der folgenden Formate aufweisen:

- **CSV**. Kann unverändert verwendet oder in GZIP- oder BZIP2-Archive komprimiert werden.
- **Parkett**. Zusätzliche Anforderungen für Parquet-Objekte:
  - S3 Select unterstützt nur spaltenweise Komprimierung mit GZIP oder Snappy. S3 Select unterstützt keine Ganzobjektkomprimierung für Parquet-Objekte.
  - S3 Select unterstützt keine Parquet-Ausgabe. Sie müssen das Ausgabeformat als CSV oder JSON angeben.
  - Die maximale unkomprimierte Zeilengruppengröße beträgt 512 MB.
  - Sie müssen die im Schema des Objekts angegebenen Datentypen verwenden.
  - Sie können die logischen Typen INTERVAL, JSON, LIST, TIME oder UUID nicht verwenden.

Endpunktanforderungen

Die SelectObjectContent-Anforderung muss an einen"StorageGRID Lastenausgleichsendpunkt" .

Die vom Endpunkt verwendeten Admin- und Gateway-Knoten müssen einer der folgenden sein:

- Ein Dienst-Appliance-Knoten
- Ein VMware-basierter Softwareknoten
- Ein Bare-Metal-Knoten, auf dem ein Kernel mit aktivierter Cgroup v2 ausgeführt wird

Allgemeine Überlegungen

Abfragen können nicht direkt an Speicherknoten gesendet werden.

> SelectObjectContent-Anfragen können die Leistung des Load Balancers für alle S3-Clients und alle Mandanten verringern. Aktivieren Sie diese Funktion nur bei Bedarf und nur für vertrauenswürdige Mandanten.

Siehe die"Anweisungen zur Verwendung von S3 Select" .

Zum Ansehen"Grafana-Diagramme" Wählen Sie für S3 Select-Operationen im Zeitverlauf **SUPPORT** > **Tools** > **Metrics** im Grid Manager.

Konfigurieren von Clientverbindungen

Konfigurieren von S3-Clientverbindungen

Als Grid-Administrator verwalten Sie die Konfigurationsoptionen, die steuern, wie S3-Clientanwendungen eine Verbindung zu Ihrem StorageGRID -System herstellen, um Daten zu speichern und abzurufen.

> Swift-Details wurden aus dieser Version der Dokumentationssite entfernt. Sehen "StorageGRID 11.8: S3- und Swift-Clientverbindungen konfigurieren" .

Konfigurationsaufgaben

1. Führen Sie die erforderlichen Aufgaben in StorageGRID aus, je nachdem, wie die Clientanwendung eine Verbindung zu StorageGRID herstellt.

Erforderliche Aufgaben

Sie müssen Folgendes besorgen:

- IP-Adressen
- Domänennamen
- SSL-Zertifikat

Optionale Aufgaben

Konfigurieren Sie optional:

- Identitätsföderation
- SSO

1. Verwenden Sie StorageGRID , um die Werte abzurufen, die die Anwendung für die Verbindung mit dem Grid benötigt. Sie können entweder den S3-Setup-Assistenten verwenden oder jede StorageGRID Einheit manuell konfigurieren.

Verwenden Sie den S3-Setup-Assistenten

Befolgen Sie die Schritte im S3-Setup-Assistenten.

Manuell konfigurieren

1. Erstellen einer Hochverfügbarkeitsgruppe
2. Erstellen eines Load Balancer-Endpunkts
3. Mieterkonto erstellen
4. Bucket und Zugriffsschlüssel erstellen
5. Konfigurieren der ILM-Regel und -Richtlinie

1. Verwenden Sie die S3-Anwendung, um die Verbindung zu StorageGRID herzustellen. Erstellen Sie DNS-Einträge, um IP-Adressen den Domänennamen zuzuordnen, die Sie verwenden möchten.

   Führen Sie bei Bedarf zusätzliche Anwendungseinstellungen durch.

2. Führen Sie laufende Aufgaben in der Anwendung und in StorageGRID aus, um den Objektspeicher im Laufe der Zeit zu verwalten und zu überwachen.

Erforderliche Informationen zum Anhängen von StorageGRID an eine Clientanwendung

Bevor Sie StorageGRID an eine S3-Clientanwendung anhängen können, müssen Sie Konfigurationsschritte in StorageGRID ausführen und bestimmte Werte abrufen.

Welche Werte benötige ich?

Die folgende Tabelle zeigt die Werte, die Sie in StorageGRID konfigurieren müssen, und wo diese Werte von der S3-Anwendung und dem DNS-Server verwendet werden.

Wert	Wo der Wert konfiguriert ist	Wo Wert verwendet wird
Virtuelle IP-Adressen (VIP)	StorageGRID > HA-Gruppe	DNS-Eintrag
Hafen	StorageGRID > Load Balancer-Endpunkt	Client-Anwendung
SSL-Zertifikat	StorageGRID > Load Balancer-Endpunkt	Client-Anwendung
Servername (FQDN)	StorageGRID > Load Balancer-Endpunkt	• Client-Anwendung • DNS-Eintrag
S3-Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel	StorageGRID > Mandant und Bucket	Client-Anwendung
Bucket-/Containername	StorageGRID > Mandant und Bucket	Client-Anwendung

Wie komme ich an diese Werte?

Je nach Ihren Anforderungen können Sie die benötigten Informationen auf folgende Weise abrufen:

- *Verwenden Sie die"S3-Setup-Assistent" *. Der S3-Setup-Assistent hilft Ihnen, die erforderlichen Werte in StorageGRID schnell zu konfigurieren und gibt ein oder zwei Dateien aus, die Sie bei der Konfiguration der S3-Anwendung verwenden können. Der Assistent führt Sie durch die erforderlichen Schritte und hilft sicherzustellen, dass Ihre Einstellungen den Best Practices von StorageGRID entsprechen.

  Wenn Sie eine S3-Anwendung konfigurieren, wird die Verwendung des S3-Setup-Assistenten empfohlen, es sei denn, Sie wissen, dass Sie besondere Anforderungen haben oder Ihre Implementierung erhebliche Anpassungen erfordert.

- *Verwenden Sie die"FabricPool -Setup-Assistent" *. Ähnlich wie der S3-Setup-Assistent hilft Ihnen der FabricPool -Setup-Assistent dabei, die erforderlichen Werte schnell zu konfigurieren und gibt eine Datei aus, die Sie beim Konfigurieren einer FabricPool Cloud-Ebene in ONTAP verwenden können.

  Wenn Sie StorageGRID als Objektspeichersystem für eine FabricPool Cloud-Ebene verwenden möchten, wird die Verwendung des FabricPool -Setup-Assistenten empfohlen, es sei denn, Sie wissen, dass Sie besondere Anforderungen haben oder Ihre Implementierung erhebliche Anpassungen erfordert.

- **Elemente manuell konfigurieren**. Wenn Sie eine Verbindung zu einer S3-Anwendung herstellen und den S3-Setup-Assistenten nicht verwenden möchten, können Sie die erforderlichen Werte erhalten, indem Sie die Konfiguration manuell durchführen. Gehen Sie folgendermaßen vor:
  a. Konfigurieren Sie die Hochverfügbarkeitsgruppe (HA), die Sie für die S3-Anwendung verwenden möchten. Sehen "Konfigurieren von Hochverfügbarkeitsgruppen" .
  b. Erstellen Sie den Load Balancer-Endpunkt, den die S3-Anwendung verwenden wird. Sehen "Konfigurieren von Load Balancer-Endpunkten" .

c. Erstellen Sie das Mandantenkonto, das die S3-Anwendung verwenden wird. Sehen "Erstellen Sie ein Mieterkonto" .

d. Melden Sie sich bei einem S3-Mandanten beim Mandantenkonto an und generieren Sie eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel für jeden Benutzer, der auf die Anwendung zugreift. Sehen "Erstellen Sie Ihre eigenen Zugriffsschlüssel" .

e. Erstellen Sie einen oder mehrere S3-Buckets innerhalb des Mandantenkontos. Für S3 siehe"S3-Bucket erstellen" .

f. Um spezifische Platzierungsanweisungen für die Objekte hinzuzufügen, die zum neuen Mandanten oder Bucket/Container gehören, erstellen Sie eine neue ILM-Regel und aktivieren Sie eine neue ILM-Richtlinie, um diese Regel zu verwenden. Sehen"ILM-Regel erstellen" Und"ILM-Richtlinie erstellen" .

Sicherheit für S3-Clients

StorageGRID Mandantenkonten verwenden S3-Clientanwendungen, um Objektdaten in StorageGRID zu speichern. Sie sollten die für Clientanwendungen implementierten Sicherheitsmaßnahmen überprüfen.

Zusammenfassung

Die folgende Liste fasst zusammen, wie die Sicherheit für die S3 REST API implementiert wird:

Verbindungssicherheit
TLS

Serverauthentifizierung
Von der Systemzertifizierungsstelle signiertes X.509-Serverzertifikat oder vom Administrator bereitgestelltes benutzerdefiniertes Serverzertifikat

Client-Authentifizierung
S3-Kontozugriffsschlüssel-ID und geheimer Zugriffsschlüssel

Client-Autorisierung
Bucket-Eigentümerschaft und alle geltenden Zugriffskontrollrichtlinien

So bietet StorageGRID Sicherheit für Clientanwendungen

S3-Clientanwendungen können eine Verbindung zum Load Balancer-Dienst auf Gateway-Knoten oder Admin-Knoten oder direkt zu Speicherknoten herstellen.

- Clients, die eine Verbindung zum Load Balancer-Dienst herstellen, können HTTPS oder HTTP verwenden, je nachdem, wie Sie"Konfigurieren Sie den Load Balancer-Endpunkt" .

  HTTPS bietet eine sichere, TLS-verschlüsselte Kommunikation und wird empfohlen. Sie müssen dem Endpunkt ein Sicherheitszertifikat beifügen.

  HTTP bietet eine weniger sichere, unverschlüsselte Kommunikation und sollte nur für Nicht-Produktions- oder Test-Grids verwendet werden.

- Clients, die eine Verbindung zu Speicherknoten herstellen, können auch HTTPS oder HTTP verwenden.

  HTTPS ist die Standardeinstellung und wird empfohlen.

HTTP bietet eine weniger sichere, unverschlüsselte Kommunikation, kann aber optional"ermöglicht" für Nicht-Produktions- oder Testnetze.

- Die Kommunikation zwischen StorageGRID und dem Client wird mit TLS verschlüsselt.
- Die Kommunikation zwischen dem Load Balancer-Dienst und den Speicherknoten innerhalb des Grids wird verschlüsselt, unabhängig davon, ob der Load Balancer-Endpunkt für die Annahme von HTTP- oder HTTPS-Verbindungen konfiguriert ist.
- Kunden müssen liefern"HTTP-Authentifizierungsheader" zu StorageGRID , um REST-API-Operationen durchzuführen.

Sicherheitszertifikate und Clientanwendungen

In allen Fällen können Clientanwendungen TLS-Verbindungen herstellen, indem sie entweder ein vom Grid-Administrator hochgeladenes benutzerdefiniertes Serverzertifikat oder ein vom StorageGRID System generiertes Zertifikat verwenden:

- Wenn Clientanwendungen eine Verbindung zum Load Balancer-Dienst herstellen, verwenden sie das Zertifikat, das für den Load Balancer-Endpunkt konfiguriert wurde. Jeder Load Balancer-Endpunkt verfügt über ein eigenes Zertifikat – entweder ein benutzerdefiniertes Serverzertifikat, das vom Grid-Administrator hochgeladen wurde, oder ein Zertifikat, das der Grid-Administrator beim Konfigurieren des Endpunkts in StorageGRID generiert hat.

  Sehen "Überlegungen zum Lastenausgleich" .

- Wenn Clientanwendungen eine direkte Verbindung zu einem Speicherknoten herstellen, verwenden sie entweder die vom System generierten Serverzertifikate, die bei der Installation des StorageGRID -Systems für Speicherknoten generiert wurden (und von der Systemzertifizierungsstelle signiert sind), oder ein einzelnes benutzerdefiniertes Serverzertifikat, das von einem Grid-Administrator für das Grid bereitgestellt wird. Sehen "Fügen Sie ein benutzerdefiniertes S3-API-Zertifikat hinzu" .

Clients sollten so konfiguriert werden, dass sie der Zertifizierungsstelle vertrauen, die das von ihnen zum Herstellen von TLS-Verbindungen verwendete Zertifikat signiert hat.

Unterstützte Hashing- und Verschlüsselungsalgorithmen für TLS-Bibliotheken

Das StorageGRID -System unterstützt eine Reihe von Verschlüsselungssammlungen, die Clientanwendungen beim Herstellen einer TLS-Sitzung verwenden können. Um Verschlüsselungen zu konfigurieren, gehen Sie zu **KONFIGURATION** > **Sicherheit** > **Sicherheitseinstellungen** und wählen Sie **TLS- und SSH-Richtlinien**.

Unterstützte Versionen von TLS

StorageGRID unterstützt TLS 1.2 und TLS 1.3.

SSLv3 und TLS 1.1 (oder frühere Versionen) werden nicht mehr unterstützt.

Verwenden Sie den S3-Setup-Assistenten

S3-Setup-Assistent verwenden: Überlegungen und Anforderungen

Sie können den S3-Setup-Assistenten verwenden, um StorageGRID als Objektspeichersystem für eine S3-Anwendung zu konfigurieren.

Wann Sie den S3-Setup-Assistenten verwenden sollten

Der S3-Setup-Assistent führt Sie durch jeden Schritt der Konfiguration von StorageGRID für die Verwendung mit einer S3-Anwendung. Beim Abschließen des Assistenten laden Sie Dateien herunter, mit denen Sie Werte in die S3-Anwendung eingeben können. Verwenden Sie den Assistenten, um Ihr System schneller zu konfigurieren und sicherzustellen, dass Ihre Einstellungen den Best Practices von StorageGRID entsprechen.

Wenn Sie die"Root-Zugriffsberechtigung" : Sie können den S3-Setup-Assistenten abschließen, wenn Sie mit der Verwendung des StorageGRID Grid Managers beginnen, oder Sie können zu einem späteren Zeitpunkt auf den Assistenten zugreifen und ihn abschließen. Je nach Bedarf können Sie auch einige oder alle benötigten Elemente manuell konfigurieren und anschließend mit dem Assistenten die Werte zusammenstellen, die eine S3-Anwendung benötigt.

Vor der Verwendung des Assistenten

Bevor Sie den Assistenten verwenden, vergewissern Sie sich, dass Sie diese Voraussetzungen erfüllt haben.

Beziehen Sie IP-Adressen und richten Sie VLAN-Schnittstellen ein

Wenn Sie eine Hochverfügbarkeitsgruppe (HA) konfigurieren, wissen Sie, mit welchen Knoten die S3-Anwendung eine Verbindung herstellt und welches StorageGRID Netzwerk verwendet wird. Sie wissen auch, welche Werte Sie für das Subnetz-CIDR, die Gateway-IP-Adresse und die virtuellen IP-Adressen (VIP) eingeben müssen.

Wenn Sie ein virtuelles LAN verwenden möchten, um den Datenverkehr von der S3-Anwendung zu trennen, haben Sie die VLAN-Schnittstelle bereits konfiguriert. Sehen "Konfigurieren von VLAN-Schnittstellen" .

Konfigurieren der Identitätsföderation und SSO

Wenn Sie Identitätsföderation oder Single Sign-On (SSO) für Ihr StorageGRID System verwenden möchten, haben Sie diese Funktionen aktiviert. Sie wissen auch, welche föderierte Gruppe Root-Zugriff auf das Mandantenkonto haben sollte, das die S3-Anwendung verwenden wird. Sehen"Verwenden der Identitätsföderation" Und"Konfigurieren der einmaligen Anmeldung" .

Domänennamen abrufen und konfigurieren

Sie wissen, welchen vollqualifizierten Domänennamen (FQDN) Sie für StorageGRID verwenden müssen. Einträge des Domänennamenservers (DNS) ordnen diesen FQDN den virtuellen IP-Adressen (VIP) der HA-Gruppe zu, die Sie mit dem Assistenten erstellen.

Wenn Sie virtuelle S3-Hosting-Anfragen verwenden möchten, sollten Sie"konfigurierte S3-Endpunktdomänennamen" . Es wird empfohlen, Anfragen im virtuellen gehosteten Stil zu verwenden.

Überprüfen Sie die Anforderungen für Load Balancer und Sicherheitszertifikate

Wenn Sie den StorageGRID Lastenausgleich verwenden möchten, haben Sie die allgemeinen Überlegungen zum Lastenausgleich überprüft. Sie verfügen über die Zertifikate, die Sie hochladen möchten, oder über die Werte, die Sie zum Generieren eines Zertifikats benötigen.

Wenn Sie einen externen Load Balancer-Endpunkt (eines Drittanbieters) verwenden möchten, verfügen Sie über den vollqualifizierten Domänennamen (FQDN), den Port und das Zertifikat für diesen Load Balancer.

Konfigurieren Sie alle Grid-Föderation-Verbindungen

Wenn Sie dem S3-Mandanten das Klonen von Kontodaten und das Replizieren von Bucket-Objekten in ein anderes Grid mithilfe einer Grid-Föderationsverbindung erlauben möchten, bestätigen Sie Folgendes, bevor Sie den Assistenten starten:

- Du hast"die Grid-Föderation-Verbindung konfiguriert" .
- Der Status der Verbindung ist **Verbunden**.
- Sie verfügen über Root-Zugriffsberechtigung.

Greifen Sie auf den S3-Setup-Assistenten zu und schließen Sie ihn ab

Sie können den S3-Setup-Assistenten verwenden, um StorageGRID für die Verwendung mit einer S3-Anwendung zu konfigurieren. Der Setup-Assistent stellt die Werte bereit, die die Anwendung benötigt, um auf einen StorageGRID Bucket zuzugreifen und Objekte zu speichern.

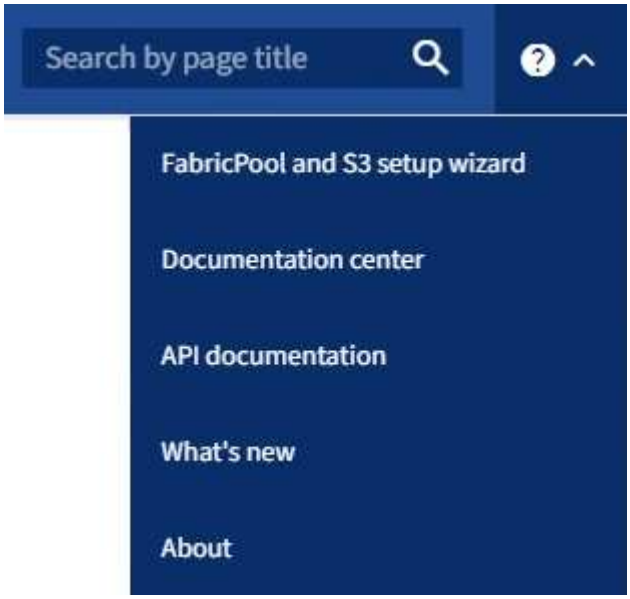
Bevor Sie beginnen

- Sie haben die"Root-Zugriffsberechtigung" .
- Sie haben die"Überlegungen und Anforderungen" zur Verwendung des Assistenten.

Zugriff auf den Assistenten

Schritte

1. Sign in beim Grid Manager an mit einem"unterstützter Webbrowser" .
2. Wenn das Banner * FabricPool und S3-Setup-Assistent* auf dem Dashboard angezeigt wird, wählen Sie den Link im Banner aus. Wenn das Banner nicht mehr angezeigt wird, wählen Sie das Hilfesymbol in der Kopfzeile im Grid Manager und wählen Sie * FabricPool und S3-Setup-Assistent*.



3. Wählen Sie im Abschnitt „S3-Anwendung“ der Seite des FabricPool und S3-Setup-Assistenten die Option „Jetzt konfigurieren“ aus.

Schritt 1 von 6: HA-Gruppe konfigurieren

Eine HA-Gruppe ist eine Sammlung von Knoten, die jeweils den StorageGRID Load Balancer-Dienst enthalten. Eine HA-Gruppe kann Gateway-Knoten, Admin-Knoten oder beides enthalten.

Sie können eine HA-Gruppe verwenden, um die Verfügbarkeit der S3-Datenverbindungen aufrechtzuerhalten. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle die Arbeitslast mit

geringen Auswirkungen auf den S3-Betrieb verwalten.

Einzelheiten zu dieser Aufgabe finden Sie unter"Verwalten von Hochverfügbarkeitsgruppen" .

Schritte

1. Wenn Sie einen externen Lastenausgleich verwenden möchten, müssen Sie keine HA-Gruppe erstellen. Wählen Sie **Diesen Schritt überspringen** und gehen Sie zuSchritt 2 von 6: Load Balancer-Endpunkt konfigurieren .
2. Um den StorageGRID Load Balancer zu verwenden, können Sie eine neue HA-Gruppe erstellen oder eine vorhandene HA-Gruppe verwenden.

HA-Gruppe erstellen

a. Um eine neue HA-Gruppe zu erstellen, wählen Sie **HA-Gruppe erstellen**.

b. Füllen Sie für den Schritt **Details eingeben** die folgenden Felder aus.

Feld	Beschreibung
HA-Gruppenname	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.

   Nutzen Sie die Spaltenüberschriften zum Sortieren der Zeilen oder geben Sie einen Suchbegriff ein, um Schnittstellen schneller zu finden.

   Sie können einen oder mehrere Knoten auswählen, aber Sie können für jeden Knoten nur eine Schnittstelle auswählen.

d. Bestimmen Sie für den Schritt **Schnittstellen priorisieren** die primäre Schnittstelle und alle Backup-Schnittstellen für diese HA-Gruppe.

   Ziehen Sie Zeilen, um die Werte in der Spalte **Prioritätsreihenfolge** 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 umfasst und die aktive Schnittstelle ausfällt, werden die virtuellen IP-Adressen (VIP) zur ersten Backup-Schnittstelle in der Prioritätsreihenfolge verschoben. Wenn diese Schnittstelle ausfällt, werden die VIP-Adressen zur nächsten Backup-Schnittstelle verschoben und so weiter. Wenn die Fehler behoben sind, werden die VIP-Adressen wieder an die Schnittstelle mit der höchsten verfügbaren Priorität weitergeleitet.

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 Subnetzlänge (0-32). Für die Netzwerkadresse dürfen keine Hostbits gesetzt sein. Beispiel: `192.16.0.0/22`.
Gateway-IP-Adresse (optional)	Wenn sich die für den Zugriff auf StorageGRID verwendeten S3-IP-Adressen nicht im selben Subnetz wie die StorageGRID VIP-Adressen befinden, geben Sie die lokale Gateway-IP-Adresse des StorageGRID VIP ein. Die lokale Gateway-IP-Adresse muss sich innerhalb des VIP-Subnetzes befinden.

Feld	Beschreibung
Virtuelle IP-Adresse	Geben Sie mindestens eine und höchstens zehn VIP-Adressen für die aktive Schnittstelle in der HA-Gruppe ein. Alle VIP-Adressen müssen sich innerhalb des VIP-Subnetzes befinden. Mindestens eine Adresse muss IPv4 sein. Optional können Sie zusätzliche IPv4- und IPv6-Adressen angeben.

f. Wählen Sie **HA-Gruppe erstellen** und dann **Fertig stellen**, um zum S3-Setup-Assistenten zurückzukehren.

g. Wählen Sie **Weiter**, um zum Schritt „Lastenausgleich“ zu gelangen.

Vorhandene HA-Gruppe verwenden

a. Um eine vorhandene HA-Gruppe zu verwenden, wählen Sie den Namen der HA-Gruppe aus der Liste **HA-Gruppe auswählen** aus.

b. Wählen Sie **Weiter**, um zum Schritt „Lastenausgleich“ zu gelangen.

Schritt 2 von 6: Load Balancer-Endpunkt konfigurieren

StorageGRID verwendet einen Load Balancer, um die Arbeitslast von Clientanwendungen zu verwalten. Durch Lastenausgleich werden Geschwindigkeit und Verbindungskapazität über mehrere Speicherknoten hinweg maximiert.

Sie können den StorageGRID Load Balancer-Dienst verwenden, der auf allen Gateway- und Admin-Knoten vorhanden ist, oder Sie können eine Verbindung zu einem externen Load Balancer (eines Drittanbieters) herstellen. Die Verwendung des StorageGRID Load Balancers wird empfohlen.

Einzelheiten zu dieser Aufgabe finden Sie unter"Überlegungen zum Lastenausgleich" .

Um den StorageGRID Load Balancer-Dienst zu verwenden, wählen Sie die Registerkarte * StorageGRID Load Balancer* und erstellen oder wählen Sie dann den Load Balancer-Endpunkt aus, den Sie verwenden möchten. Um einen externen Lastenausgleich zu verwenden, wählen Sie die Registerkarte **Externer Lastenausgleich** und geben Sie Details zu dem 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 **Endpunktdetails eingeben** die folgenden Felder aus.

Feld	Beschreibung
Name	Ein beschreibender Name für den Endpunkt.
Hafen	Der StorageGRID -Port, den Sie für den Lastenausgleich verwenden möchten. Der Standardwert dieses Felds für den ersten Endpunkt, den Sie erstellen, ist 10433. Sie können jedoch jeden beliebigen nicht verwendeten externen Port eingeben. Wenn Sie 80 oder 443 eingeben, wird der Endpunkt nur auf Gateway-Knoten konfiguriert, da diese Ports auf Admin-Knoten reserviert sind. **Hinweis:** Von anderen Grid-Diensten verwendete Ports sind nicht zulässig. Siehe die"Netzwerkportreferenz" .
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 im Schritt **Bindungsmodus auswählen** den Bindungsmodus an. Der Bindungsmodus steuert, wie auf den Endpunkt über eine beliebige IP-Adresse oder über bestimmte IP-Adressen und Netzwerkschnittstellen zugegriffen wird.

Modus	Beschreibung
Global (Standard)	Clients können über die IP-Adresse eines beliebigen Gateway-Knotens oder Admin-Knotens, die virtuelle IP-Adresse (VIP) einer beliebigen HA-Gruppe in einem beliebigen Netzwerk oder einen entsprechenden FQDN auf den Endpunkt zugreifen. Verwenden Sie die Einstellung **Global** (Standard), es sei denn, Sie müssen die Erreichbarkeit dieses Endpunkts einschränken.
Virtuelle IPs von HA-Gruppen	Clients müssen eine virtuelle IP-Adresse (oder den entsprechenden FQDN) einer HA-Gruppe verwenden, um auf diesen Endpunkt zuzugreifen. Endpunkte mit diesem Bindungsmodus können alle dieselbe Portnummer verwenden, solange sich die von Ihnen für die Endpunkte ausgewählten HA-Gruppen nicht überschneiden.

Modus	Beschreibung
Knotenschnittstellen	Clients müssen die IP-Adressen (oder entsprechenden FQDNs) ausgewählter Knotenschnittstellen verwenden, um auf diesen Endpunkt zuzugreifen.
Knotentyp	Je nach ausgewähltem 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 „Mandantenzugriff“ 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 verwenden, um auf ihre Buckets zuzugreifen.
Ausgewählte Mieter blockieren	Die ausgewählten Mandantenkonten können diesen Endpunkt nicht verwenden, um auf ihre Buckets zuzugreifen. Alle anderen Mandanten können diesen Endpunkt verwenden.

5. Wählen Sie für den Schritt **Zertifikat anhängen** eine der folgenden Optionen aus:

Feld	Beschreibung
Zertifikat hochladen (empfohlen)	Verwenden Sie diese Option, um ein von einer Zertifizierungsstelle signiertes Serverzertifikat, einen privaten Zertifikatsschlüssel und ein optionales CA-Paket hochzuladen.
Zertifikat generieren	Verwenden Sie diese Option, um ein selbstsigniertes Zertifikat zu generieren. Sehen"Konfigurieren von Load Balancer-Endpunkten" für Einzelheiten zu den einzugebenden Informationen.
StorageGRID S3-Zertifikat verwenden	Verwenden Sie diese Option nur, wenn Sie bereits eine benutzerdefinierte Version des globalen StorageGRID -Zertifikats hochgeladen oder generiert haben. Sehen"Konfigurieren von S3-API-Zertifikaten" für Details.

6. Wählen Sie **Fertig**, um zum S3-Setup-Assistenten zurückzukehren.
7. Wählen Sie **Weiter**, um zum Schritt „Mandant und Bucket“ zu gelangen.

Es kann bis zu 15 Minuten dauern, bis Änderungen an einem Endpunktzertifikat auf alle Knoten angewendet werden.

Vorhandenen Load Balancer-Endpunkt verwenden

Schritte

1. Um einen vorhandenen Endpunkt zu verwenden, wählen Sie seinen Namen aus **Wählen Sie einen Load Balancer-Endpunkt** aus.
2. Wählen Sie **Weiter**, um zum Schritt „Mandant und Bucket“ zu gelangen.

Externen Load Balancer verwenden

Schritte

1. Um einen externen Lastenausgleich zu verwenden, füllen Sie die folgenden Felder aus.

Feld	Beschreibung
FQDN	Der vollqualifizierte Domänenname (FQDN) des externen Load Balancers.
Hafen	Die Portnummer, die die S3-Anwendung zum Herstellen einer 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 Schritt „Mandant und Bucket“ zu gelangen.

Schritt 3 von 6: Mandanten und Bucket erstellen

Ein Mandant ist eine Entität, die S3-Anwendungen zum Speichern und Abrufen von Objekten in StorageGRID verwenden kann. Jeder Mandant verfügt über eigene Benutzer, Zugriffsschlüssel, Buckets, Objekte und einen bestimmten Satz an Funktionen.

Ein Bucket ist ein Container zum Speichern der Objekte und Objektmetadaten eines Mandanten. Obwohl Mandanten viele Buckets haben können, hilft Ihnen der Assistent dabei, auf schnellste und einfachste Weise einen Mandanten und einen Bucket zu erstellen. Wenn Sie später Buckets hinzufügen oder Optionen festlegen müssen, können Sie den Tenant Manager verwenden.

Einzelheiten zu dieser Aufgabe finden Sie unter"Mieterkonto erstellen" Und"S3-Bucket erstellen" .

Schritte

1. Geben Sie einen Namen für das Mandantenkonto ein.

   Mandantennamen müssen nicht eindeutig sein. Beim Anlegen des Mandantenkontos erhält dieses eine eindeutige, numerische Konto-ID.

2. Definieren Sie den Root-Zugriff für das Mandantenkonto, je nachdem, ob Ihr StorageGRID -System"Identitätsföderation" ,"Einmaliges Anmelden (SSO)" oder beides.

Option	Tun Sie dies
Wenn die Identitätsföderation nicht aktiviert ist	Geben Sie das Kennwort an, das bei der Anmeldung beim Mandanten als lokaler Root-Benutzer verwendet werden soll.

Option	Tun Sie dies
Wenn die Identitätsföderation aktiviert ist	a. Wählen Sie eine bestehende Verbundgruppe aus, die"Root-Zugriffsberechtigung" für den Mieter. b. Geben Sie optional das Kennwort an, das bei der Anmeldung beim Mandanten als lokaler Root-Benutzer verwendet werden soll.
Wenn sowohl die Identitätsföderation als auch Single Sign-On (SSO) aktiviert sind	Wählen Sie eine bestehende Verbundgruppe aus, die"Root-Zugriffsberechtigung" für den Mieter. Es können sich keine lokalen Benutzer anmelden.

3. Wenn der Assistent die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel für den Root-Benutzer erstellen soll, wählen Sie **S3-Zugriffsschlüssel für Root-Benutzer automatisch erstellen**.

   Wählen Sie diese Option, wenn der einzige Benutzer für den Mandanten der Root-Benutzer sein soll. Wenn andere Benutzer diesen Mandanten verwenden,"Verwenden Sie den Tenant Manager" um Schlüssel und Berechtigungen zu konfigurieren.

4. Wenn Sie jetzt einen Bucket für diesen Mandanten erstellen möchten, wählen Sie **Bucket für diesen Mandanten erstellen**.

   Wenn S3 Object Lock für das Raster aktiviert ist, ist S3 Object Lock für den in diesem Schritt erstellten Bucket nicht aktiviert. Wenn Sie für diese S3-Anwendung einen S3 Object Lock-Bucket verwenden müssen, wählen Sie jetzt nicht die Option zum Erstellen eines Buckets aus. Verwenden Sie stattdessen den Tenant Manager, um"Erstellen Sie den Bucket" später.

   a. Geben Sie den Namen des Buckets ein, den die S3-Anwendung verwenden wird. Beispiel: `s3-bucket` .

      Sie können den Bucket-Namen nach dem Erstellen des Buckets nicht mehr ändern.

   b. Wählen Sie die **Region** für diesen Bucket aus.

      Verwenden Sie die Standardregion(`us-east-1`), es sei denn, Sie möchten in Zukunft ILM verwenden, um Objekte basierend auf der Region des Buckets zu filtern.

5. Wählen Sie **Erstellen und fortfahren**.

Schritt 4 von 6: Daten herunterladen

Im Schritt „Daten herunterladen“ können Sie eine oder zwei Dateien herunterladen, um die Details Ihrer gerade konfigurierten Daten zu speichern.

Schritte

1. Wenn Sie **S3-Zugriffsschlüssel für Root-Benutzer automatisch erstellen** ausgewählt haben, führen Sie einen oder beide der folgenden Schritte aus:

   - Wählen Sie **Zugriffsschlüssel herunterladen**, um einen `.csv` Datei mit dem Mandantenkontonamen, der Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel.
   - Wählen Sie das Kopiersymbol ( ), um die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel

in die Zwischenablage zu kopieren.

2. Wählen Sie **Konfigurationswerte herunterladen**, um eine `.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 Schlüssel sind nicht mehr verfügbar, nachdem Sie diese Seite geschlossen haben. Stellen Sie sicher, dass Sie diese Informationen an einem sicheren Ort speichern, da sie zum Abrufen von Daten aus Ihrem StorageGRID System verwendet werden können.

4. Aktivieren Sie bei entsprechender Aufforderung das Kontrollkästchen, um zu bestätigen, dass Sie die Schlüssel heruntergeladen oder kopiert haben.
5. Wählen Sie **Weiter** aus, um zum Schritt „ILM-Regel und -Richtlinie“ zu gelangen.

Schritt 5 von 6: ILM-Regel und ILM-Richtlinie für S3 überprüfen

Regeln für das Information Lifecycle Management (ILM) steuern die Platzierung, Dauer und das Aufnahmeverhalten aller Objekte in Ihrem StorageGRID System. Die in StorageGRID enthaltene ILM-Richtlinie erstellt zwei replizierte Kopien aller Objekte. Diese Richtlinie bleibt so lange in Kraft, bis Sie mindestens eine neue Richtlinie aktivieren.

Schritte

1. Überprüfen Sie die auf der Seite bereitgestellten Informationen.
2. Wenn Sie spezifische Anweisungen für die Objekte hinzufügen möchten, die zum neuen Mandanten oder Bucket gehören, erstellen Sie eine neue Regel und eine neue Richtlinie. Sehen"ILM-Regel erstellen" Und"Verwenden von ILM-Richtlinien" .
3. Wählen Sie **Ich habe diese Schritte überprüft und verstehe, was ich tun muss**.
4. Aktivieren Sie das Kontrollkästchen, um anzugeben, dass Sie wissen, was als Nächstes zu tun ist.
5. Wählen Sie **Weiter**, um zur **Zusammenfassung** zu gelangen.

Schritt 6 von 6: Zusammenfassung der Überprüfung

Schritte

1. Lesen Sie die Zusammenfassung.
2. Notieren Sie sich die Details in den nächsten Schritten, in denen die zusätzliche Konfiguration beschrieben wird, die möglicherweise erforderlich ist, bevor Sie eine Verbindung mit dem S3-Client herstellen. Wenn Sie beispielsweise „Als Root Sign in “ auswählen, gelangen Sie zum Mandanten-Manager, wo Sie Mandantenbenutzer hinzufügen, zusätzliche Buckets erstellen und Bucket-Einstellungen aktualisieren können.
3. Wählen Sie **Fertig**.
4. Konfigurieren Sie die Anwendung mithilfe der Datei, die Sie von StorageGRID heruntergeladen haben, oder der Werte, die Sie manuell erhalten haben.

Verwalten von HA-Gruppen

Was sind Hochverfügbarkeitsgruppen (HA)?

Hochverfügbarkeitsgruppen (HA) bieten hochverfügbare Datenverbindungen für S3-

Clients und hochverfügbare Verbindungen zum Grid Manager und zum Tenant Manager.

Sie können die Netzwerkschnittstellen mehrerer Admin- und Gateway-Knoten in einer Hochverfügbarkeitsgruppe (HA) zusammenfassen. Wenn die aktive Schnittstelle in der HA-Gruppe ausfällt, kann eine Backup-Schnittstelle die Arbeitslast bewältigen.

Jede HA-Gruppe bietet Zugriff auf die gemeinsam genutzten Dienste auf den ausgewählten Knoten.

- HA-Gruppen, die Gateway-Knoten, Admin-Knoten oder beides umfassen, bieten hochverfügbare Datenverbindungen für S3-Clients.
- HA-Gruppen, die nur Admin-Knoten enthalten, bieten hochverfügbare Verbindungen zum Grid Manager und zum Tenant Manager.
- Eine HA-Gruppe, die nur Service-Appliances und VMware-basierte Softwareknoten umfasst, kann hochverfügbare Verbindungen bereitstellen für"S3-Mandanten, die S3 Select verwenden" . HA-Gruppen werden bei der Verwendung von S3 Select empfohlen, sind aber nicht erforderlich.

Wie erstellt man eine HA-Gruppe?

1. Sie wählen eine Netzwerkschnittstelle für einen oder mehrere Admin-Knoten oder Gateway-Knoten aus. Sie können eine Grid-Netzwerkschnittstelle (eth0), eine Client-Netzwerkschnittstelle (eth2), eine VLAN-Schnittstelle oder eine Zugriffsschnittstelle verwenden, die Sie dem Knoten hinzugefügt haben.

   > Sie können einer HA-Gruppe keine Schnittstelle hinzufügen, wenn diese über eine per DHCP zugewiesene IP-Adresse verfügt.

2. Sie geben eine Schnittstelle als primäre Schnittstelle an. 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 zehn virtuelle IP-Adressen (VIP) zu. Clientanwendungen können jede dieser VIP-Adressen verwenden, um eine Verbindung mit StorageGRID herzustellen.

Anweisungen hierzu finden Sie unter"Konfigurieren von Hochverfügbarkeitsgruppen" .

Was ist die aktive Schnittstelle?

Während des normalen Betriebs 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 Clients eine Verbindung mit einer beliebigen VIP-Adresse für die Gruppe herstellen. Das heißt, während des normalen Betriebs ist die primäre Schnittstelle die „aktive“ Schnittstelle für die Gruppe.

Ebenso fungieren während des Normalbetriebs alle Schnittstellen mit niedrigerer Priorität für die HA-Gruppe als „Backup“-Schnittstellen. Diese Backup-Schnittstellen werden nicht verwendet, es sei denn, die primäre (derzeit aktive) Schnittstelle ist nicht mehr verfügbar.

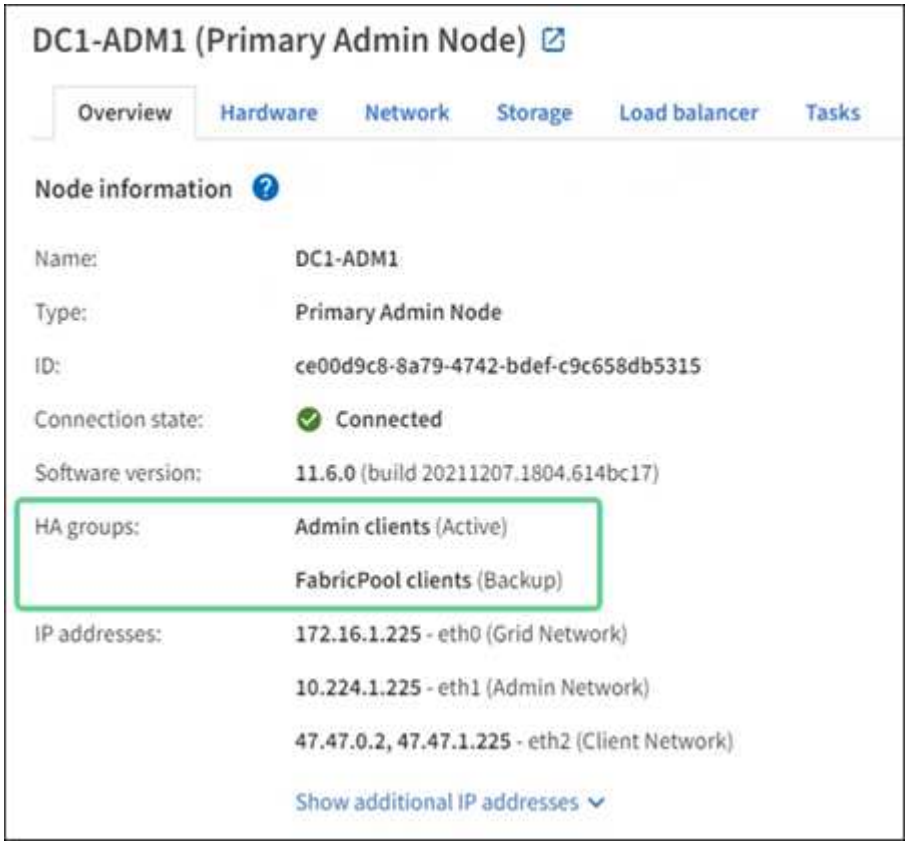
Den aktuellen HA-Gruppenstatus eines Knotens anzeigen

Um zu sehen, ob ein Knoten einer HA-Gruppe zugewiesen ist, und um seinen aktuellen Status zu bestimmen, wählen Sie **NODES** > ***node***.

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 Knotens in der HA-Gruppe:

- **Aktiv**: Die HA-Gruppe wird derzeit auf diesem Knoten gehostet.
- **Backup**: Die HA-Gruppe verwendet diesen Knoten derzeit nicht. Dies ist eine Backup-Schnittstelle.
- **Gestoppt**: Die HA-Gruppe kann auf diesem Knoten nicht gehostet werden, da der Dienst „High Availability“ (Keepalived) manuell gestoppt wurde.
- **Fehler**: Die HA-Gruppe kann aus einem oder mehreren der folgenden Gründe nicht auf diesem Knoten gehostet werden:
  - Der Load Balancer-Dienst (nginx-gw) wird auf dem Knoten nicht ausgeführt.
  - Die eth0- oder VIP-Schnittstelle des Knotens ist ausgefallen.
  - Der Knoten ist ausgefallen.

In diesem Beispiel wurde der primäre Admin-Knoten zu zwei HA-Gruppen hinzugefügt. Dieser Knoten ist derzeit die aktive Schnittstelle für die Gruppe der Admin-Clients und eine Backup-Schnittstelle für die Gruppe der FabricPool -Clients.



Was passiert, wenn die aktive Schnittstelle ausfällt?

Die Schnittstelle, die derzeit die VIP-Adressen hostet, ist die aktive Schnittstelle. Wenn die HA-Gruppe mehr als eine Schnittstelle umfasst und die aktive Schnittstelle ausfällt, werden die VIP-Adressen in der Prioritätsreihenfolge an die erste verfügbare Backup-Schnittstelle verschoben. Wenn diese Schnittstelle ausfällt, werden die VIP-Adressen zur nächsten verfügbaren Backup-Schnittstelle verschoben und so weiter.

Ein Failover kann aus folgenden Gründen ausgelöst werden:

- Der Knoten, auf dem die Schnittstelle konfiguriert ist, fällt aus.
- Der Knoten, auf dem die Schnittstelle konfiguriert ist, verliert für mindestens 2 Minuten die Verbindung zu allen anderen Knoten.

- Die aktive Schnittstelle fällt aus.
- Der Load Balancer-Dienst wird gestoppt.
- Der Hochverfügbarkeitsdienst wird gestoppt.

> Das Failover wird möglicherweise nicht durch Netzwerkfehler außerhalb des Knotens ausgelöst, der die aktive Schnittstelle hostet. Ebenso wird ein Failover nicht durch die Dienste für den Grid Manager oder den Tenant Manager ausgelöst.

Der Failover-Prozess dauert im Allgemeinen nur wenige Sekunden und ist schnell genug, sodass Client-Anwendungen nur geringe Auswirkungen erfahren und sich auf normale Wiederholungsverhalten verlassen können, um den Betrieb fortzusetzen.

Wenn der 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?

Sie können Hochverfügbarkeitsgruppen (HA) verwenden, um hochverfügbare Verbindungen zu StorageGRID für Objektdaten und zur administrativen Verwendung bereitzustellen.

- Eine HA-Gruppe kann hochverfügbare administrative Verbindungen zum Grid Manager oder Tenant Manager bereitstellen.
- Eine HA-Gruppe kann hochverfügbare Datenverbindungen für S3-Clients bereitstellen.
- Eine HA-Gruppe, die nur eine Schnittstelle enthält, ermöglicht Ihnen die Bereitstellung vieler VIP-Adressen und die explizite Festlegung von IPv6-Adressen.

Eine HA-Gruppe kann nur dann eine hohe Verfügbarkeit bieten, wenn alle in der Gruppe enthaltenen Knoten dieselben Dienste bereitstellen. Wenn Sie eine HA-Gruppe erstellen, fügen Sie Schnittstellen von den Knotentypen hinzu, die die von Ihnen benötigten Dienste bereitstellen.

- **Admin-Knoten**: Schließen Sie den Load Balancer-Dienst ein und ermöglichen Sie den Zugriff auf den Grid Manager oder den Tenant Manager.
- **Gateway-Knoten**: Schließen Sie den Load Balancer-Dienst ein.

Zweck der HA-Gruppe	Knoten dieses Typs zur HA-Gruppe hinzufügen
Zugriff auf Grid Manager	• Primärer Admin-Knoten (**Primär**) • Nicht-primäre Admin-Knoten **Hinweis:** Der primäre Admin-Knoten muss die primäre Schnittstelle sein. Einige Wartungsvorgänge können nur vom primären Admin-Knoten aus durchgeführt werden.
Zugriff nur auf den Mandantenmanager	• Primäre oder nicht-primäre Admin-Knoten

Zweck der HA-Gruppe	Knoten dieses Typs zur HA-Gruppe hinzufügen
S3-Clientzugriff – Load Balancer-Dienst	• Admin-Knoten • Gateway-Knoten
S3-Client-Zugriff für"S3 Auswählen"	• Servicegeräte • VMware-basierte Softwareknoten **Hinweis**: HA-Gruppen werden bei der Verwendung von S3 Select empfohlen, sind aber nicht erforderlich.

Einschränkungen bei der Verwendung von HA-Gruppen mit Grid Manager oder Tenant Manager

Wenn ein Grid Manager- oder Tenant Manager-Dienst ausfällt, wird kein HA-Gruppen-Failover ausgelöst.

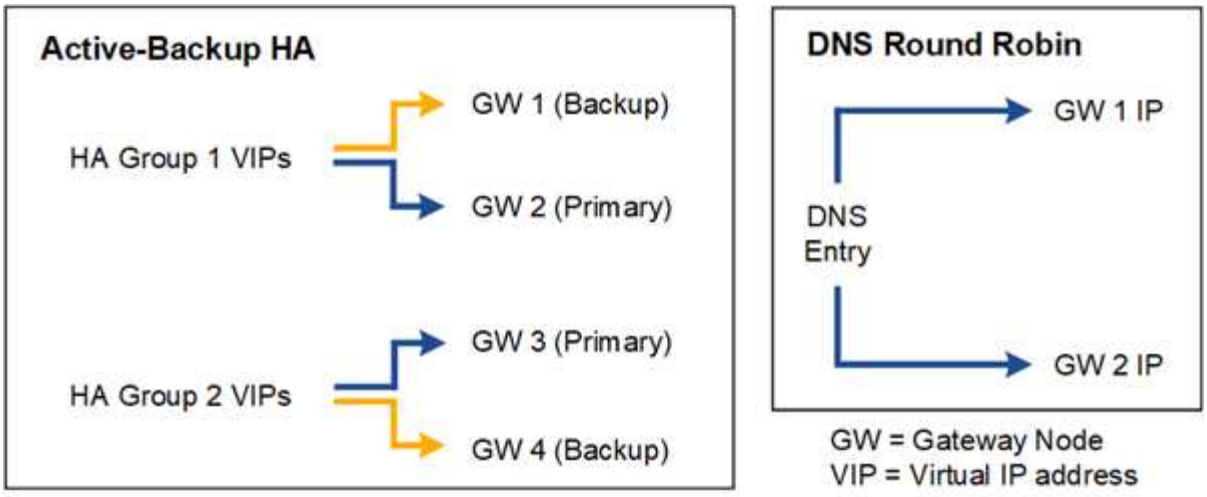
Wenn Sie beim Failover beim Grid Manager oder Tenant Manager angemeldet sind, werden Sie abgemeldet und müssen sich erneut anmelden, um Ihre Aufgabe fortzusetzen.

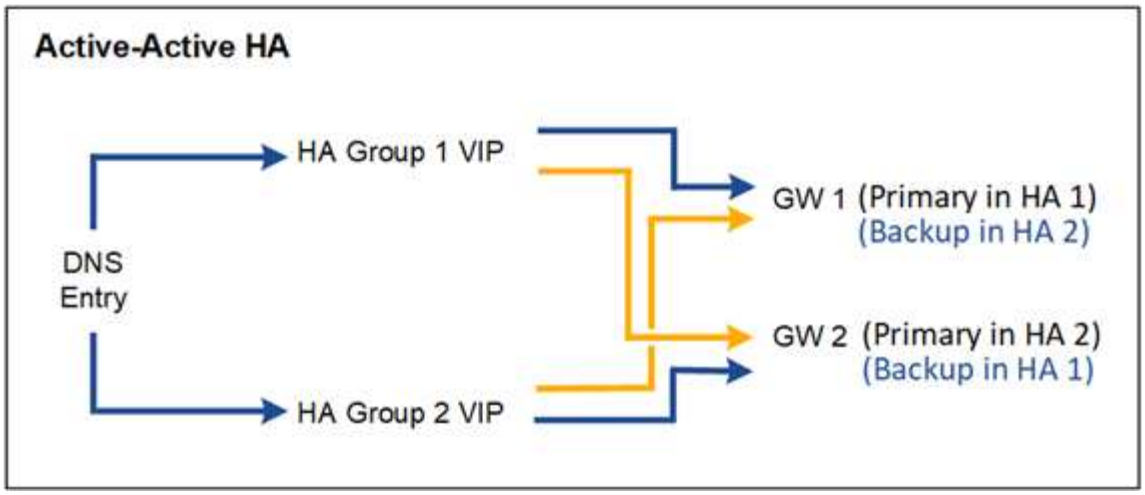
Einige Wartungsverfahren können nicht durchgeführt werden, wenn der primäre Admin-Knoten nicht verfügbar ist. Während des Failovers können Sie den Grid Manager verwenden, um Ihr StorageGRID System zu überwachen.

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 kennzeichnet Blau die primäre Schnittstelle in der HA-Gruppe und Gelb die Backup-Schnittstelle in der HA-Gruppe.





Die Tabelle fasst die Vorteile jeder im Diagramm gezeigten HA-Konfiguration zusammen.

Konfiguration	Vorteile	Nachteile
Active-Backup HA	• Verwaltet von StorageGRID ohne externe Abhängigkeiten. • Schnelles Failover.	• In einer HA-Gruppe ist nur ein Knoten aktiv. Mindestens ein Knoten pro HA-Gruppe ist im Leerlauf.
DNS-Round-Robin	• Erhöhter Gesamtdurchsatz. • Keine untätigen Hosts.	• Langsames Failover, das vom Clientverhalten abhängen kann. • Erfordert die Konfiguration der Hardware außerhalb von StorageGRID. • Benötigt einen vom Kunden durchgeführten Gesundheitscheck.

Konfiguration	Vorteile	Nachteile
Aktiv-Aktiv-HA	• Der Datenverkehr wird auf mehrere HA-Gruppen verteilt. • Hoher Gesamtdurchsatz, der mit der Anzahl der HA-Gruppen skaliert. • Schnelles Failover.	• Komplexer zu konfigurieren. • Erfordert die Konfiguration der Hardware außerhalb von StorageGRID. • Benötigt einen vom Kunden durchgeführten Gesundheitscheck.

Konfigurieren von Hochverfügbarkeitsgruppen

Sie können Hochverfügbarkeitsgruppen (HA) konfigurieren, um einen hochverfügbaren Zugriff auf die Dienste auf Admin-Knoten oder Gateway-Knoten bereitzustellen.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .
- Wenn Sie eine VLAN-Schnittstelle in einer HA-Gruppe verwenden möchten, haben Sie die VLAN-Schnittstelle erstellt. Sehen "Konfigurieren von VLAN-Schnittstellen" .
- Wenn Sie eine Zugriffsschnittstelle für einen Knoten in einer HA-Gruppe verwenden möchten, haben Sie die Schnittstelle erstellt:
  - **Red Hat Enterprise Linux (vor der Installation des Knotens)**:"Erstellen Sie Knotenkonfigurationsdateien"
  - **Ubuntu oder Debian (vor der Installation des Knotens)**:"Erstellen Sie Knotenkonfigurationsdateien"
  - **Linux (nach der Installation des Knotens)**:"Linux: Trunk oder Zugriffsschnittstellen zu einem Knoten hinzufügen"
  - **VMware (nach der Installation des Knotens)**:"VMware: Trunk- oder Zugriffsschnittstellen zu einem Knoten hinzufügen"

Erstellen einer Hochverfügbarkeitsgruppe

Wenn Sie eine Hochverfügbarkeitsgruppe erstellen, wählen Sie eine oder mehrere Schnittstellen aus und organisieren sie nach Priorität. Anschließend weisen Sie der Gruppe eine oder mehrere VIP-Adressen zu.

Eine Schnittstelle muss für einen Gateway-Knoten oder einen Admin-Knoten sein, um in eine HA-Gruppe aufgenommen zu werden. Eine HA-Gruppe kann für jeden Knoten nur eine Schnittstelle verwenden. In anderen HA-Gruppen können jedoch andere Schnittstellen für denselben Knoten verwendet werden.

Zugriff auf den Assistenten

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **Hochverfügbarkeitsgruppen**.
2. Wählen Sie **Erstellen**.

Geben Sie Details für die HA-Gruppe ein

Schritte

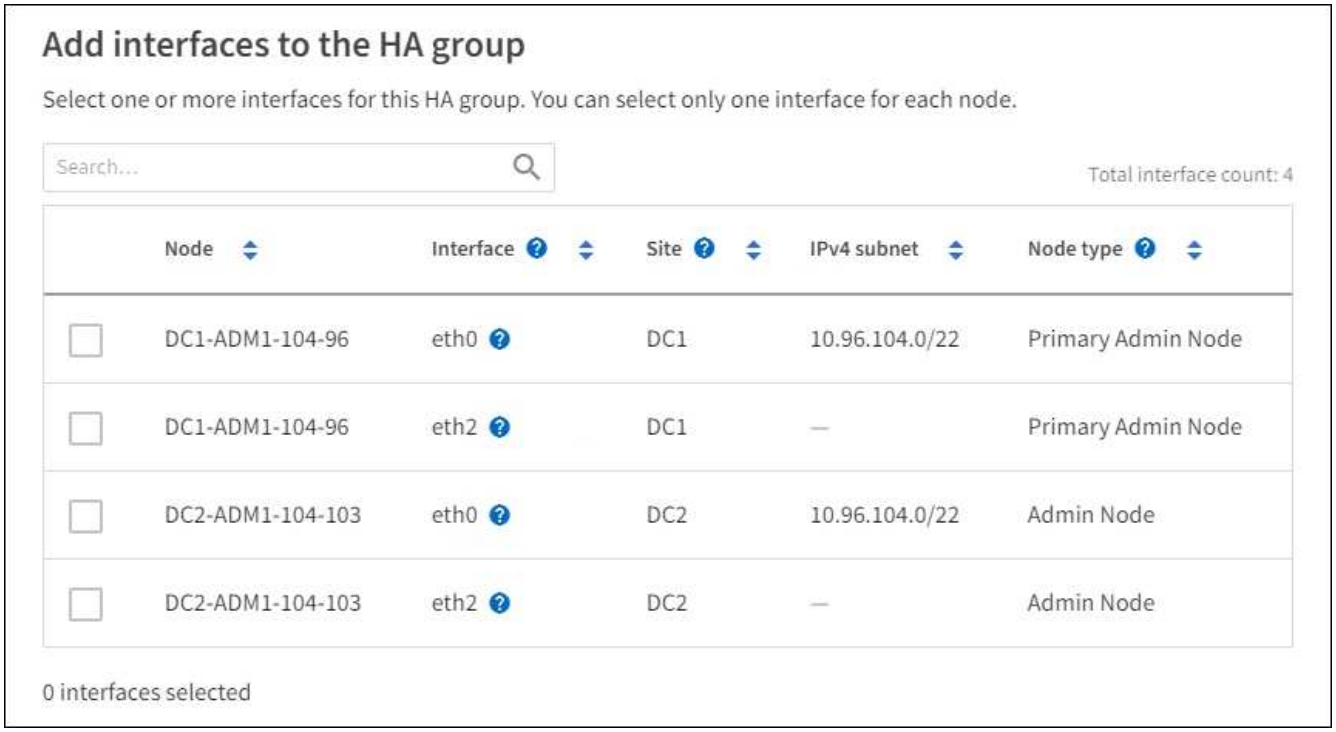
1. Geben Sie einen eindeutigen Namen für die HA-Gruppe an.
2. Geben Sie optional eine Beschreibung für die HA-Gruppe ein.
3. Wählen Sie **Weiter**.

Schnittstellen zur HA-Gruppe hinzufügen

Schritte

1. Wählen Sie eine oder mehrere Schnittstellen aus, die dieser HA-Gruppe hinzugefügt werden sollen.

   Nutzen Sie die Spaltenüberschriften zum Sortieren der Zeilen oder geben Sie einen Suchbegriff ein, um Schnittstellen schneller zu finden.

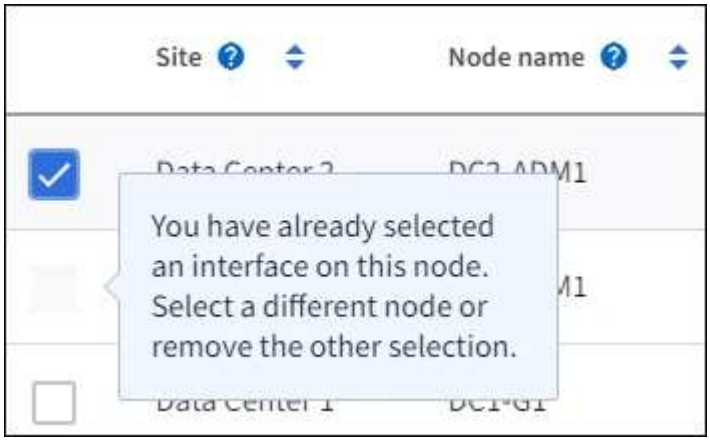


> Warten Sie nach dem Erstellen einer VLAN-Schnittstelle bis zu 5 Minuten, bis die neue Schnittstelle in der Tabelle angezeigt wird.

Richtlinien zur Auswahl von Schnittstellen

- Sie müssen mindestens eine Schnittstelle auswählen.
- Sie können für einen Knoten nur eine Schnittstelle auswählen.
- Wenn die HA-Gruppe zum HA-Schutz von Admin-Node-Diensten dient, zu denen der Grid Manager und der Tenant Manager gehören, wählen Sie nur Schnittstellen auf Admin-Nodes aus.
- Wenn die HA-Gruppe dem HA-Schutz des S3-Client-Datenverkehrs dient, wählen Sie Schnittstellen auf Admin-Knoten, Gateway-Knoten oder beiden aus.
- Wenn Sie Schnittstellen auf verschiedenen Knotentypen auswählen, wird ein Hinweis angezeigt. Bitte beachten Sie, dass bei einem Failover die vom zuvor aktiven Knoten bereitgestellten Dienste auf dem neuen aktiven Knoten möglicherweise nicht verfügbar sind. Beispielsweise kann ein Backup-Gateway-Knoten keinen HA-Schutz für Admin-Knotendienste bieten. Ebenso kann ein Backup-Admin-Knoten nicht alle Wartungsverfahren durchführen, die der primäre Admin-Knoten bereitstellen kann.
- Wenn Sie keine Schnittstelle auswählen können, ist das entsprechende Kontrollkästchen deaktiviert.

Der Tooltip bietet weitere Informationen.



- Sie können keine Schnittstelle auswählen, wenn ihr Subnetzwert oder Gateway mit einer anderen ausgewählten Schnittstelle in Konflikt steht.
- Sie können eine konfigurierte Schnittstelle nicht auswählen, wenn sie keine statische IP-Adresse hat.

2. Wählen Sie **Weiter**.

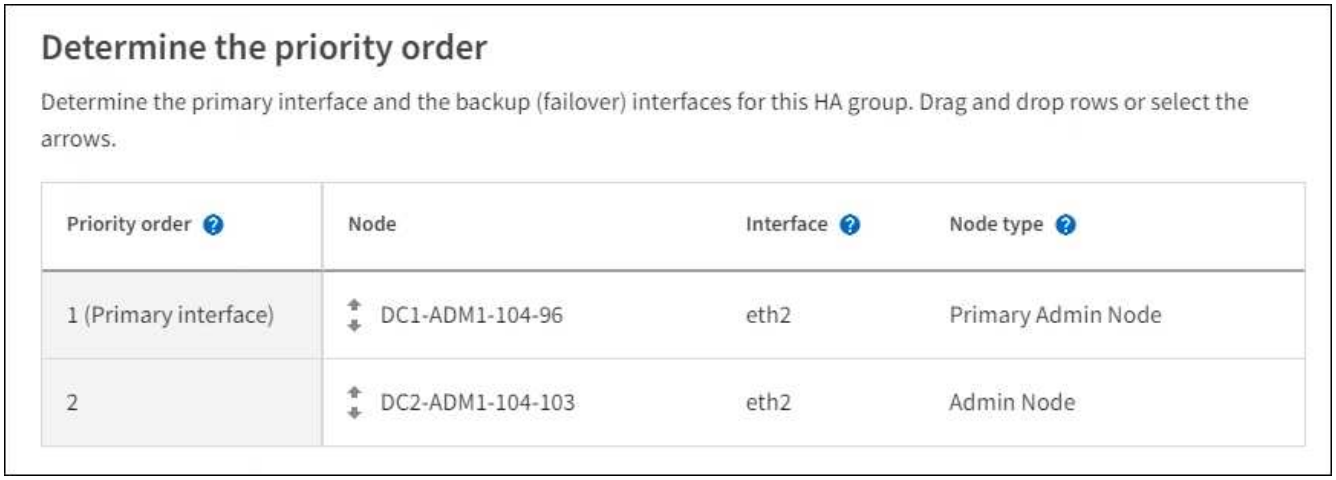
Bestimmen Sie die Prioritätsreihenfolge

Wenn die HA-Gruppe mehr als eine Schnittstelle umfasst, können Sie bestimmen, welche die primäre Schnittstelle und welche die Backup-Schnittstellen (Failover) sind. Wenn die primäre Schnittstelle ausfällt, werden die VIP-Adressen an die verfügbare Schnittstelle mit der höchsten Priorität weitergeleitet. Wenn diese Schnittstelle ausfällt, werden die VIP-Adressen zur nächsten verfügbaren Schnittstelle mit der höchsten Priorität verschoben und so weiter.

Schritte

1. Ziehen Sie Zeilen in der Spalte **Prioritätsreihenfolge**, 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 auf dem primären Admin-Knoten als primäre Schnittstelle auswählen. Einige Wartungsvorgänge können nur vom primären Admin-Knoten aus durchgeführt werden.

2. Wählen Sie **Weiter**.

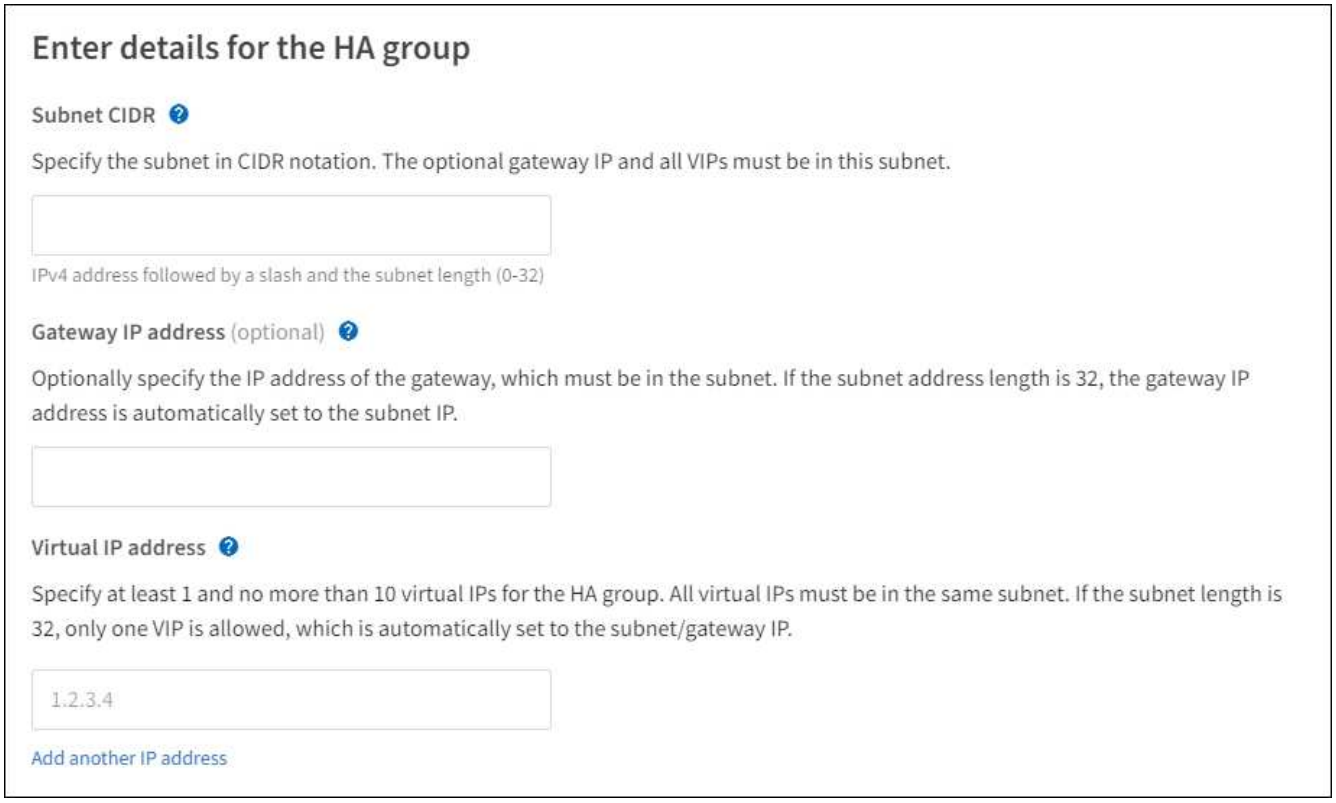
IP-Adressen eingeben

Schritte

1. Geben Sie im Feld **Subnetz-CIDR** das VIP-Subnetz in CIDR-Notation an – eine IPv4-Adresse gefolgt von einem Schrägstrich und der Subnetzlänge (0–32).

   Für die Netzwerkadresse dürfen keine Hostbits gesetzt sein. 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 S3-Verwaltungs- oder Mandantenclients von einem anderen Subnetz aus auf diese VIP-Adressen zugreifen, geben Sie optional die **Gateway-IP-Adresse** ein. Die Gateway-Adresse muss innerhalb des VIP-Subnetzes liegen.

   Client- und Administratorbenutzer verwenden dieses Gateway, um auf die virtuellen IP-Adressen zuzugreifen.

3. Geben Sie mindestens eine und höchstens zehn VIP-Adressen für die aktive Schnittstelle in der HA-Gruppe ein. Alle VIP-Adressen müssen sich innerhalb des VIP-Subnetzes befinden und alle müssen gleichzeitig auf der aktiven Schnittstelle aktiv sein.

   Sie müssen mindestens eine IPv4-Adresse angeben. Optional können Sie zusätzliche IPv4- und IPv6-Adressen angeben.

4. Wählen Sie **HA-Gruppe erstellen** und dann **Fertig stellen**.

   Die HA-Gruppe wird erstellt und Sie können jetzt die konfigurierten virtuellen IP-Adressen verwenden.

Nächste Schritte

Wenn Sie diese HA-Gruppe zum Lastenausgleich verwenden möchten, erstellen Sie einen Lastenausgleichsendpunkt, um den Port und das Netzwerkprotokoll zu bestimmen und alle erforderlichen Zertifikate anzuhängen. Sehen "Konfigurieren von Load Balancer-Endpunkten" .

Bearbeiten einer Hochverfügbarkeitsgruppe

Sie können eine Hochverfügbarkeitsgruppe (HA) 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 Knoten entfernen möchten, der einer ausgewählten Schnittstelle in einem Site- oder Knoten-Außerbetriebnahmeverfahren zugeordnet ist.

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **Hochverfügbarkeitsgruppen**.

   Auf der Seite „Hochverfügbarkeitsgruppen“ werden alle vorhandenen HA-Gruppen angezeigt.

2. Aktivieren Sie das Kontrollkästchen für die HA-Gruppe, die Sie bearbeiten möchten.
3. Führen Sie je nachdem, was Sie aktualisieren möchten, einen der folgenden Schritte aus:
   - Wählen Sie **Aktionen** > **Virtuelle IP-Adresse bearbeiten**, um VIP-Adressen hinzuzufügen oder zu entfernen.
   - Wählen Sie **Aktionen** > **HA-Gruppe bearbeiten**, 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. Aktualisieren Sie optional den Namen oder die Beschreibung der Gruppe.
   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 auf dem primären Admin-Knoten als primäre Schnittstelle auswählen. Einige Wartungsvorgänge können nur vom primären Admin-Knoten aus durchgeführt werden

   c. Ziehen Sie optional Zeilen, um die Prioritätsreihenfolge der primären Schnittstelle und aller Backup-Schnittstellen für diese HA-Gruppe zu ändern.
   d. Aktualisieren Sie optional die virtuellen IP-Adressen.
   e. Wählen Sie **Speichern** und dann **Fertig**.

Entfernen einer Hochverfügbarkeitsgruppe

Sie können eine oder mehrere Hochverfügbarkeitsgruppen (HA) gleichzeitig entfernen.

> Sie können eine HA-Gruppe nicht entfernen, wenn sie an einen Load Balancer-Endpunkt gebunden ist. Um eine HA-Gruppe zu löschen, müssen Sie sie von allen Load Balancer-Endpunkten entfernen, die sie verwenden.

Um Clientunterbrechungen zu vermeiden, aktualisieren Sie alle betroffenen S3-Clientanwendungen, bevor Sie eine HA-Gruppe entfernen. Aktualisieren Sie jeden Client, um eine Verbindung über eine andere IP-Adresse herzustellen, beispielsweise die virtuelle IP-Adresse einer anderen HA-Gruppe oder die IP-Adresse, die während der Installation für eine Schnittstelle konfiguriert wurde.

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **Hochverfügbarkeitsgruppen**.
2. Überprüfen Sie die Spalte **Load Balancer-Endpunkte** für jede HA-Gruppe, die Sie entfernen möchten. Wenn Load Balancer-Endpunkte aufgelistet sind:
   a. Gehen Sie zu **KONFIGURATION** > **Netzwerk** > **Load Balancer-Endpunkte**.
   b. Aktivieren Sie das Kontrollkästchen für den Endpunkt.
   c. Wählen Sie **Aktionen** > **Endpunktbindungsmodus bearbeiten**.
   d. Aktualisieren Sie den Bindungsmodus, um die HA-Gruppe zu entfernen.
   e. Wählen Sie **Änderungen speichern**.
3. Wenn keine Load Balancer-Endpunkte aufgelistet sind, aktivieren Sie das Kontrollkästchen für jede HA-Gruppe, die Sie entfernen möchten.
4. Wählen Sie **Aktionen** > **HA-Gruppe entfernen**.
5. Überprüfen Sie die Nachricht und wählen Sie **HA-Gruppe löschen**, um Ihre Auswahl zu bestätigen.

   Alle von Ihnen ausgewählten HA-Gruppen werden entfernt. Auf der Seite „Hochverfügbarkeitsgruppen“ wird ein grünes Erfolgsbanner angezeigt.

Verwalten des Lastenausgleichs

Überlegungen zum Lastenausgleich

Sie können den Lastenausgleich verwenden, um die Aufnahme- und Abruf-Workloads von S3-Clients zu verarbeiten.

Was ist Lastenausgleich?

Wenn eine Clientanwendung Daten auf einem StorageGRID -System speichert oder abruft, verwendet StorageGRID einen Load Balancer, um die Arbeitslast für Aufnahme und Abruf zu verwalten. Durch Lastenausgleich werden Geschwindigkeit und Verbindungskapazität maximiert, indem die Arbeitslast auf mehrere Speicherknoten verteilt wird.

Der StorageGRID Load Balancer-Dienst ist auf allen Admin-Knoten und allen Gateway-Knoten installiert und bietet Layer 7-Lastausgleich. Es führt die Transport Layer Security (TLS)-Terminierung von Clientanforderungen durch, überprüft die Anforderungen und stellt neue sichere Verbindungen zu den Speicherknoten her.

Der Load Balancer-Dienst auf jedem Knoten arbeitet unabhängig, wenn er Client-Datenverkehr an die Speicherknoten weiterleitet. Durch einen Gewichtungsprozess leitet der Load Balancer-Dienst mehr Anfragen an Speicherknoten mit höherer CPU-Verfügbarkeit weiter.

> Obwohl der StorageGRID Load Balancer-Dienst der empfohlene Lastausgleichsmechanismus ist, möchten Sie möglicherweise stattdessen einen Load Balancer eines Drittanbieters integrieren. Weitere Informationen erhalten Sie von Ihrem NetApp Kundenbetreuer oder unter "TR-4626: StorageGRID Load Balancer von Drittanbietern und globale Load Balancer" .

Wie viele Lastausgleichsknoten benötige ich?

Als allgemeine Best Practice sollte jede Site in Ihrem StorageGRID -System zwei oder mehr Knoten mit dem Load Balancer-Dienst enthalten. Beispielsweise kann eine Site zwei Gateway-Knoten oder sowohl einen Admin-Knoten als auch einen Gateway-Knoten enthalten. Stellen Sie sicher, dass für jeden Lastausgleichsknoten eine angemessene Netzwerk-, Hardware- oder Virtualisierungsinfrastruktur vorhanden ist, unabhängig davon, ob Sie Service-Appliances, Bare-Metal-Knoten oder Knoten auf Basis virtueller Maschinen (VM) verwenden.

Was ist ein Load Balancer-Endpunkt?

Ein Load Balancer-Endpunkt definiert den Port und das Netzwerkprotokoll (HTTPS oder HTTP), die eingehende und ausgehende Client-Anwendungsanforderungen verwenden, um auf die Knoten zuzugreifen, die den Load Balancer-Dienst enthalten. Der Endpunkt definiert auch den Clienttyp (S3), den Bindungsmodus und optional eine Liste zulässiger oder blockierter Mandanten.

Um einen Load Balancer-Endpunkt zu erstellen, wählen Sie entweder **KONFIGURATION** > **Netzwerk** > **Load Balancer-Endpunkte** oder schließen Sie den FabricPool und S3-Setup-Assistenten ab. Anweisungen:

- "Konfigurieren von Load Balancer-Endpunkten"
- "Verwenden Sie den S3-Setup-Assistenten"
- "Verwenden des FabricPool -Setup-Assistenten"

Überlegungen zum Port

Der Port für einen Load Balancer-Endpunkt ist für den ersten Endpunkt, den Sie erstellen, standardmäßig 10433, Sie können jedoch jeden nicht verwendeten externen Port zwischen 1 und 65535 angeben. Wenn Sie Port 80 oder 443 verwenden, verwendet der Endpunkt den Load Balancer-Dienst nur auf Gateway-Knoten. Diese Ports sind auf Admin-Knoten reserviert. Wenn Sie denselben Port für mehr als einen Endpunkt verwenden, müssen Sie für jeden Endpunkt einen anderen Bindungsmodus angeben.

Von anderen Grid-Diensten verwendete Ports sind nicht zulässig. Siehe die"Netzwerkportreferenz" .

Überlegungen zum Netzwerkprotokoll

In den meisten Fällen sollten die Verbindungen zwischen Clientanwendungen und StorageGRID die Transport Layer Security (TLS)-Verschlüsselung verwenden. Die Verbindung zu StorageGRID ohne TLS-Verschlüsselung wird unterstützt, wird jedoch insbesondere in Produktionsumgebungen nicht empfohlen. Wenn Sie das Netzwerkprotokoll für den StorageGRID Load Balancer-Endpunkt auswählen, sollten Sie **HTTPS** auswählen.

Überlegungen zu Load Balancer-Endpunktzertifikaten

Wenn Sie **HTTPS** als Netzwerkprotokoll für den Load Balancer-Endpunkt auswählen, müssen Sie ein

Sicherheitszertifikat angeben. Sie können beim Erstellen des Load Balancer-Endpunkts eine dieser drei Optionen verwenden:

- **Laden Sie ein signiertes Zertifikat hoch (empfohlen)**. Dieses Zertifikat kann entweder von einer öffentlich vertrauenswürdigen oder einer privaten Zertifizierungsstelle (CA) signiert sein. Die beste Vorgehensweise besteht darin, zur Sicherung der Verbindung ein öffentlich vertrauenswürdiges CA-Serverzertifikat zu verwenden. Im Gegensatz zu generierten Zertifikaten können von einer Zertifizierungsstelle signierte Zertifikate unterbrechungsfrei rotiert werden, wodurch Ablaufprobleme vermieden werden können.

  Sie müssen die folgenden Dateien abrufen, bevor Sie den Load Balancer-Endpunkt erstellen:

  - Die benutzerdefinierte Serverzertifikatsdatei.
  - Die private Schlüsseldatei des benutzerdefinierten Serverzertifikats.
  - Optional ein CA-Bündel der Zertifikate von jeder zwischengeschalteten ausstellenden Zertifizierungsstelle.
- **Erstellen Sie ein selbstsigniertes Zertifikat**.
- **Verwenden Sie das globale StorageGRID S3-Zertifikat**. Sie müssen eine benutzerdefinierte Version dieses Zertifikats hochladen oder generieren, bevor Sie es für den Load Balancer-Endpunkt auswählen können. Sehen "Konfigurieren von S3-API-Zertifikaten" .

Welche Werte benötige ich?

Um das Zertifikat zu erstellen, müssen Sie alle Domänennamen und IP-Adressen kennen, die S3-Clientanwendungen für den Zugriff auf den Endpunkt verwenden.

Der **Subject DN**-Eintrag (Distinguished Name) für das Zertifikat muss den vollqualifizierten Domänennamen enthalten, den die Clientanwendung 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 vollqualifizierten Domänennamen aller Admin-Knoten und Gateway-Knoten darzustellen, auf denen der Load Balancer-Dienst ausgeführt wird. Zum Beispiel, `*.storagegrid.example.com` verwendet das Platzhalterzeichen * zur Darstellung `adm1.storagegrid.example.com` Und `gn1.storagegrid.example.com` .

Wenn Sie S3 Virtual Hosted-Style-Anfragen verwenden möchten, muss das Zertifikat auch einen **Alternative Name**-Eintrag für jeden"S3-Endpunktdomänenname" Sie haben alle konfigurierten Namen, einschließlich aller Platzhalternamen. Beispiel:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

> Wenn Sie Platzhalter für Domänennamen verwenden, überprüfen Sie die"Härtungsrichtlinien für Serverzertifikate" .

Außerdem müssen Sie für jeden Namen im Sicherheitszertifikat einen DNS-Eintrag definieren.

Wie verwalte ich ablaufende Zertifikate?

> Wenn das zum Sichern der Verbindung zwischen der S3-Anwendung und StorageGRID verwendete Zertifikat abläuft, verliert die Anwendung möglicherweise vorübergehend den Zugriff auf StorageGRID.

Um Probleme mit dem Ablauf von Zertifikaten zu vermeiden, befolgen Sie diese Best Practices:

- Überwachen Sie sorgfältig alle Warnungen, die vor dem nahenden Ablaufdatum von Zertifikaten warnen, wie etwa die Warnungen „Ablauf des Load Balancer-Endpunktzertifikats“ und „Ablauf des globalen Serverzertifikats für S3-API“.
- Halten Sie die Zertifikatsversionen der StorageGRID und S3-Anwendung immer synchron. Wenn Sie das für einen Load Balancer-Endpunkt verwendete Zertifikat ersetzen oder erneuern, müssen Sie das entsprechende Zertifikat ersetzen oder erneuern, das von der S3-Anwendung verwendet wird.
- Verwenden Sie ein öffentlich signiertes CA-Zertifikat. Wenn Sie ein von einer Zertifizierungsstelle signiertes Zertifikat verwenden, können Sie bald ablaufende Zertifikate unterbrechungsfrei ersetzen.
- Wenn Sie ein selbstsigniertes StorageGRID -Zertifikat generiert haben und dieses Zertifikat bald abläuft, müssen Sie das Zertifikat sowohl in StorageGRID als auch in der S3-Anwendung manuell ersetzen, bevor das vorhandene Zertifikat abläuft.

Überlegungen zum Bindungsmodus

Mit dem Bindungsmodus können Sie steuern, 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 vollqualifizierten Domänennamen (FQDN) verwenden. Clientanwendungen, die eine andere IP-Adresse oder einen anderen FQDN verwenden, können nicht auf den Endpunkt zugreifen.

Sie können einen der folgenden Bindungsmodi angeben:

- **Global** (Standard): Clientanwendungen können über die IP-Adresse eines beliebigen Gateway-Knotens oder Admin-Knotens, die virtuelle IP-Adresse (VIP) einer beliebigen HA-Gruppe in einem beliebigen Netzwerk oder einen entsprechenden FQDN auf den Endpunkt zugreifen. Verwenden Sie diese Einstellung, es sei denn, Sie müssen die Erreichbarkeit eines Endpunkts einschränken.
- **Virtuelle IPs von HA-Gruppen**. Clientanwendungen müssen eine virtuelle IP-Adresse (oder den entsprechenden FQDN) einer HA-Gruppe verwenden.
- **Knotenschnittstellen**. Clients müssen die IP-Adressen (oder entsprechenden FQDNs) ausgewählter Knotenschnittstellen verwenden.
- **Knotentyp**. Je nach ausgewähltem 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 zum Mandantenzugriff

Der Mandantenzugriff ist eine optionale Sicherheitsfunktion, mit der Sie steuern können, welche StorageGRID Mandantenkonten einen Load Balancer-Endpunkt verwenden können, um auf ihre Buckets zuzugreifen. Sie können allen Mandanten den Zugriff auf einen Endpunkt erlauben (Standard) oder Sie können für jeden Endpunkt eine Liste der zulässigen oder blockierten Mandanten angeben.

Sie können diese Funktion verwenden, um eine bessere Sicherheitsisolierung zwischen Mandanten und ihren Endpunkten bereitzustellen. Sie können diese Funktion beispielsweise verwenden, um sicherzustellen, dass streng geheime oder streng geheime Materialien im Besitz eines Mieters für andere Mieter völlig unzugänglich

bleiben.

> Zum Zwecke der Zugriffskontrolle wird der Mandant anhand der in der Client-Anforderung verwendeten Zugriffsschlüssel ermittelt. Wenn im Rahmen der Anforderung keine Zugriffsschlüssel bereitgestellt werden (z. B. bei anonymem Zugriff), wird der Bucket-Eigentümer zur Ermittlung des Mandanten verwendet.

Beispiel für den Mandantenzugriff

Um zu verstehen, wie diese Sicherheitsfunktion funktioniert, betrachten Sie das folgende Beispiel:

1. Sie haben wie folgt zwei Load Balancer-Endpunkte erstellt:
   - **Öffentlicher** Endpunkt: Verwendet Port 10443 und ermöglicht allen Mandanten den Zugriff.
   - **Streng geheim**-Endpunkt: Verwendet Port 10444 und ermöglicht nur dem **Streng geheim**-Mandanten Zugriff. Allen anderen Mandanten ist der Zugriff auf diesen Endpunkt untersagt.
2. Der `top-secret.pdf` befindet sich in einem Eimer, der dem **streng geheimen** Mieter gehört.

Um auf die `top-secret.pdf` kann ein Benutzer im Mandanten **Top secret** eine GET-Anfrage an `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 jedoch ein Benutzer eines anderen Mandanten dieselbe Anfrage an dieselbe URL sendet, erhält er sofort die Meldung „Zugriff verweigert“. Der Zugriff wird verweigert, auch wenn die Anmeldeinformationen und die Signatur gültig sind.

CPU-Verfügbarkeit

Der Load Balancer-Dienst auf jedem Admin-Knoten und Gateway-Knoten arbeitet unabhängig, wenn er S3-Verkehr an die Speicherknoten weiterleitet. Durch einen Gewichtungsprozess leitet der Load Balancer-Dienst mehr Anfragen an Speicherknoten 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 Speicherknoten wird ein minimaler Basisgewichtungswert zugewiesen, auch wenn ein Knoten eine Auslastung von 100 % meldet oder seine Auslastung nicht meldet.

In einigen Fällen sind Informationen zur CPU-Verfügbarkeit auf den Standort beschränkt, an dem sich der Load Balancer-Dienst befindet.

Konfigurieren von Load Balancer-Endpunkten

Load Balancer-Endpunkte bestimmen die Ports und Netzwerkprotokolle, die S3-Clients beim Herstellen einer Verbindung mit dem StorageGRID Load Balancer auf Gateway- und Admin-Knoten verwenden können. Sie können auch Endpunkte verwenden, um auf den Grid Manager, den Tenant Manager oder beide zuzugreifen.

> Swift-Details wurden aus dieser Version der Dokumentationssite entfernt. Sehen "Konfigurieren Sie S3- und Swift-Clientverbindungen" .

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .
- Sie haben die"Überlegungen zum Lastenausgleich" .

- Wenn Sie zuvor einen Port neu zugeordnet haben, den Sie für den Load Balancer-Endpunkt verwenden möchten, müssen Sie"die Port-Neuzuordnung wurde entfernt" .
- Sie haben alle Hochverfügbarkeitsgruppen (HA) erstellt, die Sie verwenden möchten. HA-Gruppen werden empfohlen, sind aber nicht erforderlich. Sehen "Verwalten von Hochverfügbarkeitsgruppen" .
- Wenn der Load Balancer-Endpunkt verwendet wird von"S3-Mandanten für S3 Select" , es dürfen nicht die IP-Adressen oder FQDNs von Bare-Metal-Knoten verwendet werden. Für die für S3 Select verwendeten Load Balancer-Endpunkte sind nur Service-Appliances und VMware-basierte Softwareknoten zulässig.
- Sie haben alle VLAN-Schnittstellen konfiguriert, die Sie verwenden möchten. Sehen "Konfigurieren von VLAN-Schnittstellen" .
- Wenn Sie einen HTTPS-Endpunkt erstellen (empfohlen), verfügen Sie über die Informationen für das Serverzertifikat.

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

  - Zum Hochladen eines Zertifikats benötigen Sie das Serverzertifikat, den privaten Zertifikatsschlüssel und optional ein CA-Paket.
  - Zum Generieren eines Zertifikats benötigen Sie alle Domänennamen und IP-Adressen, die S3-Clients für den Zugriff auf den Endpunkt verwenden. Sie müssen auch den Betreff (Distinguished Name) kennen.
  - Wenn Sie das StorageGRID S3-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 wurde. Sehen "Konfigurieren von S3-API-Zertifikaten" .

Erstellen eines Load Balancer-Endpunkts

Jeder S3-Client-Load-Balancer-Endpunkt gibt einen Port, einen Clienttyp (S3) und ein Netzwerkprotokoll (HTTP oder HTTPS) an. Die Endpunkte des Lastenausgleichsmoduls der Verwaltungsschnittstelle geben einen Port, einen Schnittstellentyp und ein nicht vertrauenswürdiges Clientnetzwerk an.

Zugriff auf den Assistenten

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **Load Balancer-Endpunkte**.
2. Um einen Endpunkt für einen S3- oder Swift-Client zu erstellen, wählen Sie die Registerkarte **S3- oder Swift-Client**.
3. Um einen Endpunkt für den Zugriff auf den Grid Manager, den Tenant Manager oder beide zu erstellen, wählen Sie die Registerkarte **Verwaltungsschnittstelle**.
4. Wählen Sie **Erstellen**.

Geben Sie die Endpunktdetails ein

Schritte

1. Wählen Sie die entsprechenden Anweisungen aus, um Details für den Endpunkttyp einzugeben, den Sie erstellen möchten.

S3- oder Swift-Client

Feld	Beschreibung
Name	Ein beschreibender Name für den Endpunkt, der in der Tabelle auf der Seite „Load Balancer-Endpunkte“ angezeigt wird.
Hafen	Der StorageGRID -Port, den Sie für den Lastenausgleich verwenden möchten. Der Standardwert dieses Felds für den ersten Endpunkt, den Sie erstellen, ist 10433. Sie können jedoch jeden nicht verwendeten externen Port zwischen 1 und 65535 eingeben. Wenn Sie **80** oder **8443** eingeben, wird der Endpunkt nur auf Gateway-Knoten konfiguriert, es sei denn, Sie haben Port 8443 freigegeben. Dann können Sie Port 8443 als S3-Endpunkt verwenden und der Port wird sowohl auf dem Gateway als auch auf den Admin-Knoten konfiguriert.
Client-Typ	Der Typ der Clientanwendung, die diesen Endpunkt verwendet, entweder **S3** oder **Swift**.
Netzwerkprotokoll	Das Netzwerkprotokoll, das Clients beim Herstellen einer Verbindung mit diesem Endpunkt verwenden. • Wählen Sie **HTTPS** für eine 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 Nicht-Produktionsraster.

Verwaltungsschnittstelle

Feld	Beschreibung
Name	Ein beschreibender Name für den Endpunkt, der in der Tabelle auf der Seite „Load Balancer-Endpunkte“ angezeigt wird.
Hafen	Der StorageGRID -Port, den Sie für den Zugriff auf den Grid Manager, den Tenant Manager oder beide verwenden möchten. • Grid-Manager: **8443** • Mietermanager: **9443** • Sowohl Grid Manager als auch Tenant Manager: **443** **Hinweis**: Sie können diese voreingestellten Ports oder andere verfügbare Ports verwenden.
Schnittstellentyp	Wählen Sie das Optionsfeld für die StorageGRID -Schnittstelle aus, auf die Sie über diesen Endpunkt zugreifen.

Feld	Beschreibung
Nicht vertrauenswürdiges Client-Netzwerk	Wählen Sie **Ja**, wenn dieser Endpunkt für nicht vertrauenswürdige Clientnetzwerke zugänglich sein soll. Andernfalls wählen Sie **Nein**. Wenn Sie **Ja** auswählen, ist der Port in allen nicht vertrauenswürdigen Client-Netzwerken geöffnet. **Hinweis**: Sie können einen Port nur so konfigurieren, dass er für nicht vertrauenswürdige Client-Netzwerke geöffnet oder geschlossen ist, wenn Sie den Load Balancer-Endpunkt erstellen.

1. Wählen Sie **Weiter**.

Auswählen eines Bindungsmodus

Schritte

1. Wählen Sie einen Bindungsmodus für den Endpunkt aus, um zu steuern, wie auf den Endpunkt über eine beliebige IP-Adresse oder über bestimmte IP-Adressen und Netzwerkschnittstellen zugegriffen wird.

   Einige Bindungsmodi sind entweder für Client-Endpunkte oder Management-Schnittstellen-Endpunkte verfügbar. Hier sind alle Modi für beide Endpunkttypen aufgelistet.

Modus	Beschreibung
Global (Standard für Client-Endpunkte)	Clients können über die IP-Adresse eines beliebigen Gateway-Knotens oder Admin-Knotens, die virtuelle IP-Adresse (VIP) einer beliebigen HA-Gruppe in einem beliebigen Netzwerk oder einen entsprechenden FQDN auf den Endpunkt zugreifen. Verwenden Sie die Einstellung **Global**, es sei denn, Sie müssen die Erreichbarkeit dieses Endpunkts einschränken.
Virtuelle IPs von HA-Gruppen	Clients müssen eine virtuelle IP-Adresse (oder den entsprechenden FQDN) einer HA-Gruppe verwenden, um auf diesen Endpunkt zuzugreifen. Endpunkte mit diesem Bindungsmodus können alle dieselbe Portnummer verwenden, solange sich die von Ihnen für die Endpunkte ausgewählten HA-Gruppen nicht überschneiden.
Knotenschnittstellen	Clients müssen die IP-Adressen (oder entsprechenden FQDNs) ausgewählter Knotenschnittstellen verwenden, um auf diesen Endpunkt zuzugreifen.
Knotentyp (nur Client-Endpunkte)	Je nach ausgewähltem 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.

Modus	Beschreibung
Alle Admin-Knoten (Standard für Endpunkte der Verwaltungsschnittstelle)	Clients müssen die IP-Adresse (oder den entsprechenden FQDN) eines beliebigen Admin-Knotens verwenden, um auf diesen Endpunkt zuzugreifen.

Wenn mehr als ein Endpunkt denselben Port verwendet, verwendet StorageGRID diese Prioritätsreihenfolge, um zu entscheiden, welcher Endpunkt verwendet werden soll: **Virtuelle IPs von HA-Gruppen** > **Knotenschnittstellen** > **Knotentyp** > **Global**.

Wenn Sie Endpunkte für die Verwaltungsschnittstelle erstellen, sind nur Admin-Knoten zulässig.

2. Wenn Sie **Virtuelle IPs von HA-Gruppen** ausgewählt haben, wählen Sie eine oder mehrere HA-Gruppen aus.

   Wenn Sie Endpunkte der Verwaltungsschnittstelle erstellen, wählen Sie VIPs aus, die nur mit Admin-Knoten verknüpft sind.

3. Wenn Sie **Knotenschnittstellen** ausgewählt haben, wählen Sie eine oder mehrere Knotenschnittstellen für jeden Admin-Knoten oder Gateway-Knoten aus, den Sie diesem Endpunkt zuordnen möchten.
4. Wenn Sie **Knotentyp** ausgewählt haben, wählen Sie entweder „Admin-Knoten“, was sowohl den primären Admin-Knoten als auch alle nicht primären Admin-Knoten umfasst, oder „Gateway-Knoten“.

Steuern des Mandantenzugriffs

> Ein Management-Schnittstellen-Endpunkt kann den Mandantenzugriff nur steuern, wenn der Endpunkt über dieSchnittstellentyp des Tenant Managers .

Schritte

1. Wählen Sie für den Schritt **Mandantenzugriff** 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 verwenden, um auf ihre Buckets zuzugreifen.
Ausgewählte Mieter blockieren	Die ausgewählten Mandantenkonten können diesen Endpunkt nicht verwenden, um auf ihre Buckets zuzugreifen. Alle anderen Mandanten können diesen Endpunkt verwenden.

2. Wenn Sie einen **HTTP**-Endpunkt erstellen, müssen Sie kein Zertifikat anhängen. Wählen Sie **Erstellen** aus, um den neuen Load Balancer-Endpunkt hinzuzufügen. Gehen Sie dann zuNach Abschluss .

Andernfalls wählen Sie **Weiter**, um das Zertifikat anzuhängen.

Zertifikat anhängen

Schritte

1. Wenn Sie einen **HTTPS**-Endpunkt erstellen, wählen Sie den Typ des Sicherheitszertifikats aus, das Sie an den Endpunkt anhängen möchten.

   Das Zertifikat sichert die Verbindungen zwischen S3-Clients und dem Load Balancer-Dienst auf Admin-Knoten oder Gateway-Knoten.

   - **Zertifikat hochladen**. Wählen Sie diese Option, wenn Sie benutzerdefinierte Zertifikate hochladen möchten.
   - **Zertifikat erstellen**. Wählen Sie diese Option, wenn Sie über die zum Generieren eines benutzerdefinierten Zertifikats erforderlichen Werte verfügen.
   - **Verwenden Sie das StorageGRID S3-Zertifikat**. Wählen Sie diese Option, wenn Sie das globale S3-API-Zertifikat verwenden möchten, das auch für direkte Verbindungen zu Speicherknoten verwendet werden kann.

     Sie können diese Option nur auswählen, wenn Sie das standardmäßige S3-API-Zertifikat, das von der Grid-CA signiert ist, durch ein benutzerdefiniertes Zertifikat ersetzt haben, das von einer externen Zertifizierungsstelle signiert ist. Sehen "Konfigurieren von S3-API-Zertifikaten" .

   - **Zertifikat der Verwaltungsschnittstelle verwenden**. Wählen Sie diese Option, wenn Sie das globale Verwaltungsschnittstellenzertifikat verwenden möchten, das auch für direkte Verbindungen zu Admin-Knoten verwendet werden kann.
2. Wenn Sie das StorageGRID S3-Zertifikat nicht verwenden, laden Sie das Zertifikat hoch oder generieren Sie es.

Zertifikat hochladen

a. Wählen Sie **Zertifikat hochladen**.

b. Laden Sie die erforderlichen Serverzertifikatsdateien hoch:

- **Serverzertifikat**: Die benutzerdefinierte Serverzertifikatsdatei in PEM-Kodierung.
- **Privater Zertifikatsschlüssel**: Die benutzerdefinierte private Schlüsseldatei des Serverzertifikats(`.key`).

> Private EC-Schlüssel müssen mindestens 224 Bit lang sein. Private RSA-Schlüssel müssen mindestens 2048 Bit lang sein.

- **CA-Paket**: Eine einzelne optionale Datei, die die Zertifikate jeder zwischengeschalteten ausstellenden Zertifizierungsstelle (CA) enthält. Die Datei sollte alle PEM-codierten CA-Zertifikatsdateien enthalten, die in der Reihenfolge der Zertifikatskette aneinandergereiht sind.

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

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

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

  Beispiel: `storagegrid_certificate.pem`

- Wählen Sie **Zertifikat PEM kopieren** oder **CA-Paket PEM kopieren**, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.

d. Wählen Sie **Erstellen**. + Der Load Balancer-Endpunkt wird erstellt. Das benutzerdefinierte Zertifikat wird für alle nachfolgenden neuen Verbindungen zwischen S3-Clients oder der Verwaltungsschnittstelle und dem Endpunkt verwendet.

Zertifikat generieren

a. Wählen Sie **Zertifikat generieren**.

b. Geben Sie die Zertifikatsinformationen an:

Feld	Beschreibung
Domänenname	Ein oder mehrere vollqualifizierte Domänennamen, die in das Zertifikat aufgenommen werden sollen. Verwenden Sie ein * als Platzhalter, um mehrere Domänennamen darzustellen.
IP	Eine oder mehrere IP-Adressen, die in das Zertifikat aufgenommen werden sollen.

Feld	Beschreibung
Betreff (optional)	X.509-Betreff oder Distinguished Name (DN) des Zertifikatsinhabers. Wenn in dieses Feld kein Wert eingegeben wird, verwendet das generierte Zertifikat den ersten Domänennamen oder die erste IP-Adresse als allgemeinen Namen (CN) des Betreffs.
Gültigkeitstage	Anzahl der Tage nach der Erstellung, bis zu der das Zertifikat abläuft.
Hinzufügen von Schlüsselverwendungserweiterungen	Wenn ausgewählt (Standard und empfohlen), werden dem generierten Zertifikat Schlüsselverwendung und erweiterte Schlüsselverwendungserweiterungen hinzugefügt. Diese Erweiterungen definieren den Zweck des im Zertifikat enthaltenen Schlüssels. **Hinweis**: Lassen Sie dieses Kontrollkästchen aktiviert, es sei denn, Sie haben Verbindungsprobleme mit älteren Clients, wenn die Zertifikate diese Erweiterungen enthalten.

c. Wählen Sie **Generieren**.

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

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

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

   Beispiel: `storagegrid_certificate.pem`

   - Wählen Sie **Zertifikat PEM kopieren**, um den Zertifikatsinhalt zum Einfügen an anderer Stelle zu kopieren.

e. Wählen Sie **Erstellen**.

   Der Load Balancer-Endpunkt wird erstellt. Das benutzerdefinierte Zertifikat wird für alle nachfolgenden neuen Verbindungen zwischen S3-Clients oder der Verwaltungsschnittstelle und diesem Endpunkt verwendet.

Nach Abschluss

Schritte

1. Wenn Sie ein DNS verwenden, stellen Sie sicher, dass das DNS einen Datensatz enthält, um den vollqualifizierten Domänennamen (FQDN) von StorageGRID jeder IP-Adresse zuzuordnen, die Clients zum Herstellen von Verbindungen verwenden.

   Die IP-Adresse, die Sie in den DNS-Eintrag eingeben, hängt davon ab, ob Sie eine HA-Gruppe von Lastausgleichsknoten 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 über die IP-Adresse eines Gateway-Knotens oder Admin-Knotens eine Verbindung zum StorageGRID Load Balancer-Dienst her.

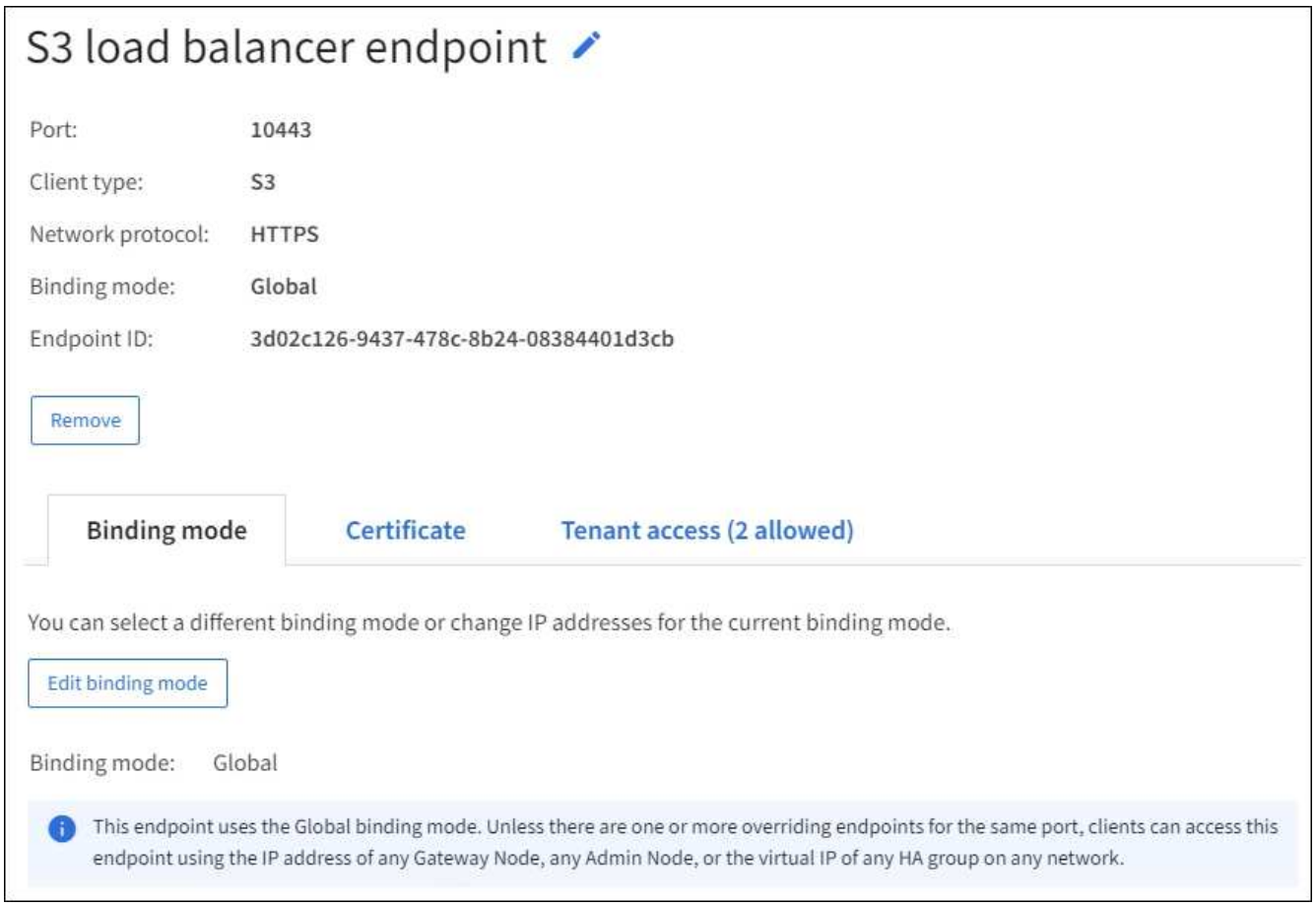
  Sie müssen außerdem sicherstellen, dass der DNS-Eintrag auf alle erforderlichen Endpunktdomänennamen verweist, einschließlich aller Platzhalternamen.

2. Stellen Sie S3-Clients die Informationen zur Verfügung, die zum Herstellen einer Verbindung mit dem Endpunkt erforderlich sind:
   - Portnummer
   - Vollqualifizierter Domänenname oder IP-Adresse
   - Alle erforderlichen Zertifikatsdetails

Anzeigen und Bearbeiten von Load Balancer-Endpunkten

Sie können Details zu vorhandenen Load Balancer-Endpunkten anzeigen, einschließlich der Zertifikatmetadaten für einen gesicherten Endpunkt. Sie können bestimmte Einstellungen für einen Endpunkt ändern.

- Um grundlegende Informationen zu allen Load Balancer-Endpunkten anzuzeigen, sehen Sie sich die Tabellen auf der Seite „Load Balancer-Endpunkte“ an.
- Um alle Details zu einem bestimmten Endpunkt anzuzeigen, einschließlich Zertifikatmetadaten, wählen Sie den Namen des Endpunkts in der Tabelle aus. Die angezeigten Informationen variieren je nach Endpunkttyp und Konfiguration.



- Um einen Endpunkt zu bearbeiten, verwenden Sie das Menü **Aktionen** auf der Seite „Load Balancer-Endpunkte“.

> Wenn Sie beim Bearbeiten des Ports eines Management-Schnittstellenendpunkts den Zugriff auf Grid Manager verlieren, aktualisieren Sie die URL und den Port, um den Zugriff wiederzuerlangen.

> Nach der Bearbeitung eines Endpunkts müssen Sie möglicherweise bis zu 15 Minuten warten, bis Ihre Änderungen auf alle Knoten angewendet werden.

Aufgabe	Menü „Aktionen“	Detailseite
Endpunktnamen bearbeiten	a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie **Aktionen** > **Endpunktnamen bearbeiten**. 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**.
Endpunkt-Port bearbeiten	a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie **Aktionen** > **Endpunktport bearbeiten** c. Geben Sie eine gültige Portnummer ein. d. Wählen Sie **Speichern**.	*n / A*
Endpunktbindungsmodus bearbeiten	a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie **Aktionen** > **Endpunktbindungsmodus bearbeiten**. c. Aktualisieren Sie den Bindungsmodus nach Bedarf. 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 nach Bedarf. d. Wählen Sie **Änderungen speichern**.

Aufgabe	Menü „Aktionen“	Detailseite
Endpunktzertifikat bearbeiten	a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie **Aktionen** > **Endpunktzertifikat bearbeiten**. c. Laden Sie ein neues benutzerdefiniertes Zertifikat hoch oder generieren Sie es, oder beginnen Sie bei Bedarf mit der Verwendung des globalen S3-Zertifikats. d. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Endpunktnamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte **Zertifikat**. c. Wählen Sie **Zertifikat bearbeiten**. d. Laden Sie ein neues benutzerdefiniertes Zertifikat hoch oder generieren Sie es, oder beginnen Sie bei Bedarf mit der Verwendung des globalen S3-Zertifikats. e. Wählen Sie **Änderungen speichern**.
Mandantenzugriff bearbeiten	a. Aktivieren Sie das Kontrollkästchen für den Endpunkt. b. Wählen Sie **Aktionen** > **Mandantenzugriff bearbeiten**. c. Wählen Sie eine andere Zugriffsoption, wählen Sie Mandanten aus der Liste aus oder entfernen Sie sie, oder tun Sie beides. d. Wählen Sie **Änderungen speichern**.	a. Wählen Sie den Endpunktnamen aus, um die Details anzuzeigen. b. Wählen Sie die Registerkarte **Mandantenzugriff**. c. Wählen Sie **Mandantenzugriff bearbeiten**. d. Wählen Sie eine andere Zugriffsoption, wählen Sie Mandanten aus der Liste aus oder entfernen Sie sie, oder tun Sie beides. e. Wählen Sie **Änderungen speichern**.

Entfernen von Load Balancer-Endpunkten

Sie können einen oder mehrere Endpunkte über das Menü **Aktionen** entfernen oder einen einzelnen Endpunkt von der Detailseite entfernen.

> Um Clientunterbrechungen zu vermeiden, aktualisieren Sie alle betroffenen S3-Clientanwendungen, 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. Denken Sie daran, auch alle erforderlichen Zertifikatsinformationen zu aktualisieren.

> Wenn Sie beim Entfernen eines Verwaltungsschnittstellen-Endpunkts den Zugriff auf Grid Manager verlieren, aktualisieren Sie die URL.

- So entfernen Sie einen oder mehrere Endpunkte:
  a. Aktivieren Sie auf der Seite „Load Balancer“ das Kontrollkästchen für jeden Endpunkt, den Sie entfernen möchten.
  b. Wählen Sie **Aktionen** > **Entfernen**.

c. Wählen Sie **OK**.

- So entfernen Sie einen Endpunkt von der Detailseite:
  a. Wählen Sie auf der Seite „Load Balancer“ den Endpunktnamen aus.
  b. Wählen Sie auf der Detailseite **Entfernen** aus.
  c. Wählen Sie **OK**.

Konfigurieren von S3-Endpunktdomänennamen

Um Anfragen im S3-Virtual-Hosting-Stil zu unterstützen, müssen Sie den Grid Manager verwenden, um die Liste der S3-Endpunktdomänennamen zu konfigurieren, mit denen S3-Clients eine Verbindung herstellen.

Die Verwendung einer IP-Adresse als Endpunktdomänenname wird nicht unterstützt. Zukünftige Versionen werden diese Konfiguration verhindern.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .
- Sie haben bestätigt, dass kein Netz-Upgrade im Gange ist.

Nehmen Sie keine Änderungen an der Domänennamenkonfiguration vor, während ein Grid-Upgrade durchgeführt wird.

Informationen zu diesem Vorgang

Damit Clients S3-Endpunktdomänennamen verwenden können, müssen Sie alle folgenden Schritte ausführen:

- Verwenden Sie den Grid Manager, um die S3-Endpunktdomänennamen zum StorageGRID -System hinzuzufügen.
- Stellen Sie sicher, dass die"Zertifikat, das der Client für HTTPS-Verbindungen zu StorageGRID verwendet" ist für alle Domänennamen signiert, die der Client benötigt.

  Wenn der Endpunkt beispielsweise `s3.company.com` müssen Sie sicherstellen, dass das für HTTPS-Verbindungen verwendete Zertifikat die `s3.company.com` Endpunkt und der Platzhalter „Subject Alternative Name“ (SAN) des Endpunkts: `*.s3.company.com` .

- Konfigurieren Sie den vom Client verwendeten DNS-Server. Fügen Sie DNS-Einträge für die IP-Adressen ein, die Clients zum Herstellen von Verbindungen verwenden, und stellen Sie sicher, dass die Einträge auf alle erforderlichen S3-Endpunktdomänennamen verweisen, einschließlich aller Platzhalternamen.

Clients können sich mit StorageGRID über die IP-Adresse eines Gateway-Knotens, eines Admin-Knotens oder eines Storage-Knotens verbinden oder indem sie sich mit der virtuellen IP-Adresse einer Hochverfügbarkeitsgruppe verbinden. Sie sollten verstehen, wie Clientanwendungen eine Verbindung zum Grid herstellen, damit Sie die richtigen IP-Adressen in die DNS-Einträge aufnehmen.

Clients, die HTTPS-Verbindungen (empfohlen) zum Grid verwenden, können eines dieser 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-Endpunktdomänennamen erkennt.
- Clients, die eine Verbindung zu einem Load Balancer-Endpunkt oder direkt zu einem Speicherknoten herstellen, können das globale S3-API-Zertifikat so anpassen, dass alle erforderlichen S3-Endpunktdomänennamen enthalten sind.

> Wenn Sie keine S3-Endpunktdomänennamen hinzufügen und die Liste leer ist, wird die Unterstützung für Anfragen im virtuell gehosteten S3-Stil deaktiviert.

Fügen Sie einen S3-Endpunktdomänennamen hinzu

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **S3-Endpunktdomänennamen**.
2. Geben Sie den Domänennamen in das Feld **Domänenname 1** ein. Wählen Sie **Weiteren Domänennamen hinzufügen**, um weitere Domänennamen hinzuzufügen.
3. Wählen Sie **Speichern**.
4. Stellen Sie sicher, dass die von den Clients verwendeten Serverzertifikate mit den erforderlichen Domänennamen des S3-Endpunkts übereinstimmen.
   - Wenn Clients eine Verbindung zu einem Load Balancer-Endpunkt herstellen, der ein eigenes Zertifikat verwendet,"Aktualisieren Sie das dem Endpunkt zugeordnete Zertifikat" .
   - Wenn Clients eine Verbindung zu einem Load Balancer-Endpunkt herstellen, der das globale S3-API-Zertifikat verwendet, oder direkt zu Storage Nodes,"Aktualisieren Sie das globale S3-API-Zertifikat" .
5. Fügen Sie die erforderlichen DNS-Einträge hinzu, um sicherzustellen, dass Domänennamenanforderungen von Endpunkten aufgelöst werden können.

Ergebnis

Wenn Clients nun den Endpunkt verwenden, `bucket.s3.company.com` , der DNS-Server löst den richtigen Endpunkt auf und das Zertifikat authentifiziert den Endpunkt wie erwartet.

Umbenennen eines S3-Endpunktdomänennamens

Wenn Sie einen von S3-Anwendungen verwendeten Namen ändern, schlagen Anfragen im virtuell gehosteten Stil fehl.

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **S3-Endpunktdomänennamen**.
2. Wählen Sie das Domänennamenfeld 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 eines S3-Endpunktdomänennamens

Wenn Sie einen von S3-Anwendungen verwendeten Namen entfernen, schlagen Anfragen im virtuell gehosteten Stil fehl.

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **S3-Endpunktdomänennamen**.
2. Wählen Sie das Löschsymbol neben dem Domänennamen.
3. Wählen Sie **Ja**, um den Löschvorgang zu bestätigen.

Ähnliche Informationen

- "Verwenden Sie die S3 REST-API"
- "IP-Adressen anzeigen"
- "Konfigurieren von Hochverfügbarkeitsgruppen"

Zusammenfassung: IP-Adressen und Ports für Clientverbindungen

Um Objekte zu speichern oder abzurufen, stellen S3-Clientanwendungen eine Verbindung zum Load Balancer-Dienst her, der auf allen Admin-Knoten und Gateway-Knoten enthalten ist, oder zum Local Distribution Router (LDR)-Dienst, der auf allen Speicherknoten enthalten ist.

Client-Anwendungen können über die IP-Adresse eines Grid-Knotens und die Portnummer des Dienstes auf diesem Knoten eine Verbindung zu StorageGRID herstellen. Optional können Sie Hochverfügbarkeitsgruppen (HA) von Lastausgleichsknoten erstellen, um hochverfügbare Verbindungen bereitzustellen, die virtuelle IP-Adressen (VIP) verwenden. Wenn Sie eine Verbindung zu StorageGRID über einen vollqualifizierten Domänennamen (FQDN) anstelle einer IP- oder VIP-Adresse herstellen möchten, können Sie DNS-Einträge konfigurieren.

Diese Tabelle fasst die verschiedenen Möglichkeiten zusammen, wie Clients eine Verbindung zu StorageGRID herstellen können, sowie die IP-Adressen und Ports, die für die einzelnen Verbindungstypen verwendet werden. Wenn Sie bereits Load Balancer-Endpunkte und Hochverfügbarkeitsgruppen (HA) erstellt haben, lesen SieWo finde ich IP-Adressen? um diese Werte im Grid Manager zu finden.

Wo die Verbindung hergestellt wird	Dienst, mit dem der Client eine Verbindung herstellt	IP-Adresse	Hafen
HA-Gruppe	Lastenausgleich	Virtuelle IP-Adresse einer HA-Gruppe	Dem Load Balancer-Endpunkt zugewiesener Port
Admin-Knoten	Lastenausgleich	IP-Adresse des Admin-Knotens	Dem Load Balancer-Endpunkt zugewiesener Port
Gateway-Knoten	Lastenausgleich	IP-Adresse des Gateway-Knotens	Dem Load Balancer-Endpunkt zugewiesener Port
Speicherknoten	LDR	IP-Adresse des Speicherknotens	Standard-S3-Ports: • HTTPS: 18082 • HTTP: 18084

Beispiel-URLs

Um eine Clientanwendung mit dem Load Balancer-Endpunkt einer HA-Gruppe von Gateway-Knoten zu verbinden, verwenden Sie eine URL mit der folgenden Struktur:

`https://VIP-of-HA-group:LB-endpoint-port`

Wenn beispielsweise die virtuelle IP-Adresse der HA-Gruppe 192.0.2.5 und die Portnummer des Load Balancer-Endpunkts 10443 ist, könnte eine Anwendung die folgende URL verwenden, um eine Verbindung zu StorageGRID herzustellen:

`https://192.0.2.5:10443`

Wo finde ich IP-Adressen?

1. Sign in beim Grid Manager an mit einem"unterstützter Webbrowser" .
2. So finden Sie die IP-Adresse eines Grid-Knotens:
   a. Wählen Sie **NODES**.
   b. Wählen Sie den Admin-Knoten, Gateway-Knoten oder Speicherknoten aus, zu dem Sie eine Verbindung herstellen möchten.
   c. Wählen Sie die Registerkarte **Übersicht**.
   d. Notieren Sie im Abschnitt „Knoteninformationen“ die IP-Adressen für den Knoten.
   e. Wählen Sie **Mehr anzeigen**, um IPv6-Adressen und Schnittstellenzuordnungen anzuzeigen.

      Sie können Verbindungen von Clientanwendungen zu jeder der IP-Adressen in der Liste herstellen:

      - **eth0:** Grid-Netzwerk
      - **eth1:** Admin-Netzwerk (optional)
      - **eth2:** Client-Netzwerk (optional)

      > Wenn Sie einen Admin-Knoten oder einen Gateway-Knoten anzeigen und dieser der aktive Knoten in einer Hochverfügbarkeitsgruppe ist, wird die virtuelle IP-Adresse der HA-Gruppe auf eth2 angezeigt.

3. So finden Sie die virtuelle IP-Adresse einer Hochverfügbarkeitsgruppe:
   a. Wählen Sie **KONFIGURATION** > **Netzwerk** > **Hochverfügbarkeitsgruppen**.
   b. Notieren Sie in der Tabelle die virtuelle IP-Adresse der HA-Gruppe.
4. So finden Sie die Portnummer eines Load Balancer-Endpunkts:
   a. Wählen Sie **KONFIGURATION** > **Netzwerk** > **Load Balancer-Endpunkte**.
   b. Notieren Sie sich die Portnummer für den Endpunkt, den Sie verwenden möchten.

      > Wenn die Portnummer 80 oder 443 ist, wird der Endpunkt nur auf Gateway-Knoten konfiguriert, da diese Ports auf Admin-Knoten reserviert sind. Alle anderen Ports sind sowohl auf Gateway-Knoten als auch auf Admin-Knoten konfiguriert.

   c. Wählen Sie den Namen des Endpunkts aus der Tabelle aus.
   d. Bestätigen Sie, dass der **Clienttyp** (S3) mit der Clientanwendung übereinstimmt, die den Endpunkt

verwenden wird.

Netzwerke und Verbindungen verwalten

Konfigurieren der Netzwerkeinstellungen

Sie können verschiedene Netzwerkeinstellungen vom Grid Manager aus konfigurieren, um den Betrieb Ihres StorageGRID -Systems zu optimieren.

Konfigurieren von VLAN-Schnittstellen

Du kannst"Erstellen Sie virtuelle LAN-Schnittstellen (VLAN)." um den Datenverkehr aus Sicherheits-, Flexibilitäts- und Leistungsgründen zu isolieren und zu partitionieren. Jede VLAN-Schnittstelle ist mit einer oder mehreren übergeordneten Schnittstellen auf Admin-Knoten und Gateway-Knoten verknüpft. Sie können VLAN-Schnittstellen in HA-Gruppen und in Load Balancer-Endpunkten verwenden, um den Client- oder Administratorverkehr nach Anwendung oder Mandant zu trennen.

Richtlinien zur Verkehrsklassifizierung

Sie können"Richtlinien zur Verkehrsklassifizierung" um verschiedene Arten von Netzwerkverkehr zu identifizieren und zu verarbeiten, einschließlich Verkehr im Zusammenhang mit bestimmten Buckets, Mandanten, Client-Subnetzen oder Load Balancer-Endpunkten. Diese Richtlinien können bei der Begrenzung und Überwachung des Datenverkehrs helfen.

Richtlinien für StorageGRID -Netzwerke

Mit dem Grid Manager können Sie StorageGRID -Netzwerke und -Verbindungen konfigurieren und verwalten.

Sehen"Konfigurieren von S3-Clientverbindungen" um zu erfahren, wie Sie S3-Clients verbinden.

Standard StorageGRID -Netzwerke

Standardmäßig unterstützt StorageGRID drei Netzwerkschnittstellen pro Grid-Knoten, sodass Sie die Vernetzung für jeden einzelnen Grid-Knoten entsprechend Ihren Sicherheits- und Zugriffsanforderungen konfigurieren können.

Weitere Informationen zur Netzwerktopologie finden Sie unter"Netzwerkrichtlinien" .

Netznetzwerk

Erforderlich. Das Grid-Netzwerk wird für den gesamten internen StorageGRID Verkehr verwendet. Es bietet Konnektivität zwischen allen Knoten im Grid, über alle Standorte und Subnetze hinweg.

Admin-Netzwerk

Optional. Das Admin-Netzwerk wird normalerweise für die Systemadministration und -wartung verwendet. Es kann auch für den Clientprotokollzugriff verwendet werden. Das Admin-Netzwerk ist normalerweise ein privates Netzwerk und muss nicht zwischen Standorten geroutet werden können.

Kundennetzwerk

Optional. Das Client-Netzwerk ist ein offenes Netzwerk, das normalerweise verwendet wird, um Zugriff auf S3-Client-Anwendungen bereitzustellen, sodass das Grid-Netzwerk isoliert und gesichert werden kann. Das Client-Netzwerk kann mit jedem Subnetz kommunizieren, das über das lokale Gateway erreichbar ist.

Richtlinien

- Jeder StorageGRID Knoten benötigt eine dedizierte Netzwerkschnittstelle, IP-Adresse, Subnetzmaske und ein Gateway für jedes Netzwerk, dem er zugewiesen ist.
- Ein Grid-Knoten kann nicht mehr als eine Schnittstelle in einem Netzwerk haben.
- Es wird ein einzelnes Gateway pro Netzwerk und Grid-Knoten unterstützt, das sich im selben Subnetz wie der Knoten befinden muss. Bei Bedarf können Sie im Gateway ein komplexeres Routing implementieren.
- Auf jedem Knoten wird jedes Netzwerk einer bestimmten Netzwerkschnittstelle zugeordnet.

Netzwerk	Schnittstellenname
Netz	eth0
Administrator (optional)	eth1
Kunde (optional)	eth2

- Wenn der Knoten mit einem StorageGRID -Gerät verbunden ist, werden für jedes Netzwerk bestimmte Ports verwendet. Einzelheiten finden Sie in der Installationsanleitung Ihres Geräts.
- 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 wird erst betriebsbereit, wenn der Grid-Knoten dem Grid beigetreten ist
- Das Admin-Netzwerk kann während der Bereitstellung des Grid-Knotens so konfiguriert werden, dass der Zugriff auf die Installationsbenutzeroberfläche möglich ist, bevor das Grid vollständig installiert ist.

Optionale Schnittstellen

Optional können Sie einem Knoten zusätzliche Schnittstellen hinzufügen. Beispielsweise möchten Sie möglicherweise eine Trunk-Schnittstelle zu einem Admin- oder Gateway-Knoten hinzufügen, sodass Sie"VLAN-Schnittstellen" um den Datenverkehr verschiedener Anwendungen oder Mandanten zu trennen. Oder Sie möchten eine Zugriffsschnittstelle hinzufügen, die Sie in einem"Hochverfügbarkeitsgruppe (HA)" .

Informationen zum Hinzufügen von Trunk- oder Zugriffsschnittstellen finden Sie im Folgenden:

- **VMware (nach der Installation des Knotens)**:"VMware: Trunk- oder Zugriffsschnittstellen zu einem Knoten hinzufügen"
  - **Red Hat Enterprise Linux (vor der Installation des Knotens)**:"Erstellen Sie Knotenkonfigurationsdateien"
  - **Ubuntu oder Debian (vor der Installation des Knotens)**:"Erstellen Sie Knotenkonfigurationsdateien"
  - **RHEL, Ubuntu oder Debian (nach der Installation des Knotens)**:"Linux: Trunk oder Zugriffsschnittstellen zu einem Knoten hinzufügen"

IP-Adressen anzeigen

Sie können die IP-Adresse für jeden Grid-Knoten in Ihrem StorageGRID System anzeigen. Mit dieser IP-Adresse können Sie sich dann über die Befehlszeile beim Grid-Knoten anmelden und verschiedene Wartungsvorgänge durchführen.

Bevor Sie beginnen

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

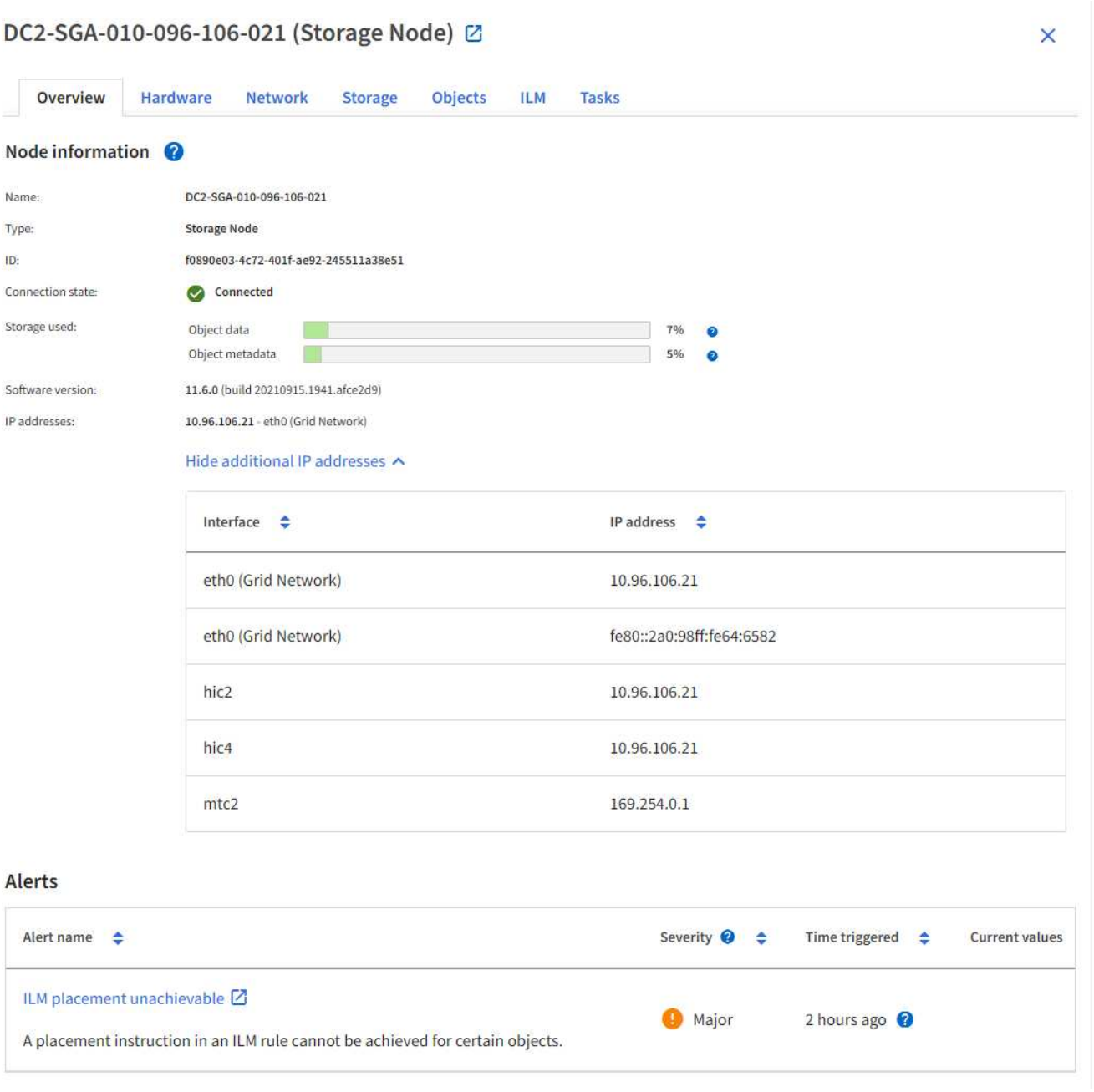
Informationen zu diesem Vorgang

Informationen zum Ändern von IP-Adressen finden Sie unter"Konfigurieren von IP-Adressen" .

Schritte

1. Wählen Sie **KNOTEN** > ***Rasterknoten*** > **Übersicht**.
2. Wählen Sie rechts neben der Überschrift „IP-Adressen“ die Option „Mehr anzeigen“ aus.

   Die IP-Adressen für diesen Grid-Knoten werden in einer Tabelle aufgelistet.



Konfigurieren von VLAN-Schnittstellen

Sie können virtuelle LAN-Schnittstellen (VLAN) auf Admin-Knoten und Gateway-Knoten erstellen und sie in HA-Gruppen und Load Balancer-Endpunkten verwenden, um den Datenverkehr aus Sicherheits-, Flexibilitäts- und Leistungsgründen zu isolieren und zu partitionieren. Die ausgewählten Knoten in der HA-Gruppe können die VLAN-Schnittstellen verwenden, um bis zu 10 virtuelle IP-Adressen gemeinsam zu nutzen, sodass beim Ausfall eines Knotens ein anderer Knoten den Datenverkehr zu und von den virtuellen IP-Adressen übernimmt.

Überlegungen zu VLAN-Schnittstellen

- Sie erstellen eine VLAN-Schnittstelle, indem Sie eine VLAN-ID eingeben und eine übergeordnete

Schnittstelle auf einem oder mehreren Knoten auswählen.

- Eine übergeordnete Schnittstelle muss als Trunk-Schnittstelle am Switch konfiguriert werden.
- Eine übergeordnete Schnittstelle kann das Grid-Netzwerk (eth0), das Client-Netzwerk (eth2) oder eine zusätzliche Trunk-Schnittstelle für die VM oder den Bare-Metal-Host (z. B. ens256) sein.
- Für jede VLAN-Schnittstelle können Sie nur eine übergeordnete Schnittstelle für einen bestimmten Knoten auswählen. Sie können beispielsweise nicht sowohl die Grid-Netzwerkschnittstelle als auch die Client-Netzwerkschnittstelle auf demselben Gateway-Knoten als übergeordnete Schnittstelle für dasselbe VLAN verwenden.
- Wenn die VLAN-Schnittstelle für den Datenverkehr des Admin-Knotens vorgesehen ist, der den Datenverkehr im Zusammenhang mit dem Grid Manager und dem Tenant Manager umfasst, wählen Sie nur Schnittstellen auf den Admin-Knoten aus.
- Wenn die VLAN-Schnittstelle für S3-Client-Datenverkehr vorgesehen ist, wählen Sie Schnittstellen entweder auf Admin-Knoten oder Gateway-Knoten aus.
- Wenn Sie Trunk-Schnittstellen hinzufügen müssen, finden Sie im Folgenden weitere Einzelheiten:
  - **VMware (nach der Installation des Knotens)**:"VMware: Trunk- oder Zugriffsschnittstellen zu einem Knoten hinzufügen"
  - **RHEL (vor der Installation des Knotens)**:"Erstellen Sie Knotenkonfigurationsdateien"
  - **Ubuntu oder Debian (vor der Installation des Knotens)**:"Erstellen Sie Knotenkonfigurationsdateien"
  - **RHEL, Ubuntu oder Debian (nach der Installation des Knotens)**:"Linux: Trunk oder Zugriffsschnittstellen zu einem Knoten hinzufügen"

Erstellen einer VLAN-Schnittstelle

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .
- Im Netzwerk wurde eine Trunk-Schnittstelle konfiguriert und an die VM oder den Linux-Knoten angeschlossen. Sie kennen den Namen der Trunk-Schnittstelle.
- Sie kennen die ID des VLAN, das Sie konfigurieren.

Informationen zu diesem Vorgang

Ihr Netzwerkadministrator hat möglicherweise eine oder mehrere Trunk-Schnittstellen und ein oder mehrere VLANs konfiguriert, um den Client- oder Administratorverkehr verschiedener Anwendungen oder Mandanten zu trennen. Jedes VLAN wird durch eine numerische ID oder ein Tag identifiziert. Beispielsweise könnte Ihr Netzwerk VLAN 100 für FabricPool -Verkehr und VLAN 200 für eine Archivierungsanwendung verwenden.

Mit dem Grid Manager können Sie VLAN-Schnittstellen 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 übergeordnete Schnittstellen (Trunk) auf einem oder mehreren Knoten aus.

Zugriff auf den Assistenten

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **VLAN-Schnittstellen**.
2. Wählen Sie **Erstellen**.

Geben Sie Details für die VLAN-Schnittstellen ein

Schritte

1. Geben Sie die ID des VLAN in Ihrem Netzwerk an. Sie können einen beliebigen Wert zwischen 1 und 4094 eingeben.

   VLAN-IDs müssen nicht eindeutig sein. Sie können beispielsweise die VLAN-ID 200 für den Administratorverkehr an einem Standort und dieselbe VLAN-ID für den Clientverkehr an einem anderen Standort verwenden. Sie können an jedem Standort separate VLAN-Schnittstellen mit unterschiedlichen Sätzen übergeordneter Schnittstellen erstellen. Allerdings können zwei VLAN-Schnittstellen mit derselben ID nicht dieselbe Schnittstelle auf einem Knoten gemeinsam nutzen. Wenn Sie eine ID angeben, die bereits verwendet wurde, erscheint eine Meldung.

2. Geben Sie optional eine kurze Beschreibung für die VLAN-Schnittstelle ein.
3. Wählen Sie **Weiter**.

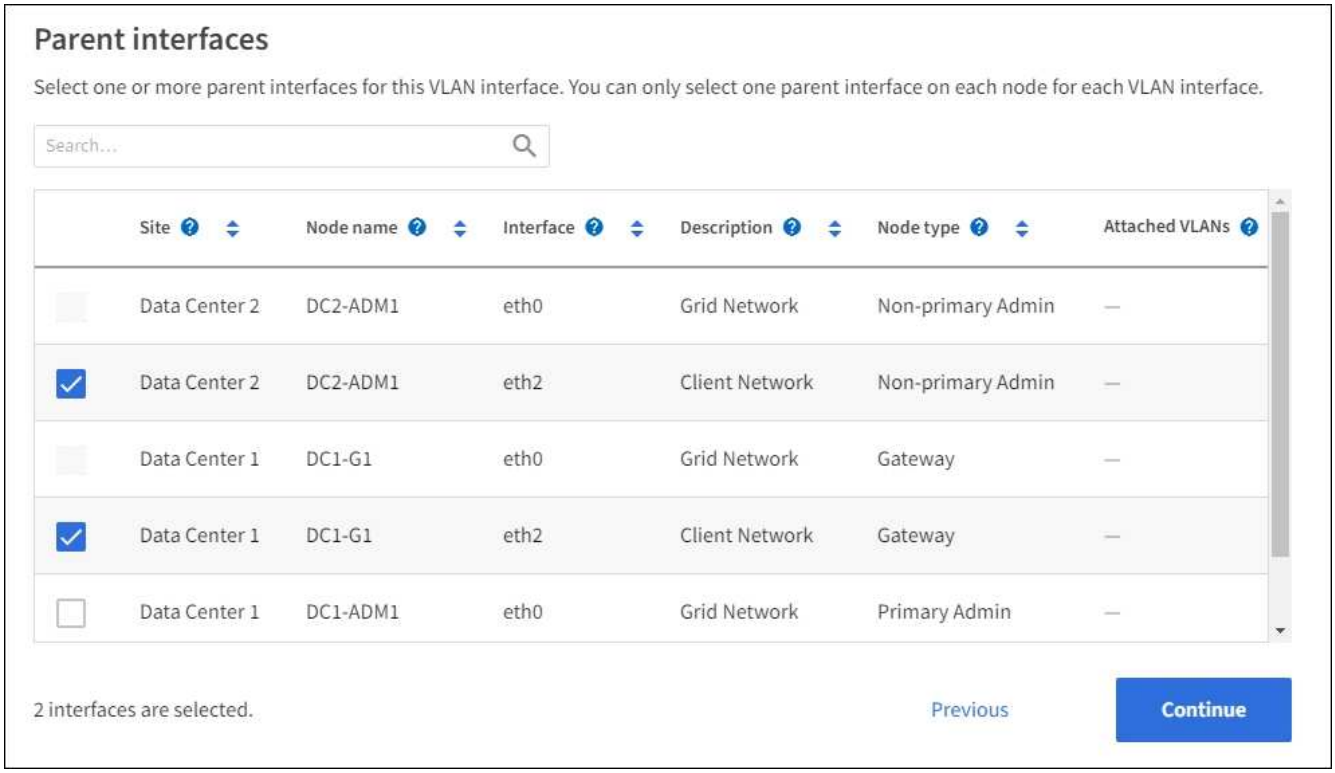
Übergeordnete Schnittstellen auswählen

Die Tabelle listet die verfügbaren Schnittstellen für alle Admin-Knoten und Gateway-Knoten an jedem Standort in Ihrem Raster auf. Admin-Netzwerkschnittstellen (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 angehängt werden soll.

   Beispielsweise möchten Sie möglicherweise ein VLAN an die Client-Netzwerkschnittstelle (eth2) für einen Gateway-Knoten und einen Admin-Knoten anhängen.



2. Wählen Sie **Weiter**.

Bestätigen Sie die Einstellungen

Schritte

1. Überprüfen Sie die Konfiguration und nehmen Sie gegebenenfalls Änderungen vor.
   - Wenn Sie die VLAN-ID oder -Beschreibung ändern müssen, wählen Sie oben auf der Seite **VLAN-Details eingeben** aus.
   - Wenn Sie eine übergeordnete Schnittstelle ändern müssen, wählen Sie oben auf der Seite **Übergeordnete Schnittstellen auswählen** oder wählen Sie **Zurück**.
   - Wenn Sie eine übergeordnete Schnittstelle entfernen möchten, wählen Sie den Papierkorb .
2. Wählen Sie **Speichern**.
3. Warten Sie bis zu 5 Minuten, bis die neue Schnittstelle als Auswahl auf der Seite „Hochverfügbarkeitsgruppen“ angezeigt und in der Tabelle **Netzwerkschnittstellen** für den Knoten aufgeführt wird (**KNOTEN** > ***übergeordneter Schnittstellenknoten*** > **Netzwerk**).

Bearbeiten einer 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.

Beispielsweise möchten Sie möglicherweise eine übergeordnete Schnittstelle aus einer VLAN-Schnittstelle entfernen, wenn Sie den zugehörigen Knoten außer Betrieb nehmen möchten.

Beachten Sie Folgendes:

- Sie können eine VLAN-ID nicht ändern, wenn die VLAN-Schnittstelle in einer HA-Gruppe verwendet wird.
- Sie können eine übergeordnete Schnittstelle nicht entfernen, wenn diese übergeordnete Schnittstelle in einer HA-Gruppe verwendet wird.

  Angenommen, VLAN 200 ist an übergeordnete Schnittstellen auf Knoten A und B angeschlossen. Wenn eine HA-Gruppe die VLAN 200-Schnittstelle für Knoten A und die eth2-Schnittstelle für Knoten B verwendet, können Sie die nicht verwendete übergeordnete Schnittstelle für Knoten B entfernen, die verwendete übergeordnete Schnittstelle für Knoten A jedoch nicht.

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**.
3. Aktualisieren Sie optional die VLAN-ID oder die Beschreibung. Wählen Sie dann **Weiter**.

   Sie können eine VLAN-ID nicht 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 dann **Weiter**.
5. Überprüfen Sie die Konfiguration und nehmen Sie gegebenenfalls Änderungen vor.
6. Wählen Sie **Speichern**.

Entfernen einer 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 Störungen im Client-Datenverkehr zu vermeiden, sollten Sie eine der folgenden Maßnahmen ergreifen:

- Fügen Sie der HA-Gruppe eine neue VLAN-Schnittstelle 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, an das Ende der Prioritätenliste. Warten Sie, bis die Kommunikation auf der neuen primären Schnittstelle hergestellt ist, und entfernen Sie dann die alte Schnittstelle aus der HA-Gruppe. Löschen Sie abschließend 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**.
3. Wählen Sie **Ja**, um Ihre Auswahl zu bestätigen.

   Alle von Ihnen ausgewählten VLAN-Schnittstellen werden entfernt. Auf der Seite „VLAN-Schnittstellen“ wird ein grünes Erfolgsbanner angezeigt.

Verwalten von Richtlinien zur Datenverkehrsklassifizierung

Was sind Verkehrsklassifizierungsrichtlinien?

Mithilfe von Richtlinien zur Verkehrsklassifizierung können Sie verschiedene Arten von Netzwerkverkehr identifizieren und überwachen. Diese Richtlinien können bei der Verkehrsbegrenzung und -überwachung helfen, um Ihre Quality-of-Service-Angebote (QoS) zu verbessern.

Richtlinien zur Verkehrsklassifizierung werden auf Endpunkte des StorageGRID Load Balancer-Dienstes für Gateway-Knoten und Admin-Knoten angewendet. Um Richtlinien zur Verkehrsklassifizierung zu erstellen, müssen Sie bereits Load Balancer-Endpunkte erstellt haben.

Übereinstimmungsregeln

Jede Datenverkehrsklassifizierungsrichtlinie enthält eine oder mehrere Übereinstimmungsregeln zur Identifizierung des Netzwerkverkehrs, der mit einer oder mehreren der folgenden Entitäten in Zusammenhang steht:

- Eimer
- Subnetz
- Mieter
- Load Balancer-Endpunkte

StorageGRID überwacht den Datenverkehr, der einer beliebigen Regel innerhalb der Richtlinie entspricht, entsprechend den Zielen der Regel. Jeglicher Datenverkehr, der einer Regel einer Richtlinie entspricht, wird von dieser Richtlinie behandelt. Umgekehrt können Sie Regeln festlegen, die auf den gesamten Datenverkehr mit Ausnahme einer bestimmten Entität angewendet werden.

Verkehrsbeschränkung

Optional können Sie einer Richtlinie die folgenden Limittypen hinzufügen:

- Gesamtbandbreite
- Bandbreite pro Anfrage
- Gleichzeitige Anfragen
- Anfragerate

Grenzwerte werden pro Load Balancer erzwungen. Wenn der Datenverkehr gleichzeitig auf mehrere Load Balancer verteilt wird, beträgt die maximale Gesamtrate ein Vielfaches der von Ihnen angegebenen Ratenbegrenzungen.

> Sie können Richtlinien erstellen, um die Gesamtbandbreite oder die Bandbreite pro Anfrage zu begrenzen. StorageGRID kann jedoch nicht beide Bandbreitenarten gleichzeitig begrenzen. Die aggregierten Bandbreitenbeschränkungen können bei nicht beschränktem Datenverkehr zusätzliche geringfügige Auswirkungen auf die Leistung haben.

Bei aggregierten oder pro Anfrage geltenden Bandbreitenbeschränkungen werden die Anfragen mit der von Ihnen festgelegten Rate ein- oder ausgehend gestreamt. StorageGRID kann nur eine Geschwindigkeit erzwingen, daher wird die spezifischste Richtlinienübereinstimmung nach Matcher-Typ erzwungen. Die von der Anfrage verbrauchte Bandbreite wird nicht auf andere, weniger spezifische Übereinstimmungsrichtlinien angerechnet, die Richtlinien zur aggregierten Bandbreitenbegrenzung enthalten. Bei allen anderen Grenzwerttypen werden Clientanforderungen um 250 Millisekunden verzögert und erhalten eine 503 Slow Down-Antwort für Anforderungen, die einen entsprechenden Richtliniengrenzwert überschreiten.

Im Grid Manager können Sie Verkehrsdiagramme anzeigen und überprüfen, ob die Richtlinien die von Ihnen erwarteten Verkehrsbeschränkungen durchsetzen.

Verwenden Sie Verkehrsklassifizierungsrichtlinien mit SLAs

Sie können Richtlinien zur Verkehrsklassifizierung in Verbindung mit Kapazitätsgrenzen und Datenschutz verwenden, um Service-Level-Agreements (SLAs) durchzusetzen, die Einzelheiten zu Kapazität, Datenschutz und Leistung enthalten.

Das folgende Beispiel zeigt drei Ebenen eines SLA. Sie können Richtlinien zur Verkehrsklassifizierung erstellen, um die Leistungsziele jeder SLA-Stufe zu erreichen.

Service-Level-Stufe	Kapazität	Datensicherung	Maximal zulässige Leistung	Kosten
Gold	1 PB Speicher zulässig	3-Kopien-ILM-Regel	25.000 Anfragen/Sek. 5 GB/s (40 Gbit/s) Bandbreite	$$$ pro Monat

Service-Level-Stufe	Kapazität	Datensicherung	Maximal zulässige Leistung	Kosten
Silber	250 TB Speicher erlaubt	2 ILM-Kopienregel	10.000 Anfragen/Sek. 1,25 GB/s (10 Gbit/s) Bandbreite	$$ pro Monat
Bronze	100 TB Speicher erlaubt	2 ILM-Kopienregel	5.000 Anfragen/Sek. 1 GB/s (8 Gbit/s) Bandbreite	$ pro Monat

Erstellen von Richtlinien zur Verkehrsklassifizierung

Sie können Richtlinien zur Verkehrsklassifizierung erstellen, wenn Sie den Netzwerkverkehr überwachen und optional nach Bucket, Bucket-Regex, CIDR, Load Balancer-Endpunkt oder Mandant begrenzen möchten. Optional können Sie Grenzwerte für eine Richtlinie basierend auf der Bandbreite, der Anzahl gleichzeitiger Anforderungen oder der Anforderungsrate festlegen.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .
- Sie haben alle Load Balancer-Endpunkte erstellt, die Sie zuordnen möchten.
- Sie haben alle Mieter erstellt, die Sie zuordnen möchten.

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **Verkehrsklassifizierung**.
2. Wählen Sie **Erstellen**.
3. Geben Sie einen Namen und eine Beschreibung (optional) für die Richtlinie ein und wählen Sie **Weiter**.

   Beschreiben Sie beispielsweise, worauf sich diese Verkehrsklassifizierungsrichtlinie bezieht und was sie einschränkt.

4. Wählen Sie **Regel hinzufügen** und geben Sie die folgenden Details an, um eine oder mehrere passende Regeln für die Richtlinie zu erstellen. Jede von Ihnen erstellte Richtlinie sollte mindestens eine passende Regel haben. Wählen Sie **Weiter**.

Feld	Beschreibung
Typ	Wählen Sie die Verkehrstypen aus, auf die die Übereinstimmungsregel angewendet wird. Verkehrstypen sind Bucket, Bucket-Regex, CIDR, Load Balancer-Endpunkt und Mandant.

Feld	Beschreibung
Übereinstimmungswert	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 zum Abgleichen einer Reihe von Bucket-Namen verwendet werden. Der reguläre Ausdruck ist nicht verankert. Verwenden Sie den ^-Anker für die Übereinstimmung am Anfang des Bucket-Namens und den $-Anker für die Übereinstimmung am Ende des Namens. Die Übereinstimmung mit regulären Ausdrücken unterstützt eine Teilmenge der PCRE-Syntax (Perl-kompatible reguläre Ausdrücke). • CIDR: Geben Sie ein oder mehrere IPv4-Subnetze in CIDR-Notation ein, die dem gewünschten Subnetz entsprechen. • Load Balancer-Endpunkt: Wählen Sie einen Endpunktnamen aus. Dies sind die Load Balancer-Endpunkte, die Sie auf der"Konfigurieren von Load Balancer-Endpunkten" . • Mandant: Für die Mandantenzuordnung wird die Zugriffsschlüssel-ID verwendet. Wenn die Anforderung keine Zugriffsschlüssel-ID enthält (z. B. anonymer Zugriff), wird der Besitz des Buckets, auf den zugegriffen wird, zur Bestimmung des Mandanten verwendet.
Inverse Übereinstimmung	Wenn Sie den gesamten Netzwerkverkehr abgleichen möchten, *außer* Verkehr, der mit dem soeben definierten Typ und Übereinstimmungswert übereinstimmt, aktivieren Sie das Kontrollkästchen **Inverse Übereinstimmung**. Andernfalls lassen Sie das Kontrollkästchen deaktiviert. Wenn Sie beispielsweise möchten, dass diese Richtlinie für alle Load Balancer-Endpunkte außer einem gilt, geben Sie den auszuschließenden Load Balancer-Endpunkt an und wählen Sie **Inverse Übereinstimmung** aus. Achten Sie bei einer Richtlinie mit mehreren Matchern, von denen mindestens einer ein inverser Matcher ist, darauf, keine Richtlinie zu erstellen, die allen Anforderungen entspricht.

5. Wählen Sie optional **Limit hinzufügen** und wählen Sie die folgenden Details aus, um ein oder mehrere Limits hinzuzufügen, um den Netzwerkverkehr zu steuern, der einer Regel entspricht.

> StorageGRID sammelt Metriken, auch wenn Sie keine Limits hinzufügen, sodass Sie Verkehrstrends verstehen können.

Feld	Beschreibung
Typ	Die Art der Begrenzung, die Sie auf den Netzwerkverkehr anwenden möchten, der der Regel entspricht. Sie können beispielsweise die Bandbreite oder die Anforderungsrate begrenzen. **Hinweis**: Sie können Richtlinien erstellen, um die Gesamtbandbreite oder die Bandbreite pro Anfrage zu begrenzen. StorageGRID kann jedoch nicht beide Bandbreitenarten gleichzeitig begrenzen. Wenn die Gesamtbandbreite verwendet wird, steht die Bandbreite pro Anforderung nicht zur Verfügung. Umgekehrt steht bei Verwendung der Bandbreite pro Anfrage keine Gesamtbandbreite zur Verfügung. Die aggregierten Bandbreitenbeschränkungen können bei nicht beschränktem Datenverkehr zusätzliche geringfügige Auswirkungen auf die Leistung haben. Für Bandbreitenbeschränkungen wendet StorageGRID die Richtlinie an, die am besten zum festgelegten Beschränkungstyp passt. Wenn Sie beispielsweise eine Richtlinie haben, die den Datenverkehr nur in eine Richtung beschränkt, ist der Datenverkehr in die entgegengesetzte Richtung unbegrenzt, selbst wenn Datenverkehr vorhanden ist, der zusätzlichen Richtlinien mit Bandbreitenbeschränkungen entspricht. StorageGRID implementiert die „besten“ Übereinstimmungen für Bandbreitenbeschränkungen in der folgenden Reihenfolge: • Genaue IP-Adresse (/32-Maske) • Genauer Bucket-Name • Bucket-Regex • Mieter • Endpunkt • Nicht exakte CIDR-Übereinstimmungen (nicht /32) • Inverse Übereinstimmungen
Gilt für:	Ob diese Begrenzung für Leseanforderungen (GET oder HEAD) oder Schreibanforderungen (PUT, POST oder DELETE) des Clients gilt.
Wert	Der Wert, auf den der Netzwerkverkehr basierend auf der von Ihnen ausgewählten Einheit begrenzt wird. Geben Sie beispielsweise 10 ein und wählen Sie MiB/s aus, um zu verhindern, dass der dieser Regel entsprechende Netzwerkverkehr 10 MiB/s überschreitet. **Hinweis**: Je nach Einheiteneinstellung sind die verfügbaren Einheiten entweder binär (z. B. GiB) oder dezimal (z. B. GB). Um die Einheiteneinstellung zu ändern, wählen Sie das Benutzer-Dropdown-Menü oben rechts im Grid Manager und dann **Benutzereinstellungen**.
Einheit	Die Einheit, die den von Ihnen eingegebenen Wert beschreibt.

Wenn Sie beispielsweise ein Bandbreitenlimit von 40 GB/s für eine SLA-Stufe erstellen möchten, erstellen Sie zwei aggregierte Bandbreitenlimits: GET/HEAD mit 40 GB/s und PUT/POST/DELETE mit 40 GB/s.

6. Wählen Sie **Weiter**.
7. Lesen und überprüfen Sie die Richtlinie zur Verkehrsklassifizierung. Verwenden Sie die Schaltfläche **Zurück**, um zurückzugehen und die gewünschten Änderungen vorzunehmen. Wenn Sie mit der Richtlinie zufrieden sind, wählen Sie **Speichern und fortfahren**.

   Der S3-Client-Verkehr wird jetzt gemäß der Verkehrsklassifizierungsrichtlinie behandelt.

Nach Abschluss

"Anzeigen von Netzwerkverkehrsmetriken"um zu überprüfen, ob die Polizei die von Ihnen erwarteten Verkehrsbeschränkungen durchsetzt.

Bearbeiten der Datenverkehrsklassifizierungsrichtlinie

Sie können eine Datenverkehrsklassifizierungsrichtlinie bearbeiten, um ihren Namen oder ihre Beschreibung zu ändern oder um Regeln oder Beschränkungen für die Richtlinie zu erstellen, zu bearbeiten oder zu löschen.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **Verkehrsklassifizierung**.

   Die Seite „Richtlinien zur Datenverkehrsklassifizierung“ wird angezeigt und die vorhandenen Richtlinien werden in einer Tabelle aufgelistet.

2. Bearbeiten Sie die Richtlinie über das Menü „Aktionen“ oder die Detailseite. Sehen"Erstellen Sie Richtlinien zur Verkehrsklassifizierung" für was eingegeben werden soll.

   Menü „Aktionen“

   a. Aktivieren Sie das Kontrollkästchen für die Richtlinie.

   b. Wählen Sie **Aktionen** > **Bearbeiten**.

   Detailseite

   a. Wählen Sie den Richtliniennamen aus.

   b. Wählen Sie die Schaltfläche **Bearbeiten** neben dem Richtliniennamen.

3. Bearbeiten Sie im Schritt „Richtliniennamen eingeben“ optional den Richtliniennamen oder die Beschreibung und wählen Sie **Weiter** aus.
4. Fügen Sie im Schritt „Übereinstimmungsregeln hinzufügen“ optional eine Regel hinzu oder bearbeiten Sie den **Typ** und den **Übereinstimmungswert** der vorhandenen Regel und wählen Sie **Weiter** aus.
5. Fügen Sie im Schritt „Grenzen festlegen“ optional eine Grenze hinzu, bearbeiten oder löschen Sie sie und wählen Sie „Weiter“ aus.
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 Verkehrsklassifizierung behandelt. Sie können Verkehrsdiagramme anzeigen und überprüfen, ob die Polizei die von Ihnen erwarteten Verkehrsbeschränkungen durchsetzt.

Löschen einer Datenverkehrsklassifizierungsrichtlinie

Sie können eine Verkehrsklassifizierungsrichtlinie löschen, wenn Sie sie nicht mehr benötigen. Stellen Sie sicher, dass Sie die richtige Richtlinie löschen, da eine gelöschte Richtlinie nicht wiederhergestellt werden kann.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **Verkehrsklassifizierung**.

   Die Seite „Richtlinien zur Datenverkehrsklassifizierung“ 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 Richtliniendetails

   a. Wählen Sie den Richtliniennamen aus.

   b. Wählen Sie die Schaltfläche **Entfernen** neben dem Richtliniennamen.

3. Wählen Sie **Ja**, um zu bestätigen, dass Sie die Richtlinie löschen möchten.

   Die Richtlinie wird gelöscht.

Anzeigen von Netzwerkverkehrsmetriken

Sie können den Netzwerkverkehr überwachen, indem Sie die Diagramme anzeigen, die auf der Seite „Richtlinien zur Verkehrsklassifizierung“ verfügbar sind.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriff oder Mandantenkontenberechtigung" .

Informationen zu diesem Vorgang

Sie können für jede vorhandene Richtlinie zur Verkehrsklassifizierung Kennzahlen für den Lastenausgleichsdienst anzeigen, um zu ermitteln, ob die Richtlinie den Verkehr im Netzwerk erfolgreich begrenzt. Mithilfe der Daten in den Diagrammen können Sie feststellen, ob Sie die Richtlinie anpassen müssen.

Auch wenn für eine Verkehrsklassifizierungsrichtlinie keine Grenzwerte festgelegt sind, werden Messwerte erfasst und die Diagramme liefern nützliche Informationen zum Verständnis von Verkehrstrends.

Schritte

1. Wählen Sie **KONFIGURATION** > **Netzwerk** > **Verkehrsklassifizierung**.

   Die Seite „Richtlinien zur Datenverkehrsklassifizierung“ wird angezeigt und die vorhandenen Richtlinien werden in der Tabelle aufgelistet.

2. Wählen Sie den Namen der Datenverkehrsklassifizierungsrichtlinie aus, für die Sie Metriken anzeigen möchten.
3. Wählen Sie die Registerkarte **Metriken**.

   Die Richtliniendiagramme zur Verkehrsklassifizierung werden angezeigt. Die Diagramme zeigen nur Metriken für den Datenverkehr an, der der ausgewählten Richtlinie entspricht.

   Die folgenden Grafiken sind auf der Seite enthalten.

   - Anforderungsrate: Dieses Diagramm zeigt die Bandbreitenmenge an, die dieser Richtlinie entspricht und von allen Lastenausgleichsmodulen verarbeitet wird. Zu den empfangenen Daten gehören Anforderungsheader für alle Anforderungen und die Textdatengröße für Antworten mit Textdaten. „Gesendet“ umfasst Antwortheader für alle Anfragen und die Datengröße des Antworttexts für Anfragen, die Textdaten in der Antwort enthalten.

     > Wenn die Anfragen abgeschlossen sind, zeigt dieses Diagramm nur die Bandbreitennutzung. Bei langsamen oder großen Objektanforderungen kann die tatsächliche momentane Bandbreite von den in diesem Diagramm angegebenen Werten abweichen.

   - Fehlerantwortrate: Dieses Diagramm zeigt die ungefähre Rate, mit der Anfragen, die dieser Richtlinie entsprechen, Fehler (HTTP-Statuscode >= 400) an Clients zurückgeben.
   - Durchschnittliche Anfragedauer (ohne Fehler): Dieses Diagramm zeigt die durchschnittliche Dauer erfolgreicher Anfragen, die dieser Richtlinie entsprechen.
   - Bandbreitennutzung der Richtlinie: Dieses Diagramm zeigt die Bandbreitenmenge an, die dieser Richtlinie entspricht und von allen Lastenausgleichsmodulen verarbeitet wird. Zu den empfangenen Daten gehören Anforderungsheader für alle Anforderungen und die Textdatengröße für Antworten mit Textdaten. „Gesendet“ umfasst Antwortheader für alle Anfragen und die Datengröße des Antworttexts für Anfragen, die Textdaten in der Antwort enthalten.
4. Positionieren Sie den Cursor über einem Liniendiagramm, um ein Popup mit Werten in einem bestimmten Teil des Diagramms anzuzeigen.
5. Wählen Sie direkt unter dem Titel „Metriken“ **Grafana-Dashboard** aus, um alle Diagramme für eine Richtlinie anzuzeigen. Zusätzlich zu den vier Diagrammen auf der Registerkarte **Metriken** können Sie zwei weitere Diagramme anzeigen:

   - Schreibanforderungsrate nach Objektgröße: Die Rate für PUT/POST/DELETE-Anforderungen, die dieser Richtlinie entsprechen. Die Positionierung auf einer einzelnen Zelle zeigt die Geschwindigkeit pro Sekunde. Die in der Hover-Ansicht angezeigten Raten werden auf ganzzahlige Werte gekürzt und geben möglicherweise 0 aus, wenn sich im Bucket Anfragen ungleich null befinden.
   - Leseanforderungsrate nach Objektgröße: Die Rate für GET/HEAD-Anforderungen, die dieser Richtlinie entsprechen. Die Positionierung auf einer einzelnen Zelle zeigt die Geschwindigkeit pro Sekunde. Die in der Hover-Ansicht angezeigten Raten werden auf ganzzahlige Werte gekürzt und geben möglicherweise 0 aus, wenn sich im Bucket Anfragen ungleich null befinden.

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 **Traffic Classification Policy** 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 anzuzeigen, das Datum und Uhrzeit der Stichprobe, in die Zählung einbezogene Objektgrößen und die Anzahl der Anfragen pro Sekunde während dieses Zeitraums anzeigt.

      Richtlinien zur Verkehrsklassifizierung werden anhand ihrer ID identifiziert. Richtlinien-IDs werden auf der Seite „Richtlinien zur Verkehrsklassifizierung“ aufgelistet.
7. Analysieren Sie die Diagramme, um festzustellen, wie oft die Richtlinie den Datenverkehr einschränkt und ob Sie die Richtlinie anpassen müssen.

Unterstützte Verschlüsselungen für ausgehende TLS-Verbindungen

Das StorageGRID -System unterstützt eine begrenzte Anzahl von Verschlüsselungssammlungen für Transport Layer Security (TLS)-Verbindungen zu den externen Systemen, die für die 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 die Identitätsföderation und Cloud-Speicherpools verwendet werden.

Die für die Verwendung mit externen Systemen unterstützten TLS-Chiffren wurden ausgewählt, um die Kompatibilität mit einer Reihe externer Systeme sicherzustellen. Die Liste ist größer als die Liste der Chiffren, die für die Verwendung mit S3-Clientanwendungen unterstützt werden. Um Verschlüsselungen zu konfigurieren, gehen Sie zu **KONFIGURATION** > **Sicherheit** > **Sicherheitseinstellungen** und wählen Sie **TLS- und SSH-Richtlinien**.

> TLS-Konfigurationsoptionen wie Protokollversionen, Chiffren, Schlüsselaustauschalgorithmen und MAC-Algorithmen sind in StorageGRID nicht konfigurierbar. Wenden Sie sich an Ihren NetApp -Kundenbetreuer, wenn Sie spezielle Anfragen zu diesen Einstellungen haben.

Vorteile aktiver, inaktiver und gleichzeitiger HTTP-Verbindungen

Die Konfiguration von HTTP-Verbindungen kann sich auf die Leistung des StorageGRID Systems auswirken. Die Konfigurationen unterscheiden sich je nachdem, ob die HTTP-Verbindung aktiv oder inaktiv ist oder ob Sie mehrere Verbindungen gleichzeitig haben.

Sie können die Leistungsvorteile für die folgenden Arten von HTTP-Verbindungen ermitteln:

- Inaktive HTTP-Verbindungen
- Aktive HTTP-Verbindungen
- Gleichzeitige HTTP-Verbindungen

Vorteile des Offenhaltens inaktiver HTTP-Verbindungen

Sie sollten HTTP-Verbindungen auch dann offen halten, wenn Clientanwendungen inaktiv sind, damit Clientanwendungen nachfolgende Transaktionen über die offene Verbindung durchführen können. Basierend auf Systemmessungen und Integrationserfahrungen sollten Sie eine inaktive HTTP-Verbindung maximal 10 Minuten lang offen halten. StorageGRID schließt möglicherweise automatisch eine HTTP-Verbindung, die länger als 10 Minuten offen und inaktiv bleibt.

Offene und inaktive HTTP-Verbindungen bieten die folgenden Vorteile:

- Reduzierte Latenzzeit von dem Zeitpunkt, an dem das StorageGRID -System feststellt, dass es eine HTTP-Transaktion durchführen muss, bis zu dem Zeitpunkt, an dem das StorageGRID System die Transaktion durchführen kann

  Der Hauptvorteil ist die geringere Latenz, insbesondere im Hinblick auf die zum Herstellen von TCP/IP- und TLS-Verbindungen erforderliche Zeit.

- Erhöhte Datenübertragungsrate durch Vorbereitung des TCP/IP-Slow-Start-Algorithmus mit zuvor durchgeführten Übertragungen
- Sofortige Benachrichtigung über verschiedene Klassen von Fehlerzuständen, die die Konnektivität zwischen der Clientanwendung und dem StorageGRID -System unterbrechen

Die Entscheidung, wie lange eine inaktive Verbindung offen gehalten werden soll, ist ein Kompromiss zwischen den Vorteilen eines langsamen Starts, der mit der bestehenden Verbindung verbunden ist, und der idealen Zuweisung der Verbindung zu internen Systemressourcen.

Vorteile aktiver HTTP-Verbindungen

Bei Verbindungen direkt zu Storage Nodes sollten Sie die Dauer einer aktiven HTTP-Verbindung auf maximal 10 Minuten begrenzen, auch wenn die HTTP-Verbindung kontinuierlich Transaktionen durchführt.

Bei der Festlegung der maximalen Dauer, die eine Verbindung offen gehalten werden sollte, handelt es sich um einen Kompromiss zwischen den Vorteilen der Verbindungspersistenz und der idealen Zuweisung der Verbindung zu internen Systemressourcen.

Für Clientverbindungen zu Speicherknoten bietet die Begrenzung aktiver HTTP-Verbindungen die folgenden Vorteile:

- Ermöglicht eine optimale Lastverteilung im gesamten StorageGRID -System.

  Mit der Zeit ist eine HTTP-Verbindung möglicherweise nicht mehr optimal, da sich die Anforderungen an den Lastenausgleich ändern. Das System erzielt die beste Lastverteilung, wenn Clientanwendungen für jede Transaktion eine separate HTTP-Verbindung herstellen. Dies macht jedoch die wesentlich wertvolleren Vorteile dauerhafter Verbindungen zunichte.

- Ermöglicht Clientanwendungen, HTTP-Transaktionen an LDR-Dienste weiterzuleiten, die über verfügbaren Speicherplatz verfügen.
- Ermöglicht den Start von Wartungsverfahren.

  Einige Wartungsverfahren beginnen erst, nachdem alle laufenden HTTP-Verbindungen abgeschlossen sind.

Bei Clientverbindungen zum Load Balancer-Dienst kann die Begrenzung der Dauer offener Verbindungen hilfreich sein, um den sofortigen Start einiger Wartungsvorgänge zu ermöglichen. Wenn die Dauer der

Clientverbindungen nicht begrenzt ist, kann es mehrere Minuten dauern, bis aktive Verbindungen automatisch beendet werden.

Vorteile gleichzeitiger HTTP-Verbindungen

Sie sollten mehrere TCP/IP-Verbindungen zum StorageGRID -System offen halten, um Parallelität zu ermöglichen und so die Leistung zu steigern. Die optimale Anzahl paralleler Verbindungen hängt von verschiedenen Faktoren ab.

Gleichzeitige HTTP-Verbindungen bieten die folgenden Vorteile:

- Reduzierte Latenz

  Transaktionen können sofort gestartet werden, anstatt auf den Abschluss anderer Transaktionen zu warten.

- Erhöhter Durchsatz

  Das StorageGRID -System kann parallele Transaktionen durchführen und den gesamten Transaktionsdurchsatz erhöhen.

Clientanwendungen sollten mehrere HTTP-Verbindungen herstellen. Wenn eine Clientanwendung eine Transaktion durchführen muss, kann sie jede bestehende Verbindung auswählen und sofort verwenden, die derzeit keine Transaktion verarbeitet.

Die Topologie jedes StorageGRID -Systems weist einen unterschiedlichen Spitzendurchsatz für gleichzeitige Transaktionen und Verbindungen auf, bevor die Leistung nachlässt. Der Spitzendurchsatz hängt von Faktoren wie Rechenressourcen, Netzwerkressourcen, Speicherressourcen und WAN-Verbindungen ab. Auch die Anzahl der Server und Dienste sowie die Anzahl der Anwendungen, die das StorageGRID -System unterstützt, spielen eine Rolle.

StorageGRID -Systeme unterstützen häufig mehrere Clientanwendungen. Sie sollten dies berücksichtigen, wenn Sie die maximale Anzahl gleichzeitiger Verbindungen bestimmen, die von einer Clientanwendung verwendet werden. Wenn die Client-Anwendung aus mehreren Software-Entitäten besteht, die jeweils Verbindungen zum StorageGRID -System herstellen, sollten Sie alle Verbindungen zwischen den Entitäten addieren. In den folgenden Situationen müssen Sie möglicherweise die maximale Anzahl gleichzeitiger Verbindungen anpassen:

- Die Topologie des StorageGRID -Systems beeinflusst die maximale Anzahl gleichzeitiger Transaktionen und Verbindungen, die das System unterstützen kann.
- Clientanwendungen, die über ein Netzwerk mit begrenzter Bandbreite mit dem StorageGRID -System interagieren, müssen möglicherweise den Grad der Parallelität reduzieren, um sicherzustellen, dass einzelne Transaktionen in angemessener Zeit abgeschlossen werden.
- Wenn viele Clientanwendungen das StorageGRID -System gemeinsam nutzen, müssen Sie möglicherweise den Grad der Parallelität reduzieren, um ein Überschreiten der Systemgrenzen zu vermeiden.

Trennung von HTTP-Verbindungspools für Lese- und Schreibvorgänge

Sie können separate Pools von HTTP-Verbindungen für Lese- und Schreibvorgänge verwenden und steuern, wie viel Pool Sie jeweils verwenden möchten. Separate Pools von HTTP-Verbindungen ermöglichen Ihnen eine bessere Kontrolle der Transaktionen und einen Lastausgleich.

Clientanwendungen können Ladevorgänge erstellen, die beim Abrufen (Lesen) oder Speichern (Schreiben)

dominant sind. Mit separaten Pools von HTTP-Verbindungen für Lese- und Schreibtransaktionen können Sie anpassen, wie viel von jedem Pool für Lese- oder Schreibtransaktionen reserviert werden soll.

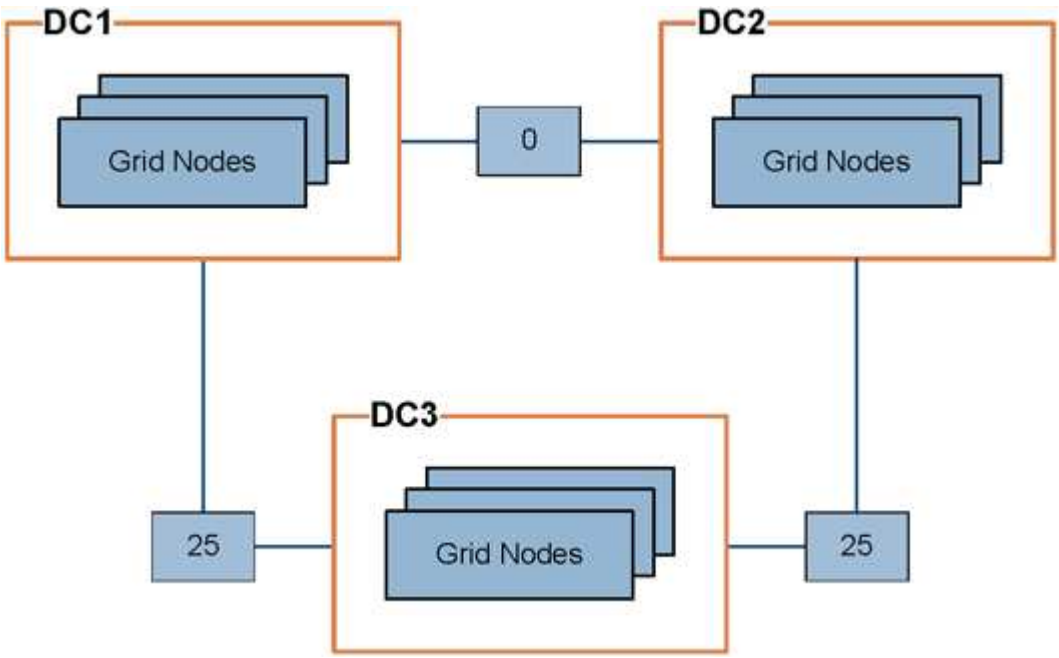
Linkkosten verwalten

Mithilfe der Verbindungskosten können Sie priorisieren, welcher Rechenzentrumsstandort einen angeforderten Dienst bereitstellt, wenn zwei oder mehr Rechenzentrumsstandorte vorhanden sind. Sie können die Verbindungskosten anpassen, um die Latenz zwischen Sites widerzuspiegeln.

Was sind Linkkosten?

- Mithilfe von Verknüpfungskosten wird priorisiert, welche Objektkopie zum Abrufen von Objekten verwendet wird.
- Die Verbindungskosten werden von der Grid Management API und der Tenant Management API verwendet, um zu bestimmen, welche internen StorageGRID -Dienste verwendet werden sollen.
- Verbindungskosten werden vom Load Balancer-Dienst auf Admin-Knoten und Gateway-Knoten verwendet, um Clientverbindungen zu leiten. Sehen "Überlegungen zum Lastenausgleich" .

Das Diagramm zeigt ein Raster mit drei Standorten, bei dem die Verbindungskosten zwischen den Standorten konfiguriert sind:



- Der Load Balancer-Dienst auf Admin-Knoten und Gateway-Knoten verteilt Clientverbindungen gleichmäßig auf alle Speicherknoten am selben Rechenzentrumsstandort und auf alle Rechenzentrumsstandorte mit Verbindungskosten von 0.

  Im Beispiel verteilt ein Gateway-Knoten am Rechenzentrumsstandort 1 (DC1) die Clientverbindungen gleichmäßig auf die Speicherknoten bei DC1 und die Speicherknoten bei DC2. Ein Gateway-Knoten bei DC3 sendet Client-Verbindungen nur an Speicherknoten bei DC3.

- Beim Abrufen eines Objekts, das in mehreren replizierten Kopien vorliegt, ruft StorageGRID die Kopie im Rechenzentrum ab, das die niedrigsten Verbindungskosten aufweist.

Wenn im Beispiel eine Clientanwendung 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 betragen und damit niedriger sind als die Verbindungskosten von DC3 zu DC2 (25).

Bei den Linkkosten handelt es sich um beliebige relative Zahlen ohne spezifische Maßeinheit. Beispielsweise werden Verbindungskosten von 50 weniger bevorzugt verwendet als Verbindungskosten von 25. Die Tabelle zeigt häufig verwendete Verbindungskosten.

Link	Linkkosten	Hinweise
Zwischen physischen Rechenzentrumsstandorten	25 (Standard)	Rechenzentren, die über eine WAN-Verbindung verbunden sind.
Zwischen logischen Rechenzentrumsstandorten am gleichen physischen Standort	0	Logische Rechenzentren im selben physischen Gebäude oder Campus, die über ein LAN verbunden sind.

Linkkosten aktualisieren

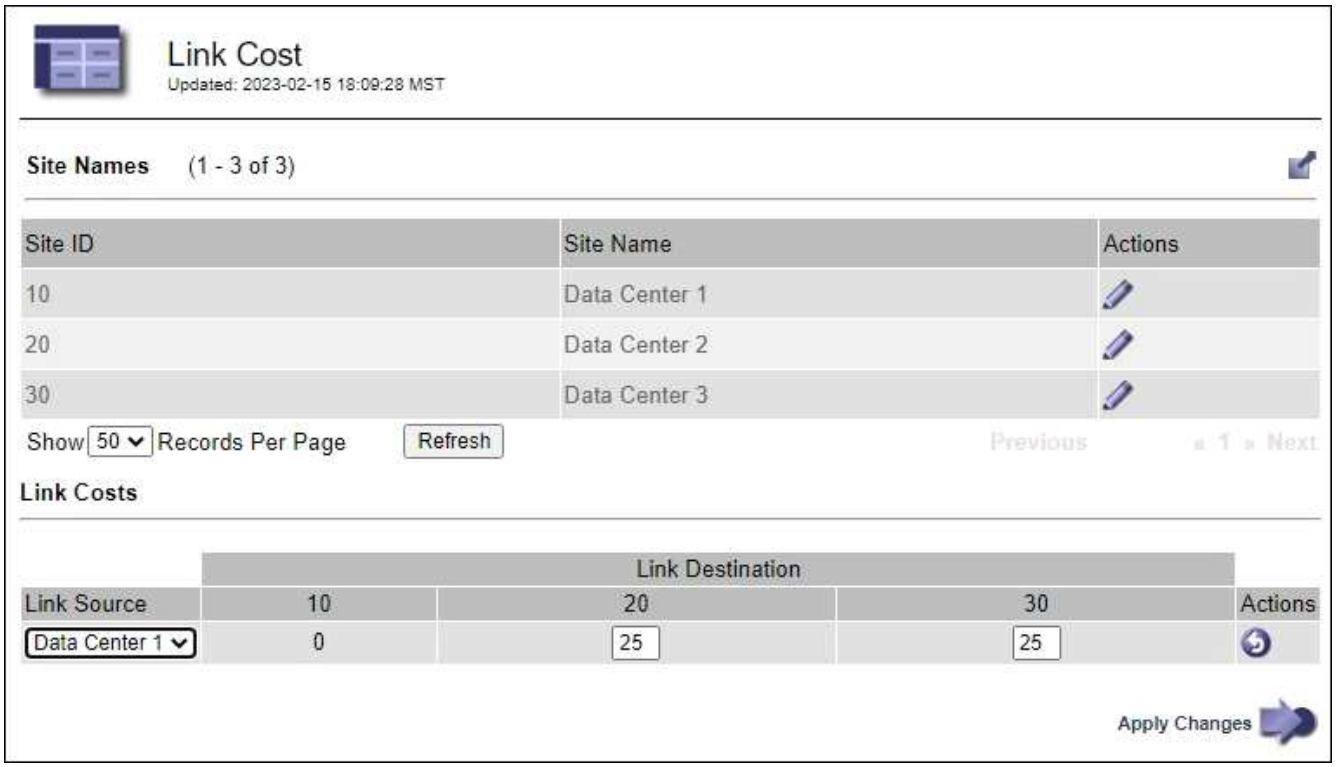
Sie können die Verbindungskosten zwischen Rechenzentrumsstandorten aktualisieren, um die Latenz zwischen den Standorten widerzuspiegeln.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Berechtigung zur Konfiguration der Grid-Topologieseite" .

Schritte

1. Wählen Sie **SUPPORT** > **Sonstiges** > **Linkkosten**.



2. Wählen Sie unter **Linkquelle** eine Site aus und geben Sie unter **Linkziel** einen Kostenwert zwischen 0 und 100 ein.

   Sie können die Linkkosten nicht ändern, wenn die Quelle mit dem Ziel identisch ist.

   Um die Änderungen abzubrechen, wählen Sie **Zurücksetzen**.

3. Wählen Sie **Änderungen übernehmen**.

Verwenden Sie AutoSupport

Was ist AutoSupport?

Mit der AutoSupport -Funktion kann StorageGRID Integritäts- und Statuspakete an den technischen Support von NetApp senden.

Die Verwendung von AutoSupport kann die Problembestimmung und -lösung erheblich beschleunigen. Der technische Support kann auch den Speicherbedarf Ihres Systems überwachen und Ihnen dabei helfen, festzustellen, ob Sie neue Knoten oder Sites hinzufügen müssen. Optional können Sie AutoSupport Pakete so konfigurieren, dass sie an ein zusätzliches Ziel gesendet werden.

StorageGRID bietet zwei Arten von AutoSupport:

- * StorageGRID AutoSupport* meldet Probleme mit der StorageGRID -Software. Standardmäßig aktiviert, wenn Sie StorageGRID zum ersten Mal installieren. Du kannst"Ändern Sie die Standardkonfiguration von AutoSupport" falls erforderlich.

Wenn StorageGRID AutoSupport nicht aktiviert ist, wird eine Meldung auf dem Grid Manager-Dashboard angezeigt. Die Nachricht enthält einen Link zur AutoSupport Konfigurationsseite. Wenn Sie die Nachricht schließen, wird sie erst wieder angezeigt, wenn Ihr Browser-Cache geleert wird, auch wenn AutoSupport deaktiviert bleibt.

- * AutoSupport für Appliance-Hardware * meldet Probleme mit StorageGRID Geräten. Sie müssen"Konfigurieren Sie Hardware AutoSupport auf jedem Gerät" .

Was ist Active IQ?

Active IQ ist ein cloudbasierter digitaler Berater, der prädiktive Analysen und das Wissen der Community aus der installierten Basis von NetApp nutzt. Die kontinuierlichen Risikobewertungen, prädiktiven Warnmeldungen, präskriptiven Anleitungen und automatisierten Aktionen helfen Ihnen, Probleme zu verhindern, bevor sie auftreten, was zu einer verbesserten Systemintegrität und höheren Systemverfügbarkeit führt.

Wenn Sie die Active IQ Dashboards und -Funktionen auf der NetApp -Support-Site verwenden möchten, müssen Sie AutoSupport aktivieren.

"Active IQ Digital Advisor Dokumentation"

Im AutoSupport Paket enthaltene Informationen

Ein AutoSupport -Paket enthält die folgenden Dateien und Details.

Dateiname	Felder	Beschreibung
AUTOSUPPORT-HISTORY.XML	AutoSupport Sequenznummer + Ziel für diesen AutoSupport + Status der Zustellung + Zustellungsversuche + AutoSupport Betreff + Zustellungs-URI + Letzter Fehler + AutoSupport -PUT -Dateiname + Zeitpunkt der Generierung + Komprimierte AutoSupport-Größe + Dekomprimierte AutoSupport-Größe + Gesamte Erfassungszeit (ms)	AutoSupport -Verlaufsdatei.
AUTOSUPPORT.XML	Knoten + Protokoll zur Kontaktaufnahme mit dem Support + Support-URL für HTTP/HTTPS + Support-Adresse + AutoSupport OnDemand-Status + AutoSupport OnDemand-Server-URL + AutoSupport OnDemand-Abfrageintervall	AutoSupport -Statusdatei. Bietet Details zum verwendeten Protokoll, zur URL und Adresse des technischen Supports, zum Abfrageintervall und zu OnDemand AutoSupport , falls aktiviert oder deaktiviert.

Dateiname	Felder	Beschreibung
BUCKETS.XML	Bucket-ID + Konto-ID + Build-Version + Standortbeschränkungskonfiguration + Compliance aktiviert + Compliance-Konfiguration + S3-Objektsperre aktiviert + S3-Objektsperre-Konfiguration + Konsistenzkonfiguration + CORS aktiviert + CORS-Konfiguration + Letzter Zugriffszeitpunkt aktiviert + Richtlinie aktiviert + Richtlinienkonfiguration + Benachrichtigungen aktiviert + Benachrichtigungskonfiguration + Cloud Mirror aktiviert + Cloud Mirror-Konfiguration + Suche aktiviert + Suchkonfiguration + Bucket-Tagging aktiviert + Bucket-Tagging-Konfiguration + Versionierungskonfiguration	Bietet Konfigurationsdetails und Statistiken auf Bucket-Ebene. Beispiele für Bucket-Konfigurationen sind Plattformdienste, Compliance und Bucket-Konsistenz.
GRID-CONFIGURATIONEN.XML	Attribut-ID + Attributname + Wert + Index + Tabellen-ID + Tabellenname	Gridweite Konfigurationsinformationsdatei. Enthält Informationen zu Grid-Zertifikaten, reserviertem Speicherplatz für Metadaten, Grid-weiten Konfigurationseinstellungen (Compliance, S3 Object Lock, Objektkomprimierung, Warnungen, Syslog und ILM-Konfiguration), Details zum Erasure-Coding-Profil, DNS-Namen und"NMS-Name" .
GRID-SPEC.XML	Rasterspezifikationen, Roh-XML	Wird zum Konfigurieren und Bereitstellen von StorageGRID verwendet. Enthält Grid-Spezifikationen, NTP-Server-IP, DNS-Server-IP, Netzwerktopologie und Hardwareprofile der Knoten.
GRID-TASKS.XML	Knoten + Servicepfad + Attribut-ID + Attributname + Wert + Index + Tabellen-ID + Tabellenname	Statusdatei für Grid-Aufgaben (Wartungsverfahren). Bietet Details zu den aktiven, beendeten, abgeschlossenen, fehlgeschlagenen und ausstehenden Aufgaben des Rasters.
GRID.JSON	Raster + Revision + Softwareversion + Beschreibung + Lizenz + Passwörter + DNS + NTP + Sites + Knoten	Rasterinformationen.

Dateiname	Felder	Beschreibung
ILM-CONFIGURATION.XML	Attribut-ID + Attributname + Wert + Index + Tabellen-ID + Tabellenname	Liste der Attribute für ILM-Konfigurationen.
ILM-STATUS.XML	Knoten + Dienstpfad + Attribut-ID + Attributname + Wert + Index + Tabellen-ID + Tabellenname	Informationsdatei zu ILM-Metriken. Enthält ILM-Bewertungsraten für jeden Knoten und netzweite Metriken.
ILM.XML	ILM-Roh-XML	Aktive ILM-Richtliniendatei. Enthält Details zu den aktiven ILM-Richtlinien, z. B. Speicherpool-ID, Aufnahmeverhalten, Filter, Regeln und Beschreibung.
LOG.TGZ	*n / A*	Herunterladbare Protokolldatei. Enthält `bycast-err.log` Und `servermanager.log` von jedem Knoten.
MANIFEST.XML	Sammelreihenfolge + AutoSupport -Inhaltsdateiname für diese Daten + Beschreibung dieses Datenelements + Anzahl der gesammelten Bytes + Zeitaufwand für die Sammlung + Status dieses Datenelements + Beschreibung des Fehlers + AutoSupport -Inhaltstyp für diese Daten	Enthält AutoSupport Metadaten und kurze Beschreibungen aller AutoSupport Dateien.
NMS-ENTITIES.XML	Attributindex + Entitäts-OID + Knoten-ID + Gerätemodell-ID + Gerätemodellversion + Entitätsname	Konzern- und Servicegesellschaften in der"NMS-Baum" . Bietet Details zur Netztopologie. Der Knoten kann anhand der auf dem Knoten laufenden Dienste ermittelt werden.
OBJECTS-STATUS.XML	Knoten + Dienstpfad + Attribut-ID + Attributname + Wert + Index + Tabellen-ID + Tabellenname	Objektstatus, einschließlich Hintergrundscanstatus, aktive Übertragung, Übertragungsrate, Gesamtübertragungen, Löschrate, beschädigte Fragmente, verlorene Objekte, fehlende Objekte, Reparaturversuch, Scanrate, geschätzter Scanzeitraum und Status der Reparaturfertigstellung.

Dateiname	Felder	Beschreibung
SERVER-STATUS.XML	Knoten + Dienstpfad + Attribut-ID + Attributname + Wert + Index + Tabellen-ID + Tabellenname	Serverkonfigurationen. Enthält diese Details für jeden Knoten: Plattformtyp, Betriebssystem, installierter Speicher, verfügbarer Speicher, Speicherkonnektivität, Seriennummer des Speichergerätegehäuses, Anzahl ausgefallener Laufwerke des Speichercontrollers, Gehäusetemperatur des Compute-Controllers, Compute-Hardware, Seriennummer des Compute-Controllers, Stromversorgung, Laufwerksgröße und Laufwerkstyp.
SERVICE-STATUS.XML	Knoten + Dienstpfad + Attribut-ID + Attributname + Wert + Index + Tabellen-ID + Tabellenname	Serviceknoten-Informationsdatei. Enthält Details wie zugewiesenen Tabellenspeicherplatz, freien Tabellenspeicherplatz, Reaper-Metriken der Datenbank, Segmentreparaturdauer, Reparaturauftragsdauer, automatische Auftragsneustarts und automatische Auftragsbeendigung.
STORAGE-GRADES.XML	Speicherklassen-ID + Speicherklassenname + Speicherknoten-ID + Speicherknotenpfad	Datei mit Speicherklassendefinitionen für jeden Speicherknoten.
SUMMARY-ATTRIBUTES.XML	Gruppen-OID + Gruppenpfad + Zusammenfassungsattribut-ID + Zusammenfassungsattributname + Wert + Index + Tabellen-ID + Tabellenname	Ausführliche Systemstatusdaten, die StorageGRID Nutzungsinformationen zusammenfassen. Bietet Details wie den Namen des Grids, die Namen der Sites, die Anzahl der Speicherknoten pro Grid und pro Site, den Lizenztyp, die Lizenzkapazität und -nutzung, die Bedingungen für den Software-Support und Details zu S3-Vorgängen.
SYSTEM-ALERTS.XML	Name + Schweregrad + Knotenname + Alarmstatus + Sitename + Auslösezeit des Alarms + Lösungszeit des Alarms + Regel-ID + Knoten-ID + Site-ID + Stummgeschaltet + Andere Anmerkungen + Andere Bezeichnungen	Aktuelle Systemwarnungen, die auf mögliche Probleme im StorageGRID -System hinweisen.

Dateiname	Felder	Beschreibung
USERAGENTS.XML	Benutzeragent + Anzahl der Tage + Gesamtzahl der HTTP-Anfragen + Gesamtzahl der aufgenommenen Bytes + Gesamtzahl der abgerufenen Bytes + PUT-Anfragen + GET-Anfragen + DELETE-Anfragen + HEAD-Anfragen + POST-Anfragen + OPTIONS-Anfragen + Durchschnittliche Anfragezeit (ms) + Durchschnittliche PUT-Anfragezeit (ms) + Durchschnittliche GET-Anfragezeit (ms) + Durchschnittliche DELETE-Anfragezeit (ms) + Durchschnittliche HEAD-Anfragezeit (ms) + Durchschnittliche POST-Anfragezeit (ms) + Durchschnittliche OPTIONS-Anfragezeit (ms)	Statistiken basierend auf den Benutzeragenten der Anwendung. Beispielsweise die Anzahl der PUT/GET/DELETE/HEAD-Operationen pro Benutzeragent und die Gesamtbytegröße jeder Operation.
X-HEADER-DATA	X-Netapp-asup-generated-on + X-Netapp-asup-hostname + X-Netapp-asup-os-version + X-Netapp-asup-serial-num + X-Netapp-asup-subject	AutoSupport -Headerdaten.

Konfigurieren Sie AutoSupport

Standardmäßig ist die StorageGRID AutoSupport Funktion aktiviert, wenn Sie StorageGRID zum ersten Mal installieren. Sie müssen jedoch die Hardware AutoSupport auf jedem Gerät konfigurieren. Bei Bedarf können Sie die AutoSupport Konfiguration ändern.

Wenn Sie die Konfiguration von StorageGRID AutoSupport ändern möchten, nehmen Sie Ihre Änderungen nur am primären Admin-Knoten vor. Sie müssenKonfigurieren Sie die AutoSupport Hardware auf jedem Gerät.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .
- Wenn Sie HTTPS zum Senden von AutoSupport Paketen verwenden, haben Sie ausgehenden Internetzugriff auf den primären Admin-Knoten bereitgestellt, entweder direkt oder"Verwendung eines Proxyservers" (eingehende Verbindungen nicht erforderlich).
- Wenn HTTP auf der StorageGRID AutoSupport Seite ausgewählt ist, haben Sie"einen Proxy-Server

konfiguriert" um AutoSupport -Pakete als HTTPS weiterzuleiten. Die AutoSupport -Server von NetApp lehnen per HTTP gesendete Pakete ab.

- Wenn Sie SMTP als Protokoll für AutoSupport Pakete verwenden, haben Sie einen SMTP-Mailserver konfiguriert.

Informationen zu diesem Vorgang

Sie können eine beliebige Kombination der folgenden Optionen verwenden, um AutoSupport -Pakete an den technischen Support zu senden:

- **Wöchentlich**: Senden Sie automatisch einmal pro Woche AutoSupport -Pakete. Standardeinstellung: Aktiviert.
- **Ereignisgesteuert**: Senden Sie AutoSupport Pakete automatisch jede Stunde oder wenn wichtige Systemereignisse auftreten. Standardeinstellung: Aktiviert.
- **Auf Anfrage**: Erlauben Sie dem technischen Support, Ihr StorageGRID -System aufzufordern, automatisch AutoSupport Pakete zu senden. Dies ist nützlich, wenn aktiv an einem Problem gearbeitet wird (erfordert das HTTPS- AutoSupport Übertragungsprotokoll). Standardeinstellung: Deaktiviert.
- **Vom Benutzer ausgelöst**: Senden Sie AutoSupport Pakete jederzeit manuell.

Geben Sie das Protokoll für AutoSupport Pakete an

Sie können zum Senden von AutoSupport -Paketen eines der folgenden Protokolle verwenden:

- **HTTPS**: Dies ist die Standardeinstellung und wird für Neuinstallationen empfohlen. Dieses Protokoll verwendet Port 443. Wenn Sie wollenAktivieren Sie die AutoSupport on Demand-Funktion , müssen Sie HTTPS verwenden.
- **HTTP**: Wenn Sie HTTP auswählen, müssen Sie einen Proxyserver konfigurieren, um AutoSupport Pakete als HTTPS weiterzuleiten. Die AutoSupport -Server von NetApp lehnen per HTTP gesendete Pakete ab. Dieses Protokoll verwendet Port 80.
- **SMTP**: Verwenden Sie diese Option, wenn Sie AutoSupport Pakete per E-Mail versenden möchten.

Das von Ihnen festgelegte Protokoll wird zum Senden aller Arten von AutoSupport Paketen verwendet.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > * AutoSupport* > **Einstellungen**.
2. Wählen Sie das Protokoll aus, das Sie zum Senden von AutoSupport -Paketen verwenden möchten.
3. Wenn Sie **HTTPS** ausgewählt haben, wählen Sie aus, ob ein NetApp -Supportzertifikat (TLS-Zertifikat) verwendet werden soll, um die Verbindung zum technischen Supportserver zu sichern.
   - **Zertifikat überprüfen** (Standard): Stellt sicher, dass die Übertragung von AutoSupport -Paketen sicher ist. Das NetApp -Support-Zertifikat ist bereits mit der StorageGRID -Software installiert.
   - **Zertifikat nicht überprüfen**: Wählen Sie diese Option nur aus, wenn Sie einen guten Grund haben, die Zertifikatsüberprüfung nicht zu verwenden, beispielsweise wenn ein vorübergehendes Problem mit einem Zertifikat vorliegt.
4. Wählen Sie **Speichern**. Alle wöchentlichen, benutzer- und ereignisgesteuerten Pakete werden mit dem ausgewählten Protokoll gesendet.

Wöchentlichen AutoSupport deaktivieren

Standardmäßig ist das StorageGRID -System so konfiguriert, dass einmal pro Woche ein AutoSupport Paket an den technischen Support gesendet wird.

Um zu bestimmen, wann das wöchentliche AutoSupport Paket gesendet wird, gehen Sie zur Registerkarte * AutoSupport* > **Ergebnisse**. Sehen Sie sich im Abschnitt **Wöchentlicher AutoSupport** den Wert für **Nächster geplanter Zeitpunkt** an.

Sie können das automatische Senden wöchentlicher AutoSupport Pakete jederzeit deaktivieren.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > * AutoSupport* > **Einstellungen**.
2. Deaktivieren Sie das Kontrollkästchen **Wöchentlichen AutoSupport aktivieren**.
3. Wählen Sie **Speichern**.

Deaktivieren Sie ereignisgesteuerten AutoSupport

Standardmäßig ist das StorageGRID -System so konfiguriert, dass stündlich ein AutoSupport -Paket an den technischen Support gesendet wird.

Sie können den ereignisgesteuerten AutoSupport jederzeit deaktivieren.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > * AutoSupport* > **Einstellungen**.
2. Deaktivieren Sie das Kontrollkästchen **Ereignisgesteuerten AutoSupport aktivieren**.
3. Wählen Sie **Speichern**.

Aktivieren Sie AutoSupport on Demand

AutoSupport on Demand kann bei der Lösung von Problemen helfen, an denen der technische Support aktiv arbeitet.

Standardmäßig ist AutoSupport on Demand deaktiviert. Durch Aktivieren dieser Funktion kann der technische Support anfordern, dass Ihr StorageGRID -System automatisch AutoSupport Pakete sendet. Der technische Support kann auch das Abfragezeitintervall für AutoSupport on Demand-Abfragen festlegen.

Der technische Support kann AutoSupport on Demand nicht aktivieren oder deaktivieren.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > * AutoSupport* > **Einstellungen**.
2. Wählen Sie **HTTPS** als Protokoll aus.
3. Aktivieren Sie das Kontrollkästchen **Wöchentlichen 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 Suche nach Softwareupdates

Standardmäßig kontaktiert StorageGRID NetApp , um festzustellen, ob Software-Updates für Ihr System verfügbar sind. Wenn ein StorageGRID Hotfix oder eine neue Version verfügbar ist, wird die neue Version auf der StorageGRID Upgradeseite angezeigt.

Bei Bedarf können Sie die Suche nach Software-Updates optional deaktivieren. Wenn Ihr System beispielsweise keinen WAN-Zugriff hat, sollten Sie die Prüfung deaktivieren, um Downloadfehler zu vermeiden.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > * AutoSupport* > **Einstellungen**.
2. Deaktivieren Sie das Kontrollkästchen **Nach Software-Updates suchen**.
3. Wählen Sie **Speichern**.

Fügen Sie ein zusätzliches AutoSupport Ziel hinzu

Wenn Sie AutoSupport aktivieren, werden Gesundheits- und Statuspakete an den technischen Support gesendet. Sie können ein zusätzliches Ziel für alle AutoSupport Pakete angeben.

Um das zum Senden von AutoSupport Paketen verwendete Protokoll zu überprüfen oder zu ändern, lesen Sie die Anweisungen zuGeben Sie das Protokoll für AutoSupport -Pakete an .

> Sie können das SMTP-Protokoll nicht verwenden, um AutoSupport Pakete an ein zusätzliches Ziel zu senden.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > * AutoSupport* > **Einstellungen**.
2. Wählen Sie **Zusätzliches AutoSupport Ziel aktivieren**.
3. Geben Sie Folgendes an:

   Hostname
   Der Server-Hostname oder die IP-Adresse eines zusätzlichen AutoSupport Zielservers.

   > Sie können nur ein weiteres Ziel eingeben.

   Hafen
   Der Port, der für die Verbindung mit einem zusätzlichen AutoSupport Zielserver verwendet wird. Der Standard ist Port 80 für HTTP oder Port 443 für HTTPS.

   Zertifikatsvalidierung
   Ob ein TLS-Zertifikat verwendet wird, um die Verbindung zum zusätzlichen Ziel zu sichern.

   - Wählen Sie **Zertifikat überprüfen**, um die Zertifikatsvalidierung zu verwenden.
   - Wählen Sie **Zertifikat nicht überprüfen**, um Ihre AutoSupport -Pakete ohne Zertifikatsvalidierung zu senden.

     Wählen Sie diese Option nur aus, wenn Sie einen guten Grund haben, die Zertifikatsvalidierung nicht zu verwenden, beispielsweise wenn ein vorübergehendes Problem mit einem Zertifikat vorliegt.

4. Wenn Sie **Zertifikat überprüfen** ausgewählt haben, gehen Sie wie folgt vor:
   a. Navigieren Sie zum Speicherort des CA-Zertifikats.
   b. Laden Sie die CA-Zertifikatsdatei hoch.

      Die Metadaten des CA-Zertifikats werden angezeigt.

5. Wählen Sie **Speichern**.

   Alle zukünftigen wöchentlichen, ereignis- und benutzergesteuerten AutoSupport Pakete werden an das zusätzliche Ziel gesendet.

AutoSupport für Appliances konfigurieren

AutoSupport für Appliances meldet StorageGRID Hardwareprobleme und StorageGRID AutoSupport meldet StorageGRID -Softwareprobleme, mit einer Ausnahme: Für SGF6112 meldet StorageGRID AutoSupport sowohl Hardware- als auch Softwareprobleme. Sie müssen AutoSupport auf jedem Gerät konfigurieren, mit Ausnahme des SGF6112, für das keine zusätzliche Konfiguration erforderlich ist. AutoSupport wird für Service-Appliances und Speicher-Appliances unterschiedlich implementiert.

Sie verwenden SANtricity , um AutoSupport für jedes Speichergerät zu aktivieren. Sie können SANtricity AutoSupport während der Ersteinrichtung der Appliance oder nach der Installation einer Appliance konfigurieren:

- Für SG6000- und SG5700-Geräte, "AutoSupport im SANtricity System Manager konfigurieren"

AutoSupport -Pakete von E-Series-Geräten können in StorageGRID AutoSupport aufgenommen werden, wenn Sie die AutoSupport -Bereitstellung per Proxy in konfigurieren"SANtricity Systemmanager" .

StorageGRID AutoSupport meldet keine Hardwareprobleme wie DIMM- oder Host Interface Card (HIC)-Fehler. Allerdings können einige Komponentenfehler"Hardwarewarnungen" . Für StorageGRID -Geräte mit einem Baseboard Management Controller (BMC) können Sie E-Mail- und SNMP-Traps konfigurieren, um Hardwarefehler zu melden:

- "E-Mail-Benachrichtigungen für BMC -Warnmeldungen einrichten"
- "Konfigurieren Sie die SNMP-Einstellungen für BMC"

Ähnliche Informationen

"NetApp Support"

Manuelles Auslösen eines AutoSupport -Pakets

Um den technischen Support bei der Behebung von Problemen mit Ihrem StorageGRID -System zu unterstützen, können Sie manuell das Senden eines AutoSupport Pakets auslösen.

Bevor Sie beginnen

- Sie müssen beim Grid Manager mit einem"unterstützter Webbrowser" .
- Sie müssen über Root-Zugriff oder die Berechtigung „Andere Rasterkonfiguration“ verfügen.

Schritte

1. Wählen Sie **SUPPORT** > **Tools** > * AutoSupport*.
2. Wählen Sie auf der Registerkarte **Aktionen** die Option **Benutzergesteuerten AutoSupport senden**.

   StorageGRID versucht, ein AutoSupport Paket an die NetApp Support-Site zu senden. Wenn der Versuch erfolgreich ist, werden die Werte **Neuestes Ergebnis** und **Letzter erfolgreicher Zeitpunkt** auf der Registerkarte **Ergebnisse** aktualisiert. Wenn ein Problem auftritt, wird der Wert **Neuestes Ergebnis** auf „Fehlgeschlagen“ aktualisiert und StorageGRID versucht nicht, das AutoSupport Paket erneut zu senden.

Aktualisieren Sie nach dem Senden eines vom Benutzer ausgelösten AutoSupport Pakets die AutoSupport -Seite in Ihrem Browser nach 1 Minute, um auf die aktuellsten Ergebnisse zuzugreifen.

Fehlerbehebung bei AutoSupport -Paketen

Wenn der Versuch, ein AutoSupport Paket zu senden, fehlschlägt, ergreift das StorageGRID System je nach Art des AutoSupport Pakets unterschiedliche Maßnahmen. Sie können den Status von AutoSupport -Paketen überprüfen, indem Sie **SUPPORT** > **Tools** > * AutoSupport* > **Ergebnisse** auswählen.

Wenn das Senden des AutoSupport Pakets fehlschlägt, wird auf der Registerkarte **Ergebnisse** der * AutoSupport*-Seite „Fehlgeschlagen“ angezeigt.

Wenn Sie einen Proxy-Server konfiguriert haben, um AutoSupport Pakete an NetApp weiterzuleiten, sollten Sie"Überprüfen Sie, ob die Konfigurationseinstellungen des Proxyservers korrekt sind" .

Wöchentlicher AutoSupport Paketfehler

Wenn das Senden eines wöchentlichen AutoSupport Pakets fehlschlägt, ergreift das StorageGRID -System die folgenden Maßnahmen:

1. Aktualisiert das Attribut „Neuestes Ergebnis“ auf „Wiederholen“.
2. Versucht eine Stunde lang alle vier Minuten 15 Mal, das AutoSupport Paket erneut zu senden.
3. Nach einer Stunde ohne Sendefehler wird das Attribut „Neuestes Ergebnis“ auf „Fehlgeschlagen“ aktualisiert.
4. Versucht, zum nächsten geplanten Zeitpunkt erneut ein AutoSupport Paket zu senden.
5. Behält den regulären AutoSupport Zeitplan bei, wenn das Paket fehlschlägt, weil der NMS-Dienst nicht verfügbar ist, und wenn ein Paket vor Ablauf von sieben Tagen gesendet wird.
6. Wenn der NMS-Dienst wieder verfügbar ist, sendet er sofort ein AutoSupport Paket, wenn sieben Tage oder länger kein Paket gesendet wurde.

Vom Benutzer oder Ereignis ausgelöster AutoSupport Paketfehler

Wenn das Senden eines benutzer- oder ereignisgesteuerten AutoSupport Pakets fehlschlägt, ergreift das StorageGRID -System die folgenden Maßnahmen:

1. Zeigt eine Fehlermeldung an, wenn der Fehler bekannt ist. Wenn ein Benutzer beispielsweise das SMTP-Protokoll auswählt, ohne die richtigen E-Mail-Konfigurationseinstellungen anzugeben, wird der folgende Fehler angezeigt: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. Versucht nicht, das Paket erneut zu versenden.
3. Protokolliert den Fehler in `nms.log` .

Wenn ein Fehler auftritt und SMTP das ausgewählte Protokoll ist, überprüfen Sie, ob der E-Mail-Server des StorageGRID Systems richtig konfiguriert ist und ob Ihr E-Mail-Server ausgeführt wird (**SUPPORT** > **Alarme (Legacy)** > **Legacy-E-Mail-Setup**). Auf der AutoSupport -Seite wird möglicherweise die folgende

Fehlermeldung angezeigt: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Erfahren Sie, wie Sie "Konfigurieren der E-Mail-Servereinstellungen" .

Korrigieren eines AutoSupport Paketfehlers

Wenn ein Fehler auftritt und SMTP das ausgewählte Protokoll ist, überprüfen Sie, ob der E-Mail-Server des StorageGRID Systems richtig konfiguriert ist und ob Ihr E-Mail-Server ausgeführt wird. Auf der AutoSupport -Seite wird möglicherweise die folgende Fehlermeldung angezeigt: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Senden Sie E-Series AutoSupport -Pakete über StorageGRID

Sie können E-Series SANtricity System Manager AutoSupport -Pakete über einen StorageGRID -Admin-Knoten statt über den Verwaltungsport des Speichergeräts an den technischen Support senden.

Sehen "E-Serie Hardware AutoSupport" Weitere Informationen zur Verwendung von AutoSupport mit Geräten der E-Serie.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Speichergeräteadministrator oder Root-Zugriffsberechtigung" .
- Sie haben SANtricity AutoSupport konfiguriert:
  - Für SG6000- und SG5700-Geräte, "AutoSupport im SANtricity System Manager konfigurieren"

> Sie müssen über die SANtricity -Firmware 8.70 oder höher verfügen, um über den Grid Manager auf den SANtricity System Manager zugreifen zu können.

Informationen zu diesem Vorgang

E-Series AutoSupport -Pakete enthalten Details zur Speicherhardware und sind spezifischer als andere AutoSupport Pakete, die vom StorageGRID -System gesendet werden.

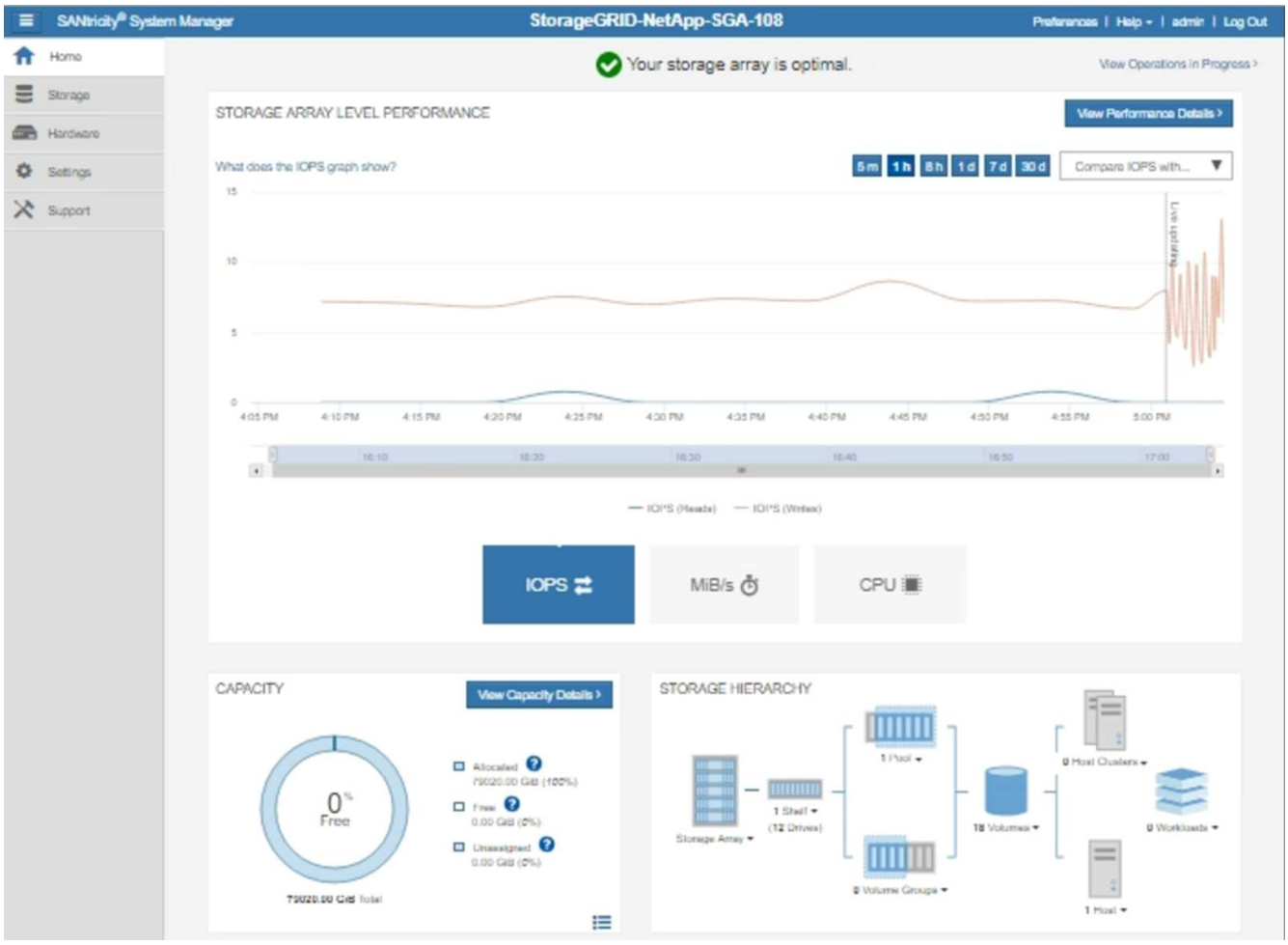
Sie können im SANtricity System Manager eine spezielle Proxyserveradresse konfigurieren, um AutoSupport Pakete über einen StorageGRID Admin-Knoten zu übertragen, ohne den Verwaltungsport des Geräts zu verwenden. Die so übermittelten AutoSupport -Pakete werden von der"bevorzugter Absender-Admin-Knoten" und sie verwenden jede"Admin-Proxy-Einstellungen" die im Grid Manager konfiguriert wurden.

> Dieses Verfahren dient nur zum Konfigurieren eines StorageGRID -Proxyservers für E-Series AutoSupport Pakete. Weitere Informationen zur E-Series AutoSupport Konfiguration finden Sie im "Dokumentation zu NetApp E-Series und SANtricity" .

Schritte

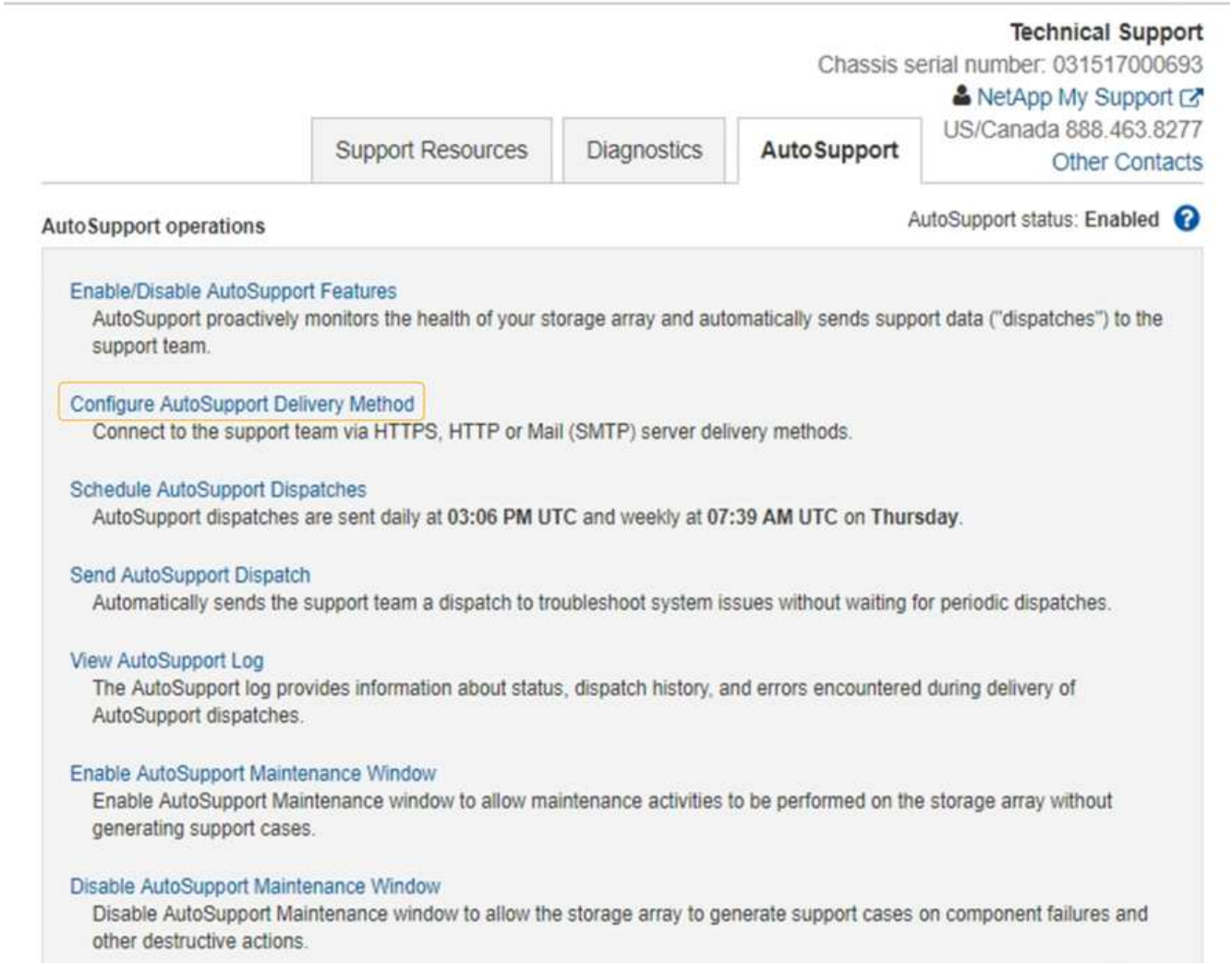
1. Wählen Sie im Grid Manager **NODES** aus.
2. Wählen Sie aus der Knotenliste auf der linken Seite den Speichergeräteknoten aus, den Sie konfigurieren möchten.
3. Wählen Sie * SANtricity System Manager*.

   Die Homepage des SANtricity System Managers wird angezeigt.



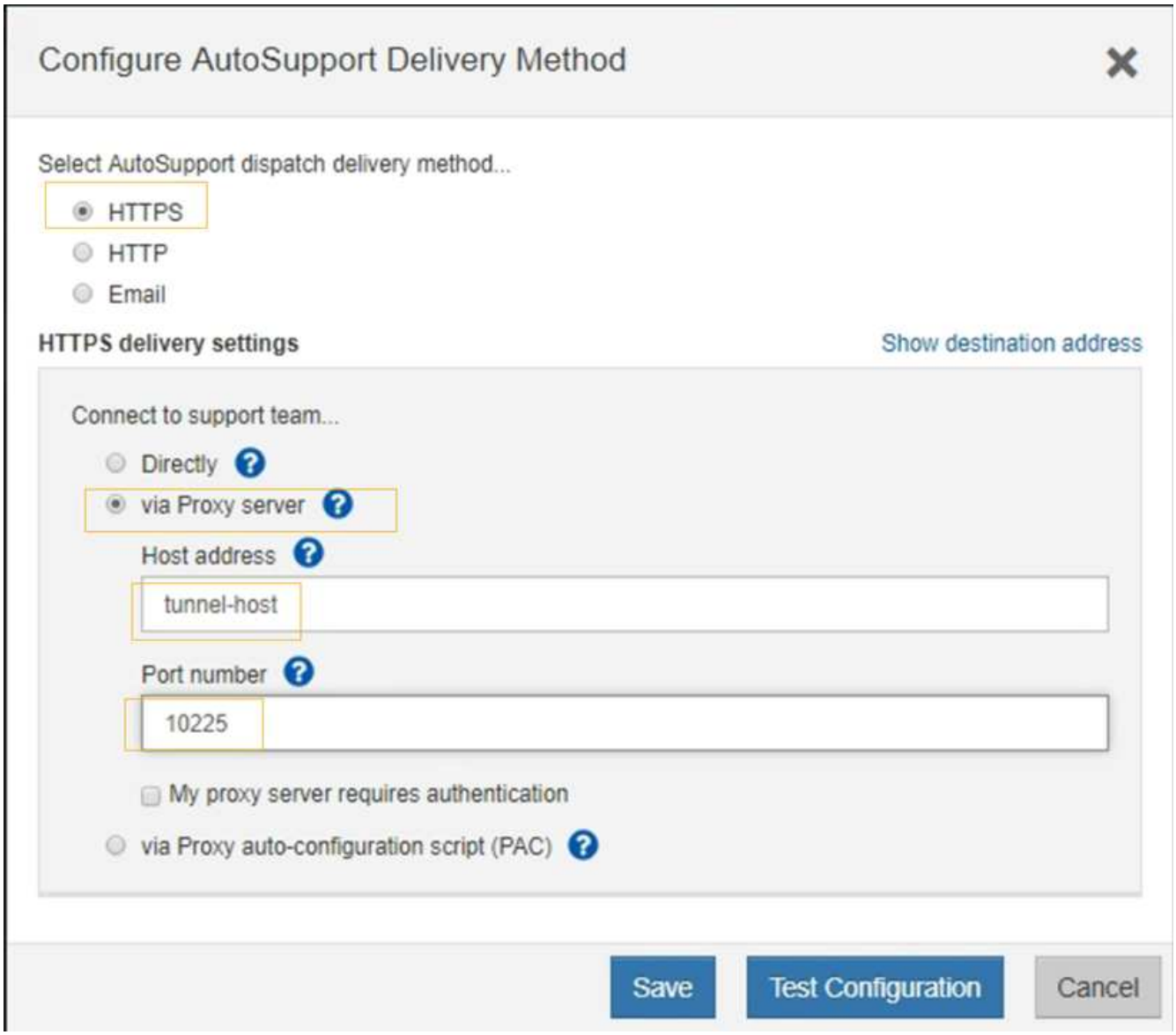
4. Wählen Sie **SUPPORT** > **Supportcenter** > * AutoSupport*.

   Die AutoSupport -Betriebsseite wird angezeigt.



5. Wählen Sie * AutoSupport Liefermethode konfigurieren*.

   Die Seite „AutoSupport -Übermittlungsmethode konfigurieren“ wird angezeigt.



6. Wählen Sie **HTTPS** als Übermittlungsmethode.

   Das Zertifikat, das HTTPS ermöglicht, ist vorinstalliert.

7. Wählen Sie **über Proxyserver**.
8. Eingeben `tunnel-host` für die **Hostadresse**.

   `tunnel-host`ist die spezielle Adresse zum Verwenden eines Admin-Knotens zum Senden von E-Series AutoSupport Paketen.

9. Eingeben `10225` für die **Portnummer**.

   `10225`ist die Portnummer auf dem StorageGRID -Proxyserver, der AutoSupport Pakete vom E-Series-Controller im Gerät empfängt.

10. Wählen Sie **Testkonfiguration**, um das Routing und die Konfiguration Ihres AutoSupport Proxyservers zu testen.

    Wenn alles korrekt ist, wird in einem grünen Banner die Meldung „Ihre AutoSupport Konfiguration wurde

überprüft“ angezeigt.

Wenn der Test fehlschlägt, wird eine Fehlermeldung in einem roten Banner angezeigt. Überprüfen Sie Ihre StorageGRID -DNS-Einstellungen und das Netzwerk, stellen Sie sicher,"bevorzugter Absender-Admin-Knoten" Sie können eine Verbindung zur NetApp Support-Site herstellen und den Test erneut versuchen.

11. Wählen Sie **Speichern**.

    Die Konfiguration wird gespeichert und eine Bestätigungsmeldung wird angezeigt: „Die AutoSupport Übermittlungsmethode wurde konfiguriert.“

Speicherknoten verwalten

Speicherknoten verwalten

Speicherknoten stellen Festplattenspeicherkapazität und -dienste bereit. Die Verwaltung von Speicherknoten umfasst Folgendes:

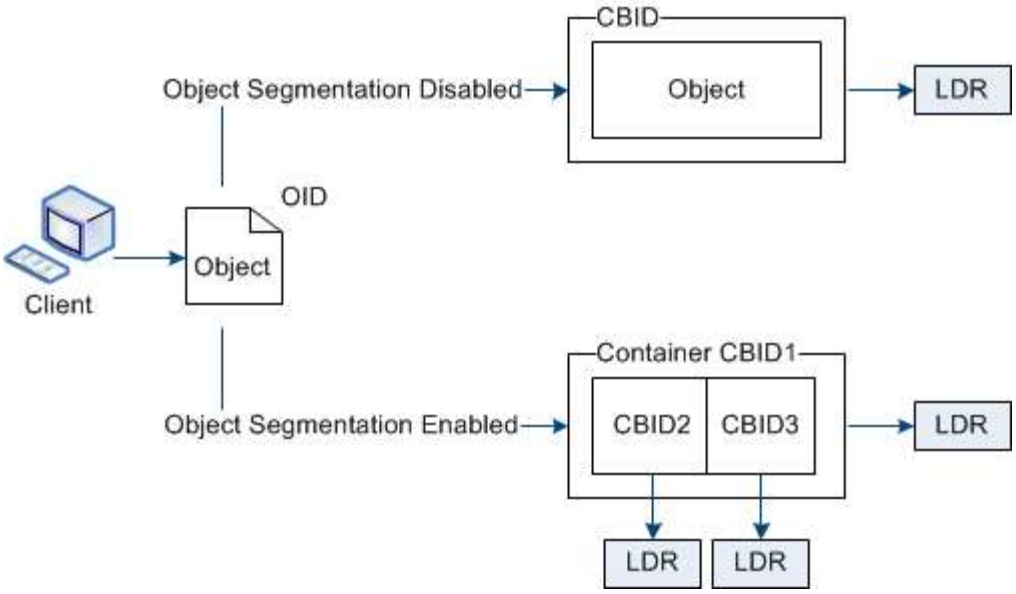
- Verwalten von Speicheroptionen
- Verstehen, was Speichervolumen-Wasserzeichen sind und wie Sie mithilfe von Wasserzeichen-Überschreibungen steuern können, wann Speicherknoten schreibgeschützt werden.
- Überwachung und Verwaltung des für Objektmetadaten verwendeten Speicherplatzes
- Konfigurieren globaler Einstellungen für gespeicherte Objekte
- Anwenden der Storage Node-Konfigurationseinstellungen
- Verwalten vollständiger Speicherknoten

Speicheroptionen verwenden

Was ist Objektsegmentierung?

Bei der Objektsegmentierung handelt es sich um den Prozess, ein Objekt in eine Sammlung kleinerer Objekte mit fester Größe aufzuteilen, um den Speicher- und Ressourcenverbrauch für große Objekte zu optimieren. Der mehrteilige S3-Upload erstellt auch segmentierte Objekte, wobei jedes Teil durch ein Objekt dargestellt wird.

Wenn ein Objekt in das StorageGRID -System aufgenommen wird, teilt der LDR-Dienst das Objekt in Segmente auf und erstellt einen Segmentcontainer, der die Header-Informationen aller Segmente als Inhalt auflistet.



Beim Abrufen eines Segmentcontainers setzt der LDR-Dienst das ursprüngliche Objekt aus seinen Segmenten zusammen und gibt das Objekt an den Client zurück.

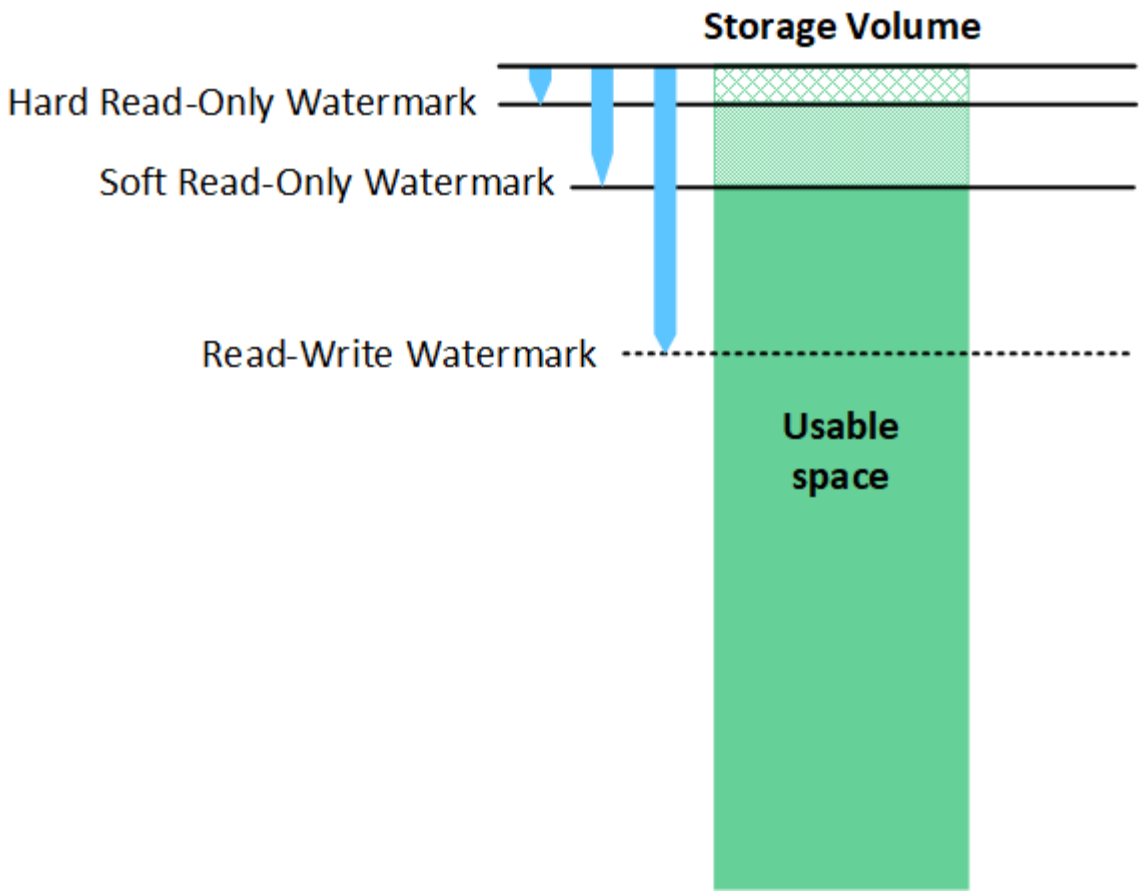
Der Container und die Segmente werden nicht unbedingt auf demselben Speicherknoten gespeichert. Container und Segmente können auf jedem Speicherknoten innerhalb des in der ILM-Regel angegebenen Speicherpools gespeichert werden.

Jedes Segment wird vom StorageGRID -System unabhängig behandelt und trägt zur Anzahl von Attributen wie verwalteten Objekten und gespeicherten Objekten bei. Wenn beispielsweise ein im StorageGRID -System gespeichertes Objekt in zwei Segmente aufgeteilt wird, erhöht sich der Wert von Managed Objects nach Abschluss der Aufnahme wie folgt um drei:

```
segment container + segment 1 + segment 2 = three stored objects
```

Was sind Speichervolumen-Wasserzeichen?

StorageGRID verwendet drei Speichervolumen-Wasserzeichen, um sicherzustellen, dass Speicherknoten sicher in einen schreibgeschützten Zustand versetzt werden, bevor der Speicherplatz kritisch knapp wird, und um Speicherknoten, die in einen schreibgeschützten Zustand versetzt wurden, wieder den Lese-/Schreibzugriff zu ermöglichen.



Speichervolumen-Wasserzeichen gelten nur für den Speicherplatz, der für replizierte und löschcodierte Objektdaten verwendet wird. Um mehr über den für Objektmetadaten auf Volume 0 reservierten Speicherplatz zu erfahren, gehen Sie zu"Verwalten des Objektmetadatenspeichers" .

Was ist das weiche, schreibgeschützte Wasserzeichen?

Das **Soft-Read-Only-Wasserzeichen des Speichervolumes** ist das erste Wasserzeichen, das anzeigt, dass der nutzbare Speicherplatz eines Speicherknotens für Objektdaten voll wird.

Wenn jedes Volume in einem Speicherknoten weniger freien Speicherplatz hat als das weiche schreibgeschützte Wasserzeichen dieses Volumes, wechselt der Speicherknoten in den *schreibgeschützten Modus*. Der Nur-Lese-Modus bedeutet, dass der Speicherknoten dem Rest des StorageGRID -Systems Nur-Lese-Dienste ankündigt, aber alle ausstehenden Schreibanforderungen erfüllt.

Nehmen wir beispielsweise an, dass jedes Volume in einem Speicherknoten ein weiches, schreibgeschütztes Wasserzeichen von 10 GB hat. Sobald auf jedem Volume weniger als 10 GB freier Speicherplatz vorhanden sind, wechselt der Speicherknoten in den Soft-Read-Only-Modus.

Was ist das Hard Read-Only-Wasserzeichen?

Das **Wasserzeichen „Speichervolume hart schreibgeschützt“** ist das nächste Wasserzeichen, das anzeigt, dass der nutzbare Speicherplatz eines Knotens für Objektdaten voll wird.

Wenn der freie Speicherplatz auf einem Volume kleiner ist als die harte schreibgeschützte Wassermarke dieses Volumes, schlagen Schreibvorgänge auf das Volume fehl. Schreibvorgänge auf anderen Volumes können jedoch fortgesetzt werden, bis der freie Speicherplatz auf diesen Volumes kleiner ist als ihre festen

schreibgeschützten Wasserzeichen.

Nehmen wir beispielsweise an, dass jedes Volume in einem Speicherknoten ein festes schreibgeschütztes Wasserzeichen von 5 GB hat. Sobald jedes Volume weniger als 5 GB freien Speicherplatz hat, akzeptiert der Storage Node keine Schreibanfragen mehr.

Das harte schreibgeschützte Wasserzeichen ist immer kleiner als das weiche schreibgeschützte Wasserzeichen.

Was ist das Lese-/Schreibwasserzeichen?

Das **Lese-/Schreib-Wasserzeichen für Speichervolumes** gilt nur für Speicherknoten, die in den schreibgeschützten Modus gewechselt sind. Es bestimmt, wann der Knoten wieder lese- und schreibgeschützt werden kann. Wenn der freie Speicherplatz auf einem beliebigen Speichervolume in einem Speicherknoten größer ist als die Lese-/Schreibgrenze dieses Volumes, wechselt der Knoten automatisch zurück in den Lese-/Schreibzustand.

Nehmen wir beispielsweise an, der Speicherknoten ist in den schreibgeschützten Modus gewechselt. Nehmen wir außerdem an, dass jedes Volume ein Lese-/Schreibwasserzeichen von 30 GB hat. Sobald der freie Speicherplatz für ein beliebiges Volume auf 30 GB ansteigt, wird der Knoten wieder lese- und schreibgeschützt.

Das Lese-/Schreibwasserzeichen ist immer größer als das weiche und das harte Nur-Lese-Wasserzeichen.

Wasserzeichen des Speichervolumens anzeigen

Sie können die aktuellen Wasserzeicheneinstellungen und die systemoptimierten Werte anzeigen. Wenn keine optimierten Wasserzeichen verwendet werden, können Sie feststellen, ob Sie die Einstellungen anpassen können oder sollten.

Bevor Sie beginnen

- Sie haben das Upgrade auf StorageGRID 11.6 oder höher abgeschlossen.
- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .

Aktuelle Wasserzeicheneinstellungen anzeigen

Sie können die aktuellen Speicherwasserzeicheneinstellungen im Grid Manager anzeigen.

Schritte

1. Wählen Sie **SUPPORT** > **Sonstiges** > **Speicherwasserzeichen**.
2. Aktivieren Sie auf der Seite „Speicherwasserzeichen“ das Kontrollkästchen „Optimierte Werte verwenden“.
   - Wenn das Kontrollkästchen aktiviert ist, werden alle drei Wasserzeichen für jedes Speichervolume auf jedem Speicherknoten basierend auf der Größe des Speicherknotens und der relativen Kapazität des Volumes optimiert.

     Dies ist die Standardeinstellung und die empfohlene Einstellung. Aktualisieren Sie diese Werte nicht. Optional können SieOptimierte Speicherwasserzeichen anzeigen .
   - Wenn das Kontrollkästchen „Optimierte Werte verwenden“ deaktiviert ist, werden benutzerdefinierte (nicht optimierte) Wasserzeichen verwendet. Die Verwendung benutzerdefinierter Wasserzeicheneinstellungen wird nicht empfohlen. Verwenden Sie die Anweisungen für"Fehlerbehebung bei Warnungen zum Überschreiben des schreibgeschützten Wasserzeichens bei

niedrigem Wert" um festzustellen, ob Sie die Einstellungen anpassen können oder sollten.

Wenn Sie benutzerdefinierte Wasserzeicheneinstellungen angeben, müssen Sie Werte größer als 0 eingeben.

Optimierte Speicherwasserzeichen anzeigen

StorageGRID verwendet zwei Prometheus-Metriken, um die optimierten Werte anzuzeigen, die es für das Soft Read-Only-Wasserzeichen des Speichervolumes 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 zum Zugriff auf die Prometheus-Benutzeroberfläche aus.
3. Um das empfohlene minimale Soft-Read-Only-Wasserzeichen anzuzeigen, geben Sie die folgende Prometheus-Metrik ein und wählen Sie **Ausführen**:

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   Die letzte Spalte zeigt den minimal optimierten Wert des weichen schreibgeschützten Wasserzeichens für alle Speichervolumes auf jedem Speicherknoten. Wenn dieser Wert größer ist als die benutzerdefinierte Einstellung für das weiche schreibgeschützte Wasserzeichen des Speichervolumes, wird für den Speicherknoten die Warnung **Niedriges schreibgeschütztes Wasserzeichen außer Kraft setzen** ausgelöst.

4. Um das empfohlene maximale Soft-Read-Only-Wasserzeichen anzuzeigen, geben Sie die folgende Prometheus-Metrik ein und wählen Sie **Ausführen**:

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   Die letzte Spalte zeigt den maximal optimierten Wert des weichen schreibgeschützten Wasserzeichens für alle Speichervolumes auf jedem Speicherknoten.

Verwalten des Objektmetadatenspeichers

Die Objektmetadatenkapazität eines StorageGRID -Systems steuert die maximale Anzahl von Objekten, die auf diesem System gespeichert werden können. Um sicherzustellen, dass Ihr StorageGRID -System über ausreichend Speicherplatz zum Speichern neuer Objekte verfügt, müssen Sie wissen, wo und wie StorageGRID Objektmetadaten speichert.

Was sind Objektmetadaten?

Objektmetadaten sind alle Informationen, die ein Objekt beschreiben. StorageGRID verwendet Objektmetadaten, um die Standorte aller Objekte im gesamten Grid zu verfolgen und den Lebenszyklus jedes Objekts im Laufe der Zeit zu verwalten.

Für ein Objekt in StorageGRID umfassen die Objektmetadaten die folgenden Arten von Informationen:

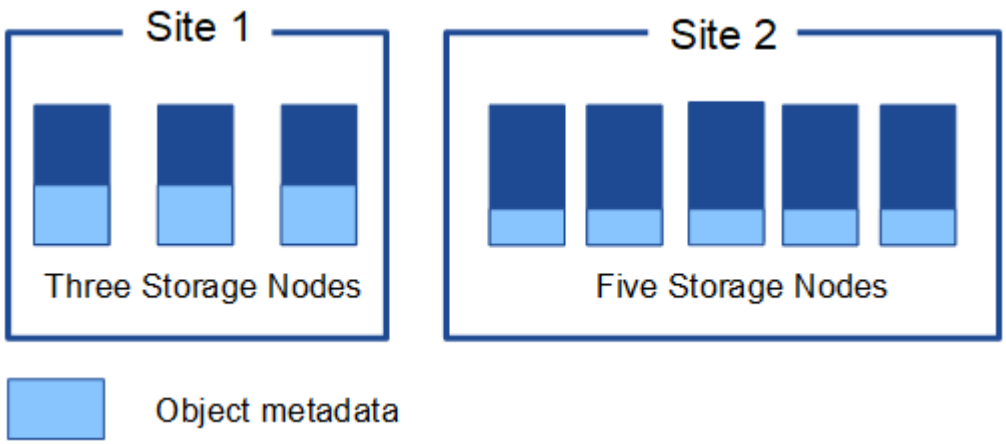
- Systemmetadaten, einschließlich einer eindeutigen ID für jedes Objekt (UUID), des Objektnamens, des Namens des S3-Buckets, des Mandantenkontonamens oder der ID, der logischen Größe des Objekts, des Datums und der Uhrzeit der ersten Objekterstellung sowie des Datums und der Uhrzeit der letzten Objektänderung.

- Alle benutzerdefinierten Schlüssel-Wert-Paare der Benutzermetadaten, die mit dem Objekt verknüpft sind.
- Bei S3-Objekten alle mit dem Objekt verknüpften Schlüssel-Wert-Paare des Objekt-Tags.
- Bei replizierten Objektkopien der aktuelle Speicherort jeder Kopie.
- Bei Erasure-Coded-Objektkopien der aktuelle Speicherort jedes Fragments.
- Bei Objektkopien in einem Cloud Storage Pool der Speicherort des Objekts, einschließlich des Namens des externen Buckets und der eindeutigen Kennung des Objekts.
- Für segmentierte Objekte und mehrteilige Objekte: Segmentkennungen und Datengrößen.

Wie werden Objektmetadaten gespeichert?

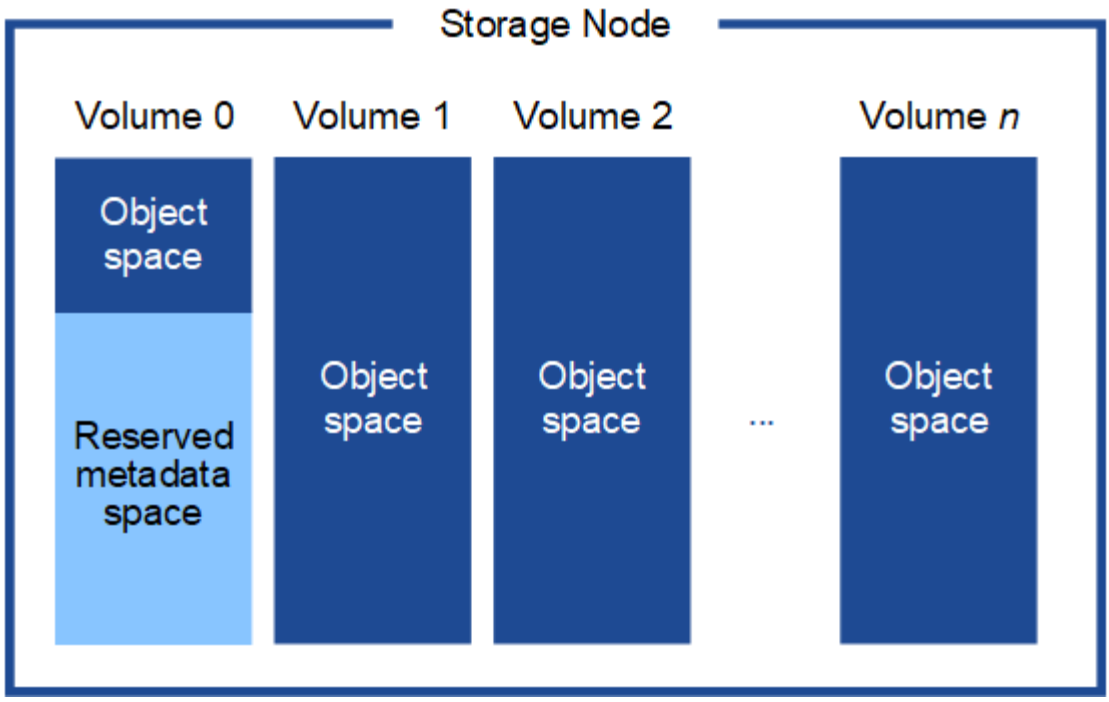
StorageGRID verwaltet Objektmetadaten in einer Cassandra-Datenbank, die unabhängig von Objektdaten gespeichert wird. Um Redundanz zu gewährleisten und Objektmetadaten vor Verlust zu schützen, speichert StorageGRID an jedem Standort drei Kopien der Metadaten für alle Objekte im System.

Diese Abbildung stellt die Speicherknoten an zwei Standorten dar. Jeder Standort verfügt über die gleiche Menge an Objektmetadaten und die Metadaten jedes Standorts werden auf alle Speicherknoten an diesem Standort aufgeteilt.



Wo werden Objektmetadaten gespeichert?

Diese Abbildung stellt die Speichervolumina für einen einzelnen Speicherknoten dar.



Wie in der Abbildung gezeigt, reserviert StorageGRID Speicherplatz für Objektmetadaten auf Speichervolume 0 jedes Speicherknotens. Es verwendet den reservierten Speicherplatz zum Speichern von Objektmetadaten und zum Ausführen wichtiger Datenbankvorgänge. Der verbleibende Speicherplatz auf Speichervolume 0 und allen anderen Speichervolumes im Speicherknoten wird ausschließlich für Objektdaten (replizierte Kopien und Erasure-Coded-Fragmente) verwendet.

Die Menge an Speicherplatz, die für Objektmetadaten auf einem bestimmten Speicherknoten reserviert ist, hängt von mehreren Faktoren ab, die im Folgenden beschrieben werden.

Einstellung für reservierten Speicherplatz für Metadaten

Der *Reservierte Speicherplatz für Metadaten* ist eine systemweite Einstellung, die die Speicherplatzmenge darstellt, die auf Volume 0 jedes Speicherknotens für Metadaten 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 Speicherknoten.

Für die Erstinstallation von StorageGRID verwendete Version	RAM-Menge auf Speicherknoten	Standardeinstellung für reservierten Speicherplatz für Metadaten
11,5 bis 11,9	128 GB oder mehr auf jedem Speicherknoten im Grid	8 TB (8.000 GB)
	Weniger als 128 GB auf einem beliebigen Speicherknoten im Grid	3 TB (3.000 GB)
11,1 bis 11,4	128 GB oder mehr auf jedem Speicherknoten an einem beliebigen Standort	4 TB (4.000 GB)

Für die Erstinstallation von StorageGRID verwendete Version	RAM-Menge auf Speicherknoten	Standardeinstellung für reservierten Speicherplatz für Metadaten
	Weniger als 128 GB auf jedem Speicherknoten an jedem Standort	3 TB (3.000 GB)
11.0 oder früher	Beliebiger Betrag	2 TB (2.000 GB)

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** > **Speichereinstellungen**.
2. Erweitern Sie auf der Seite „Speichereinstellungen“ den Abschnitt „Reservierter Speicherplatz für Metadaten“.

Für StorageGRID 11.8 oder höher muss der Wert für den reservierten Speicherplatz für Metadaten mindestens 100 GB und höchstens 1 PB betragen.

Die Standardeinstellung für eine neue Installation von StorageGRID 11.6 oder höher, bei der jeder Speicherknoten über 128 GB oder mehr RAM verfügt, beträgt 8.000 GB (8 TB).

Tatsächlich reservierter Speicherplatz für Metadaten

Im Gegensatz zur systemweiten Einstellung für reservierten Speicherplatz für Metadaten wird der *tatsächlich reservierte Speicherplatz* für Objektmetadaten für jeden Speicherknoten bestimmt. Für jeden Speicherknoten hängt der tatsächlich reservierte Speicherplatz für Metadaten von der Größe des Volumes 0 für den Knoten und der systemweiten Einstellung für den reservierten Speicherplatz für Metadaten ab.

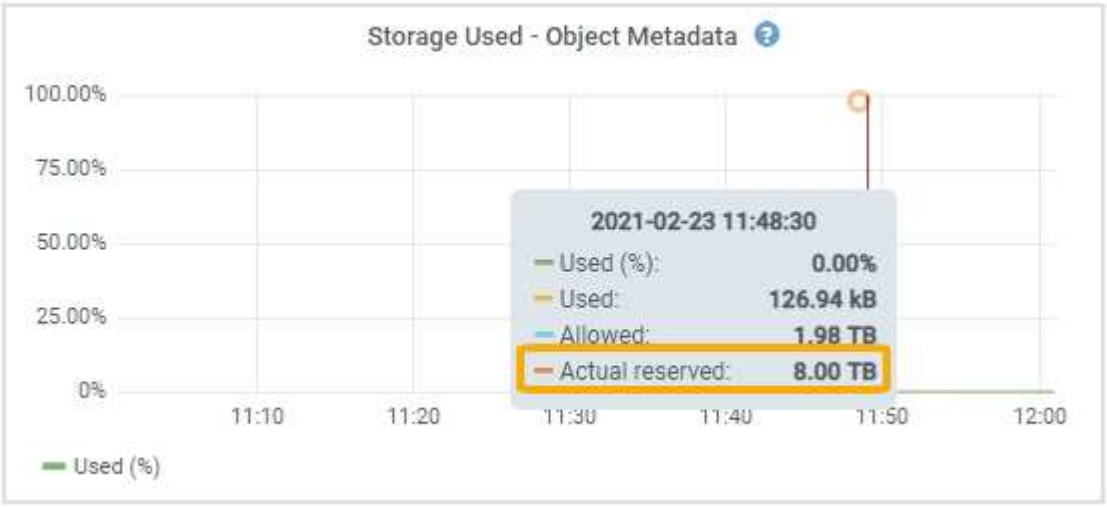
Größe des Datenträgers 0 für den Knoten	Tatsächlich reservierter Speicherplatz für Metadaten
Weniger als 500 GB (nicht produktive Nutzung)	10% des Volumens 0
500 GB oder mehr + oder + Nur-Metadaten-Speicherknoten	Der kleinere dieser Werte: • Band 0 • Einstellung für reservierten Speicherplatz für Metadaten **Hinweis**: Für reine Metadaten-Speicherknoten ist nur eine Rangedb erforderlich.

Tatsächlich reservierten Speicherplatz für Metadaten anzeigen

Befolgen Sie diese Schritte, um den tatsächlich reservierten Speicherplatz für Metadaten auf einem bestimmten Speicherknoten anzuzeigen.

Schritte

1. Wählen Sie im Grid Manager **NODES** > ***Storage Node***.
2. Wählen Sie die Registerkarte **Speicher**.
3. Positionieren Sie den Cursor über dem Diagramm „Benutzter Speicher – Objektmetadaten“ und suchen Sie den Wert **Tatsächlich reserviert**.



Im Screenshot beträgt der **tatsächlich reservierte** Wert 8 TB. Dieser Screenshot zeigt einen großen Speicherknoten in einer neuen StorageGRID 11.6-Installation. Da die systemweite Einstellung für den reservierten Speicherplatz für Metadaten kleiner ist als Volume 0 für diesen Speicherknoten, entspricht der tatsächlich reservierte Speicherplatz für diesen Knoten der Einstellung für den reservierten Speicherplatz für Metadaten.

Beispiel für tatsächlich reservierten Metadatenspeicherplatz

Angenommen, Sie installieren ein neues StorageGRID System mit Version 11.7 oder höher. Gehen Sie für dieses Beispiel davon aus, dass jeder Speicherknoten über mehr als 128 GB RAM verfügt und dass Volume 0 von Speicherknoten 1 (SN1) 6 TB groß ist. Basierend auf diesen Werten:

- Der systemweite **Reservierte Speicherplatz für Metadaten** ist auf 8 TB festgelegt. (Dies ist der Standardwert für eine neue Installation von StorageGRID 11.6 oder höher, wenn jeder Speicherknoten über mehr als 128 GB RAM verfügt.)
- Der tatsächlich reservierte Speicherplatz für Metadaten für SN1 beträgt 6 TB. (Das gesamte Volume ist reserviert, da Volume 0 kleiner ist als die Einstellung **Reservierter Speicherplatz für Metadaten**.)

Zulässiger Metadatenspeicherplatz

Der tatsächlich für Metadaten reservierte Speicherplatz jedes Speicherknotens ist unterteilt in den für Objektmetadaten verfügbaren Speicherplatz (den *zulässigen Metadatenspeicherplatz*) und den für wichtige Datenbankvorgänge (wie Komprimierung und Reparatur) sowie zukünftige Hardware- und Software-Upgrades erforderlichen Speicherplatz. Der zulässige Metadatenspeicherplatz bestimmt die Gesamtobjektkapazität.

Die folgende Tabelle zeigt, wie StorageGRID den **zulässigen Metadatenspeicherplatz** für verschiedene Speicherknoten berechnet, basierend auf der Speichermenge für den Knoten und dem tatsächlich reservierten Speicherplatz für Metadaten.

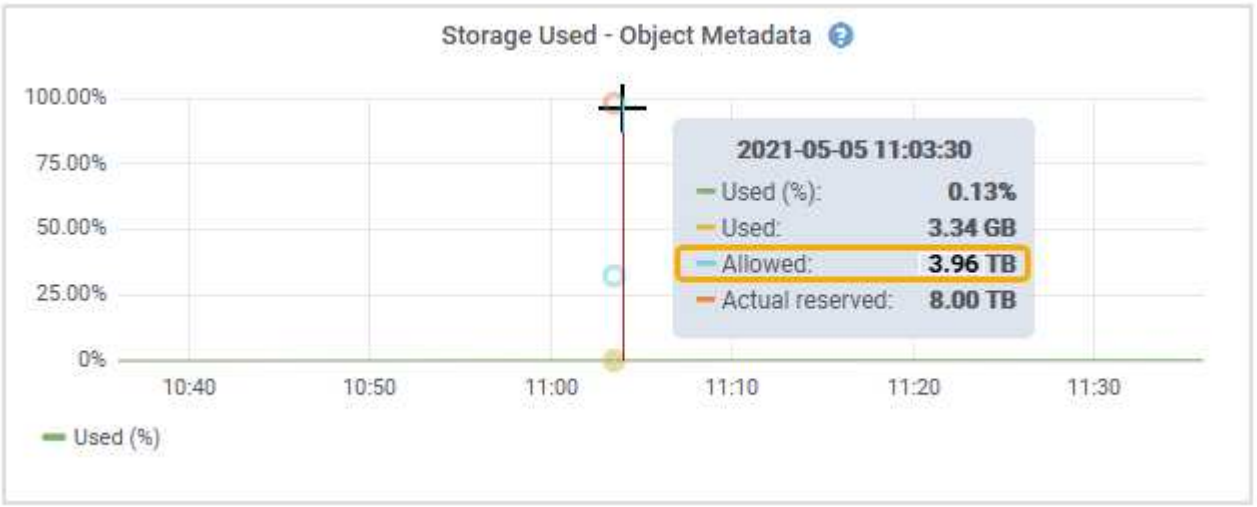
		Speichermenge auf dem Speicherknoten	
	< 128 GB	>= 128 GB	**Tatsächlich reservierter Speicherplatz für Metadaten**
⇐ 4 TB	60 % des tatsächlich reservierten Speicherplatzes für Metadaten, bis zu einem Maximum von 1,32 TB	60 % des tatsächlich reservierten Speicherplatzes für Metadaten, bis zu einem Maximum von 1,98 TB	4 TB

Zugelassenen Metadatenspeicherplatz anzeigen

Befolgen Sie diese Schritte, um den zulässigen Metadatenspeicherplatz für einen Speicherknoten anzuzeigen.

Schritte

1. Wählen Sie im Grid Manager **NODES** aus.
2. Wählen Sie den Speicherknoten aus.
3. Wählen Sie die Registerkarte **Speicher**.
4. Positionieren Sie den Cursor über dem Diagramm „Verwendeter Speicher – Objektmetadaten“ und suchen Sie den Wert **Zulässig**.



Im Screenshot beträgt der **zulässige** Wert 3,96 TB. Dies ist der Maximalwert für einen Speicherknoten, dessen tatsächlich 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. Gehen Sie für dieses Beispiel davon aus, dass jeder Speicherknoten über mehr als 128 GB RAM verfügt und dass Volume 0 von Speicherknoten 1 (SN1) 6 TB groß ist. Basierend auf diesen Werten:

- Der systemweite **Reservierte Speicherplatz für Metadaten** ist auf 8 TB festgelegt. (Dies ist der Standardwert für StorageGRID 11.6 oder höher, wenn jeder Speicherknoten über mehr als 128 GB RAM verfügt.)
- Der tatsächlich reservierte Speicherplatz für Metadaten für SN1 beträgt 6 TB. (Das gesamte Volume ist reserviert, da Volume 0 kleiner ist als die Einstellung **Reservierter Speicherplatz für Metadaten**.)
- Der zulässige Speicherplatz für Metadaten auf SN1 beträgt 3 TB, basierend auf der Berechnung imTabelle für zulässigen Speicherplatz für Metadaten : (Tatsächlich reservierter Speicherplatz für Metadaten − 1 TB) × 60 %, bis zu einem Maximum von 3,96 TB.

Wie sich Speicherknoten unterschiedlicher Größe auf die Objektkapazität auswirken

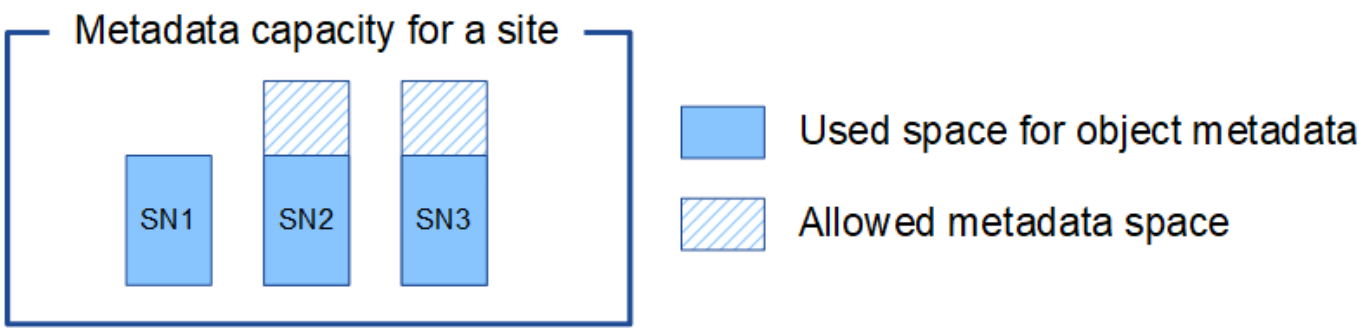
Wie oben beschrieben, verteilt StorageGRID die Objektmetadaten gleichmäßig auf die Speicherknoten an jedem Standort. Wenn eine Site Speicherknoten unterschiedlicher Größe enthält, bestimmt daher der kleinste Knoten an der Site die Metadatenkapazität der Site.

Betrachten Sie das folgende Beispiel:

- Sie verfügen über ein Single-Site-Raster mit drei Speicherknoten unterschiedlicher Größe.
- Die Einstellung für **Reservierter Speicherplatz für Metadaten** beträgt 4 TB.
- Die Speicherknoten haben die folgenden Werte für den tatsächlich reservierten Metadatenspeicherplatz und den zulässigen Metadatenspeicherplatz.

Speicherknoten	Größe des Datenträgers 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 die Objektmetadaten gleichmäßig auf die Speicherknoten an einem Standort verteilt sind, kann jeder Knoten in diesem Beispiel nur 1,32 TB Metadaten speichern. Die zusätzlichen 0,66 TB zulässiger Metadatenspeicherplatz für SN2 und SN3 können nicht verwendet werden.



Da StorageGRID alle Objektmetadaten für ein StorageGRID -System an jedem Standort verwaltet, wird die Gesamtmetadatenkapazität eines StorageGRID -Systems durch die Objektmetadatenkapazität des kleinsten Standorts bestimmt.

Und da die Kapazität der Objektmetadaten die maximale Objektanzahl steuert, ist das Grid effektiv voll, wenn einem Knoten die Metadatenkapazität ausgeht.

Ähnliche Informationen

- Informationen zum Überwachen der Objektmetadatenkapazität für jeden Speicherknoten finden Sie in den Anweisungen für"Überwachung von StorageGRID" .
- Um die Objektmetadatenkapazität für Ihr System zu erhöhen,"ein Raster erweitern" durch Hinzufügen neuer Speicherknoten.

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 beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung oder Berechtigungen für die Konfiguration der Grid-Topologieseite und andere Grid-Konfigurationen" .

> Die Seite „Grid-Topologie“ ist veraltet und wird in einer zukünftigen Version entfernt.

Informationen zu diesem Vorgang

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 ausführliche Erklärung, wie sich die Einstellung „Reservierter Speicherplatz für Metadaten“ auf den zulässigen Speicherplatz für die Speicherung von Objektmetadaten auf einem bestimmten Speicherknoten auswirkt, finden Sie unter"Verwalten des Objektmetadatenspeichers" .

Schritte

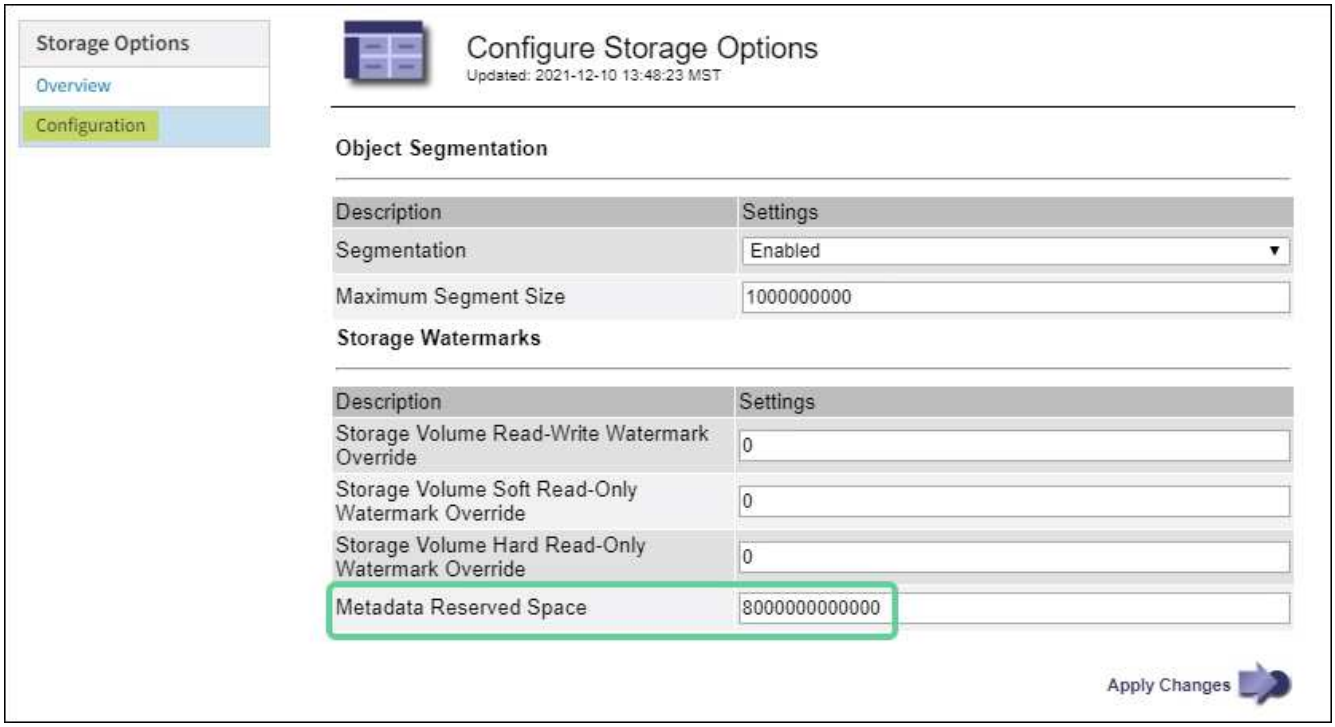
1. Ermitteln Sie die aktuelle Einstellung für den reservierten Speicherplatz für Metadaten.
   a. Wählen Sie **KONFIGURATION** > **System** > **Speicheroptionen**.
   b. Beachten Sie im Abschnitt „Speicherwasserzeichen“ den Wert von „**Reservierter Speicherplatz für Metadaten**“.
2. Stellen Sie sicher, dass auf dem Speichervolume 0 jedes Speicherknotens genügend Speicherplatz verfügbar ist, um diesen Wert zu erhöhen.
   a. Wählen Sie **NODES**.
   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 **NODES**.
   b. Wählen Sie den ersten Speicherknoten im Raster aus.
   c. Wählen Sie die Registerkarte **Hardware**.
   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. Wählen Sie im Abschnitt „Speicherwasserzeichen“ **Reservierter Speicherplatz für Metadaten** 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 übernehmen**.

Gespeicherte Objekte komprimieren

Sie können die Objektkomprimierung aktivieren, um die Größe der in StorageGRID gespeicherten Objekte zu reduzieren, sodass die Objekte weniger Speicherplatz belegen.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Standardmäßig ist die Objektkomprimierung deaktiviert. Wenn Sie die Komprimierung aktivieren, versucht StorageGRID, jedes Objekt beim Speichern verlustfrei zu komprimieren.

> Wenn Sie diese Einstellung ändern, dauert es etwa eine Minute, bis die neue Einstellung übernommen wird. Der konfigurierte Wert wird aus Leistungs- und Skalierungsgründen zwischengespeichert.

Bevor Sie die Objektkomprimierung aktivieren, beachten Sie Folgendes:

- Sie sollten **Gespeicherte Objekte komprimieren** nur auswählen, wenn Sie wissen, dass die gespeicherten Daten komprimierbar sind.
- Anwendungen, die Objekte in StorageGRID speichern, komprimieren Objekte möglicherweise vor dem Speichern. Wenn eine Clientanwendung ein Objekt bereits komprimiert hat, bevor es in StorageGRID gespeichert wurde, wird die Größe eines Objekts durch Auswahl dieser Option nicht weiter reduziert.
- Wählen Sie **Gespeicherte Objekte komprimieren** nicht aus, wenn Sie NetApp FabricPool mit StorageGRID verwenden.

- Wenn **Gespeicherte Objekte komprimieren** ausgewählt ist, sollten S3-Clientanwendungen die Durchführung von GetObject-Operationen vermeiden, die einen zurückzugebenden Bytebereich angeben. Diese „Range Read“-Operationen sind ineffizient, da StorageGRID die Objekte effektiv dekomprimieren muss, um auf die angeforderten Bytes zuzugreifen. GetObject-Operationen, die einen kleinen Bytebereich aus einem sehr großen Objekt anfordern, sind besonders ineffizient. Beispielsweise ist es ineffizient, einen 10 MB großen Bereich aus einem komprimierten 50 GB-Objekt zu lesen.

  Wenn Bereiche aus komprimierten Objekten gelesen werden, kann es bei Clientanforderungen zu einer Zeitüberschreitung kommen.

  > Wenn Sie Objekte komprimieren müssen und Ihre Clientanwendung Bereichslesevorgänge verwenden muss, erhöhen Sie das Lesezeitlimit für die Anwendung.

Schritte

1. Wählen Sie **KONFIGURATION** > **System** > **Speichereinstellungen** > **Objektkomprimierung**.
2. Aktivieren Sie das Kontrollkästchen **Gespeicherte Objekte komprimieren**.
3. Wählen Sie **Speichern**.

Vollständige Speicherknoten verwalten

Wenn die Speicherknoten ihre Kapazitätsgrenze erreichen, müssen Sie das StorageGRID -System durch Hinzufügen von neuem Speicher erweitern. Es stehen drei Optionen zur Verfügung: Hinzufügen von Speichervolumes, Hinzufügen von Speichererweiterungsregalen und Hinzufügen von Speicherknoten.

Speichervolumes hinzufügen

Jeder Speicherknoten unterstützt eine maximale Anzahl von Speichervolumes. Das definierte Maximum variiert je nach Plattform. Wenn ein Speicherknoten weniger als die maximale Anzahl an Speichervolumes enthält, können Sie Volumes hinzufügen, um seine Kapazität zu erhöhen. Siehe die Anweisungen für"Erweiterung eines StorageGRID -Systems" .

Fügen Sie Speichererweiterungsregale hinzu

Einige StorageGRID -Geräte-Speicherknoten, wie z. B. SG6060 oder SG6160, können zusätzliche Speicherregale unterstützen. Wenn Sie über StorageGRID -Geräte mit Erweiterungsmöglichkeiten verfügen, die noch nicht auf die maximale Kapazität erweitert wurden, können Sie Speicherregale hinzufügen, um die Kapazität zu erhöhen. Siehe die Anweisungen für"Erweiterung eines StorageGRID -Systems" .

Speicherknoten hinzufügen

Sie können die Speicherkapazität durch Hinzufügen von Speicherknoten erhöhen. Beim Hinzufügen von Speicher müssen die derzeit aktiven ILM-Regeln und Kapazitätsanforderungen sorgfältig berücksichtigt werden. Siehe die Anweisungen für"Erweiterung eines StorageGRID -Systems" .

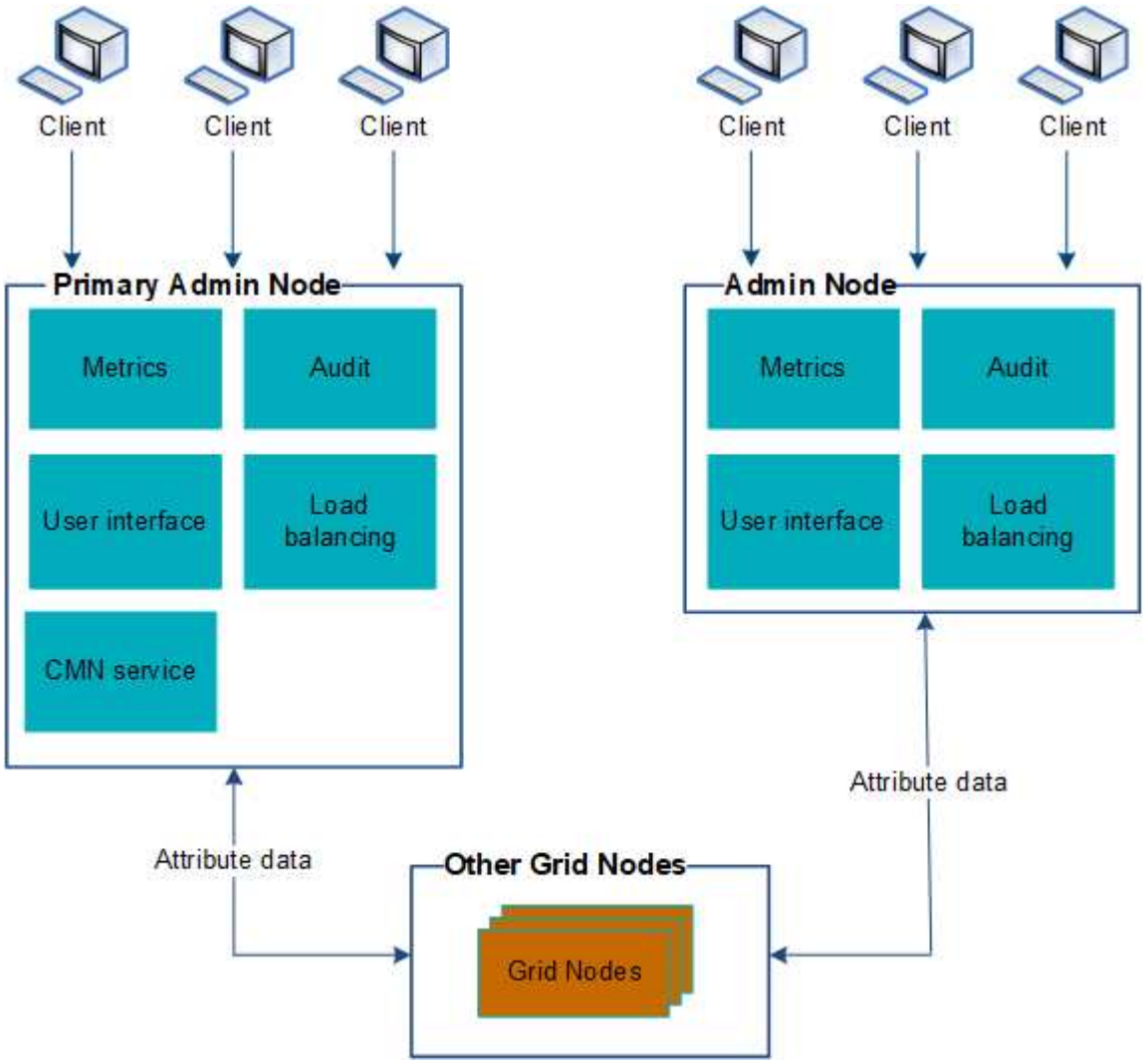
Admin-Knoten verwalten

Verwenden Sie mehrere Admin-Knoten

Ein StorageGRID -System kann mehrere Admin-Knoten umfassen, damit Sie Ihr

StorageGRID System kontinuierlich überwachen und konfigurieren können, selbst wenn ein Admin-Knoten ausfällt.

Wenn ein Admin-Knoten nicht mehr verfügbar ist, wird die Attributverarbeitung fortgesetzt, Warnungen werden weiterhin ausgelöst und E-Mail-Benachrichtigungen und AutoSupport Pakete werden weiterhin gesendet. Allerdings bietet das Vorhandensein mehrerer Admin-Knoten keinen Failover-Schutz, mit Ausnahme von Benachrichtigungen und AutoSupport Paketen.



Es gibt zwei Möglichkeiten, das StorageGRID -System weiterhin anzuzeigen und zu konfigurieren, wenn ein Admin-Knoten ausfällt:

- Webclients können die Verbindung zu jedem anderen verfügbaren Admin-Knoten wiederherstellen.
- Wenn ein Systemadministrator eine Hochverfügbarkeitsgruppe von Admin-Knoten konfiguriert hat, können Webclients weiterhin über die virtuelle IP-Adresse der HA-Gruppe auf den Grid Manager oder den Tenant Manager zugreifen. Sehen "Verwalten von Hochverfügbarkeitsgruppen" .

> Bei Verwendung einer HA-Gruppe wird der Zugriff unterbrochen, wenn der aktive Admin-Knoten ausfällt. Benutzer müssen sich erneut anmelden, nachdem die virtuelle IP-Adresse der HA-Gruppe auf einen anderen Admin-Knoten in der Gruppe umgeschaltet wurde.

Einige Wartungsaufgaben können nur mit dem primären Admin-Knoten durchgeführt werden. Wenn der

primäre Admin-Knoten ausfällt, muss er wiederhergestellt werden, bevor das StorageGRID -System wieder voll funktionsfähig ist.

Identifizieren Sie den primären Admin-Knoten

Der primäre Admin-Knoten bietet mehr Funktionen als nicht-primäre Admin-Knoten. Beispielsweise müssen einige Wartungsvorgänge mithilfe des primären Admin-Knotens durchgeführt werden.

Weitere Informationen zu Admin-Knoten finden Sie unter"Was ist ein Admin-Knoten?" .

Bevor Sie beginnen

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

Schritte

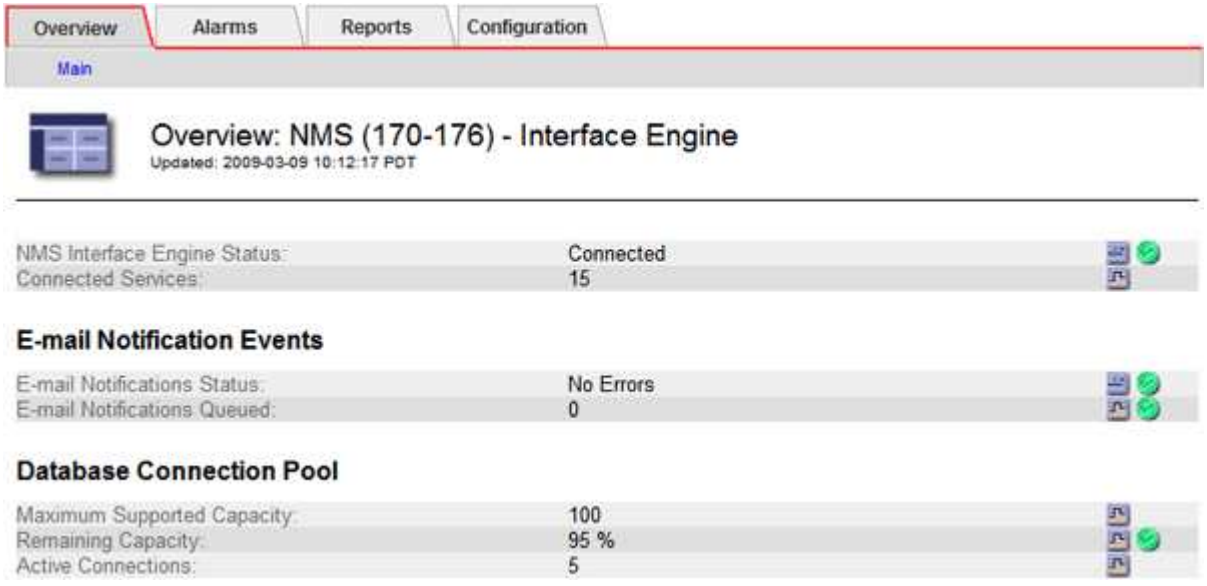
1. Wählen Sie **NODES**.
2. Geben Sie **primary** in das Suchfeld ein.

   Identifizieren Sie in den Suchergebnissen den Knoten, bei dem in der Spalte „Typ“ „Primärer Admin-Knoten“ angezeigt wird. Ein primärer Admin-Knoten sollte aufgelistet sein.

Benachrichtigungsstatus und Warteschlangen anzeigen

Der Network Management System (NMS)-Dienst auf Admin-Knoten sendet Benachrichtigungen an den Mailserver. Sie können den aktuellen Status des NMS-Dienstes und die Größe seiner Benachrichtigungswarteschlange auf der Seite „Interface Engine“ anzeigen.

Um auf die Seite „Interface Engine“ zuzugreifen, wählen Sie **SUPPORT** > **Tools** > **Grid-Topologie**. Wählen Sie dann ***site*** > ***Admin Node*** > **NMS** > **Interface Engine**.



Benachrichtigungen werden über die E-Mail-Benachrichtigungswarteschlange verarbeitet und in der

Reihenfolge, in der sie ausgelöst werden, nacheinander an den Mailserver gesendet. Wenn ein Problem auftritt (beispielsweise ein Netzwerkverbindungsfehler) und der Mailserver beim Versuch, die Benachrichtigung zu senden, nicht verfügbar ist, wird für einen Zeitraum von 60 Sekunden ein Best-Effort-Versuch unternommen, die Benachrichtigung erneut an den Mailserver zu senden. 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.